

**SOPHOS**

Security made simple.

# Sophos Endpoint Security and Control

## Ayuda

Versión: 10.6

Edición: agosto de 2016



# Contenido

1	Acerca de Sophos Endpoint Security and Control.....	5
2	Acerca de la página de inicio.....	6
3	Grupos de Sophos.....	7
3.1	Acerca de los grupos de Sophos.....	7
3.2	Añadir usuarios a grupos de Sophos.....	8
3.3	Configurar los derechos sobre el área de cuarentena.....	8
4	Sophos Anti-Virus.....	10
4.1	Acerca del escaneado en acceso y en demanda.....	10
4.2	Escaneado en acceso.....	10
4.3	Escaneado en demanda.....	15
4.4	Excluir elementos del escaneado.....	26
4.5	Control de comportamiento de Sophos.....	31
4.6	Protección activa de Sophos.....	33
4.7	Protección web de Sophos.....	35
4.8	Autorizar el uso de elementos.....	37
4.9	Gestionar elementos en cuarentena.....	39
4.10	Limpieza.....	46
4.11	Configurar alertas.....	47
4.12	Registro del escaneado.....	50
5	Restricción de aplicaciones de Sophos.....	52
5.1	Acerca del escaneado de aplicaciones restringidas.....	52
5.2	Desactivar el escaneado de aplicaciones restringidas.....	52
6	Control de dispositivos de Sophos.....	53
6.1	Acerca del control de dispositivos.....	53
6.2	Tipos de dispositivos controlados.....	53
6.3	Desactivar temporalmente el control de dispositivos.....	54
6.4	Configurar el registro del control de dispositivos.....	54
6.5	Ver el registro del control de dispositivos.....	54
7	Control de datos de Sophos.....	55
7.1	Acerca del control de datos.....	55
7.2	Desactivar temporalmente el control de datos.....	55
7.3	Copiar archivos a un dispositivo de almacenamiento.....	55
7.4	Configurar el registro del control de datos.....	55
7.5	Ver el registro del control de datos.....	56
8	Control web de Sophos.....	57

8.1	Acerca del control web.....	57
8.2	Desactivar temporalmente el control web.....	57
9	Sophos Client Firewall.....	58
9.1	Empezar a usar el cortafuegos.....	58
9.2	Configurar el cortafuegos.....	58
9.3	Modo interactivo.....	66
9.4	Archivos de configuración del cortafuegos.....	69
9.5	Reglas del cortafuegos.....	70
9.6	Detección de la ubicación.....	77
9.7	Informes del cortafuegos.....	79
9.8	Registro del cortafuegos.....	81
10	Sophos AutoUpdate.....	85
10.1	Actualización inmediata.....	85
10.2	Programar las actualizaciones.....	85
10.3	Configurar la fuente de actualización.....	85
10.4	Establecer una fuente alternativa de actualización.....	86
10.5	Realizar la actualización vía proxy.....	86
10.6	Actualización a través de conexión telefónica a redes.....	86
10.7	Limitar el ancho de banda empleado en las actualizaciones.....	86
10.8	Registrar las actividades de actualización.....	87
10.9	Ver el registro de actualización.....	87
11	Protección contra manipulaciones de Sophos.....	88
11.1	Protección contra manipulaciones.....	88
11.2	Activar la protección contra manipulaciones.....	89
11.3	Desactivar la protección contra manipulaciones.....	89
11.4	Reactivar la protección contra manipulaciones.....	90
11.5	Contraseña de la protección contra manipulaciones.....	90
11.6	Introducir la contraseña para configurar el software.....	90
11.7	Cambiar la contraseña de la protección contra manipulaciones.....	91
11.8	Desinstalar el software de seguridad de Sophos.....	91
11.9	Ver el registro de la protección contra manipulaciones.....	92
12	Solución de problemas.....	93
12.1	La última actualización no se completó debido a algún error.....	93
12.2	No se pudo limpiar la amenaza.....	94
12.3	Fragmento de virus/spyware detectado.....	95
12.4	Amenaza detectada parcialmente.....	96
12.5	Programas publicitarios o aplicaciones no deseadas eliminados de la cuarentena.....	96
12.6	El sistema va muy lento.....	96

12.7	Permitir el acceso a unidades con sectores de arranque infectados.....	97
12.8	Imposible acceder a áreas de Sophos Endpoint Security and Control.....	97
12.9	Recuperación tras una infección.....	97
12.10	Recuperación tras una infección de programas publicitarios o aplicaciones no deseadas.....	98
12.11	Error de contraseña.....	99
12.12	Mensaje de error "fallo del servicio".....	99
12.13	La base de datos del registro del cortafuegos está corrupta.....	99
13	Glosario.....	101
14	Soporte técnico.....	107
15	Aviso legal.....	108

# 1 Acerca de Sophos Endpoint Security and Control

Sophos Endpoint Security and Control 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. Además, Malicious Traffic Detector puede detectar las comunicaciones entre su equipo y los servidores de comando y control utilizados en un ataque de bots u otros ataques maliciosos.

**Sophos Behavior Monitoring** utiliza la tecnología HIPS para proteger equipos Windows contra amenazas desconocidas y comportamiento sospechoso.

**Sophos Live Protection** 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.

**Sophos Web Protection** 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. También escanea los datos y archivos descargados y comprueba la reputación de los archivos.

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

**Sophos Device Control** bloquea dispositivos de almacenamiento externo no autorizados y tecnologías de conexión inalámbrica.

**Sophos Data Control** impide la fuga accidental de información personal de equipos afectados.

**Sophos Web Control** ofrece protección, control y notificación para equipos móviles o ubicados fuera de la red empresarial.

**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 88.

## 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**.

<b>Limpiar sectores</b>	Los usuarios pueden limpiar sectores de arranque de disquetes.
<b>Limpiar archivos</b>	Los usuarios pueden limpiar documentos y programas.
<b>Borrar archivos</b>	Los usuarios pueden eliminar archivos infectados.
<b>Mover archivos</b>	Los usuarios pueden mover archivos infectados a otra carpeta.
<b>Autorizar</b>	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 <b>Gestor de autorización</b> como al <b>Área de cuarentena</b> .

## 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 abrir, guardar, copiar o cambiar el nombre de 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.

Para más información, consulte [Configurar el escaneado en acceso](#) en la página 10.

#### 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 de las recomendaciones para el escaneado en acceso

Esta sección contiene recomendaciones para sacar el mayor provecho 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. Para más información sobre la configuración recomendada del escaneado en acceso, vea el artículo 114345 en la base de conocimiento de Sophos (<http://www.sophos.com/es-es/support/knowledgebase/114345.aspx>).

#### 4.2.2 Configurar el escaneado en acceso



**Advertencia:** 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 encriptación, consulte el artículo 12790 de la base de conocimiento de Sophos (<http://www.sophos.com/es-es/support/knowledgebase/12790.aspx>).

**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, 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.
Rename	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
<b>Adware y PUA</b>	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..
<b>Archivos sospechosos</b>	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
<b>Permitir el acceso a unidades con sectores de arranque infectados</b>	<p>Permite el acceso a unidades externas como CD-ROM, disquetes o unidades USB que tengan el sector de arranque infectado.</p> <p>Sólo debería utilizar esta opción bajo las indicaciones del soporte técnico de Sophos.</p> <p>Más información en la sección <a href="#">Permitir el acceso a unidades con sectores de arranque infectados</a> en la página 97.</p>
<b>Escanear todos los archivos</b>	<p>Se recomienda <b>desactivar</b> esta opción ya que puede ralentizar el equipo. Sólo debe escanear todos los archivos en escaneados semanales.</p>
<b>Escanear archivos comprimidos</b>	<p>Active esta opción si desea escanear dentro de archivos comprimidos. Sólo necesita hacerlo si descarga y distribuye este tipo de archivos sin extraer el contenido.</p> <p>Se recomienda <b>desactivar</b> 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"> <li>▪ Cuando se realiza la extracción.</li> <li>▪ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.</li> </ul>
<b>Escanear memoria del sistema</b>	<p>Active esta opción para disponer de un escaneo en segundo plano cada hora que detecte amenazas en la memoria del sistema.</p> <p><b>Nota:</b> esta opción sólo está disponible para sistemas operativos de 32 bits.</p>

### 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 escaneados 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 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.

Para configurar la limpieza del escaneo en acceso:

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

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

4. En **Virus/spyware**, seleccione la acción que desea que realice Sophos Anti-Virus para actuar contra los elementos infectados si ha desactivado la limpieza automática o si esta no se realiza correctamente:

Opción	Descripción
<b>Sólo denegar acceso</b>	Sophos Anti-Virus pedirá confirmación antes de continuar. Esta es la opción predeterminada.
<b>Eliminar Denegar acceso y mover a</b>	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los virus y programas espía de su equipo que encuentre Sophos Anti-Virus. Consulte <a href="#">Revisar virus y programas espía en cuarentena</a> en la página 41.

5. En la sección **Archivos sospechosos**, seleccione la acción que desea que realice Sophos Anti-Virus cuando detecte código utilizado habitualmente en el software malicioso:

Opción	Descripción
<b>Denegar acceso</b>	Sophos Anti-Virus pedirá confirmación antes de continuar. Esta es la opción predeterminada.
<b>Eliminar Denegar acceso y mover a</b>	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 <a href="#">Revisar archivos sospechosos en cuarentena</a> en la página 43.

## 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 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.

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.

## 4.3 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.

- [Realizar un escaneado de botón derecho](#) en la página 19

#### 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.

- [Ejecutar un escaneado personalizado](#) en la página 24
- [Programar un escaneado personalizado](#) en la página 24

#### Escaneado exhaustivo

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

- [Realizar un escaneado exhaustivo](#) en la página 25

### 4.3.2 Especificar extensiones de archivo del escaneado en demanda

**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.

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 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.

### 4.3.3 Escaneado de botón derecho

#### 4.3.3.1 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 escaneado del botón derecho:

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

Para configurar el escaneado de botón derecho:

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



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

Opción	Descripción
<b>Adware y PUA</b>	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..
<b>Archivos sospechosos</b>	Archivos con características habituales de virus, aunque no exclusivas.

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

Opción	Descripción
<b>Escanear todos los archivos</b>	Se recomienda <b>desactivar</b> esta opción ya que puede ralentizar el equipo. Sólo debe escanear todos los archivos en escaneados semanales.
<b>Escanear archivos comprimidos</b>	Active esta opción si desea escanear dentro de archivos comprimidos. Sólo necesita hacerlo si descarga y distribuye este tipo de archivos sin extraer el contenido.  Se recomienda <b>desactivar</b> esta opción ya que puede ralentizar el escaneo.  El contenido de los archivos comprimidos se escanea: <ul style="list-style-type: none"> <li>▪ Cuando se realiza la extracción.</li> <li>▪ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.</li> </ul>

#### 4.3.3.2 Configurar la limpieza del escaneo de botón derecho

**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.

Para configurar la limpieza del escaneo de botón derecho:

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

4. Seleccione la acción que desea que realice Sophos Anti-Virus para actuar contra los elementos infectados si no ha activado la limpieza automática o si esta no se realiza correctamente:

Opción	Descripción
<b>Sólo registrar</b>	Sophos Anti-Virus registra los elementos infectados en el registro de escaneado sin realizar ninguna otra acción. Consulte <a href="#">Ver el registro del escaneado</a> en la página 51. Esta es la opción predeterminada.
<b>Eliminar</b> <b>Mover a</b>	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los virus y programas espía de su equipo que encuentre Sophos Anti-Virus. Consulte <a href="#">Revisar virus y programas espía en cuarentena</a> en la página 41.

5. En la sección **Archivos sospechosos**, seleccione la acción que desea que realice Sophos Anti-Virus cuando detecte código utilizado habitualmente en el software malicioso:

Opción	Descripción
<b>Sólo registrar</b>	Sophos Anti-Virus registra los elementos infectados en el registro de escaneado sin realizar ninguna otra acción. Esta es la opción predeterminada.
<b>Eliminar</b> <b>Mover a</b>	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los virus y programas espía de su equipo que encuentre Sophos Anti-Virus. Consulte <a href="#">Revisar archivos sospechosos en cuarentena</a> en la página 43.

6. Para eliminar todos los componentes conocidos de 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 sobre la visualización de datos en el sitio web de Sophos sobre los efectos secundarios de los programas publicitarios o las aplicaciones no deseadas, consulte [Información de limpieza](#) en la página 47.
- Para más información sobre cómo limpiar programas publicitarios y aplicaciones no deseadas de su equipo desde el Área de cuarentena, consulte [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 42.

### 4.3.3.3 Realizar un escaneo de botón derecho

Desde el Explorador de Windows y en el escritorio es posible escanear archivos, carpetas y unidades mediante el escaneo 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.
2. 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*.

## 4.3.4 Escaneados personalizados





### 4.3.4.1 Crear un 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 6.
2. Haga clic en **Crear un nuevo escaneo**.
3. En el cuadro de texto **Nombre del escaneo**, indique un nombre descriptivo para el nuevo escaneo.
4. 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, vea la [Representación de los elementos a escanear](#) en la página 19.  
**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.
5. Haga clic en **Configurar el escaneo** para ver más opciones (consulte [Configurar escaneados personalizados](#) en la página 20 para más información).
6. Para disponer de escaneo programado, haga clic en **Programar el escaneo** (consulte [Programar un escaneo personalizado](#) en la página 24 para más información).
7. Haga clic en el botón **Guardar** para guardar el escaneo, o en **Guardar e iniciar** para guardar y ejecutar el escaneo.

### 4.3.4.2 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 escaneo.
<input checked="" type="checkbox"/>	El elemento y subelementos <i>están</i> seleccionados para el escaneo.

Icono	Significado
	El elemento está seleccionado parcialmente, es decir, algunos subelementos están seleccionados para el escaneo.
	El elemento y subelementos están excluidos en este escaneo.
	El elemento está excluido parcialmente, es decir, algunos subelementos están excluidos en este escaneo.
	El elemento y subelementos están excluidos en todos los escaneos en demanda al existir una exclusión general en demanda. Para obtener información, consulte <a href="#">Excluir elementos del escaneo en acceso</a> en la página 26.

#### 4.3.4.3 Configurar escaneados personalizados

**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, Sophos Anti-Virus detecta y limpia las siguientes amenazas durante un escaneo personalizado:

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

Para configurar un 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 6.
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. En la sección **Detectar**, seleccione las opciones necesarias según se describe a continuación.

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

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

Opción	Descripción
<b>Escanear todos los archivos</b>	Sólo se recomienda utilizar esta opción en un escaneo semanal, ya que puede afectar al rendimiento del sistema.
<b>Escanear archivos comprimidos</b>	<p>Active esta opción si desea escanear dentro de archivos comprimidos. Sólo necesita hacerlo si descarga y distribuye este tipo de archivos sin extraer el contenido.</p> <p>Se recomienda <b>desactivar</b> 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"> <li>▪ Cuando se realiza la extracción.</li> <li>▪ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.</li> </ul>
<b>Escanear memoria del sistema</b>	<p>Active esta opción para disponer de un escaneo en segundo plano cada hora que detecte amenazas en la memoria del sistema.</p> <p><b>Nota:</b> esta opción sólo está disponible para sistemas operativos de 32 bits.</p>
<b>Ejecutar escaneo con baja prioridad</b>	En Windows Vista y posterior, realiza los escaneos personalizados en baja prioridad para minimizar el impacto en los recursos del sistema.

#### 4.3.4.4 Configurar la limpieza del escaneo personalizado

**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.

Para configurar la limpieza del escaneo personalizado:

1. En la página **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 6.
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 **Virus/spyware**, active la opción **Limpiar automáticamente elementos con virus/spyware** para limpiar los archivos infectados automáticamente.

6. Seleccione la acción que desea que realice Sophos Anti-Virus para actuar contra los elementos infectados si no ha activado la limpieza automática o si esta no se realiza correctamente:

Opción	Descripción
<b>Sólo registrar</b>	Sophos Anti-Virus registra los elementos infectados en el registro del escaneado personalizado sin realizar ninguna otra acción. Consulte <a href="#">Ver el registro de un escaneado personalizado</a> en la página 25. Esta es la opción predeterminada.
<b>Eliminar</b> <b>Mover a</b>	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los virus y programas espía de su equipo que encuentre Sophos Anti-Virus. Consulte <a href="#">Revisar virus y programas espía en cuarentena</a> en la página 41.

7. En la sección **Archivos sospechosos**, seleccione la acción que desea que realice Sophos Anti-Virus cuando detecte código utilizado habitualmente en el software malicioso:

Opción	Descripción
<b>Sólo registrar</b>	Sophos Anti-Virus registra los elementos infectados en el registro de escaneado sin realizar ninguna otra acción. Esta es la opción predeterminada.
<b>Eliminar</b> <b>Mover a</b>	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los virus y programas espía de su equipo que encuentre Sophos Anti-Virus. Consulte <a href="#">Revisar archivos sospechosos en cuarentena</a> en la página 43.

8. Para eliminar todos los componentes conocidos de 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 sobre la visualización de datos en el sitio web de Sophos sobre los efectos secundarios de los programas publicitarios o las aplicaciones no deseadas, consulte Información de limpieza [Información de limpieza](#) en la página 47.
- Para más información sobre cómo limpiar programas publicitarios y aplicaciones no deseadas de su equipo desde el Área de cuarentena, consulte Revisar programas publicitarios y aplicaciones no deseadas en cuarentena [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 42.

#### 4.3.4.5 Programar un escaneo personalizado

Si pertenece al grupo SophosAdministrator, puede programar los escaneos personalizados, además de poder ver y editar escaneos 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 6.
2. En la lista de **Escaneados disponibles**, seleccione el escaneo que desee editar y haga clic en **Editar**.
3. Haga clic en **Programar el escaneo**.
4. En el cuadro de diálogo **Programar el escaneo**, seleccione **Activar escaneo programado**.  
Seleccione el día o días en los que desea que se lleve a cabo el escaneo.  
Haga clic en el botón **Añadir** para indicar las horas a las que se ejecutará el escaneo.  
Utilice los botones **Eliminar** y **Editar** para modificar la lista de horas del escaneo.
5. Escriba el *nombre de usuario y contraseña*. La contraseña no puede estar en blanco.  
El escaneo 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 escaneo se detiene. Esto se debe a que si se continúa con el escaneo, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneo.

#### 4.3.4.6 Ejecutar un escaneo personalizado

**Nota:** los escaneos programados no se pueden ejecutar de forma manual. Los escaneos 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 [Acerca de la página de inicio](#) en la página 6.
2. En la lista de **Escaneados disponibles**, seleccione el escaneo que desee ejecutar y haga clic en **Iniciar**.  
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, 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*.

#### 4.3.4.7 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 [Acerca de la página de inicio](#) en la página 6.
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.

#### 4.3.4.8 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 6.
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.

#### 4.3.4.9 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 6.
2. En la lista de **Escaneados disponibles**, haga clic en **Resumen**.

#### 4.3.4.10 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 6.
2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee eliminar y haga clic en **Borrar**.

### 4.3.5 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 6.

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 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*.

## 4.4 Excluir elementos del escaneado

### 4.4.1 Excluir elementos del escaneado en acceso

**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.

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. Haga clic en la ficha **Exclusiones** y elija una de las opciones siguientes.
  - Haga clic en **Añadir** para especificar un archivo, carpeta o unidad a excluir del escaneado en acceso.
  - Para eliminar una exclusión, haga clic en **Eliminar**.
  - Para modificar una exclusión, haga clic en **Editar**.
3. Para añadir o modificar un elemento excluido, en el cuadro de diálogo **Exclusión de elementos**, seleccione **Tipo de elemento**

El tipo de elemento **Todos los archivos remotos** sirve para excluir archivos que no están guardados en unidades locales. Seleccione esta opción si desea incrementar la velocidad de acceso a archivos remotos en ubicaciones seguras.
4. Indique el **Nombre del elemento** con el botón **Examinar** o escribiéndolo en el cuadro de texto.

**Nota:** si trabaja en una plataforma de 64 bits, el botón **Examinar** no estará visible en el cuadro de diálogo **Exclusión de elementos**.

Para obtener más información sobre cómo especificar nombres de elementos, consulte [Especificar exclusiones de escaneado](#) en la página 27.

### 4.4.2 Excluir elementos del escaneado en demanda

**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.

El procedimiento descrito a continuación se aplica a **todos** los escaneados en demanda. Para más información sobre cómo excluir elementos de un escaneado personalizado, consulte [Crear un escaneado personalizado](#) en la página 19.

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

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Configuración > Extensiones y exclusiones en demanda**.

2. Haga clic en la ficha **Exclusiones** y elija una de las opciones siguientes.
  - Haga clic en **Añadir** para especificar un archivo, carpeta o unidad a excluir del escaneado en demanda.
  - Para eliminar una exclusión, haga clic en **Eliminar**.
  - Para modificar una exclusión, haga clic en **Editar**.
3. Para añadir o modificar un elemento excluido, en el cuadro de diálogo **Exclusión de elementos**, seleccione **Tipo de elemento**
4. Indique el **Nombre del elemento** con el botón **Examinar** o escribiéndolo en el cuadro de texto.

**Nota:** si trabaja en una plataforma de 64 bits, el botón **Examinar** no estará visible en el cuadro de diálogo **Exclusión de elementos**.

Para obtener más información sobre cómo especificar nombres de elementos, consulte [Especificar exclusiones de escaneado](#) en la página 27.

### 4.4.3 Especificar exclusiones de escaneado

#### 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.

#### 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.

#### Excluir archivos, carpetas, procesos o unidades específicos

Tipo de exclusión	Descripción	Ejemplos	Comentarios
Archivo específico	Para excluir un archivo, debe especificar el nombre y la ruta de acceso. La ruta de acceso puede incluir una letra de unidad o un nombre de recurso compartido de red.	C:\Documentos\CV.doc <del>\\servidor\Usuarios\Donato\CV.doc</del>	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 el <a href="#">artículo 13045 de la base de conocimiento</a> .

Tipo de exclusión	Descripción	Ejemplos	Comentarios
Proceso específico	Para excluir un archivo ejecutable (proceso), debe especificar el nombre del archivo y la ruta de acceso.	C:\Windows\notepad.exe	Debe especificar la ruta de acceso completa.
Todos los archivos con el mismo nombre	Especifique un nombre de archivo sin una ruta de acceso para excluir todos los archivos con ese nombre independientemente de su ubicación en el sistema de archivos.	spacer.gif	
Todos los elementos de una unidad o un recurso compartido de red	Especifique una letra de unidad o un nombre de recurso compartido de red para excluir todos los elementos de esa unidad o recurso compartido de red.	C: \\Servidor\ <sharename></sharename>	Cuando especifique un recurso compartido de red, incluya una barra diagonal al final del nombre del recurso compartido.
Carpeta específica	Especifique la ruta de acceso de la carpeta incluida la letra de unidad o el nombre de recurso compartido de red para excluir todos los elementos de esa carpeta y niveles inferiores.	D:\Herramientas\registros\	Incluya una barra diagonal al final del nombre de la carpeta.
Todas las carpetas con el mismo nombre	Para excluir todas las carpetas con el mismo nombre en <b>cualquier</b> unidad local o compartida, indique el nombre de la carpeta sin la unidad.	\Herramientas\registros\ (excluye las siguientes carpetas: C:\Herramientas\registros\ \\servidor\Herramientas\registros\)	Debe especificar la ruta de acceso sin la unidad, local o compartida. En este ejemplo, si se especifica \registros\, no se excluirá ningún archivo.

## Caracteres comodín

Puede utilizar los caracteres comodines incluidos en esta tabla.

**Nota:** en Windows Server 2003 sólo se pueden utilizar \* y ?.

Token	Coincide	Comentarios
* (Asterisco)	Cero o más de cualquier carácter excepto \ o /.	Por ejemplo: c:\*.txt excluye todos los archivos con el nombre *.txt de

Token	Coincide	Comentarios
		las carpetas de nivel superior en C:\. <b>Nota:</b> * no se puede utilizar con carpetas
** (Asterisco Asterisco)	Cero o más de cualquier carácter incluidos \ y /, cuando van entre los caracteres \ o / o se utilizan al principio o al final de una exclusión.  Cualquier otro uso de ** se trata como un único * y coincide con cero o más de cualquier carácter excluidos \ y /.	Por ejemplo: <ul style="list-style-type: none"> <li>▪ c:\foo\**\bar coincide con: c:\foo\bar, c:\foo\more\bar, c:\foo\even\more\bar</li> <li>▪ **\bar coincide con c:\foo\bar</li> <li>▪ c:\foo\** coincide con c:\foo\more\bar</li> <li>▪ c:\foo\**\bar coincide con c:\foomore\bar pero NO con c:\foo\more\bar</li> </ul>
\ (Barra invertida)	Bien \ o /.	
/ (Barra diagonal)	Bien / o \.	
? (Signo de interrogación)	Un solo carácter, a menos que esté al final de una cadena en cuyo caso puede coincidir con cero caracteres.	
. (Punto)	Un punto O la cadena vacía al final de un nombre de archivo, si el patrón termina en un punto y el nombre del archivo no tiene una extensión.	Tenga en cuenta que: <ul style="list-style-type: none"> <li>▪ *.* coincide con todos los archivos</li> <li>▪ *. coincide con todos los archivos sin extensión</li> <li>▪ "foo." coincide con "foo" y "foo."</li> </ul>

## Ejemplos

He aquí algunos ejemplos de uso de caracteres comodín.

Expresión	Se interpreta como	Descripción
foo	**\foo	Excluir cualquier archivo con el nombre foo (en cualquier lugar).
foo\bar	**\foo\bar	Excluir cualquier archivo con el nombre bar en una carpeta llamada foo (en cualquier lugar).

Expresión	Se interpreta como	Descripción
*.txt	**\*.txt	Excluir todos los archivos con el nombre *.txt (en cualquier lugar).
C:	C:	Excluir la unidad C: del escaneo (incluido el registro de arranque maestro de la unidad).
C:\	C:\	Excluir todos los archivos de la unidad C: del escaneo (pero escanear el registro de arranque maestro de la unidad).
C:\foo\	C:\foo\	Todos los archivos y carpetas dentro de C:\foo, incluida la propia C:\foo.
C:\foo\*.txt	C:\foo\*.txt	Todos los archivos contenidos en C:\foo con el nombre *.txt.

## Variables para exclusiones

Puede utilizar variables al configurar las exclusiones de escaneo.

La tabla siguiente muestra las variables y los ejemplos de las ubicaciones a las que corresponden en cada sistema operativo.

Variable	Windows 7 o posterior, Windows Server 2008 o posterior	Windows Server 2003, Windows XP, Windows Vista
%allusersprofile%\	C:\ProgramData\	C:\Documents and Settings\All Users\
%appdata%\	C:\Users\*\AppData\Roaming\	C:\Documents and Settings\*\Application Data\
%commonprogramfiles%\	C:\Program Files\Common Files\	C:\Program Files\Common Files\
%commonprogramfiles(x86)%\	C:\Program Files (x86)\Common Files\	C:\Program Files (x86)\Common Files\
%localappdata%\	C:\Users\*\AppData\Local\	C:\Documents and Settings\*\Local Settings\Application Data\
%programdata%\	C:\ProgramData\	C:\Documents and Settings\All Users\Application Data\

Variable	Windows 7 o posterior, Windows Server 2008 o posterior	Windows Server 2003, Windows XP, Windows Vista
%programfiles%\	C:\Program Files\	C:\Program Files\
%programfiles(x86)%\	C:\Program Files (x86)\	C:\Program Files (x86)\
%systemdrive%\	C:	C:
%systemroot%\	C:\Windows\	C:\Windows\
%temp%\ o %tmp%\	C:\Users\*\AppData\Local\Temp\	C:\Documents and Settings\*\Local Settings\Temp\
%userprofile%\	C:\Users\*\	C:\Documents and Settings\*\
%windir%\	C:\Windows\	C:\Windows\

## 4.5 Control de comportamiento de Sophos

### 4.5.1 Acerca del control de comportamiento

Integrado en el escaneo en acceso, el sistema de control de comportamiento de Sophos protege equipos Windows 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 los siguientes 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.

## 4.5.2 Activar el control de comportamiento

**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 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**.

## 4.5.3 Bloquear comportamiento malicioso

**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.

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 de 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**.

## 4.5.4 Evitar comportamiento sospechoso

**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.

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 de 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 10
- [Configurar escaneados de botón derecho](#) en la página 16
- [Configurar escaneados personalizados](#) en la página 20

## 4.5.5 Evitar desbordamiento del búfer

**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.

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 alertar ante el desbordamiento del búfer, seleccione la opción **Sólo alertar**.

## 4.6 Protección activa de Sophos

### 4.6.1 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 escaneado 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 automáticamente muestras de archivos 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.

## 4.6.2 Activar o desactivar las opciones de la protección activa de Sophos

**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 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.

## 4.6.3 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 6.

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.

## 4.7 Protección web de Sophos

### 4.7.1 Acerca de la protección web de Sophos

La protección web de Sophos ofrece una protección mejorada contra las amenazas de Internet. Incluye las siguientes funciones:

- Filtrado activo de direcciones web
- Escaneado de contenido descargado
- Comprobación de la reputación de archivos descargados

#### Filtrado activo de direcciones web

Filtrado activo de direcciones web para bloquear sitios web que albergan programas maliciosos. Para este filtrado se utiliza la base de datos online de Sophos.

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 51.

#### Escaneado de contenido

El escaneado de contenido escanea tanto datos como archivos descargados de Internet (o intranet), para detectar contenido malicioso. Esta función escanea contenido alojado en cualquier ubicación, incluyendo ubicaciones que no figuran en la base de datos de sitios web infectados.

#### Reputación de descargas

La reputación se calcula a partir de la antigüedad del archivo, el origen, la prevalencia, análisis de contenido profundo y otras características.

**Nota:** la reputación de descarga solo es compatible en Windows 7 o posterior.

Por defecto se muestra una alerta cuando se descarga un archivo de baja reputación o desconocida. Recomendamos no descargar este tipo de archivos. Si el origen y el publicador son de confianza puede permitir la descarga. Su elección y la dirección web del archivo se guardan en el registro de escaneado.

**Nota:** la reputación de descargas se calcula a partir de los datos de la base de datos de SophosLabs en la nube y requiere que la protección activa de Sophos esté activada para poder realizar las búsquedas y obtener los datos. (Por defecto, la protección activa de Sophos está activada.)

Para más información sobre la reputación de descargas, consulte el [artículo de la base de conocimiento 121319](#).

#### Opciones de configuración de la protección web

Por defecto, la protección web está activada: el acceso a sitios web maliciosos está bloqueado, se escanea el contenido descargado y se comprueba la reputación de los archivos descargados.

Para más información sobre las opciones de configuración de la protección web y cómo cambiarlas, consulte [Configurar la protección web de Sophos](#) en la página 36.

## Navegadores de Internet compatibles

La protección web es compatible con los siguientes navegadores de Internet:

- Internet Explorer
- Edge
- Google Chrome
- Firefox (excepto para reputación de descargas)
- Safari (excepto para reputación de descargas)
- Opera

El uso de otros navegadores web no compatibles no permitirá filtrar ni bloquear sitios web.

### 4.7.2 Configurar la protección web de Sophos

**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.

Para cambiar la configuración de la protección web de Sophos:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Configuración > Protección web.**
2. Para bloquear o desbloquear sitios web maliciosos, junto a **Bloquear acceso a sitios web maliciosos**, seleccione **Sí** o **No**. Esta opción está activada por defecto.  
Para más información sobre cómo autorizar sitios web clasificados como maliciosos, consulte [Autorizar sitios web](#) en la página 38.
3. Para activar o desactivar escaneado de datos y archivos descargados, junto a **Escaneado de contenido**, seleccione **Como en acceso**, **Sí**, o **No**.  
La opción predeterminada es **Como en acceso**, es decir, se ajusta al estado del escaneado en acceso.
4. Para cambiar lo que sucede cuando se descarga un archivo de baja reputación o desconocida, en **Reputación de descarga**, junto a **Acciones**, seleccione **Alerta** (por defecto) o **Solo registro**.
  - Si se selecciona **Alerta**, cada vez que se descargue un archivo de baja reputación se mostrará una alerta preguntando si se desea bloquear o permitir la descarga. Recomendamos no descargar este tipo de archivos. Si el origen y el publicador son de confianza puede permitir la descarga. La elección realizada, bloqueo o permiso para descarga el archivo, y la URL del archivo se guardan en el registro de escaneado.
  - Si se selecciona **Solo registro**, no se muestra ninguna alerta y la descarga se permite y se guarda en el registro de escaneado.
5. Para seleccionar el nivel de rigurosidad del escaneado de reputación, junto a **Umbral**, seleccione **Recomendado** (predeterminado) o **Estricto**.
  - Con **Recomendado** se muestra una alerta y/o se crea un registro cada vez que se descarga un archivo de baja reputación o desconocida.
  - Con **Estricto** se muestra una alerta y/o se crea un registro cada vez que se descarga un archivo de baja reputación o desconocida.

Para más información sobre la reputación de descargas, consulte el [artículo de la base de conocimiento 121319](#).

Para más información sobre el registro de escaneado, consulte [Ver el registro del escaneado](#) en la página 51.

## 4.8 Autorizar el uso de elementos

### 4.8.1 Autorizar programas publicitarios y otras aplicaciones no deseadas

**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.

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

Para autorizar programas publicitarios y otras 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, vea la sección [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 42.

### 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 elementos sospechosos

**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.

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 43
- [Revisar comportamientos sospechosos en cuarentena](#) en la página 44

#### 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 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.

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 más información, consulte la sección [Realizar un escaneo exhaustivo](#) en la página 25.
- El elemento muestra un comportamiento sospechoso.
- El elemento es una aplicación restringida.

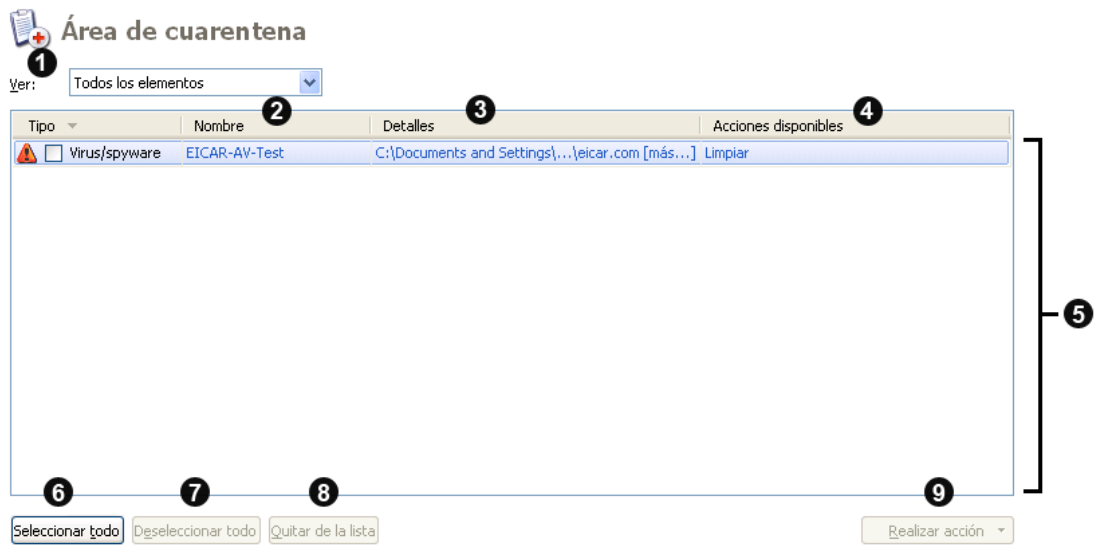
**Nota:** los programas publicitarios, aplicaciones no deseadas e infecciones de varios componentes detectados durante el escaneo en acceso se enumeran siempre en el Área de cuarentena. Desde el escaneo en acceso no es posible realizar la limpieza automática de aplicaciones no deseadas, programas publicitarios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



<b>1</b>	En el cuadro de lista <b>Ver</b> , seleccione el tipo de elemento que desea mostrar.
<b>2</b>	Identidad del elemento, con un enlace al análisis correspondiente en la web de Sophos.
<b>3</b>	Nombre del archivo y ubicación del elemento. Si el elemento está asociado con un rootkit, aparece como <b>Oculto</b> . Si el elemento está afectado por una infección múltiple, aparecerá un enlace con <b>más</b> 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.
<b>4</b>	Las acciones disponibles. Si el elemento no está oculto, puede: <b>Limpiar, Borrar y Mover</b> . Haga clic en la acción que desee llevar a cabo. Los archivos ocultos sólo se pueden limpiar.
<b>5</b>	La lista de elementos detectados. Para ordenar la lista, haga clic en el encabezado de la columna adecuada.
<b>6</b>	Utilice el botón <b>Seleccionar todo</b> para realizar la misma acción en todos los elementos de la lista. Para deseleccionar un elemento, desactive la casilla correspondiente en la columna <b>Tipo</b> .
<b>7</b>	Para deseleccionar todos los elementos seleccionados, haga clic en el botón <b>Deseleccionar todo</b> . Para seleccionar un elemento, active la casilla correspondiente en la columna <b>Tipo</b> .



<b>8</b>	Haga clic en <b>Quitar de la lista</b> para quitar los elementos seleccionados de la lista <b>sin</b> realizar ninguna acción. Esta acción no borra los archivos del disco duro.
<b>9</b>	Haga clic en <b>Realizar acción</b> 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.

- 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 6.
- 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 más información sobre cómo ponerse en contacto con el servicio de soporte, consulte [Soporte técnico](#) en la página 107.

Consulte cómo [Configurar los derechos sobre el área de cuarentena](#) en la página 8 si desea modificar las acciones disponibles.

#### 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 6.
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.

Consulte cómo [Configurar los derechos sobre el área de cuarentena](#) en la página 8 si desea modificar las acciones disponibles.

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 6.
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.

Consulte cómo [Configurar los derechos sobre el área de cuarentena](#) en la página 8 si desea modificar las acciones disponibles.

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 6.
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.

Consulte cómo [Configurar los derechos sobre el área de cuarentena](#) en la página 8 si desea modificar las acciones disponibles.

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 6.
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. Vea [Información de limpieza](#) en la página 47 para obtener desde la web de Sophos información sobre cada elemento.

### 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 escaneado de páginas web ya que las amenazas no se encuentran en su ordenador.

**Nota:** la limpieza de amenazas no puede deshacer el daño que se haya podido causar. Por ejemplo, si la amenaza ha modificado el valor de ciertas opciones, durante la limpieza no se podrá conocer el valor original de dichas opciones. Deberá revisar la configuración del equipo. La limpieza de documentos infectados no puede deshacer el daño que la amenaza haya podido causar.

## 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 (escaneado en acceso)
- Desde el cuadro de diálogo del escaneado (escaneados personalizados y de botón derecho)
- Desde el área de cuarentena (todos los tipos de escaneado)

### Obtener información desde el mensaje de alerta

Si tiene activado el escaneado 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 escaneado

Para los escaneados personalizados y de botón derecho, en el cuadro de diálogo del escaneado, 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 6.
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 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.

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.

**Nota:** los mensajes definidos por el usuario no se mostrarán en Windows 8 o posterior.

### 4.11.2 Configurar las alertas antivirus por email

**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.

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 escaneo** incluye ocasiones en que Sophos Anti-Virus no tiene acceso a algún elemento.

Sophos Anti-Virus no enviará alertas por email 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.

#### **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	
<b>Servidor SMTP</b>	Indique el nombre o dirección IP de su servidor SMTP. Haga clic en <b>Probar</b> para verificar el acceso al servidor SMTP (no se enviará <i>ningún</i> mensaje de prueba).



Configurar correo SMTP	
<b>Dirección remitente</b>	Indique la dirección de email a la que llegarán mensajes devueltos o rechazados.
<b>Dirección de respuesta</b>	Indique la dirección a la que se enviarán las respuestas que el mensaje de alerta pueda generar.
<b>Language</b>	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 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.

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.

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 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.

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:

<b>Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2:</b>	C:\ProgramData\Sophos\Sophos Anti-Virus\logs\SAV.txt
<b>Otros sistemas Windows</b>	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 6.

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 Restricción de aplicaciones de Sophos

### 5.1 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 10.

### 5.2 Desactivar el escaneado de aplicaciones restringidas

**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.

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**.

## 6 Control de dispositivos de Sophos

### 6.1 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 54.

### 6.2 Tipos de dispositivos controlados

El control de dispositivos bloquea o permite los siguientes tipos de dispositivos en este ordenador: *almacenamiento*, *red*, *corto alcance*. y *medios*.

#### 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)

#### Medios

- MTP/PTP

Esto incluye teléfonos móviles, tabletas, cámaras digitales, reproductores multimedia y otros dispositivos que se conectan a un ordenador mediante el protocolo de transferencia multimedia (MTP) o el protocolo de transferencia de imágenes (PTP).

## 6.3 Desactivar temporalmente el control de dispositivos

**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.

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**.

## 6.4 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.

## 6.5 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 6.

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 Control de datos de Sophos

## 7.1 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 55.

## 7.2 Desactivar temporalmente el control de datos

**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.

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**.

## 7.3 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.

## 7.4 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.

## 7.5 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 [Acerca de la página de inicio](#) en la página 6.

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.



## 8 Control web de Sophos

### 8.1 Acerca del control web

El control web de Sophos ofrece protección, control y notificación para equipos móviles o ubicados fuera de la red empresarial.

**Nota:** esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia.

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

El control web se gestiona mediante la política correspondiente desde la consola de administración. Si pertenece al grupo SophosAdministrator, puede desactivar de forma temporal el control web en los equipos: Para más información sobre cómo hacerlo, consulte [Desactivar temporalmente el control web](#) en la página 57.

### 8.2 Desactivar temporalmente el control web

**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.

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

Para desactivar el control web en un equipo:

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

## 9 Sophos Client Firewall

### 9.1 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 58.

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 67.

#### **¿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 66.

El modo interactivo no está disponible en Windows 8 y posterior. Debe añadir reglas específicas para autorizar o bloquear aplicaciones. Si lo prefiere, puede utilizar el visualizador de eventos en la consola para gestionar las aplicaciones.

### 9.2 Configurar el cortafuegos

#### 9.2.1 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 la funciones comunes:

- [Activar el modo interactivo](#) en la página 66
- [Filtrar mensajes ICMP](#) en la página 64
- [Permitir todo el tráfico en la red local](#) en la página 60
- [Permitir descargas FTP](#) en la página 60
- [Crear reglas globales](#) en la página 71
- [Permitir una aplicación](#) en la página 62
- [Permitir que las aplicaciones inicien procesos ocultos](#) en la página 75
- [Permitir que las aplicaciones utilicen conexiones de bajo nivel](#) en la página 76
- [Utilizar sumas de verificación para autenticar aplicaciones](#) en la página 76

## 9.2.2 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 6.
2. En la sección **Configuración**, active la opción **Permitir todo el tráfico** junto a la ubicación primaria o secundaria.

## 9.2.3 Permitir aplicaciones de correo electrónico

**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.

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 6.
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**.

## 9.2.4 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 6.
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**.

## 9.2.5 Permitir descargas FTP

**Nota:** si ha permitido el uso de navegadores de Internet que pueden acceder a servidores FTP, no es necesario permitir también las descargas 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 6.
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**.

## 9.2.6 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 6.
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 red** 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. Esta opción no está disponible en Windows 8 y posterior. Para más información sobre la detección de la red local, consulte [Acerca de la detección de red local](#) en la página 71.

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.

### 9.2.7 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 6.
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 red** 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. Esta opción no está disponible en Windows 8 y posterior. Para más información sobre la detección de la red local, consulte [Acerca de la detección de red local](#) en la página 71.
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 62
- [Control flexible del uso compartido de archivos e impresoras](#) en la página 62

Para más información sobre cómo permitir todo el tráfico en la red, consulte [Permitir todo el tráfico en la red local](#) en la página 60.

## 9.2.8 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 6.
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**.

## 9.2.9 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 6.
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**.

## 9.2.10 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 6.
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 73
- [Aplicar reglas de aplicaciones predefinidas](#) en la página 73

## 9.2.11 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 6.
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**.

## 9.2.12 Bloquear IPv6

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 6.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Según el sistema operativo:
  - En Windows 7 y anterior, en la ficha **General**, en la sección **Bloqueo**, seleccione **Bloquear paquetes IPv6**.
  - En Windows 8 o posterior, en la ficha **Reglas globales**, seleccione **Bloquear todo el tráfico IPv6**.

## 9.2.13 Activar o desactivar el uso de sumas de verificación

Si activa el uso de sumas de verificación, al autorizar o bloquear una aplicación será identificada mediante la suma de verificación de forma automática (las sumas de verificación también se pueden añadir de forma manual). Si la aplicación difiere de la suma de verificación, será bloqueada.

Si desactiva esta opción, las aplicaciones se identificarán mediante el nombre.

Para activar o desactivar el uso 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 6.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Según el sistema operativo:
  - En Windows 7 y anterior, en la sección **Bloqueo**, utilice la opción **Autenticar aplicaciones mediante sumas de verificación**.
  - En Windows 8 o posterior, haga clic en la ficha **Aplicaciones** y desactive la casilla **Autenticar aplicaciones mediante sumas de verificación**.

Para activar el uso de sumas de verificación, seleccione la opción mencionada.

## 9.2.14 Activar o desactivar el bloqueo de procesos modificados

**Nota:** esta opción no está disponible en Windows 8 y posterior porque la tecnología antivirus y HIPS de Sophos se encarga automáticamente.

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 6.
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 (sólo para sistemas operativos de 32 bits)** 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.

## 9.2.15 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 65.

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 6.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **ICMP**. Según el sistema operativo:
  - En Windows 7 y anterior, en la ficha ICMP, active las casillas **Entrada** o **Salida** para permitir los mensajes entrantes o salientes de cada tipo.



- En Windows 8 y posterior, los tipos de mensajes ICMP se categorizan en secciones. Seleccione las opciones comunes en el cuadro de lista desplegable o haga clic en **Detalles** para ver o modificar la configuración.

## 9.2.16 Explicación de los tipos de mensajes ICMP

### notificación de errores de red

<b>Destino no alcanzado, Respuesta eco</b>	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.
<b>Acallar fuente</b>	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.
<b>Tiempo agotado</b>	Enviado por un router cuando el datagrama alcanza el número máximo de routers por los que puede pasar.
<b>Problema de parámetro</b>	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.

### Solución de problemas de red

<b>Petición eco, Respuesta eco</b>	Se utilizan para probar la accesibilidad y el estado de los destinos. El host envía una <b>Petición eco</b> y espera la <b>Respuesta eco</b> correspondiente. La operación suele llevarse a cabo con el comando <b>ping</b> .
------------------------------------	---

### Configuración de enrutamiento y dirección de red IPv4

<b>Redireccionar</b>	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.
<b>Anuncio de router, Solicitud de router</b>	Permite al host descubrir la existencia de routers. Los routers retransmiten de forma periódica las direcciones IP mediante mensajes <b>Anuncio de router</b> . Los hosts también pueden solicitar la dirección de un router retransmitiendo un mensaje <b>Solicitud de router</b> al que responderá el router con un <b>Anuncio de router</b> .
<b>Petición de sincronización, Respuesta timestamp</b>	Se utiliza para sincronizar los relojes entre los hosts para calcular el tiempo de tránsito.

<b>Solicitar información, Respuesta de información</b>	Obsoletos. Los hosts utilizaban estos mensajes para determinar las direcciones entre redes, pero ya no deberían utilizarse.
<b>Petición de máscara de red, Respuesta de máscara de red</b>	Se utiliza para encontrar la máscara de la subred (es decir, las partes de la dirección que definen la red). Un host envía una <b>Petición de máscara de red</b> a un router y recibe una <b>Respuesta de máscara de red</b> .

### 9.2.17 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 6.
2. En la sección **Opciones de configuración**, haga clic en **Predeterminado**.

## 9.3 Modo interactivo

### 9.3.1 Acerca del modo interactivo

**Nota:** el modo interactivo no está disponible en Windows 8 y posterior. Debe añadir reglas específicas para autorizar o bloquear aplicaciones. Si lo prefiere, puede utilizar el visualizador de eventos en la consola para gestionar las aplicaciones.

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 67
- [Cuadros de diálogo de aprendizaje de protocolo](#) en la página 67
- [Cuadros de diálogo de aprendizaje de aplicaciones](#) en la página 68
- [Cuadros de aprendizaje de conexiones de bajo nivel](#) en la página 68
- [Cuadros de diálogo de aprendizaje de sumas de verificación](#) en la página 68

### 9.3.2 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 6.
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**.

### 9.3.3 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 6.
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**.

### 9.3.4 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 67

### 9.3.5 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 6.
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**.

### 9.3.6 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.

### 9.3.7 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 remotos.

### 9.3.8 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 68

### 9.3.9 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 6.
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**.

### 9.3.10 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.

El cuadro de diálogo de aprendizaje de sumas de verificación sólo se mostrará si utiliza sumas de verificación para autenticar aplicaciones. Para más información, consulte [Activar o desactivar el uso de sumas de verificación](#) en la página 63.

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.

## 9.4 Archivos de configuración del cortafuegos

### 9.4.1 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.

### 9.4.2 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 6.
2. Haga clic en **Exportar**.
3. Escriba un nombre para el archivo de configuración, seleccione la ubicación y haga clic en **Guardar**.

### 9.4.3 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 6.
2. Haga clic en **Importar**.
3. Seleccione un archivo de configuración y haga clic en **Abrir**.
4. Siga las instrucciones en pantalla.

## 9.5 Reglas del cortafuegos

### 9.5.1 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.

Para más información sobre la configuración de estas reglas, consulte <http://www.sophos.com/es-es/support/knowledgebase/57757.aspx>.

### 9.5.2 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 con 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. Este modo no está disponible en Windows 8 o posterior.

**Nota:** inicialmente, el cortafuegos se encuentra en el modo **Bloquear por defecto**.

### 9.5.3 Acerca de la detección de red local

**Nota:** esta opción no está disponible en Windows 8 y posterior.

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 78.

### 9.5.4 Reglas globales

#### 9.5.4.1 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 6.
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. En Windows 8 o posterior, en **Protocolo**, seleccione el protocolo que desee utilizar.
7. Para aplicar la regla antes que otras reglas de aplicaciones o reglas globales de prioridad normal, active la opción **Prioritaria ante reglas de aplicaciones**.  
Para más información sobre el orden de aplicación de las reglas, consulte [Orden de aplicación de las reglas](#) en la página 70.
8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.

9. En **Seleccione la acción que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
  10. Escoja una de las siguientes opciones:
    - Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**. Esta opción sólo está disponible para reglas TCP.
    - Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**. Esta opción sólo está disponible para reglas UDP.
- Nota:** estas opciones no se muestran en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.
11. En **Descripción de la regla**, haga clic en un valor subrayado.

#### 9.5.4.2 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 6.
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 71.

#### 9.5.4.3 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 6.
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**.

#### 9.5.4.4 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 6.
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**.



### 9.5.4.5 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 6.
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**.

## 9.5.5 Reglas de aplicaciones

### 9.5.5.1 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 6.
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 **Personalizar**.
5. Señale **Predefinidas** y haga clic en una regla predefinida.

### 9.5.5.2 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 6.
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 Windows 8 o posterior, en **Protocolo**, seleccione el protocolo que desee utilizar.
8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
9. En **Seleccione la acción que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.

10. Escoja una de las siguientes opciones:

- Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**. Esta opción sólo está disponible para reglas TCP.
- Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**. Esta opción sólo está disponible para reglas UDP.

**Nota:** estas opciones no se muestran en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.

11. En **Descripción de la regla**, haga clic en un valor subrayado.

### 9.5.5.3 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 6.

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 Windows 8 o posterior, en **Protocolo**, seleccione el protocolo que desee utilizar.

8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.

9. En **Seleccione la acción que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.

10. Escoja una de las siguientes opciones:

- Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**. Esta opción sólo está disponible para reglas TCP.
- Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**. Esta opción sólo está disponible para reglas UDP.

**Nota:** estas opciones no se muestran en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.

11. En **Descripción de la regla**, haga clic en un valor subrayado.

### 9.5.5.4 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 6.

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**, seleccione la regla que desea copiar y haga clic en **Copiar**.

#### 9.5.5.5 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 6.
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**, seleccione la regla que desea eliminar y haga clic en **Eliminar**.

#### 9.5.5.6 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 6.
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**.

#### 9.5.5.7 Permitir que las aplicaciones inicien procesos ocultos

**Nota:** esta opción no está disponible en Windows 8 y posterior porque la tecnología antivirus y HIPS de Sophos se encarga automáticamente.

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 6.
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 66
- [Activar cuadros de diálogo de aprendizaje de procesos ocultos](#) en la página 67

#### 9.5.5.8 Permitir que las aplicaciones utilicen conexiones de bajo nivel

**Nota:** esta opción no está disponible en Windows 8 y posterior. Las conexiones de bajo nivel se tratarán como el resto de conexiones.

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 6.
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 66
- [Activar los cuadros de diálogo de aprendizaje de conexiones de bajo nivel](#) en la página 68

#### 9.5.5.9 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 6.

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 66
- [Activar cuadros de diálogo de aprendizaje de procesos ocultos](#) en la página 67

## 9.6 Detección de la ubicación

### 9.6.1 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.

### 9.6.2 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.

### 9.6.3 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 6.
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:

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

4. Siga las instrucciones en pantalla.

### 9.6.4 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 6.
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 58 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.

### 9.6.5 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 6.

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

Opción	Descripción
<b>Ubicación detectada</b>	El cortafuegos aplica la configuración primaria o secundaria según la conexión detectada (establecida en <a href="#">Configurar la detección de la ubicación</a> en la página 77).
<b>Ubicación primaria</b>	El cortafuegos aplica la configuración primaria.
<b>Ubicación secundaria</b>	El cortafuegos aplica la configuración secundaria.

## 9.7 Informes del cortafuegos

### 9.7.1 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 la sección [Activar o desactivar notificación de cambios locales](#) en la página 79.

#### 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 la sección [Desactivar la notificación de tráfico desconocido](#) en la página 80.

### 9.7.2 Activar o desactivar notificación de cambios locales

**Nota:** esta opción no está disponible en Windows 8 y posterior.

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 6.
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.

### 9.7.3 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 6.
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**.

### 9.7.4 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 6.
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**.



## 9.7.5 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 6.
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**.

## 9.8 Registro del cortafuegos

### 9.8.1 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

### 9.8.2 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 6.

### 9.8.3 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 6.
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**.

#### 9.8.4 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 6.
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.

#### 9.8.5 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 6.
2. En el menú **Ver**, haga clic en **Personalizar**.
3. Seleccione las opciones correspondientes.

## 9.8.6 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 6.
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.

## 9.8.7 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 6.
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.

## 9.8.8 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 6.
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.

## 9.8.9 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 6.
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.

## 9.8.10 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 6.
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.

# 10 Sophos AutoUpdate

## 10.1 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**.

## 10.2 Programar las actualizaciones

**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.

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.

## 10.3 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.

## 10.4 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.

## 10.5 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*.

## 10.6 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.

## 10.7 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.

## 10.8 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.

## 10.9 Ver el registro de actualización

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

# 11 Protección contra manipulaciones de Sophos

## 11.1 Protección contra manipulaciones

La protección contra manipulaciones permite evitar que programas maliciosos o usuarios no autorizados (usuarios con conocimientos limitados) 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 escaneo de amenazas y comportamientos sospechosos. Para más información, consulte la sección Sophos Anti-Virus (capítulo 4).

### 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 7.

#### **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 escaneo en acceso o de la detección de comportamiento sospechoso. Para más información, consulte [Introducir la contraseña para configurar el software](#) en la página 90.
- Desactivar la protección contra manipulaciones. Para más información, consulte [Desactivar la protección contra manipulaciones](#) en la página 89.
- 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 90.

## 11.2 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 6.
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.

## 11.3 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 90 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 6.
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**.

## 11.4 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 6.
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**.

## 11.5 Contraseña de la protección contra manipulaciones

Si tiene activada la protección contra manipulaciones, deberá introducir la contraseña correspondiente para configurar el escaneado 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.

## 11.6 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 6.
2. En el cuadro de diálogo **Autenticación de la protección contra manipulaciones**, introduzca la contraseña correspondiente y haga clic en **Aceptar**.

## 11.7 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 90 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 6.
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.

## 11.8 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 6.
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.

## 11.9 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 6.

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.

## 12 Solución de problemas

### 12.1 La última actualización no se completó debido a algún error

#### 12.1.1 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 87.

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 93
- [Sophos Endpoint Security and Control no siempre puede restaurar toda la configuración](#) en la página 93
- [La actualización automática no está configurada correctamente](#) en la página 93
- [No se ha mantenido la fuente de actualización](#) en la página 94

#### 12.1.2 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 85.

#### 12.1.3 Sophos Endpoint Security and Control no siempre puede restaurar toda la configuración

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 86.

#### 12.1.4 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 85.)
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**.

### 12.1.5 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.

## 12.2 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 13
- [Configurar la limpieza del escaneado de botón derecho](#) en la página 17
- [Configurar la limpieza del escaneado personalizado](#) en la página 22

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 25.
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 obtener información, consulte [Excluir elementos del escaneado en acceso](#) en la página 26. 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 XP 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 la sección [Fragmento de virus/spyware detectado](#) en la página 95.

# 12.3 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 85
  - [Realizar un escaneado exhaustivo](#) en la página 25

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

- [Soporte técnico](#) en la página 107

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 más información sobre cómo ponerse en contacto con el servicio de soporte, consulte [Soporte técnico](#) en la página 107.

## 12.4 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 25

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.

- [Excluir elementos del escaneo en demanda](#) en la página 26

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.

## 12.5 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 más información, consulte la sección [Autorizar programas publicitarios y otras aplicaciones no deseadas](#) en la página 37.

## 12.6 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 25.

**Nota:** si se detecta una aplicación no deseada después del escaneo, vea el paso 2 de la sección [Amenaza detectada parcialmente](#) en la página 96.

2. Limpie el programa publicitario o la aplicación no deseada. Para más información, vea la sección [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 42.



## 12.7 Permitir el acceso a unidades con sectores de arranque infectados

**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, 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.

## 12.8 Imposible acceder a 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 7.

## 12.9 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 cómo [Información de limpieza](#) en la página 47 desde la web de Sophos para conocer los efectos secundarios de 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 más información sobre cómo ponerse en contacto con el servicio de soporte, consulte [Soporte técnico](#) en la página 107.

## 12.10 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 cómo [Información de limpieza](#) en la página 47 desde la web de Sophos para conocer los efectos secundarios de cada programa publicitario o aplicación no deseada.

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 más información sobre cómo ponerse en contacto con el servicio de soporte, consulte [Soporte técnico](#) en la página 107.

## 12.11 Error de contraseña

Si está intentando programar un escaneo 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**.

## 12.12 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**.

## 12.13 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 seleccione **Iniciar**.

## Notas

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

## 13 Glosario

<b>adware y PUA</b>	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.
<b>análisis de comportamiento de ejecución</b>	Análisis dinámico para detectar comportamiento sospechoso y desbordamiento del búfer.
<b>aplicación de confianza</b>	Aplicación a la que se da acceso incondicional a la red.
<b>aplicación restringida</b>	Aplicación cuya ejecución no está permitida en el equipo por la política de seguridad de la empresa.
<b>archivo de detección (IDE)</b>	Archivo que permite a Sophos Anti-Virus detectar y desinfectar un virus, gusano o troyano.
<b>archivo sospechoso</b>	Archivo con características habituales de virus, aunque no exclusivas.
<b>barra de descripción</b>	Barra en el visor del registro, sobre la vista de datos, que muestra el elemento seleccionado.
<b>bloqueada</b>	Estado que indica que se ha denegado el acceso a la red a una aplicación (incluyendo procesos oculto), conexiones, protocolos, mensajes ICMP, etc.
<b>coincidencia</b>	Se corresponde con el contenido definido en la lista de control de contenido.
<b>conexión de bajo nivel</b>	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.
<b>configuración de procesos</b>	Configuración que especifica si los procesos modificados u ocultos tienen permiso de acceso a la red.
<b>configuración de purgado del registro</b>	Opciones que especifican cuando se borran las entradas del registro.
<b>configuración ICMP</b>	Configuración que especifica los tipos de comunicaciones de administración de la red permitidos.
<b>configuración primaria</b>	Configuración del cortafuegos utilizada para la red empresarial, a la que se conectan los usuarios a diario.

<b>configuración secundaria</b>	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.
<b>control de datos</b>	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.
<b>control de dispositivos</b>	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.
<b>cuadro de diálogo de aprendizaje</b>	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. Esta opción únicamente se aplica a Sophos Client Firewall para Windows 7 y anteriores.
<b>detección de comportamiento sospechoso</b>	Análisis dinámico del comportamiento de todos los programas para detectar y bloquear aquellos cuya actividad parezca maliciosa.
<b>detección de desbordamiento del búfer</b>	Detección de ataques de desbordamiento del búfer.
<b>Detección de tráfico malicioso</b>	Una función que detecta comunicaciones entre equipos secuestrados y los servidores de comando y control de atacantes.
<b>dispositivo de almacenamiento</b>	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).
<b>error de escaneado</b>	Error que se produce durante el escaneado de algún archivo, por ejemplo, acceso denegado.
<b>escaneado del botón derecho</b>	Escaneado de archivos desde Windows Explorer o en el escritorio mediante el menú contextual.
<b>escaneado en acceso</b>	Es la principal forma de protección contra 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.

<b>escaneado en demanda</b>	Escaneado iniciado por el usuario. Puede escanear desde un solo archivo a todo el contenido del equipo con permiso de lectura.
<b>escaneado exhaustivo</b>	Escaneado íntegro de cada archivo.
<b>escaneado normal</b>	Escaneado de las partes de cada archivo que pueden contener virus.
<b>escaneado programado</b>	Escaneado del ordenador, o parte, que se ejecuta a las horas establecidas.
<b>evento de amenaza</b>	Detección o desinfección de alguna amenaza.
<b>evento del cortafuegos</b>	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.
<b>filtrado dinámico</b>	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.
<b>gestor de autorización</b>	Módulo que permite autorizar programas publicitarios y aplicaciones no deseadas, archivos sospechosos, aplicaciones que presentan comportamientos sospechosos y desbordamientos del búfer.
<b>HIPS (sistema de prevención contra intrusiones)</b>	Término general para el análisis de comportamiento previo y durante la ejecución.
<b>ICMP</b>	Siglas del inglés que hacen referencia al "Protocolo de mensajes de control de Internet", Una capa de red para el protocolo de Internet que proporciona corrección de errores e información relevante a el procesamiento de paquetes IP.
<b>limpieza</b>	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.
<b>limpieza automática</b>	Limpieza que se realiza sin la intervención del usuario o tras la confirmación del usuario.
<b>limpieza manual</b>	Limpieza que se realiza mediante herramientas específicas o borrando archivos de forma manual.

<b>lista de control de contenido (LCC)</b>	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.
<b>memoria del sistema</b>	Memoria que funciona como puente entre las aplicaciones y los datos procesados a nivel de hardware. La utiliza el sistema operativo.
<b>mensajería instantánea</b>	Categoría de aplicaciones restringidas donde se incluyen programas de chat (como MSN).
<b>modo de funcionamiento</b>	Configuración que determina si el cortafuegos lleva a cabo acciones con la interacción del usuario (modo interactivo) o de forma automática (modos no interactivos). El modo interactivo se eliminó en Sophos Client Firewall para Windows 8 y posterior.
<b>modo interactivo</b>	Modo en el que el cortafuegos muestra cuadros de diálogo de aprendizaje al detectar tráfico de red para el que no dispone de reglas. Esta opción únicamente se aplica a Sophos Client Firewall para Windows 7 y anteriores.
<b>modo no interactivo</b>	Modo en el que el cortafuegos bloquea o permite todo el tráfico de red para el que no dispone de reglas.
<b>NetBIOS</b>	Abreviatura de "Sistema básico de entrada/salida de red". Programa 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.
<b>política del cortafuegos</b>	Configuración proporcionada por la consola de administración que utiliza el cortafuegos para controlar la conexión del equipo a Internet y a otras redes.
<b>proceso oculto</b>	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.
<b>programas espía</b>	Programa que se instala en un equipo de forma inadvertida y envía información sin conocimiento ni autorización del usuario.
<b>Protección activa de Sophos</b>	Función que utiliza la conexión a Internet para comprobar archivos sospechosos.
<b>protección contra manipulaciones</b>	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.



<b>protocolo de red</b>	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.
<b>regla de aplicación</b>	Regla que afecta sólo a los paquetes de datos transferidos en la red entrantes o salientes de una aplicación.
<b>regla de contenido</b>	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.
<b>regla del sistema</b>	Regla que se asigna a todas las aplicaciones y que permite o bloquea comunicaciones de bajo nivel.
<b>regla global de alta prioridad</b>	Regla global que se aplica antes que otras reglas globales o reglas de aplicaciones.
<b>regla personalizada</b>	Regla creada por el usuario para especificar las circunstancias bajo las cuales una aplicación se puede ejecutar.
<b>reglas globales</b>	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).
<b>reputación de descargas</b>	Reputación de un archivo descargado de Internet. La reputación se calcula a partir de la antigüedad del archivo, el origen, la prevalencia, análisis de contenido profundo y otras características. Ayuda a establecer si el archivo es seguro o si representa un riesgo potencial que puede dañar el ordenador de un usuario si se descarga.
<b>rootkit</b>	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.
<b>suma de verificación</b>	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.
<b>tipo de archivo verdadero</b>	Tipo de archivo establecido mediante el análisis de la estructura del archivo, en contraposición a la extensión del mismo. Este método es más fiable.
<b>tráfico desconocido</b>	Forma de acceso de una aplicación o servicio a la red para la que el cortafuegos no dispone de una regla.

<b>virus no identificado</b>	Virus para el que todavía no existe un archivo de detección específico.
<b>visor del registro</b>	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.
<b>vista de datos</b>	Vista que muestra los datos según el elemento seleccionado.
<b>vista de árbol</b>	Vista que lista los elementos que se pueden seleccionar en el visor del registro.
<b>voz sobre IP</b>	Categoría de aplicaciones restringidas donde se incluyen programas de llamadas por Internet.
<b>área de cuarentena</b>	Módulo que permite revisar los elementos que se han puesto en cuarentena.

## 14 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar la comunidad de Sophos en [community.sophos.com/](https://community.sophos.com/) para consultar casos similares.
- Visitar la base de conocimiento de Sophos en [www.sophos.com/es-es/support.aspx](https://www.sophos.com/es-es/support.aspx).
- Descargar la documentación correspondiente desde [www.sophos.com/es-es/support/documentation.aspx](https://www.sophos.com/es-es/support/documentation.aspx).
- Abrir un ticket de incidencia con nuestro equipo de soporte en <https://secure2.sophos.com/support/contact-support/support-query.aspx>.

## 15 Aviso legal

Copyright © 1989-2016 Sophos Limited. All rights reserved. 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, Sophos Anti-Virus y SafeGuard son marcas registradas de Sophos Limited, Sophos Group o Utimaco Safeware AG, según corresponda. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

### Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>

### Boost C++ Libraries

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### 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, el código fuente está disponible mediante solicitudes por correo ordinario a Sophos, por correo electrónico a [sophos@support.sophos.com](mailto:sophos@support.sophos.com) o desde la página web <https://www.sophos.com/es-es/support/contact-support.aspx>. A copy of the license

agreement for any such included software can be found at  
<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.

### crt

```
# $FreeBSD$
# @(#)COPYRIGHT 8.2 (Berkeley) 3/21/94
```

The compilation of software known as FreeBSD is distributed under the following terms:

Copyright (c) 1992-2013 The FreeBSD Project. All rights reserved.

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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "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 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

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 acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "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 REGENTS 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 Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation. This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTA: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at <http://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License>. Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

"3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins  
Director, Office of Technology Licensing  
University of California, Berkeley

## dtoa.c

The author of this software is David M. Gay.

Copyright © 1991, 2000 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

## ICU

ICU version 1.8.1 or later

### COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995–2008 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

## IEEE Software Taggant Library

This software was developed by The Institute of Electrical and Electronics Engineers, Incorporated (IEEE), through the Industry Connections Security Group (ICSG) of its Standards Association. Portions of it include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>), and those portions are governed by the OpenSSL Toolkit License.

### IEEE License

Copyright (c) 2012 IEEE. All rights reserved.

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 IEEE Industry Connections Security Group (ICSG)".

4. The name "IEEE" must not be used to endorse or promote products derived from this software without prior written permission from the IEEE Standards Association ([stds.ipr@ieee.org](mailto:stds.ipr@ieee.org)).
5. Products derived from this software may not contain "IEEE" in their names without prior written permission from the IEEE Standards Association ([stds.ipr@ieee.org](mailto:stds.ipr@ieee.org)).
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the IEEE Industry Connections Security Group (ICSG)".

THIS SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." IEEE AND ITS CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (B) ANY WARRANTY OF NON-INFRINGEMENT; AND (C) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, EFFECTIVENESS, CURRENCY OR COMPLETENESS OF THE SOFTWARE.

IN NO EVENT SHALL IEEE 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 AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

THIS SOFTWARE USES STRONG CRYPTOGRAPHY, WHICH MAY BE SUBJECT TO LAWS AND REGULATIONS GOVERNING ITS USE, EXPORTATION OR IMPORTATION. YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS AND REGULATIONS, INCLUDING, BUT NOT LIMITED TO, ANY THAT GOVERN YOUR USE, EXPORTATION OR IMPORTATION OF THIS SOFTWARE. IEEE AND ITS CONTRIBUTORS



DISCLAIM ALL LIABILITY ARISING FROM YOUR USE OF THE SOFTWARE IN VIOLATION OF ANY APPLICABLE LAWS OR REGULATIONS.

## Info-ZIP

Copyright © 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases—including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

## Jansson

Copyright (c) 2009-2013 Petri Lehtinen <[petri@digip.org](mailto:petri@digip.org)>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Lua

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Lua License. A copy of the license agreement for any such included software can be found at <http://www.lua.org/copyright.html>

## Software de Microsoft

This Sophos product may include certain Microsoft software, licensed to Sophos for inclusion and use herein.

## Mersenne Twister (mt19937ar.c)

Copyright (c) 1997–2002 Makoto Matsumoto and Takuji Nishimura. All rights reserved.

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. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

## OpenSSL Cryptography and SSL/TLS 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](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998–2011 The OpenSSL Project. All rights reserved.

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](mailto: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 ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay license**

Copyright © 1995–1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@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](mailto: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](mailto: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](mailto: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.]

## Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

## pstdint

Copyright (c) 2005-2007 Paul Hsieh  
All rights reserved.

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. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

## Simple ECMAScript Engine (SEE)

Copyright © 2003, 2004, 2005, 2006, 2007 David Leonard. All rights reserved.

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. Neither the name of David Leonard nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

## SQLCipher

Copyright © 2008-2012 Zetetic LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of the ZETETIC LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ZETETIC LLC "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 ZETETIC LLC 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.

## strcasestr.c

Copyright © 1990, 1993 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

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. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "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 REGENTS 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.

## Udis86

Copyright (c) 2002-2009 Vivek Thampi  
All rights reserved.

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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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 views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

## Unicode

### UNICODE, INC. LICENSE AGREEMENT – DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories <http://www.unicode.org/Public/>, <http://www.unicode.org/reports/>, and <http://www.unicode.org/cldr/data/>. Unicode Software includes any source code published in the Unicode Standard or under the directories <http://www.unicode.org/Public/>, <http://www.unicode.org/reports/>, and <http://www.unicode.org/cldr/data/>.

**NOTICE TO USER:** Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

### COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991–2007 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in <http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any

associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

## UnRAR

The source code of UnRAR utility is freeware. This means:

1. All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.
2. The UnRAR sources may be used in any software to handle RAR archives without limitations free of charge, but cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified UnRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.
3. The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.
4. THE RAR ARCHIVER AND THE UnRAR UTILITY ARE DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.
5. Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.
6. If you don't agree with terms of the license you must remove UnRAR files from your storage devices and cease to use the utility.

Thank you for your interest in RAR and UnRAR.

Alexander L. Roshal



## Windows Template Library (WTL)

This product may contain Windows Template Library (WTL) and/or WixToolset code, which are licensed under the Common Public License 1.0. The source code for the components is available from Sophos, upon request, by emailing [TPCRequest@sophos.com](mailto:TPCRequest@sophos.com)

## wow64ext library

This is used in Sophos Virus Removal Tool as a shared library (wow64ext.dll), which may be removed or substituted without affecting other functionality. Its use is covered by the following license:

### **GNU LESSER GENERAL PUBLIC LICENSE**

#### **Version 3, 29 June 2007**

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

#### ▪ **0. Additional Definitions.**

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

#### **1. Exception to Section 3 of the GNU GPL.**

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

#### **2. Conveying Modified Versions.**

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

- a. under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or
- b. under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

### 3. **Object Code Incorporating Material from Library Header Files.**

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

- a. Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.
- b. Accompany the object code with a copy of the GNU GPL and this license document.

### 4. **Combined Works.**

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

- a. Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.
- b. Accompany the Combined Work with a copy of the GNU GPL and this license document.
- c. For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.
- d. *Escoja una de las siguientes opciones:*
  - 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source
  - 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.
- e. Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

### 5. **Combined Libraries.**

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

- a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.
- b. Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

**6. Revised Versions of the GNU Lesser General Public License.**

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

# Índice

## A

- acceso a discos [10, 97](#)
- activar el cuadro de diálogo de aprendizaje de sumas de verificación [63](#)
- activar el escaneado en acceso [12](#)
- actualización [85, 87, 93](#)
- actualización inmediata [85](#)
- actualización mediante conexión telefónica [85](#)
- adware [10, 16–17, 20, 22, 37, 96, 98](#)
  - autorización [37](#)
  - detectar [10, 16, 20](#)
  - limpieza automática [17, 22](#)
- adware autorizado, bloquear [37](#)
- amenaza detectada parcialmente [96](#)
- análisis de amenazas [47](#)
- análisis de comportamiento de ejecución [32](#)
- ancho de banda de actualización, limitar [86](#)
- antivirus [47–50](#)
  - configurar el registro de eventos [50](#)
  - configurar la mensajería SNMP [49](#)
  - configurar las alertas por email [48](#)
  - configurar, mensajería de escritorio [47](#)
- añadir usuarios a grupos de Sophos [8](#)
- aplicaciones [62–63, 76](#)
  - bloquear [63](#)
  - permitir [62](#)
  - sumas de verificación para autenticar aplicaciones [76](#)
- aplicaciones no deseadas en cuarentena, revisar [42](#)
- aplicaciones restringidas [45, 52](#)
  - autorización [45](#)
  - detectar [52](#)
  - gestionar [45](#)
- archivos comprimidos, escaneado [10, 16, 20](#)
- archivos de configuración del cortafuegos [69](#)
  - exportar [69](#)
  - importar [69](#)
- archivos sospechosos [10, 13, 16–17, 20, 22, 37](#)
  - autorización [37](#)
  - detectar [10, 16, 20](#)
  - limpieza automática [13, 17, 22](#)
- archivos sospechosos en cuarentena, revisar [43](#)
- autenticación de aplicaciones, sumas de verificación [76](#)
- autorización [37–38, 44–45](#)
  - adware [37](#)
  - aplicaciones restringidas [45](#)
  - archivos sospechosos [37](#)
  - comportamiento sospechoso [37, 44](#)
  - desbordamientos del búfer [37, 44](#)
  - PUA (aplicaciones no deseadas) [37](#)
  - sitios web [38](#)

## B

- bloquear [36–37, 62–63](#)
  - adware autorizado [37](#)

- bloquear (*continuación*)
  - aplicaciones [63](#)
  - IPv6 [63](#)
  - PUA autorizadas [37](#)
  - sitios web maliciosos [36](#)
  - uso compartido de archivos e impresoras [62](#)
- borrar escaneados personalizados [25](#)

## C

- cambiar el nombre de un escaneado programado [25](#)
- comportamiento malicioso [32](#)
  - detectar [32](#)
- comportamiento sospechoso [32, 37, 44](#)
  - autorización [37, 44](#)
  - detectar [32](#)
- comportamientos sospechosos en cuarentena, revisar [44](#)
- conexiones de bajo nivel, permitir [76](#)
- configuración secundaria [78](#)
  - crear [78](#)
- configurar [8, 10, 16, 20, 47–50, 79, 81](#)
  - alertas antivirus por email [48](#)
  - derechos sobre el área de cuarentena [8](#)
  - escaneado de botón derecho [16](#)
  - escaneado en acceso [10](#)
  - escaneados personalizados [20](#)
  - informes centrales [79](#)
  - mensajería de escritorio del antivirus [47](#)
  - mensajería SNMP del antivirus [49](#)
  - registro de eventos del antivirus [50](#)
  - registro del cortafuegos [81](#)
  - registro del escaneado [50](#)
- configurar reglas globales [71, 73, 75](#)
- configurar una regla [72](#)
- control de comportamiento [31–32](#)
  - activar [32](#)
- control de datos, desactivar temporalmente [55](#)
- control de dispositivos [53–54](#)
  - bloqueo de puentes de red [53](#)
  - dispositivos controlados [53](#)
- control web [57](#)
  - desactivar [57](#)
  - descripción [57](#)
- correo electrónico, permitir [59](#)
- cortafuegos [59](#)
  - desactivar [59](#)
- crear escaneados personalizados [19](#)
- cuadro de diálogo de aprendizaje de sumas de verificación [63, 68](#)
  - activar [63](#)
  - modo interactivo [68](#)

## D

- derechos de acceso [7, 97](#)
- derechos de usuario [7, 97](#)
- derechos sobre el área de cuarentena, configurar [8](#)

- desactivar el control web [57](#)
- desactivar el cortafuegos [59](#)
- desactivar el escaneado en acceso [12](#)
- desactivar escaneado [54](#)
- desactivar la detección de aplicaciones restringidas [52](#)
- desbordamientos del búfer [33](#), [37](#), [44](#)
  - autorización [37](#), [44](#)
  - detectar [33](#)
- descargas FTP, permitir [60](#)
- desinfección [94](#)
- desinstalar el software de seguridad de Sophos [91](#)
- detección de la ubicación [77–78](#)
  - acerca de [77](#)
  - crear configuración secundaria [78](#)
  - definir las ubicaciones primarias [78](#)
  - usar dos adaptadores de red [77](#)
- detección parcial [96](#)
- detectar aplicaciones restringidas [52](#)
- detectar archivos sospechosos [10](#), [16](#), [20](#)
- detectar comportamiento malicioso [32](#)
- detectar comportamiento sospechoso [32](#)
- detectar desbordamientos del búfer [33](#)
- detectar programas publicitarios y aplicaciones no deseadas [10](#), [16](#), [20](#)
- detectar rootkits [20](#)
- detectar virus de Mac [10](#)
- dos adaptadores de red [77](#)
  - usar [77](#)

## E

- efectos secundarios [98](#)
- ejecutar escaneado con baja prioridad [20](#)
- ejecutar escaneados personalizados [24](#)
- elementos sospechosos, preautorizar [38](#)
- eliminar sumas de verificación de archivos escaneados [14](#)
- entradas de registro [83](#)
  - filtrar [83](#)
- error de contraseña [99](#)
- escaneado de aplicaciones restringidas, desactivar [52](#)
- escaneado de botón derecho [19](#)
- escaneado de botón derecho, configurar [16](#)
- escaneado de botón derecho, ejecutar [19](#)
- escaneado de contenido [35–36](#)
- escaneado de la memoria del sistema [10](#), [20](#)
- escaneado de un elemento [19](#)
- escaneado en acceso [10](#), [12](#), [14](#), [26](#)
  - activar [12](#)
  - configurar [10](#)
  - desactivar [12](#)
  - especificar extensiones de archivo [14](#)
  - excluir elementos [26](#)
- escaneado en acceso y en demanda, diferencias [10](#)
- escaneado en demanda [15](#)
  - especificar extensiones de archivo [15](#)
- Escaneado en demanda [26](#)
  - excluir elementos [26](#)
- escaneado exhaustivo, realizar [25](#)
- escaneados en demanda, tipos de [15](#)
- escaneados personalizados [19–20](#), [24–25](#)
  - cambiar el nombre [25](#)

- escaneados personalizados (*continuación*)
  - configurar [20](#)
  - crear [19](#)
  - ejecutar [24](#)
  - eliminar [25](#)
  - programación [24](#)
- escanear archivos comprimidos [10](#), [16](#), [20](#)
- escanear memoria del sistema [10](#), [20](#)
- escanear todos los archivos [10](#), [16](#), [20](#)
- escanear un elemento [19](#)
- especificar extensiones de archivo del escaneado en acceso [14](#)
- excluir elementos del escaneado en acceso [26](#)
- excluir elementos del escaneado en demanda [26](#)
- exportar archivos de configuración del cortafuegos [69](#)
- exportar entradas del visualizador del registro del cortafuegos [84](#)

## F

- filtrado URL [35–36](#)
- filtrar entradas de registro [83](#)
- filtrar mensajes ICMP [64](#)
- fragmento [94](#)
- fragmento detectado, solución de problemas [95](#)

## G

- gestionar las aplicaciones restringidas [45](#)
- Grupos de Sophos [7–8](#)
  - añadir usuarios [8](#)
- grupos de usuario [7](#), [97](#)

## H

- HIPS [31](#)

## I

- icono de la bandeja del sistema. [93](#)
- iconos [19](#)
  - elementos a escanear [19](#)
- importar archivos de configuración del cortafuegos [69](#)
- información de limpieza [47](#)
- información de seguridad [47](#)
- informes centrales, configuración [79](#)
- IPv6 [63](#)
  - bloquear [63](#)

## L

- limitar el ancho de banda de actualización [86](#)
- limpieza [46](#), [94](#)
  - acerca de [46](#)
  - solución de problemas [94](#)
- limpieza automática [13](#), [17](#), [22](#)
  - adware [17](#), [22](#)
  - archivos sospechosos [13](#), [17](#), [22](#)
  - programas espía [13](#), [17](#), [22](#)
  - PUA (aplicaciones no deseadas) [17](#), [22](#)
  - virus [13](#), [17](#), [22](#)

## M

- mensajes ICMP 64–65
  - filtrar 64
  - información sobre 65
- modo de funcionamiento, activar modo interactivo 66
- modo interactivo 67–68
  - cuadro de diálogo de aprendizaje de sumas de verificación 68
  - mensajes de aplicaciones 68
  - mensajes de conexiones de bajo nivel 68
  - mensajes de procesos ocultos 67
  - mensajes de protocolo 67
- modo interactivo, acerca de 66
- modo interactivo, activar 66
- modo no interactivo, cambiar a 67

## N

- navegadores de Internet, permitir 60

## O

- obtener instrucciones de limpieza 47

## P

- página de inicio 6
- para empezar 58
  - por dónde empezar 58
- permitir 59–62, 75–76
  - aplicaciones 62
  - conexiones de bajo nivel 76
  - correo electrónico 59
  - descargas FTP 60
  - navegadores de Internet 60
  - procesos ocultos 75
  - tráfico de red local 60
  - uso compartido de archivos e impresoras 61–62
- preautorizar elementos sospechosos 38
- prioridad de reglas 70
- prioridad, escaneo 20
- procesos ocultos, permitir 75
- programar escaneados programados 24
- programar la actualización 85
- programar un escaneo 99
- programas espía 13, 17, 22
  - limpieza automática 13, 17, 22
- programas espía en cuarentena, revisar 41
- programas publicitarios en cuarentena, revisar 42
- Protección activa de Sophos 33–34
  - activar 34
  - apagar 34
  - desactivar 34
  - descripción 33
  - encender 34
  - registro 34
  - tecnología en la nube 33
- protección contra manipulaciones 88–92
  - activar 89
  - apagar 89

- protección contra manipulaciones (*continuación*)
  - autenticación de usuario 90
  - cambiar contraseña 91
  - configurar el software 90
  - desactivar 89
  - descripción 88
  - desinstalar el software de seguridad de Sophos 91
  - desinstalar Sophos Endpoint Security and Control 91
  - encender 89
  - introducir contraseña 90
  - reactivar 90
  - registro 92
- protección web 35–36
  - bloqueo de sitios web maliciosos 35–36
  - configurar 36
  - descripción 35
  - escaneo de contenido 35–36
  - filtrado URL 35–36
  - reputación de descargas 35–36
- PUA (aplicaciones no deseadas) 10, 16–17, 20, 22, 37, 96, 98
  - autorización 37
  - detectar 10, 16, 20
  - limpieza automática 17, 22
- PUA autorizadas, bloquear 37

## R

- realizar un escaneo de botón derecho 19
- realizar un escaneo exhaustivo 25
- recuperación 98
- registro de actualización 87
- registro de un escaneo personalizado 25
  - visualizar 25
- registro del cortafuegos 81
  - configurar 81
- registro del escaneo 50–51
  - configurar 50
  - visualizar 51
- regla 72
  - configurar 72
- reglas globales 71, 73, 75
  - configurar 71, 73, 75
- reputación de descargas 35–36
- revisar aplicaciones no deseadas en cuarentena 42
- revisar archivos sospechosos en cuarentena 43
- revisar comportamientos sospechosos en cuarentena 44
- revisar programas espía en cuarentena 41
- revisar programas publicitarios en cuarentena 42
- revisar virus en cuarentena 41
- rootkits, detectar 20

## S

- sector de arranque infectado 10, 97
- servidor primario 85
- servidor proxy 86
- servidor secundario 86
- sistema de prevención contra intrusiones 31
- sistema lento, solución de problemas 96

- sitios web [38](#)
  - autorización [38](#)
- sitios web maliciosos [36](#)
  - protección [36](#)
- software de cifrado [10](#)
  - escaneado en acceso [10](#), [12](#), [14](#), [26](#)
- Sophos Endpoint Security and Control [5](#)
- sumas de verificación de archivos escaneados, eliminar [14](#)
- sumas de verificación, autenticación de aplicaciones [76](#)
- suspender escaneado [54](#)

## T

- tecnología en la nube [33](#)
- tipos de escaneado en demanda [15](#)
- todos los archivos, escaneado [10](#), [16](#), [20](#)
- tráfico de red local, permitir [60](#)

## U

- ubicaciones primarias [78](#)
  - definir [78](#)

- uso compartido de archivos e impresoras, permitir [61–62](#)
- uso compartido de archivos, bloquear [62](#)
- uso compartido de archivos, permitir [61–62](#)
- uso compartido de impresoras, bloquear [62](#)
- uso compartido de impresoras, permitir [61–62](#)

## V

- virus [13](#), [17](#), [22](#), [97](#)
  - limpieza automática [13](#), [17](#), [22](#)
  - recuperación [97](#)
- virus de Mac, detectar [10](#)
- virus en cuarentena, revisar [41](#)
- visor del registro [81](#)
  - acerca de [81](#)
- visualizador del registro del cortafuegos [84](#)
  - exportar entradas [84](#)
- visualizar [25](#), [51](#)
  - registro de un escaneado personalizado [25](#)
  - registro del escaneado [51](#)