

# SOPHOS

## Sophos Anti-Virus para Windows versión 7 manual de usuario

Para Windows 2000 o posterior

Edición: junio de 2007





# Contenido

1	Acerca de Sophos Anti-Virus.....	4
2	Comprobar que el equipo está protegido.....	9
3	Escaneado en demanda.....	11
4	Escanear un elemento.....	15
5	Restringir derechos de acceso.....	16
6	Modificar la configuración para múltiples usuarios.....	17
7	Configurar el escaneado.....	18
8	Configurar el análisis de comportamiento.....	27
9	Configurar alertas.....	28
10	Registro.....	32
11	Actualización.....	33
12	Limpieza.....	39
13	Revisar elementos en cuarentena.....	44
14	Autorizar el uso de elementos.....	54
15	Solución de problemas.....	56
	Index .....	65

# 1 Acerca de Sophos Anti-Virus

## Sophos Anti-Virus

Sophos Anti-Virus es un programa que detecta y se ocupa de:

- amenazas: virus, gusanos, troyanos, programas espía, archivos y comportamientos sospechosos, aplicaciones no deseadas y programas publicitarios
- aplicaciones restringidas

en equipos o redes. Concretamente permite:

- escanear equipos o redes en busca de amenazas y aplicaciones restringidas
- comprobar si los archivos a los que se accede son amenazas o aplicaciones restringidas
- recibir avisos cuando se encuentren amenazas o aplicaciones restringidas
- limpiar elementos afectados
- detener comportamientos sospechosos
- impedir la ejecución en el equipo de programas publicitarios y aplicaciones no deseadas
- eliminar programas publicitarios y aplicaciones no deseadas del equipo
- mantener un registro de su actividad
- actualizarse para detectar nuevas amenazas.

Sophos Anti-Virus puede instalarse en equipos con sistemas operativos Windows 2000 o posteriores.

Sophos Anti-Virus se integra con una consola de gestión, que permite administrar Sophos Anti-Virus de forma centralizada en redes.

Sophos Anti-Virus también se integra con Cisco® Network Admission Control (NAC), lo que permite incluir el estado de Sophos Anti-Virus al validar la política de admisión a la red. Para más información, consulte la ayuda de la consola de gestión y la Guía de

integración de *Sophos Anti-Virus con Cisco NAC*.

Sophos Anti-Virus puede utilizarse de dos formas:

- desde la ventana de Sophos Anti-Virus
- desde el icono de Sophos Anti-Virus.

Sophos Anti-Virus puede realizar:

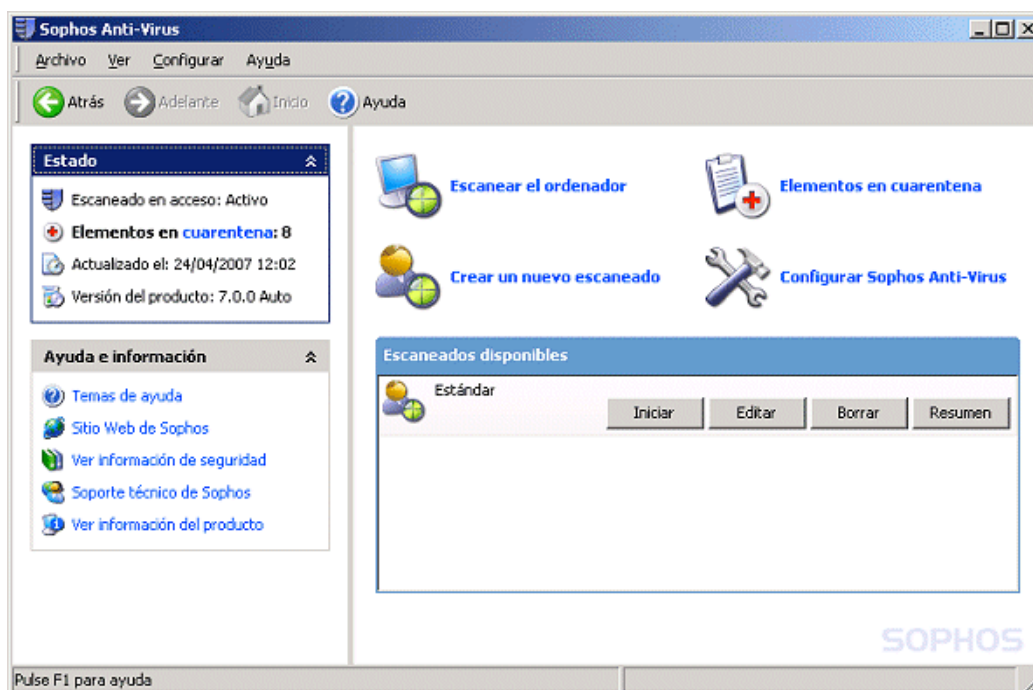
- escaneados en acceso
- escaneados en demanda
- escaneados de botón derecho
- análisis de comportamiento en tiempo de ejecución.

## La ventana de Sophos Anti-Virus

Para abrir la ventana de **Sophos Anti-Virus**, haga clic con el botón derecho del ratón en el icono de Sophos Anti-Virus en la bandeja del sistema.



Seleccione **Abrir Sophos Anti-Virus**. A continuación se describen los componentes de la ventana principal.



## Barra de herramientas

Contiene botones de ayuda y de navegación entre las páginas en el panel de la derecha de la ventana de Sophos Anti-Virus.

## Barra de estado

Incluye información sobre el escaneado en acceso, el número de elementos en cuarentena, la última actualización de Sophos Anti-Virus y las versiones del producto.

## Ayuda e información

Información de contacto con soporte técnico de Sophos, acceso a la ayuda de Sophos Anti-Virus e información sobre amenazas y aplicaciones restringidas. Para información más detallada sobre la versión de Sophos Anti-Virus y su sistema, haga clic en **Ver información del producto**.

## Resumen de actividad

Aparecerá cuando realice algún escaneado, y mostrará información sobre elementos detectados.

## Página de inicio

Se muestra en el panel de la derecha al abrir la ventana de **Sophos Anti-Virus**. Incluye la lista de tareas y la lista de **Escaneados disponibles**. Al utilizar la ventana de **Sophos Anti-Virus**, el contenido del panel de la derecha cambiará en consonancia. Puede volver a la página inicial haciendo clic en el botón **Inicio**.

La lista de tareas se mostrará en la parte superior de la página de inicio, desde donde podrá:

- escanear su ordenador
- configurar el escaneado
- acceder al área de cuarentena
- configurar Sophos Anti-Virus.

La lista de **Escaneados disponibles** muestra los escaneados configurados. Desde aquí, podrá editar o borrar escaneados, y ver un resumen de la última vez que se utilizó cada escaneado.

## El icono de Sophos Anti-Virus

El icono de Sophos Anti-Virus aparecerá en la bandeja de tareas del sistema incluso si se cierra la ventana de **Sophos Anti-Virus**.

Al situar el puntero del ratón sobre el icono, se mostrará la fecha de la última actualización de Sophos Anti-Virus.

Si hace clic con el botón derecho del ratón sobre el icono, se mostrará un menú desde el que podrá:







- actualizar Sophos Anti-Virus
- configurar la actualización
- comprobar la evolución de la actualización
- abrir la ventana de **Sophos Anti-Virus**.



Para configurar las actualizaciones, es necesario pertenecer al grupo de administradores de Sophos.


El icono tendrá un aspecto diferente según el escaneado en acceso esté activo o no, si Sophos Anti-Virus se está actualizando o si la última

actualización de Sophos Anti-Virus se completó con éxito.

Icono	Significado
	Un escudo azul indica que el escaneo en acceso se encuentra activo. Sophos Anti-Virus se actualizó correctamente.
	Si en el escudo azul aparecen unas bandas verdes animadas, Sophos Anti-Virus se encuentra en proceso de actualización. El escaneo en acceso se encuentra activo.
	Si aparece una cruz roja sobre el escudo azul, la actualización ha fallado. El escaneo en acceso se encuentra activo.
	Un escudo gris indica que el escaneo en acceso se encuentra inactivo. Sophos Anti-Virus se actualizó correctamente.
	Si en el escudo gris aparecen unas bandas verdes animadas, Sophos Anti-Virus se encuentra en proceso de actualización. El escaneo en acceso se encuentra inactivo.
	Si aparece una cruz roja sobre el escudo gris, la actualización ha fallado. El escaneo en acceso se encuentra inactivo.


Para saber qué hacer si el escudo muestra una cruz roja o si el escudo es de color gris, vea la sección [El icono de Sophos en la bandeja del sistema tiene una cruz roja](#) o [El icono de Sophos en la bandeja del sistema aparece gris](#) respectivamente.

## El escaneo en acceso

 El escaneo en acceso intercepta cada archivo que se intenta utilizar en el sistema, permitiendo su acceso sólo si no resulta una amenaza o está permitido su uso.


Para más información sobre el escaneo en acceso, vea las secciones *Comprobar que el equipo está protegido* y *Configurar el escaneo*.

## El escaneado en demanda

 El **escaneado en demanda** es el escaneado que inicia el usuario en un momento dado, de forma manual o programada.


Para más información sobre el escaneado en demanda, vea las secciones *Escaneado en demanda* y *Configurar el escaneado*.

## El escaneado de botón derecho

 El **escaneado de botón derecho** es el escaneado de los elementos seleccionados desde Explorador de Windows o en el escritorio, que se inicia haciendo clic con el botón derecho del ratón y seleccionando **Escanear con Sophos Anti-Virus**.

Para más información sobre el escaneado de botón derecho, vea las secciones Escanear un elemento y *Configurar el escaneado*.

## ¿Qué es el análisis de comportamiento?


 El **análisis de comportamiento** comprende la detección de comportamientos sospechosos y la detección del desbordamiento del búfer. La detección de comportamientos sospechosos consiste en el análisis dinámico de todos los programas en ejecución en el equipo para detectar y bloquear actividades que parezcan maliciosas.

Para más información sobre el análisis de comportamiento, vea la sección Detectar comportamientos sospechosos y desbordamientos del búfer.

# 2 Comprobar que el equipo está protegido

## Comprobar que la protección está activa


El equipo debe estar protegido de forma permanente por el escaneado en acceso.

 El escaneo en acceso intercepta cada archivo que se intenta utilizar en el sistema, permitiendo su acceso sólo si no resulta una amenaza o está permitido su uso.

Cuando el escaneo en acceso se encuentra activo, el icono de Sophos en la bandeja del sistema se mostrará azul.




Cuando el escaneo en acceso se encuentra inactivo, el icono de Sophos en la bandeja del sistema se mostrará gris.

 El estado del escaneo en acceso también se muestra en la ventana de **Sophos Anti-Virus** en el panel **Estado**.

Si su equipo se encuentra en red, seguramente el escaneo en acceso ya ha sido configurado. Si desea comprobar o modificar la configuración, vea la sección *Configurar el escaneo*.

## Activar/desactivar la protección para un equipo

 Si *desactiva* la protección, Sophos Anti-Virus *no* escaneará los archivos que utiliza.


 Para activar o desactivar la protección de un equipo, es necesario pertenecer al grupo de administradores de Sophos.


1. En el menú **Configurar**, seleccione **Escaneo en acceso**.
2. En el cuadro de diálogo **Configuración del escaneo en acceso para este equipo**, abra la ficha **Escaneo**.

Para *activar* el escaneo en acceso en el equipo, active la opción **Activar el escaneo en acceso en este equipo** y haga clic en **Aplicar**. El icono de Sophos Anti-Virus en la bandeja del sistema se volverá azul.

Para *desactivar* el escaneo en acceso en el equipo, desactive la opción **Activar el escaneo en acceso en este equipo** y haga clic en **Aplicar**. El icono de Sophos Anti-Virus en la bandeja del sistema se volverá gris.


En la ventana de **Sophos Anti-Virus**, se actualizará el panel **Estado**.

 Sophos Anti-Virus mantendrá la configuración incluso tras reiniciar el equipo. Si desactiva el escaneo en acceso, seguirá *inactivo* hasta que lo active de nuevo.

 Podrá realizar escaneados en demanda incluso cuando tenga la protección en acceso desactivada.

## 3 Escaneo en demanda

### Escaneo en demanda

 El **escaneo en demanda** es el escaneo que inicia el usuario en un momento dado, de forma manual o programada.

### Escanear el ordenador


Para realizar un escaneo de los discos duros del equipo, incluyendo sectores de arranque, haga lo siguiente.

En la página de inicio de la ventana de **Sophos Anti-Virus**, haga clic en **Escanear el ordenador**.

Se abrirá un cuadro de diálogo con una barra de evolución y, en la ventana de **Sophos Anti-Virus** se mostrará el panel **Resumen de actividad**.

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

Para detener el escaneo, haga clic en el botón **Detener**.

 Cuando ejecuta **Escanear el ordenador** no se escanearán archivos Macintosh guardados en estaciones Windows. Si desea escanear con Sophos Anti-Virus archivos ejecutables de Macintosh, debe crear un escaneo en demanda en el que activar el escaneo de archivos Macintosh.

Para más información sobre la creación, programación, ejecución y configuración de un escaneo, vea el resto de apartados en esta sección y también la sección *Configurar el escaneo*.

## Crear un escaneado

1. En el menú **Archivo**, haga clic en **Nuevo escaneado** para ver la página de configuración de escaneados.
2. En el cuadro de texto **Nombre el escaneado**, indique un nombre descriptivo para el nuevo escaneado.
3. 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 en las casillas de activación, vea la [Representación de los elementos a escanear](#).



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.

4. Haga clic en **Configurar el escaneado** para ver más opciones (vea la sección [Configurar el escaneado](#) para más información).
5. Para disponer de escaneado programado, haga clic en **Programar el escaneado** (vea [Programar el escaneado](#) para más información).



No es posible ejecutar de forma manual un escaneado programado. Los escaneados programados aparecerán en la lista de **Escaneados disponibles** con un reloj.

6. Haga clic en el botón **Guardar** para guardar el escaneado, o en **Guardar e iniciar** para guardar y ejecutar el escaneado.

## Programar un escaneado



Necesitará pertenecer al grupo de administradores para programar un escaneado o para ver o modificar uno existente creado por otro usuario.

Para programar un escaneado que está creando o editando, haga lo siguiente.



No es posible ejecutar de forma manual un escaneo programado. Los escaneados programados aparecerán en la lista de **Escaneados disponibles** con un reloj.

1. En la ventana de **Sophos Anti-Virus**, haga clic en **Programar el escaneo**.
2. 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.

3. 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.

## Iniciar un escaneo

Para iniciar un escaneo que ha creado, haga lo siguiente.

En la [página de inicio](#) de la ventana de **Sophos Anti-Virus**, en la lista de **Escaneados disponibles**, seleccione el escaneo que desee iniciar. Haga clic en el botón **Iniciar**.



No es posible ejecutar de forma manual un escaneo programado. Los escaneados programados aparecerán en la lista de **Escaneados disponibles** con un reloj.

Se abrirá un cuadro de diálogo con una barra de evolución y, en la ventana de **Sophos Anti-Virus** se mostrará el panel **Resumen de actividad**.

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

Para detener el escaneo, haga clic en el botón **Detener**.

Para más información sobre la creación, programación y configuración de un escaneado, vea el resto de apartados en esta sección y también la sección *Configurar el escaneado*.

## Editar un escaneado

Para editar un escaneado que ha creado, haga lo siguiente.

1. En la página de inicio de la ventana de **Sophos Anti-Virus**, en la lista de **Escaneados disponibles**, seleccione el escaneado que desee editar. Haga clic en el botón **Editar**.
2. Para cambiar el nombre del escaneado, indique el nuevo nombre en el cuadro de texto **Nombre del escaneado**.
3. 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 elementos a escanear.



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.

4. Haga clic en **Configurar el escaneado** para ver más opciones (vea *Configurar el escaneado* para más información).
5. Para disponer de escaneado programado, haga clic en **Programar el escaneado** (vea Programar el escaneado para más información).



No es posible ejecutar de forma manual un escaneado programado. Los escaneados programados aparecerán en la lista de **Escaneados disponibles** con un reloj.

6. Haga clic en el botón **Guardar** para guardar el escaneado, o en **Guardar e iniciar** para guardar y ejecutar el escaneado.

Para borrar un escaneado, en la página de inicio de la ventana de **Sophos Anti-Virus**, en la lista de **Escaneados disponibles**, seleccione el escaneado correspondiente. Haga clic en **Borrar** y, a continuación,

haga clic en Sí para confirmar la eliminación.

## Representación de los elementos a escanear


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

Icono	Significado
<input type="checkbox"/>	El elemento y subelementos <i>no están</i> seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento y subelementos <i>están</i> seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento está seleccionado parcialmente, es decir, algunos subelementos están seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento y subelementos están excluidos en este escaneado.
<input checked="" type="checkbox"/>	El elemento está excluido parcialmente, es decir, algunos subelementos están excluidos en este escaneado.
<input checked="" type="checkbox"/>	El elemento y subelementos están excluidos en todos los escaneados en demanda al existir una <u>exclusión</u> general en demanda.

## 4 Escanear un elemento

### Escanear un elemento

Puede escanear un elemento mediante el escaneado de botón derecho.

 El **escaneado de botón derecho** es el escaneado de los elementos seleccionados desde Explorador de Windows o en el escritorio, que se inicia haciendo clic con el botón derecho del ratón y seleccionando **Escanear con Sophos Anti-Virus**.

1. Abra el Explorador de Windows. Seleccione **Inicio|Programas|Accesorios|Explorador de Windows**.
2. Seleccione los archivos, carpetas y/o unidades a escanear.
3. Haga clic con el botón derecho del ratón sobre la selección y seleccione **Escanear con Sophos Anti-Virus** en el menú contextual.

Se abrirá un cuadro de diálogo con la barra de evolución del escaneado.

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

Para detener el escaneado, haga clic en el botón **Detener**.

Para más información sobre las opciones de escaneado, vea *Configurar el escaneado*.

## 5 Restringir derechos de acceso

### Tipos de usuario

Sophos Anti-Virus restringe el acceso a diferentes partes del programa según el tipo de usuario. El sistema de seguridad se basa en la política de grupos de usuarios creados en Windows en el equipo. Al instalar Sophos Anti-Virus, cada usuario será asignado a los grupos de Sophos basándose en el grupo de Windows al que pertenezca, de la siguiente manera:

- Miembros del grupo de administradores de Windows serán incluidos en el grupo SophosAdministrator.
- Miembros del grupo de usuarios avanzados de Windows serán incluidos en el grupo SophosPowerUser.
- Miembros del grupo de usuarios de Windows serán incluidos en el grupo SophosUser.

Cualquier usuario que no tenga asignado un grupo de Sophos, incluyendo el grupo de invitados, sólo dispondrá de:

- escaneado en acceso
- escaneado de botón derecho.

Miembros del grupo SophosUser dispondrán de estas funciones además de:

- acceso a la ventana de Sophos Anti-Virus
- configuración y ejecución de escaneados en demanda
- configuración del escaneado de botón derecho
- gestión, con derechos limitados, del área de cuarentena.

Los miembros del grupo SophosPowerUser tienen los mismos derechos que los del grupo SophosUser, más derecho total sobre el Área de cuarentena y el Gestor de autorización.

Miembros del grupo SophosAdministrator pueden utilizar o configurar cualquier parte de Sophos Anti-Virus.

## Modificar los miembros de los grupos de Sophos

Para cambiar el grupo de Sophos al que pertenece un usuario, haga lo siguiente (vea la documentación de Windows si es necesario).

1. Utilice las herramientas de Windows para mover usuarios de un grupo de Sophos a otro.
2. Cuando el usuario inicie la sesión de nuevo, los derechos de acceso se actualizarán.

# 6 Modificar la configuración para múltiples usuarios

## Modificar la configuración para todos los ordenadores

Para configurar Sophos Anti-Virus en una red desde una ubicación

central, consulte la Ayuda de la consola de gestión.

## **Modificar la configuración para todos los usuarios del ordenador**

Para configurar Sophos Anti-Virus para todos los usuarios del ordenador, utilice el menú **Configurar**. Desde ese menú, puede configurar las opciones siguientes.

- el escaneado en acceso
- las extensiones y exclusiones en demanda
- el análisis de comportamiento
- Restricción de aplicaciones
- Derechos sobre el área de cuarentena
- Lista de programas publicitarios, aplicaciones no deseadas y elementos sospechosos
- las notificaciones
- Registro
- la actualización

Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.

## **7 Configurar el escaneado**

### **Abrir el cuadro de diálogo de opciones de escaneado**

Las opciones para cada tipo de escaneado aparecen en tres cuadros de diálogo diferentes.


Para abrir el cuadro de diálogo de las opciones de *escaneado en acceso*, en el menú **Configurar**, haga clic en **Escaneado en acceso**.

Para abrir el cuadro de diálogo de las opciones de *escaneado en*

**demanda**, en la página de inicio de la ventana de Sophos Anti-Virus, en la lista **Escaneados disponibles**, seleccione el escaneado que desea modificar. Haga clic en el botón **Editar**. En la página del escaneado, haga clic en **Configurar el escaneado**.

Para abrir el cuadro de diálogo de las opciones de *escaneado con el botón derecho*, en el menú **Configurar**, haga clic en **Escaneado con el botón derecho**.

## Tipos de archivo a escanear

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.


1. Para cambiar la configuración del *escaneado en acceso*, en el menú **Configurar**, seleccione **Escaneado en acceso**.

Para cambiar la configuración del *escaneado en demanda* y del *escaneado con el botón derecho*, en el menú **Configurar**, seleccione **Extensiones y exclusiones en demanda**.

2. Abra la ficha **Extensiones**. Las opciones disponibles se describen a continuación.


### Escanear todos los archivos

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

 Sophos no recomienda el uso de esta opción a menos que así se le indique desde Soporte técnico de Sophos. Escanear **todos los archivos** hará el escaneado más lento y es normalmente innecesario.

### 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).

 La lista de extensiones incluye los tipos de archivo que Sophos 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**.

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

## Excluir elementos del escaneado



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.



El procedimiento descrito a continuación se aplica a *todos* los escaneados en demanda. Para excluir elementos de un escaneado en demanda *particular*, vea la sección [Editar un escaneado](#).

1. Para cambiar la configuración del *escaneado en acceso*, en el menú **Configurar**, seleccione **Escanear en acceso**.

Para cambiar la configuración del *escaneado en demanda* y del *escaneado con el botón derecho*, en el menú **Configurar**, seleccione **Extensiones y exclusiones en demanda**.

2. Abra la ficha **Exclusiones**. Las opciones disponibles se describen a continuación.

### Elementos excluidos

Para añadir un elemento a la lista de elementos excluidos, haga clic en **Añadir**. En el cuadro de diálogo **Exclusión de elementos**, indique el tipo y nombre del elemento a excluir. Vea la sección *Especificar elementos a excluir*.

Para borrar un elemento de la lista de exclusiones, selecciónelo y

haga clic en **Eliminar**.

Para modificar un elemento de la lista de exclusiones, selecciónelo y haga clic en **Editar**.

## Especificar elementos a excluir

En el cuadro de diálogo **Exclusión de elementos**, seleccione el tipo de elemento en la lista desplegable **Elemento**. **Todos los archivos remotos** hace referencia a todos los archivos que no se hallan en este ordenador. A menos que seleccione **Todos los archivos remotos**, determine el nombre del elemento en **Nombre** utilizando el botón **Examinar** o introduciendo el nombre en el cuadro de texto.



Si utiliza un sistema de 64-bit, el botón **Examinar** no estará visible en el cuadro de diálogo **Exclusión de elementos**.

A continuación se ofrecen más detalles sobre el modo de selección.

- **Nombre**

Puede especificar el nombre del archivo para que Sophos Anti-Virus excluya cualquier tipo de archivo con dicho nombre. Por ejemplo:

fred.bmp

hará que Sophos Anti-Virus excluya dicho archivo en cualquier ubicación.

- **Ruta completa**

También puede indicar la ubicación y el nombre del archivo para que Sophos Anti-Virus excluya ese archivo específico. La ruta de acceso puede incluir la unidad local o compartida. Por ejemplo:

C:\Miscelaneo\fred.bmp

hará que Sophos Anti-Virus excluya fred.bmp en la carpeta Miscelaneo de la unidad C.

\\Servidor1\usuarios\Fred\Carta.rtf

hará que Sophos Anti-Virus excluya Carta.rtf en la carpeta Fred de la unidad compartida Usuarios en el servidor Servidor1.

Si no indica la unidad, local o compartida, Sophos Anti-Virus excluirá el archivo en cualquier unidad que incluya la ruta de

acceso especificada.

- **Ruta parcial**

Puede especificar la unidad local o compartida para que Sophos Anti-Virus la excluya del escaneo. Por ejemplo:

A:

hace que Sophos Anti-Virus excluya cualquier disquete en la unidad A.

Puede especificar una carpeta para que Sophos Anti-Virus excluya su contenido, incluyendo subcarpetas. Por ejemplo:

D:\Herramientas\

hará que Sophos Anti-Virus excluya el contenido de la carpeta Herramientas, y subcarpetas, en la unidad D.

Puede especificar una carpeta y archivo para que Sophos Anti-Virus excluya dicho archivo en carpetas con ese nombre. Por ejemplo:

logs\log.txt

hace que Sophos Anti-Virus excluya el archivo log.txt en carpetas con el nombre logs, cualquiera que sea la unidad local o compartida.

## **Caracteres comodín**

El carácter comodín ? sólo puede utilizarse en el nombre del archivo o extensión y sustituye a cualquier carácter. Sin embargo, al utilizarse al final de un nombre de archivo o extensión, puede sustituir a uno o ningún carácter. Por ejemplo, archivo?.txt incluiría archivo.txt, archivo1.txt y archivo12.txt, pero no archivo123.txt.

El carácter comodín \* sólo puede utilizarse en el nombre del archivo o extensión, en la forma [archivo].\* o \*. [extensión]. Por ejemplo, no serían válidos archivo\*.txt, archivo.txt\* o archivo.\*txt.

## **Archivos con múltiples extensiones**

Archivos con múltiples extensiones serán tratados como si la última extensión es la extensión y el resto es el nombre del archivo. Por ejemplo,

[archivo].[extensión1].[extensión2] se interpretará como [archivo].[extensión1] para el nombre del archivo y [extensión2] para la extensión.

### Nomenclatura estándar

Los nombres de carpetas y archivos serán validados según la nomenclatura estándar (por ejemplo, el nombre de una carpeta puede contener espacios, pero no sólo espacios).

## Especificar cuándo ocurre el escaneo en acceso



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.

Puede especificar que Sophos Anti-Virus escanee los archivos cuando se abren, cuando se guardan o cuando cambian de nombre.

1. En el menú **Configurar**, seleccione **Escaneo en acceso**.
2. En el cuadro de diálogo **Configuración del escaneo en acceso para este equipo**, abra la ficha **Escaneo**. Las opciones disponibles se describen a continuación.

Active la opción **Leer** si desea que se comprueben los archivos al abrirse. Esta es la opción recomendada.


Active la opción **Escribir** si desea que se comprueben los archivos al guardarse.

Active la opción **Cambiar nombre** si desea que se comprueben los archivos cuando cambien de nombre.

## Detectar archivos sospechosos




Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.


 Un **archivo sospechoso** es un archivo que puede estar infectado con un virus para el que no existe identidad específica.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneado que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneado](#)).
2. En el cuadro de diálogo de opciones de escaneado, abra la ficha **Limpieza**.
3. Seleccione **Detectar archivos sospechosos (HIPS)**.


## Detectar programas publicitarios y aplicaciones no deseadas


 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneado que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneado](#)).
2. En el cuadro de diálogo de opciones de escaneado, abra la ficha **Limpieza**.
3. Seleccione **Detectar adware/PUA**.

 Sólo debería utilizar las opciones avanzadas con el asesoramiento de soporte técnico de Sophos.

## Detectar aplicaciones restringidas

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

 Una **aplicación restringida** es una aplicación legítima que puede afectar a la productividad y al rendimiento de la red.

El escaneado en acceso para aplicaciones restringidas puede impedir la desinstalación de ciertas aplicaciones cuando está activada. Si lo

desea, puede desactivarlo de la forma siguiente.



Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.

1. En el menú **Configurar**, seleccione **Restricción de aplicaciones**.
2. En el cuadro de diálogo **Restricción de aplicaciones**, desactive la opción **Detectar el acceso a aplicaciones restringidas no autorizadas**.
3. Cuando haya desinstalado la aplicación, vuelva a activar la opción **Detectar el acceso a aplicaciones restringidas no autorizadas**.

## Escanear archivos comprimidos



El escaneo de archivos comprimidos, dependiendo del tamaño, puede hacer el escaneo bastante más lento y normalmente no es necesario. Incluso si no activa esta opción, el contenido del archivo será escaneado cuando se extraiga. Sophos no recomienda el uso generalizado de esta opción.

Archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) serán siempre escaneados aunque no active esta opción.


1. Abra el cuadro de diálogo de las opciones del tipo de escaneo que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneo](#)).
2. En el cuadro de diálogo de opciones de escaneo, abra la ficha **Limpieza**.
3. Active la opción **Escanear dentro de archivos comprimidos**.

Para especificar el escaneo dentro de ciertos archivos comprimidos, haga clic en **Avanzadas**. En el cuadro de diálogo **Opciones avanzadas de escaneo**, seleccione los tipos de archivos comprimidos que desea escanear con Sophos Anti-Virus.



Sólo debería utilizar las opciones avanzadas con el asesoramiento de soporte técnico de Sophos.


## Escanear archivos de Macintosh

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.


Puede configurar Sophos Anti-Virus para escanear archivos de Macintosh almacenados en equipos Windows.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneo que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneo](#)).
2. En el cuadro de diálogo de opciones de escaneo, abra la ficha **Limpieza**.
3. Active la opción **Detectar virus de Macintosh**. para que Sophos Anti-Virus compruebe archivos ejecutables de Macintosh.

## Escanear el contenido completo de archivos

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.

Para detectar algunos virus, es necesario activar el escaneo del contenido completo de los archivos.

 Sophos no recomienda el uso de esta opción a menos que así se le indique desde Soporte técnico de Sophos.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneo que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneo](#)).
2. En el cuadro de diálogo de opciones de escaneo, abra la ficha **Limpieza**.
3. En el panel **Nivel de escaneo**, seleccione **Exhaustivo**.
4. Una vez que haya limpiado los virus, haga clic en **Normal**.

# 8 Configurar el análisis de comportamiento

## Detectar comportamientos sospechosos y desbordamientos del búfer



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.



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

Si desea cambiar las opciones de detección de comportamientos sospechosos y desbordamientos del búfer, haga lo siguiente.



Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.


1. En el menú **Configurar**, haga clic en **Análisis de comportamiento (HIPS)** para abrir el cuadro de diálogo **Análisis de comportamiento (HIPS)**.
2. Para activar o desactivar la detección de comportamientos sospechosos, active o desactive la opción **Detectar comportamiento sospechoso**.

Para activar o desactivar la detección de desbordamientos del búfer, active o desactive la opción **Detectar desbordamientos del búfer**.



La función de detección de desbordamientos del búfer no está disponible para Windows Vista o versiones de 64 bits de Windows. Dichos sistemas operativos cuentan con protección contra los desbordamientos del búfer gracias a la función de prevención de ejecución de datos (DEP) de Microsoft.


3. Si utiliza una instalación nueva de Sophos Anti-Virus, por defecto, los comportamientos sospechosos y los desbordamientos del búfer se *detectan* pero no se *bloquean*. Si utiliza una actualización, por defecto, los comportamientos sospechosos y los desbordamientos del búfer no se detectan.

 Sophos recomienda ejecutar Sophos Anti-Virus en modo de sólo detección por un tiempo y autorizar los programas que necesite antes de activar el bloqueo automático de comportamientos sospechosos y desbordamientos del búfer. De esta manera, se evita el bloqueo de programas que los usuarios puedan necesitar.

Para activar el *bloqueo* de comportamientos sospechosos y desbordamientos del búfer, además de la *detección*, desactive la casilla **Sólo alertar**.

## 9 Configurar alertas

### Mensajes de escritorio

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.

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. En el menú **Configurar**, seleccione **Notificación**.
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 definido por el usuario

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

## Notificación por email

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.

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

### Activar alerta por email

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

### Notificar

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

### 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 (vea la sección *Configurar correo SMTP*).

## Configurar correo SMTP

### Servidor SMTP

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

### Dirección remitente

Indique la dirección de email a la que llegarán mensajes devueltos o rechazados.

### Dirección de respuesta

Indique la dirección a la que se enviarán las respuestas que el mensaje de alerta pueda generar.

### Idioma

Seleccione en la lista desplegable el idioma en el que desea enviar las alertas.

## Mensaje SNMP



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la ayuda de la consola.

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. En el menú **Configurar**, seleccione **Notificación**.
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 escaneado** incluye ocasiones en que Sophos Anti-Virus no tiene acceso a algún elemento.

### 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.

## Registro de eventos

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

1. En el menú **Configurar**, seleccione **Notificación**.
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.

## 10 Registro


### Ver el registro del equipo

 El registro del equipo recoge información sobre la actividad de todos los escaneados en el equipo.

1. En la página de inicio de la ventana de Sophos Anti-Virus, haga clic en **Configurar Sophos Anti-Virus**.
2. En la página **Configuración**, haga clic en **Ver registro**.
3. 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.

### Configurar el registro del equipo

 El registro del equipo recoge información sobre la actividad de todos los escaneados en el equipo.

La ubicación del archivo de registro es:

C:\Documents and Settings\All Users\Datos de programa\Sophos  
\Sophos Anti-Virus\logs\SAV.txt

1. En el menú **Configurar**, seleccione **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.


## Ver el registro de un escaneado en demanda

 El registro de un escaneado en demanda es un registro de lo ocurrido en la última ejecución del escaneado.

1. En la página de inicio de la ventana de **Sophos Anti-Virus**, en la lista de **Escaneados disponibles**, seleccione el escaneado del que desee ver el registro. Haga clic en el botón **Resumen**.
2. En el cuadro de diálogo de resumen, haga clic en el enlace de la parte inferior.
3. Desde la ventana del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

# 11 Actualización

## Realizar una actualización inmediata


 Si ha realizado la instalación recomendada de Sophos Anti-Virus según se indica en la documentación, la actualización se realizará de forma automática.

Si desea realizar una actualización manual.

1. Haga clic con el botón derecho del ratón en el icono de Sophos

Anti-Virus en la bandeja del sistema. 

2. Seleccione **Actualizar ahora**.

 También puede hacer doble clic en el icono de Sophos Anti-Virus.

Si Sophos Anti-Virus está configurado correctamente, la actualización

se realizará en seguida.

Para más información sobre la actualización, vea los otros apartados en esta sección.


## Configurar la actualización automática

Si su equipo está en red, o si su administrador instaló Sophos Anti-Virus, Sophos Anti-Virus debe estar configurado para actualizarse de forma automática.

Si desea configurar la actualización automática o modificar la configuración existente, siga estos pasos. Para más información sobre cada opción, vea el apartado correspondiente.




Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.

1. Haga clic con el botón derecho del ratón en el icono de Sophos Anti-Virus en la barra de tareas. 
2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Servidor primario** e indique la fuentes de actualización. El administrador de su red dispondrá de la información necesaria.
4. Abra la ficha **Programado** y configure la actualización automática.

## Configurar la fuente de actualización

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

1. Haga clic con el botón derecho del ratón en el icono de Sophos Anti-Virus en la barra de tareas. 
2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.

3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Servidor primario** e introduzca la siguiente información necesaria.

### Dirección

Introduzca la dirección (web o ruta de acceso UNC) desde la que Sophos Anti-Virus realizará las descargas. Si selecciona **Sophos**, las descargas se realizarán directamente desde la web de Sophos a través de Internet.



El administrador de su red le proporcionará los datos necesarios.

### Nombre de usuario

Si es necesario, introduzca el **Nombre de usuario** y la **Contraseña** de la cuenta de acceso.



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

Si desea limitar el ancho de banda utilizado, haga clic en **Avanzadas**.

Si el acceso va a ser a través de un servidor proxy, haga clic en **Aplicar** y, a continuación, en **Detalles del proxy**. Algunos proveedores de acceso a Internet utilizan servidores proxy.

## Configurar la fuente alternativa de actualización

Es posible configurar una fuente alternativa de actualización. Si Sophos Anti-Virus no puede contactar con el servidor primario, lo intentará con el secundario.

1. Haga clic con el botón derecho del ratón en el icono de Sophos



Anti-Virus en la barra de tareas.

2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Servidor secundario**. Introduzca la siguiente

información necesaria.

### Dirección

Introduzca la **Dirección** (web o ruta de acceso UNC) desde la que Sophos Anti-Virus realizará las descargas si no puede contactar con el servidor primario. Si selecciona **Sophos**, las descargas se realizarán directamente desde la web de Sophos a través de Internet.



El administrador de su red le proporcionará los datos necesarios.

### Nombre de usuario

Si es necesario, introduzca el **Nombre de usuario** y la **Contraseña** de la cuenta de acceso.



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

Si desea limitar el ancho de banda utilizado, haga clic en **Avanzadas**.

Si el acceso va a ser a través de un servidor proxy, haga clic en **Aplicar** y, a continuación, en **Detalles del proxy**. Algunos proveedores de acceso a Internet utilizan servidores proxy.

## Programar la actualización

Puede especificar la frecuencia de actualización de Sophos Anti-Virus.



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

1. Haga clic con el botón derecho del ratón en el icono de Sophos

Anti-Virus en la barra de tareas.



2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**,

abra la ficha **Programado**. Introduzca la siguiente información necesaria.

Si desea que Sophos Anti-Virus se actualice a intervalos regulares, seleccione la opción **Activar actualización automática**. Especifique la frecuencia (en minutos) con la que Sophos Anti-Virus comprobará si existe alguna actualización. Por defecto será cada 60 minutos.




Si selecciona Sophos como fuente de actualización, la frecuencia máxima será 60 minutos.

Si utiliza conexión telefónica a redes, active la opción **Utilizar conexión telefónica**. Sophos Anti-Virus comprobará si existe alguna actualización cada vez que se conecte a Internet.

## Realizar la actualización vía proxy

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


1. Haga clic con el botón derecho del ratón en el icono de Sophos

Anti-Virus en la barra de tareas. 

2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Servidor primario** o **Servidor secundario**. Compruebe que los datos en esta página son correctos. Haga clic en **Aplicar** y, a continuación, haga clic en **Detalles del proxy**.
4. En el cuadro de diálogo **Detalles del proxy**, seleccione **Usar servidor proxy**. Especifique la **Dirección** y **Puerto** a utilizar. 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.


## Limitar el ancho de banda

El posible limitar el ancho de banda utilizado por Sophos Anti-Virus, de manera que no interfiera con otras aplicaciones.

1. Haga clic con el botón derecho del ratón en el icono de Sophos Anti-Virus en la barra de tareas. 
2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Servidor primario** o **Servidor secundario**. Haga clic en el botón **Avanzadas**.
4. En el cuadro de diálogo **Configuración avanzada**, active la opción **Limitar el ancho de banda** y utilice el selector para especificar el ancho de banda en Kbits/segundo. Si el ancho de banda es mayor del que dispone el equipo, Sophos Anti-Virus utilizará el máximo disponible.

## Registro de actualización

Puede configurar Sophos Anti-Virus para registrar la actividad de actualización en un archivo de registro.

1. Haga clic con el botón derecho del ratón en el icono de Sophos Anti-Virus en la barra de tareas. 
2. Haga clic con el botón derecho para mostrar un menú y seleccione **Configurar actualización**.
3. En el cuadro de diálogo **Propiedades de Sophos AutoUpdate**, abra la ficha **Registro**. Active la opción **Registrar la actividad de Sophos AutoUpdate**. Las otras opciones disponibles se describen a continuación. Si desea ver el registro, haga clic en **Ver registro**.

### Tamaño máximo


Especifique el tamaño máximo en MB.

### Nivel del informe

Puede seleccionar **Normal** o **Detallado**. El registro detallado ofrece más información y las acciones están más detalladas. Utilice la segunda opción si existen problemas.

## 12 Limpieza

### El proceso de limpieza

 El proceso de limpieza permite eliminar amenazas en su ordenador. En concreto, elimina virus de archivos o sectores de arranque, mueve o elimina archivos sospechosos, o elimina elementos de programas publicitarios o aplicaciones no deseadas. Sin embargo, no es posible deshacer el daño que la amenaza haya podido causar.

### Obtener instrucciones 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. Podrá acceder a las descripciones

- desde el propio mensaje de alerta (escaneado en acceso)
- desde el cuadro de diálogo del escaneado (escaneados en demanda 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 en demanda 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

Abra el área de cuarentena. En la página de inicio de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.

En la columna **Nombre del elemento**, 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.

## Configurar la limpieza automática de virus y programas espía



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

Sophos Anti-Virus puede proteger su sistema con diferentes acciones automáticas durante el escaneado en acceso, en demanda o desde el escaneado de botón derecho:

- limpiar elementos infectados
- evitar la ejecución o acceso a elementos infectados.



La limpieza automática de infecciones múltiples no está disponible para el escaneado en acceso. Para limpiar infecciones múltiples, utilice el Área de cuarentena.

Las acciones que Sophos Anti-Virus realice quedarán anotadas en el registro del equipo o en el registro del escaneado en demanda.

Para limpiar completamente algunas infecciones múltiples, será

necesario que reinicie el equipo. En este caso, tendrá la opción de reiniciar el sistema de forma inmediata o más tarde. El proceso de limpieza continuará cuando reinicie el sistema.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneado que desea configurar (vea la sección [Abrir el cuadro de diálogo de opciones de escaneado](#)).
2. En el cuadro de diálogo de opciones de escaneado, abra la ficha **Limpieza**. Las opciones disponibles se describen a continuación.
  - § Seleccione **Limpiar automáticamente elementos con virus/spyware** para que Sophos Anti-Virus pueda desinfectar sectores de arranque de disquetes, documentos, programas y demás elementos seleccionados para escanear. La limpieza de documentos no puede deshacer los efectos secundarios que el virus haya podido causar. Vea cómo [Obtener instrucciones de limpieza](#) desde la web de Sophos para conocer los efectos secundarios de cada virus.
  - § Sophos Anti-Virus puede evitar la activación de archivos infectados de varias formas. Seleccione la acción que desea llevar a cabo si Sophos Anti-Virus no puede llevar a cabo la limpieza automática. Sin embargo,



Sólo debería utilizar estas opciones bajo las indicaciones de soporte técnico de Sophos. Utilice el [Área de cuarentena](#) para limpiar virus y programas espía que encuentre Sophos Anti-Virus.


Seleccione **Borrar** para eliminar el archivo. Seleccione **Mover a** para ponerlo en otra carpeta, que puede especificar haciendo clic en **Examinar**. Mover un archivo ejecutable reduce la probabilidad de activarlo.

No es posible mover de forma automática componentes de una infección múltiple.




Para más información sobre cómo limpiar virus y programas espía desde el Área de cuarentena, vea la sección [Revisar virus y programas espía en cuarentena](#).

## Configurar la limpieza automática de archivos sospechosos


 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

Sophos Anti-Virus puede eliminar o mover archivos sospechosos de forma automática durante el escaneo en acceso, en demanda o durante el escaneo con el botón derecho.


 Un **archivo sospechoso** es un archivo que puede estar infectado con un virus para el que no existe identidad específica.

Las acciones que Sophos Anti-Virus realice quedarán anotadas en el registro del equipo o en el registro del escaneo en demanda.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneo que desea configurar (vea la sección Abrir el cuadro de diálogo de opciones de escaneo).
2. En el cuadro de diálogo de opciones de escaneo, abra la ficha **Limpieza**. En el panel **Archivos sospechosos**, configure las opciones que se describen a continuación.

 Sólo debería utilizar estas opciones bajo las indicaciones de soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar archivos sospechosos que Sophos Anti-Virus encuentre en el equipo.

Seleccione **Borrar** para eliminar el archivo. Seleccione **Mover a** para ponerlo en otra carpeta, que puede especificar haciendo clic en **Examinar**. Mover un archivo ejecutable reduce la probabilidad de activarlo.

 Para más información sobre cómo limpiar archivos sospechosos desde el Área de cuarentena, vea la sección Tratar archivos sospechosos en cuarentena.

## Configurar la limpieza automática de programas publicitarios y aplicaciones no deseadas

Al ejecutar un escaneo en demanda o con el botón derecho, Sophos Anti-Virus puede limpiar automáticamente programas publicitarios y aplicaciones no deseadas del equipo.



La limpieza automática de programas publicitarios y aplicaciones no deseadas no está disponible para el escaneo en acceso. Para limpiar programas publicitarios y aplicaciones no deseadas del equipo, utilice el Área de cuarentena.

Las acciones que Sophos Anti-Virus realice quedarán anotadas en el registro del equipo o en el registro del escaneo en demanda.

Para completar la eliminación de ciertos programas publicitarios y aplicaciones no deseadas con múltiples componentes, es posible que tenga que reiniciar el sistema. 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.

1. Abra el cuadro de diálogo de las opciones del tipo de escaneo que desea configurar (vea la sección Abrir el cuadro de diálogo de opciones de escaneo).
2. En el cuadro de diálogo de opciones de escaneo, abra la ficha **Limpieza**.
3. Active la opción **Limpiar automáticamente elementos con adware/PUA** para que Sophos Anti-Virus elimine todos los componentes conocidos de programas publicitarios y aplicaciones no deseadas de los equipos de todos los usuarios. La limpieza no repara los daños que el programa publicitario o la aplicación no deseada haya podido realizar (vea cómo Obtener instrucciones de limpieza desde la web de Sophos para conocer los efectos secundarios de cada virus).



Para más información sobre cómo limpiar programas publicitarios y aplicaciones no deseadas desde el Área de cuarentena, vea la sección Revisar aplicaciones en cuarentena.

## Escaneo exhaustivo

Es posible que deba ejecutar un escaneo exhaustivo del sistema para determinar todos los elementos de amenazas, programas publicitarios o aplicaciones no deseadas multicomponente, antes de que Sophos Anti-Virus pueda proceder a su limpieza.

1. Para escanear los discos duros del equipo, incluidos los sectores de arranque, ejecute el escaneado **Escanear el ordenador**. Para más información, vea la sección Escanear el ordenador.
2. Si la amenaza, aplicación no deseada o programa publicitario se han detectado tan sólo de forma parcial, es posible que no disponga de derechos de acceso suficientes o a que algunas unidades o carpetas del ordenador, donde se hallan los componentes de la aplicación, estén excluidos del escaneado. Compruebe la lista de elementos excluidos del escaneado. Para más información, vea la sección Excluir elementos del escaneado. Si la lista contiene varios elementos, bórrelos de la lista y vuelva a escanear el ordenador.

Si no dispone de permisos para escanear todo el sistema, póngase en contacto con su responsable informático.

Sophos Anti-Virus podría no detectar o eliminar de forma completa aplicaciones no deseadas o programas publicitarios con componentes instalados en unidades de red.

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

## **13 Revisar elementos en cuarentena**

### **El área de cuarentena**

El Área de cuarentena permite gestionar los elementos encontrados durante el escaneado 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 escaneado que encontró el elemento.
- No se pudo llevar a cabo la acción indicada para el escaneado.
- El elemento tiene múltiples infecciones y todavía contiene amenazas.
- La amenaza ha sido detectada sólo de forma parcial y se requiere un escaneado exhaustivo del ordenador. Para más información,

vea la sección Escaneado exhaustivo.

- El elemento muestra un comportamiento sospechoso.
- El elemento es una aplicación restringida.



Los programas publicitarios, aplicaciones no deseadas e infecciones de varios componentes detectados durante el escaneado en acceso se enumeran siempre en el Área de cuarentena. Desde el escaneado 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.

## Revisar virus y programas espía en cuarentena



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

1. Abra el área de cuarentena. En la página de inicio de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.
2. En la página del Área de cuarentena, abra el cuadro **Ver** y seleccione **Virus/spyware**.

### Detalles de los elementos infectados

Las columnas contienen información sobre cada elemento.

**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.

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

**Acciones disponibles** muestra las acciones que puede realizar con

el elemento. Existen tres acciones: Limpiar, Eliminar y Mover, que se describen a continuación. Para ejecutar cualquiera de las acciones, selecciónela.

## Tratar elementos infectados

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

### Seleccionar todos, Deseleccionar todos

Utilice estos botones para seleccionar/deseleccionar todos los elementos en 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.



Para completar la eliminación de ciertos virus y programas espía con múltiples componentes, es posible que tenga que reiniciar el sistema. 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.


- § 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 la carpeta indicada en

la configuración de limpieza. Mover un archivo ejecutable reduce la probabilidad de activarlo. Tenga precaución al utilizar este botón.

 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.

Vea cómo Configurar los derechos sobre el área de cuarentena si desea modificar las acciones disponibles.

## Tratar comportamientos sospechosos en cuarentena

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

1. Abra el área de cuarentena. En la página de inicio de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.
2. En la página del **Área de cuarentena**, abra el cuadro **Ver** y seleccione **Comportamiento sospechoso**.

### Detalles de comportamientos sospechosos

Las columnas contienen información sobre cada elemento.

**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.

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

**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 todos, Deseleccionar todos**

Utilice estos botones para seleccionar/deseleccionar todos los elementos en la lista. De esta forma podrá realizar una acción en todo 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.

Vea cómo [Configurar los derechos sobre el área de cuarentena](#) si desea modificar las acciones disponibles.

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

## **Tratar archivos sospechosos en cuarentena**

 Un **archivo sospechoso** es un archivo que puede estar infectado con un virus para el que no existe identidad específica.

1. Abra el área de cuarentena. En la [página de inicio](#) de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.
2. En la página del Área de cuarentena, abra el cuadro **Ver y seleccione Archivos sospechosos**.

### **Detalles de archivos sospechosos**

Las columnas contienen información sobre cada elemento.

**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.

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

**Acciones disponibles** muestra las acciones que puede realizar con el elemento. Existen tres acciones: Autorizar, Eliminar y Mover, que se describen a continuación. Para ejecutar cualquiera de las acciones, selecciónela.

## Tratar archivos sospechosos

Las opciones disponibles se describen a continuación.

### Seleccionar todos, Deseleccionar todos

Utilice estos botones para seleccionar/deseleccionar todos los elementos en la lista. De esta forma podrá realizar una acción en todo 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 la carpeta indicada en la configuración de limpieza. Mover un archivo ejecutable reduce la probabilidad de activarlo. Tenga precaución al utilizar este botón.

 A veces, al eliminar o mover un archivo sospechoso, el equipo puede dejar de funcionar correctamente porque no puede encontrar el archivo.

Vea cómo [Configurar los derechos sobre el área de cuarentena](#) si desea modificar las acciones disponibles.

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

## Revisar programas publicitarios y aplicaciones no deseadas en cuarentena

1. Abra el área de cuarentena. En la [página de inicio](#) de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.
2. En la página del **Área de cuarentena**, abra el cuadro **Ver y seleccione Adware/PUA**.

### Detalles de programas publicitarios o aplicaciones no deseadas

Las columnas contienen información sobre cada elemento.

**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.

**Detalles** muestra el subtipo de programa publicitario o aplicación no deseada. 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.

**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 todos, Deseleccionar todos**

Utilice estos botones para seleccionar/deseleccionar todos los elementos en la lista. De esta forma podrá realizar una acción en todo 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.



Para completar la eliminación de ciertos programas publicitarios y aplicaciones no deseadas con múltiples componentes, es posible que tenga que reiniciar el sistema. 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.

Vea cómo [Configurar los derechos sobre el área de cuarentena](#) si desea modificar las acciones disponibles.

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

## Revisar las aplicaciones restringidas en cuarentena



Una **aplicación restringida** es una aplicación legítima que puede afectar a la productividad y al rendimiento de la red.

1. Abra el área de cuarentena. En la [página de inicio](#) de la ventana de Sophos Anti-Virus, haga clic en **Elementos en cuarentena**.
2. En la página del **Área de cuarentena**, abra el cuadro **Ver** y seleccione **Aplicaciones restringidas**.

### Detalles de aplicaciones restringidas

Las columnas contienen información sobre cada elemento.

**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.

**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.

**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 todos, Deseleccionar todos

Utilice estos botones para seleccionar/deseleccionar todos los elementos en la lista. De esta forma podrá realizar una acción en todo 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.

## Configurar los derechos sobre el área de cuarentena



Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.

1. En el menú **Configurar**, haga clic en **Configurar derechos sobre el área de cuarentena**.
2. En el cuadro de diálogo **Configurar derechos sobre el área de cuarentena**, seleccione los niveles de usuario que pueden realizar cada acción. Para más información sobre los tipos de usuario, vea [Tipos de usuario](#). Recuerde que estos derechos sólo afectan al área de cuarentena. Los tipos de acción se explican a continuación.

### Limpiar sectores

Hace referencia a la limpieza de sectores de arranque de disquetes.

### Limpiar archivos

Hace referencia a la limpieza de documentos y programas. La limpieza de documentos no puede deshacer el daño que el virus

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

### **Borrar archivos**

Hace referencia a la eliminación de archivos infectados.

### **Mover archivos**

Hace referencia al cambio de ubicación de archivos infectados. Mover un archivo ejecutable reduce la probabilidad de activarlo.

### **Autorizar**

Hace referencia a la autorización de elementos sospechosos y programas publicitarios o aplicaciones no deseadas, para permitir su ejecución en el equipo. Es aplicable al Gestor de autorización y al Área de cuarentena.



Para limpiar una programas publicitarios o aplicaciones no deseadas, debe pertenecer a los grupos de administradores de Windows y administradores de Sophos.

## **14 Autorizar el uso de elementos**

### **Autorizar el uso de programas publicitarios y aplicaciones no deseadas**



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

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

1. En el menú **Configurar**, seleccione **Elementos autorizados**.
2. En el cuadro de diálogo del **Gestor de autorización**, abra la ficha **Adware/PUA**.

3. En el cuadro de la lista **Adware/PUA conocidos**, seleccione los programas publicitarios o aplicaciones no deseadas que desea autorizar y haga clic en **Añadir** para que aparezca en el cuadro de la lista **Adware/PUA autorizados**.

Si quiere impedir que los programas publicitarios o aplicaciones no deseadas autorizados actualmente se ejecuten en su equipo, selecciónelos en la lista **Adware/PUA autorizados** y haga clic en **Quitar**.



También es posible autorizar programas publicitarios y aplicaciones no deseadas desde el Área de cuarentena. Para más información, vea la sección Revisar aplicaciones en cuarentena.

## Autorizar el uso de elementos sospechosos



Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

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

1. En el menú **Configurar**, seleccione **Gestor de autorización**.
2. En el cuadro de diálogo **Gestor de autorización**, haga clic en la ficha del tipo de elemento detectado (por ejemplo, **Desbordamiento del búfer**).
3. Para autorizar el elemento, selecciónelo en la lista de elementos **conocidos** y muévelo a la lista de elementos **autorizados**.



También es posible autorizar elementos sospechosos desde el Área de cuarentena. Para más información, vea las secciones Tratar archivos sospechosos en cuarentena y Tratar comportamientos sospechosos en cuarentena.

Si desea autorizar un elemento que Sophos Anti-Virus *no* ha clasificado aún como sospechoso, preautorícelo según se explica a continuación.

1. Haga clic en **Nueva entrada**.
2. Vaya hasta el elemento y selecciónelo para añadirlo a la lista de elementos **autorizados**.

## 15 Solución de problemas

### El icono de Sophos en la bandeja del sistema tiene una cruz roja

Si aparece una marca roja en el icono de Sophos Anti-Virus en la bandeja del sistema, significa que ha fallado la actualización.



Encontrará información sobre el problema en el registro de actualización. Haga clic con el botón derecho del ratón sobre el icono de Sophos Anti-Virus en la bandeja del sistema. Seleccione **Configurar actualización**. Abra la ficha **Registro** y haga clic en el botón **Ver registro**.

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



Para cambiar estas opciones, es necesario pertenecer al grupo de administradores de Sophos.

### Sophos Anti-Virus tiene una dirección incorrecta del servidor

1. Haga clic con el botón derecho del ratón sobre el icono de Sophos Anti-Virus en la bandeja del sistema. Seleccione **Configurar actualización**.
2. Abra la ficha **Servidor primario**. Compruebe la dirección del servidor.

### Sophos Anti-Virus tiene una configuración incorrecta del proxy

Si Sophos Anti-Virus se actualiza a través de Internet y utiliza un servidor proxy para la conexión, debe configurarlo correctamente.

1. Haga clic con el botón derecho del ratón sobre el icono de Sophos Anti-Virus en la bandeja del sistema. Seleccione **Configurar actualización**.
2. Abra la ficha **Servidor primario**. Haga clic en el botón **Detalles del proxy**.

3. En el cuadro de diálogo **Detalles del proxy**, indique la dirección y puerto del proxy y la cuenta de acceso.

### **La actualización automática no está configurada correctamente**

1. Haga clic con el botón derecho del ratón sobre el icono de Sophos Anti-Virus en la bandeja del sistema. Seleccione **Configurar actualización**.
2. Abra la ficha **Programado**. 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**.

### **No se ha mantenido la fuente de actualización**

Es posible que la fuente de actualización haya sido movida (en la red o servidor web) o haya sido borrada. Póngase en contacto con el administrador de la red.

### **El icono de Sophos en la bandeja del sistema aparece gris**

Si el icono de Sophos Anti-Virus en la bandeja del sistema aparece gris, el sistema no está protegido por el escaneado en acceso.



Para activar el escaneado en acceso en todos los usuarios del equipo, vea Activar/desactivar la protección para un equipo.

### **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 activar la limpieza

automática, consulte el apartado *Limpieza*. La limpieza automática de programas publicitarios y aplicaciones no deseadas no está disponible para el escaneo 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 escaneo exhaustivo del ordenador**

Es posible que deba ejecutar un escaneo exhaustivo del ordenador para determinar todos los elementos de una amenaza multicomponente, antes de que Sophos Anti-Virus pueda proceder a su limpieza.

1. Para escanear los discos duros del equipo, incluyendo sectores de arranque, ejecute el escaneo Escanear el ordenador.
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 escaneo. Compruebe la lista de elementos excluidos del escaneo. Si la lista contiene varios elementos, bórrelos de la lista y vuelva a escanear el ordenador.

### **La unidad extraíble está protegida contra escritura**

No se encuentra en un disco protegido contra escritura.

### **El volumen NTFS está protegido contra escritura**

No se encuentra en un volumen NTFS (Windows 2000 o posterior) protegido 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. Vea la sección Fragmento de virus/spyware detectado

## **Fragmento de virus/spyware detectado**

Si se informa de la presencia de un fragmento de virus/spyware, actualice Sophos Anti-Virus en el ordenador afectado, para que cuente con los archivos de identidad de virus más recientes. Después, realice un escaneado en el ordenador. Si se siguen detectando fragmentos de virus, póngase en contacto con el soporte técnico de Sophos para recibir ayuda.

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 soporte técnico de Sophos si necesita ayuda.

## **Amenaza detectada parcialmente**

Si Sophos Anti-Virus ha detectado parcialmente una amenaza (troyano, programa publicitario o aplicación no deseada), será necesario un escaneado exhaustivo del ordenador para determinar los componentes de la amenaza.

1. Para escanear los discos duros del equipo, incluyendo sectores de arranque, ejecute el escaneado Escanear el ordenador.
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. Compruebe la lista de elementos excluidos del escaneado. Si la lista contiene varios elementos, bórrelos de la lista y vuelva a escanear el ordenador.

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

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

## Programas publicitarios y 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 gestión 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, vea la sección Autorizar el uso de programas publicitarios y aplicaciones no deseadas.

## 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 escaneado 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.



Si se detecta una aplicación no deseada después del escaneado, vea el paso 2 de la sección Amenaza detectada parcialmente.


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.

## No se puede acceder a un disco con el sector de arranque infectado

 Si utiliza una consola de gestión para administrar Sophos Anti-Virus en las estaciones de trabajo, se podrían modificar los cambios aquí realizados. Para evitar esto, vea la Ayuda de la consola.

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. En el menú **Configurar**, seleccione **Escaneado en acceso**.
2. En el cuadro de diálogo **Configuración del escaneado en acceso para este equipo**, abra la ficha **Escaneado**.
3. Active la opción **Permitir el acceso a unidades con sectores de arranque infectados**.

 Desactive esta opción cuando no la necesite. Retire el disco del equipo para que no pueda intentar infectarlo de nuevo durante el reinicio.

## No se puede acceder a ciertas áreas de Sophos Anti-Virus

Si no puede usar o configurar ciertas áreas de Sophos Anti-Virus, es posible que tenga el acceso restringido según el tipo de usuario. Para más detalles, vea la sección *Restringir derechos de acceso*.

## Recuperación tras una infección de virus

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

### Efectos secundarios de los virus

Algunos virus no dejan 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 [Obtener instrucciones de limpieza](#) 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 [soporte técnico de Sophos](#) si necesita ayuda.

## **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 [Obtener instrucciones de limpieza](#) 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](#).

## **Error de contraseña**

Si, al intentar configurar un escaneado en demanda, aparece un mensaje de error sobre la contraseña, compruebe que:

- utiliza la contraseña correcta para la cuenta
- el campo de contraseña no está vacío.

Consulte las propiedades de la cuenta en el Panel de control para comprobar que la contraseña es la correcta (vea la documentación de Windows si es necesario).

## **Soporte técnico**

Para más información sobre el soporte técnico, vaya a <http://esp>.

[sophos.com/support](https://sophos.com/support).

Si necesita ponerse en contacto con soporte técnico, debe proporcionar toda la información posible, incluyendo:

- la versión del software de Sophos
- sistema operativo y nivel de actualización
- texto exacto de cualquier mensaje de error

# Índice

## A

acceso a discos 61  
activar o desactivar la protección 10  
actualización 38  
actualización automática 34  
actualización inmediata 33  
actualizar 33  
adware 60  
amenaza detectada parcialmente 59  
análisis de amenazas 39  
análisis de comportamiento 27  
ancho de banda 38  
aplicaciones no deseadas 54  
archivos comprimidos 25  
archivos de Macintosh 26  
archivos sospechosos 48  
autorizar 47  
ayuda 5

## B

barra de herramientas 5

## C

comportamiento sospechoso 47  
comprobar la activación de la protección 9  
configuración central 17

configuración para todos los ordenadores 17  
configuración para todos los usuarios de un ordenador 18  
configurar un escaneado 12  
control del escaneado en acceso 9  
crear un escaneado 12

## D

derechos de acceso 61  
derechos de usuario 61  
desbordamiento del búfer 47  
desbordamientos del búfer 27  
desinfección 57  
detección 27  
detección parcial 59  
detener escaneado en acceso 10

## E

efectos secundarios 62  
escaneado 15  
escaneado con el botón derecho 15  
escaneado de botón derecho 9  
escaneado en acceso 10  
escaneado en demanda 14  
escaneado exhaustivo 26  
escaneados disponibles 13  
escanear un elemento 15  
escudo 57  
estado 5  
excluir elementos del escaneado 20  
extensiones de archivo escaneadas 19

## **F**

fragmento 59

## **G**

grupo de usuarios 53  
grupos de usuario 61  
grupos de usuarios 17

## **I**

icono de la bandeja de Sophos Anti-Virus 57  
icono de la bandeja del sistema 57  
icono de la bandeja del sistema de Sophos Anti-Virus 56  
icono de Sophos Anti-Virus 7  
icono en la bandeja del sistema 7  
iconos:elementos a escanear 15  
información 5  
información de limpieza 39  
información de seguridad 39  
iniciar escaneado en acceso 10  
interfaz de usuario 5

## **L**

limpiar 57  
limpieza 39  
limpieza automática 42

## **M**

mensaje SNMP 30  
mensajes de escritorio 28  
modificar un escaneado 14

## **N**

nivel de escaneado 26  
notificación por email 29

## **P**

página de inicio 5  
programar actualización 36  
programar un escaneado 12  
programas espía 45  
programas publicitarios 54  
protección 10  
PUA 60

## **R**

recuperación tras una infección 62  
recuperación tras una infección de virus 61  
registrar actualizaciones 38  
registro de eventos 31  
registro de un escaneado en demanda 33  
registro del equipo 32

## **S**

- sector de arranque infectado 61
- servidor primario 34
- servidor proxy 37
- servidor secundario 35
- sistema lento 60
- soporte 63
- soporte técnico 63
- sumario de actividad 5

## **T**

- tipos de archivo escaneados 19
- todos los archivos:escaneado 19

## **V**

- ventana de Sophos Anti-Virus 5
- virus 45