SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

Ayuda

Versión del producto: 5.5

Contenido

1 Acerca de Sophos Enterprise Console

Sophos Enterprise Console es una consola única automatizada para la administración y actualización del software de seguridad de Sophos en equipos Windows, Mac OS X, Linux y UNIX y entornos virtuales con VMware vShield.

Enterprise Console permite:

- Proteger la red contra aplicaciones maliciosas, tipos de archivos y sitios web peligrosos, así como programas publicitarios y otras aplicaciones no deseadas.
- Restringir los sitios web a los que se permite el acceso.
- Restringir el uso de aplicaciones en las estaciones de la red.
- Administrar la protección del cortafuegos en las estaciones.
- Comprobar la presencia de parches de seguridad en las estaciones.
- Reducir las pérdidas accidentales de datos, como las transferencias no intencionadas de datos delicados desde las estaciones.
- Impedir que los usuarios utilicen dispositivos de almacenamiento externo no autorizados o tecnologías de conexión inalámbrica en las estaciones.
- Impedir que el usuario pueda cambiar la configuración, desactivar o desinstalar el software de seguridad de Sophos.

Nota
No todas las funciones anteriores se incluyen en todas las licencias. Si desea utilizarlas, deberá incorporarlas a su licencia. Para más información sobre las licencias disponibles, consulte www.sophos.com/es-es/products/enduser-protection-suites/how-to-buy.aspx y www.sophos.com/es-es/products/server-security/how-to-buy.aspx.

2 Descripción de la ventana de Enterprise Console

2.1 Ventana principal

La ventana principal de Enterprise Console se compone de las siguientes áreas:

Barra de herramientas

La barra de herramientas ofrece acceso directo a los comandos más utilizados.

Para obtener más información, consulte Botones de la barra de herramientas (página 2).

Panel de control

El **Panel de control** ofrece una visión general del estado de seguridad de la red.

Para obtener más información, consulte Paneles de control (página 4).

Lista de ordenadores

La lista de ordenadores se muestra en la parte inferior derecha. Dispone de dos vistas:

- La vista **Estaciones** muestra los ordenadores del grupo seleccionado en el panel **Grupos**. Para obtener más información, consulte Descripción de la vista Estaciones (página 6).
- La vista **Gestores de actualización** muestra los equipos en los que está instalado Sophos Update Manager. Para obtener más información, consulte Descripción de la vista Gestores de actualización (página 10).

2.2 Botones de la barra de herramientas

A continuación se describen los botones de la barra de herramientas. Ciertos botones sólo están disponibles situaciones específicas. Por ejemplo, el botón **Proteger** sólo está disponible si ha seleccionado algún **Grupo** en la vista **Estaciones**.

Botón	Descripción	Notas
	**Detectar ordenadores**	Busca equipos en la red para añadirlos a la consola. Para obtener más información, consulte Detectar ordenadores en la red (página 32).

Botón	Descripción	Notas
	**Crear grupo**	Crea un grupo nuevo de equipos: Para obtener más información, consulte Crear un grupo (página 23).
	**Ver/Editar política**	Abre la política seleccionada en el panel **Políticas**. Para obtener más información, consulte Editar políticas (página 30).
	**Proteger**	Instala el antivirus y el cortafuegos en las estaciones seleccionadas. Para obtener más información, consulte Proteger ordenadores de forma automática (página 43).
	**Estaciones**	Cambia a la vista **Estaciones**. La vista **Estaciones** muestra los equipos del grupo seleccionado en el panel **Grupos**. Para obtener más información, consulte Descripción de la vista Estaciones (página 6).
	**Gestores de actualización**	Cambia a la vista **Gestores de actualización**. La vista **Gestores de actualización** muestra los equipos en los que está instalado Sophos Update Manager. Para obtener más información, consulte Descripción de la vista Gestores de actualización (página 10).
	**Panel de control**	Muestra u oculta el **Panel de control**. El **Panel de control** ofrece una visión general del estado de seguridad de la red. Para obtener más información, consulte Paneles de control (página 4).
	**Informes**	Abre el **Gestor de informes**, desde donde podrá generar informes sobre alertas y eventos en su red. Para obtener más información, consulte Generar informes (página 196).
	**Sophos Central**	Le lleva a Sophos Central. Para obtener información acerca de Sophos Central, consulte el artículo 119598 de la base de conocimiento. Para obtener información acerca de la migración a Sophos Central, consulte el artículo 122264 de la base de conocimiento.

Botón	Descripción	Notas
	**Sophos Mobile**	Cuando la URL de Sophos Mobile está configurada, esta abre la consola web de Sophos Mobile. Es una solución de administración de dispositivos para dispositivos móviles (p. ej., teléfonos inteligentes y tabletas) que le ayuda a administrar las aplicaciones y la configuración de seguridad. Para obtener más información, consulte Configurar URL Sophos Mobile (página 41).

2.3 Paneles de control

El **Panel de control** incluye las siguientes secciones:

Panel	Descripción
Ordenadores	Muestra el número total de equipos de la red y el número de equipos conectados, administrados y sin administrar. Para ver una lista de los ordenadores administrados, no administrados, conectados o de todos ellos, haga clic en los enlaces de la sección **Ordenadores**.
Actualizaciones	Muestra el estado de los gestores de actualización.
Ordenadores con alertas	Muestra el número y el porcentaje de equipos administrados con alertas sobre: • Virus y programas espía • Comportamientos y archivos sospechosos • Programas publicitarios y otras aplicaciones no deseadas Para ver la lista de ordenadores administrados con alertas pendientes, haga clic en **Ordenadores con alertas.**
Ordenadores con umbrales superados	Muestra el número de equipos con eventos que superan los umbrales en la última semana. Para ver una lista de los equipos con eventos de control de dispositivos, control de datos, restricción de aplicaciones o eventos del cortafuegos, haga clic en el enlace correspondiente de la sección **Ordenadores con umbrales superados**. **Nota** En función de su licencia, es posible que algunos de los tipos de eventos no se muestren.

Panel	Descripción
Políticas	Muestra el número y el porcentaje de equipos administrados con errores de comparación de políticas o que incumplen políticas de grupo. También incluye los equipos que aún no han respondido al cambio de política enviado desde la consola. Para ver la lista de ordenadores administrados cuya política difiere, haga clic en **Políticas**.
Protección	Muestra el número y el porcentaje de equipos administrados y conectados en los que Sophos Endpoint Security and Control o Sophos Anti-Virus no está actualizado o utiliza datos de detección desconocidos. Para ver la lista de ordenadores administrados conectados no actualizados, haga clic en **Protección**.
Errores	Muestra el número y el porcentaje de equipos administrados con errores pendientes de escaneado, actualización o del cortafuegos. Para ver la lista de ordenadores administrados con errores pendientes del software de Sophos, haga clic en **Errores**.

2.4 Iconos del estado de seguridad

A continuación se describen los iconos de estado que aparecen en el **Panel de control** y en la barra de estado de Enterprise Console.

Icono	Descripción
	**Normal** El número de equipos afectados está por debajo del nivel de aviso.
	**Aviso** Se ha superado el umbral de aviso.
	**Crítico** Se ha superado el umbral crítico.

Iconos de estado general

Los iconos de estado general del **Panel de control** se muestran en la esquina superior derecha de cada panel. Este icono muestra el estado general de dicho panel.

Los indicadores de estado general de cada panel muestran el estado más grave dentro de cada sección, es decir:

- El indicador de estado del panel cambia de **Normal** a **Aviso** cuando al menos uno de los indicadores de la sección supera el umbral de aviso.
- El indicador de estado del panel cambia de **Aviso** a **Crítico** cuando al menos uno de los indicadores de la sección supera el umbral crítico.

Icono de estado de la red

El icono de estado de la red se muestra en la parte derecha de la barra de estado de Enterprise Console. Este icono muestra el estado de seguridad de la red.

El indicador del estado de la red muestra el estado más grave del **panel de control**, es decir:

- El indicador de estado de la red cambia de **Normal** a **Aviso** cuando al menos uno de los paneles supera el umbral de aviso.
- El indicador de estado de la red cambia de **Aviso** a **Crítico** cuando al menos uno de los paneles supera el umbral de aviso.

Al instalar o actualizar Enterprise Console por primera vez, el **panel de control** utiliza los umbrales de aviso y críticos predeterminados. Para configurar los umbrales de aviso y críticos, consulte Paneles de control (página 4).

También puede configurar el envío de notificaciones a determinados destinatarios cuando se superen los umbrales de aviso y críticos de alguna sección del **panel de control**. Para más información, consulte Alertas por email sobre el estado de la red (página 183).

2.5 Descripción de la vista Estaciones

Lista de ordenadores

En la vista **Estaciones**, en el panel **Grupos**, seleccione el grupo de ordenadores que desea mostrar.

Esta vista está formada por varias fichas. En la ficha **Estado** se puede ver si los equipos están protegidos por el escaneado en acceso, si cumplen las políticas del grupo, qué funciones están activadas y si el software está actualizado. Esta ficha también muestra las alertas. El resto de fichas aportan más datos sobre cada uno de los siguientes aspectos.

Puede filtrar la lista de ordenadores mediante la opción **Ver**. En la lista **Ver**, seleccione el tipo de estaciones que desea mostrar. Por ejemplo, seleccione **Ordenadores con posibles problemas** para mostrar equipos con problemas.

También se puede filtrar la lista de ordenadores por el nombre del elemento detectado, como p. ej., programa malicioso, aplicación potencialmente no deseada o archivo sospechoso. Para obtener más información, consulte Filtrar ordenadores por el nombre de un elemento detectado (página 8).

Puede buscar ordenadores mediante el nombre, la descripción o la dirección IP. Para obtener más información, consulte Buscar ordenadores en Enterprise Console (página 9).

Para más información sobre los iconos utilizados en la lista de ordenadores, vea Iconos de lista de ordenadores (página 7).

Si lo desea, puede copiar o imprimir la información que aparece en la lista de ordenadores. Para más información, consulte Copiar datos de la lista de ordenadores (página 208) y Imprimir datos de la lista de ordenadores (página 208).

Panel Grupos

En el panel **Grupos**, puede crear grupos  en los que colocar equipos de la red. Los grupos se pueden crear o importar desde los contenedores de Active Directory, con o sin equipos, para utilizarlos como grupos de equipos de Enterprise Console.

Para obtener más información, consulte Crear y usar grupos (página 22).

El grupo **No asignados**  contiene los ordenadores que aún no han sido adjudicados a un grupo.

Panel Políticas

En el panel **Políticas**, puede crear o modificar las políticas aplicadas a grupos de ordenadores. Para obtener más información, consulte Crear y usar políticas (página 25).

2.6 Iconos de lista de ordenadores

Alerts

Icono	Significado
	La detección de virus, gusanos, troyanos, programas espía o comportamientos sospechosos se indica mediante iconos de aviso rojos en la columna **Alertas y errores** de la ficha **Estado**.
	Los iconos de aviso amarillos que aparecen en la columna **Alertas y errores** de la ficha **Estado** indican uno de los problemas siguientes: • Se ha detectado un archivo sospechoso. • Se ha detectado un programa publicitario o aplicación no deseada. • Se ha producido algún error. Los iconos de aviso amarillos que aparecen en la columna **Cumplimiento de políticas** indican que el equipo no utiliza las mismas políticas que el resto de equipos del grupo.

Si existen varias alertas o errores en un equipo, el icono de la alerta más importante aparecerá en la columna **Alertas y errores**. A continuación se enumeran los tipos de alertas en orden descendente de prioridad.

1. Alertas de virus y programas espía
2. Alertas de comportamientos sospechosos
3. Alertas de archivos sospechosos
4. Alertas de programas publicitarios y otras aplicaciones no deseadas

5. Errores del software (por ejemplo, errores de instalación)

Si se reciben diferentes alertas del mismo equipo con la misma prioridad, en la lista de ordenadores se mostrará la alerta más reciente.

Protección desactivada u obsoleta

Un icono gris en la ficha **Estado** indica que la función a la que hace referencia se encuentra desactivada. Por ejemplo, un escudo gris

en la columna **En acceso** indica que el escaneado en acceso se encuentra desactivado.

Un reloj

en la columna **Actualizado** indica que el software no se encuentra actualizado.

Estado del ordenador

Icono	Significado
	El icono del ordenador con una conexión verde indica que el equipo está administrado desde Enterprise Console.
	El icono del ordenador con un reloj de arena amarillo indica que la instalación del software de seguridad está pendiente.
	El icono del ordenador con una flecha amarilla hacia abajo indica que la instalación del software de seguridad está en progreso.
	El icono del ordenador gris indica que el ordenador no se administra desde Enterprise Console.
	El icono del ordenador con una cruz roja indica que un equipo normalmente administrado con Enterprise Console está desconectado de la red (no se mostrarán los ordenadores desconectados no administrados).

2.7 Filtrar ordenadores por el nombre de un elemento detectado

Es posible filtrar la lista de ordenadores por el nombre del elemento detectado, como p. ej., programa malicioso, aplicación potencialmente no deseada o archivo sospechoso. Para ello configure el filtro "Ordenadores administrados afectados por...". El filtro se muestra en la lista desplegable **Ver** junto con los demás filtros para listas de ordenadores.

Para configurar el informe:

1. En el menú **Herramientas**, haga clic en **Configurar filtros**.
2. En el cuadro de diálogo **Configurar filtro de lista de ordenadores**, introduzca el nombre del elemento detectado con el que desea ordenar la lista. Puede encontrar los nombres de los elementos detectados en su red en:

- Vista de lista de ordenadores, pestaña **Detalles de alertas y errores**, columna **Elemento detectado**.

  Tenga en cuenta que si se han detectado diferentes elementos en un ordenador, la columna **Elemento detectado** sólo mostrará el elemento de mayor prioridad, que puede no ser el que ha utilizado para ordenar la lista.

- Cuadro de diálogo **Resolver alertas y errores**. Para abrir el cuadro de diálogo, seleccione un ordenador o varios en la lista de ordenadores o un grupo de ordenadores en el panel **Grupos**, y haga clic con el botón derecho y seleccione **Resolver alertas y errores**.
- Cuadro de diálogo **Detalles del ordenador**. Para abrir el cuadro de diálogo haga doble clic en el ordenador afectado. Vaya a la sección **Alertas y errores pendientes**.
- **Informes** (p. ej., **Resumen de alertas** o **Alertas y eventos por nombre**). Para abrir el **Gestor de informes**, en el menú **Herramientas**, haga clic en **Administrar informes**.

Es posible utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres. P. ej., si introduce "Mal*" y aplica el filtro, la lista de ordenadores incluirá todos los ordenadores infectados con programas maliciosos cuyo nombre comience por "Mal", como "Mal/Conficker-A" y "Mal/Packer".

2.8 Buscar ordenadores en Enterprise Console

Puede buscar ordenadores en Enterprise Console mediante:

- Nombre del ordenador
- Descripción del ordenador
- Dirección IP

1. Para buscar ordenadores, siga uno de los procedimientos siguientes:
   - Pulse CTRL+F.
   - En el menú **Edición**, seleccione **Buscar ordenadores**.
   - Haga clic con el botón derecho del ratón en la lista de ordenadores y seleccione **Buscar ordenadores**.
2. En el cuadro de diálogo **Buscar**, introduzca el criterio de búsqueda.

   No se diferencia entre mayúsculas y minúsculas. Caracteres comodín al final son implícitos.

   Se permite el uso de los caracteres comodín * y ?

   Por ejemplo:

Criterio de búsqueda	Resultado de la búsqueda
UKlapt	Cadenas que comiencen por “uklapt”, por ejemplo, UKlaptop-011, UKlaptop-155, uklaptop132.
Ukla*	Cadenas que comience por “ukla”. El carácter comodín no es necesario ya que es implícito; el resultado de la búsqueda será el mismo que en el ejemplo anterior, UKlaptop-011, UKlaptop-155, uklaptop132.
***ukla**	Cadenas con “ukla”, por ejemplo, UKlaptop-011, 055uklax, 056-Dukla-sales.

Criterio de búsqueda	Resultado de la búsqueda
Ukl*t	Cadenas que comiencen por “ukl”, que contenga “t” con cualquier terminación, por ejemplo, UKlaptop-011, ukLite55.
?klap	Cadenas que comiencen por cualquier caracter seguido de “klap” con cualquier terminación, por ejemplo, UKlaptop-011, uklapland33.
UKl??t	Cadenas que comiencen por “ukl”, seguido de dos caracteres cualquiera, seguidos de “t” con cualquier terminación, por ejemplo, UKlaptop-011, uklist101.

2.9 Descripción de la vista Gestores de actualización

Lista de ordenadores

En la vista **Gestores de actualización**, es posible configurar la actualización automática del software desde el sitio web de Sophos y ver el estado e información de los gestores de actualización.

La lista de ordenadores muestra los equipos en los que está instalado Sophos Update Manager.

Suscripciones de software

En el panel **Suscripciones**, puede crear o editar suscripciones de software que indiquen qué versiones del software se descargan desde Sophos para cada plataforma.

3 Empezar a usar Sophos Enterprise Console

En esta sección se describen las tareas que debe realizar para proteger la red después de instalar Enterprise Console y finalizar el **Asistente para descargar el software de seguridad**. Para más información sobre el uso de Enterprise Console, consulte el resto de documentación y secciones mencionadas.

Se recomienda consultar la *Guía de configuración de políticas de Sophos Enterprise Console* para conocer el uso y administración recomendados para el software de seguridad de Sophos. La documentación de Sophos se encuentra en http://www.sophos.com/es-es/support/documentation.

Si no ha completado el **Asistente para descargar el software de seguridad**, consulte Ejecutar el Asistente para descargar el software de seguridad (página 64).

Para proteger la red, siga estos pasos:

1. **Crear grupos.**

   Los grupos se pueden crear uno por uno o importar desde los contenedores de Active Directory, con o sin equipos, para utilizarlos como grupos de equipos de Enterprise Console.

   Si desea importar contenedores de Active Directory, consulte Importar contenedores y equipos de Active Directory (página 32). Se recomienda importar primero los contenedores de Active Directory sin ordenadores, asignar políticas a los grupos y añadir después los ordenadores a los grupos, por ejemplo, sincronizando los grupos con Active Directory.

   Para más información sobre la creación manual de grupos, consulte Crear y usar grupos (página 22).
2. **Configurar políticas.**

   Enterprise Console cuenta con un conjunto de políticas predeterminadas que son esenciales para mantener protegida la red. Si lo desea, puede utilizar las políticas de **Actualización** y **Antivirus y HIPS** de forma instantánea. Para configurar la política cortafuegos, utilice el **Asistente de políticas del cortafuegos**: Consulte Configurar una política básica del cortafuegos (página 106).
3. **Detectar equipos en la red y añadirlos a la consola.**

   Si ha importado contenedores y equipos de Active Directory en el paso 1, no necesita hacer nada más. De lo contrario, consulte Detectar ordenadores en la red (página 32).
4. **Proteger los ordenadores.**

   Puede elegir entre los dos métodos siguientes según sus necesidades.

   - **Asistente para proteger ordenadores**

     Al arrastrar un ordenador desde el grupo **No asignados** y soltarlo en otro grupo, se inicia un asistente para ayudarle a proteger los ordenadores. Consulte Proteger ordenadores de forma automática (página 43).

   - **Proteger ordenadores de forma automática en la sincronización con Active Directory**

     Si va a utilizar la sincronización con Active Directory, también puede disponer de protección automática para estaciones Windows. Podrá activar esta opción desde el **Asistente de sincronización con Active Directory** o el cuadro de configuración **Opciones de sincronización**. Para más información, consulte Usar la sincronización para proteger ordenadores (página 39).
5. **Comprobar que los ordenadores están protegidos.**

Verifique la lista de ordenadores protegidos en el nuevo grupo tras concluir la instalación. En la columna **En acceso**, debería ver la palabra *Activo*: esto indica que el ordenador está protegido por el escaneado en acceso, y que está siendo administrado por Enterprise Console. Para obtener más información, consulte Comprobar la protección de la red (página 45).

6. **Limpiar ordenadores.**

   Si se detecta un virus, una aplicación no deseada u otra amenaza en la red, limpie los ordenadores afectados como se describe en Realizar una limpieza inmediata (página 51).

Otras opciones de protección

Por defecto, Sophos Endpoint Security and Control detecta programas maliciosos (virus, troyanos, gusanos y programas espía), programas publicitarios y otras aplicaciones potencialmente no deseadas, comportamientos sospechosos y tráfico de red malicioso. También bloquea el acceso a sitios web que alojan programas maliciosos y escanea los contenidos descargados de Internet. Es posible activar funciones de seguridad y productividad adicionales, según se describe en Crear y usar grupos (página 22).

Opciones administrativas

En Enterprise Console, se pueden configurar diferentes *roles* con diferentes privilegios a los que asignar a los usuarios y grupos de Windows. El rol de administrador del sistema que incluye el grupo de Windows Sophos Full Administrators tiene derechos totales y no es necesario configurarlo. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Divida el entorno informático en subentornos y asigne grupos de equipos de Enterprise Console a los subentornos. De esta forma, es posible controlar el acceso a los subentornos mediante la asignación de usuarios y grupos de Windows a los mismos. El subentorno **predeterminado** contiene todos los grupos de Enterprise Console, incluido el grupo **No asignados**. Para más información sobre subentornos, consulte Administrar roles y subentornos (página 13).

Sugerencia
Vea los vídeos sobre cómo configurar y utilizar Enterprise Console en el canal de YouTube SophosGlobalSupport, sección Sophos Enduser Protection.

4 Configurar Enterprise Console

4.1 Administrar roles y subentornos

Importante
Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para configurar roles y subentornos. El rol de administrador del sistema que incluye el grupo de Windows Sophos Full Administrators tiene derechos totales y no es necesario configurarlo. Para más información, consulte Roles preconfigurados (página 14) y Qué tareas autoriza cada permiso (página 17).

Puede configurar el acceso delegado a la consola configurando roles con diferentes privilegios y asignando a los usuarios y grupos de Windows a estos roles. Por ejemplo, un técnico de soporte puede actualizar y limpiar ordenadores, pero no puede configurar políticas, de lo que es responsable el administrador.

Para abrir Enterprise Console, los usuarios deben pertenecer al grupo Sophos Console Administrators y tener asignado, como mínimo, un rol de Enterprise Console y un subentorno. Los miembros del grupo Full Administrators de Sophos tienen acceso total a Enterprise Console.

Nota
Si desea permitir que un usuario utilice una consola de administración adicional o remota, consulte Uso de Enterprise Console por otro usuario (página 21) para más información.

Puede crear los roles o utilizar los roles preconfigurados.

Los usuarios se pueden asignar a varios roles, añadiendo el usuario o el grupo al que pertenece a cada rol.

Aunque un usuario no tenga permiso para realizar una tarea determinada en la consola, podrá ver la configuración de dicha tarea en modo de sólo lectura. Los usuarios que no están asignados a ningún rol no pueden abrir Enterprise Console.

También puede restringir los equipos y grupos en los que los usuarios pueden realizar operaciones. Divida el entorno informático en subentornos y asigne grupos de equipos de Enterprise Console a los subentornos. De esta forma, es posible controlar el acceso a los subentornos mediante la asignación de usuarios y grupos de Windows a los mismos. El subentorno **predeterminado** contiene todos los grupos de Enterprise Console, incluido el grupo **No asignados**.

Los usuarios sólo pueden ver el subentorno al que están asignados. Si un usuario está asignado a más de un subentorno, puede elegir cuál quiere ver, pero sólo puede ver uno. El subentorno abierto en Enterprise Console es el *subentorno activo*. Los usuarios no pueden modificar políticas aplicadas fuera de su subentorno activo.

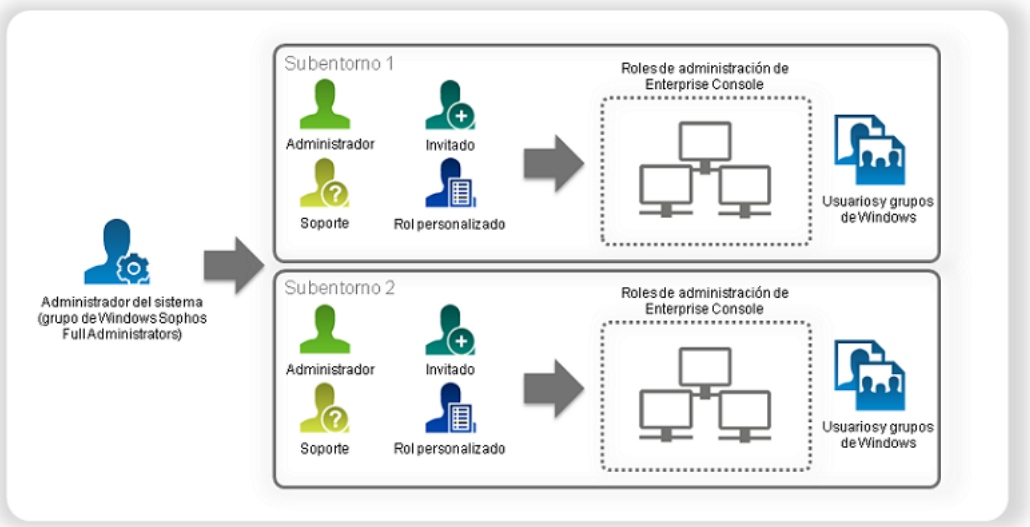


Figura 1: Roles y subentornos

4.1.1 Roles preconfigurados

En Enterprise Console, existen cuatro roles preconfigurados:

Rol	Descripción
Administrador del sistema	Usuario de Enterprise Console con derechos suficientes para administrar el software de seguridad de Sophos en la red y los derechos de usuarios. El rol Administrador del sistema no se puede modificar ni borrar.
Administrador	Usuario de Enterprise Console con derechos suficientes para administrar el software de seguridad de Sophos en la red, pero no puede administrar roles en Enterprise Console. El rol Administrador se puede modificar, cambiar de nombre y eliminar.
Soporte	Rol preconfigurado que sólo tiene derechos de remediación, por ejemplo, para limpiar o actualizar equipos. El rol Soporte se puede modificar, cambiar de nombre y eliminar.
Invitado	Usuario de Enterprise Console que sólo cuenta con derecho de lectura. El rol Invitado se puede modificar, cambiar de nombre y eliminar.

Si lo desea, puede modificar los roles Administrador, Soporte e Invitado, o crear otros según se describe en Crear roles (página 14).

4.1.2 Crear roles

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.

2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar roles**, haga clic en **Crear**.
   Aparece el cuadro de diálogo **Crear rol**.
3. En el campo **Nombre del rol**, escriba un nombre para el rol.
4. En el panel **Permisos**, seleccione los permisos que desea asignar al rol y haga clic en **Añadir**.
5. En el panel **Usuarios y grupos**, haga clic en **Añadir**.
6. En el cuadro de diálogo **Seleccionar Usuarios o Grupos**, introduzca el nombre del usuario o grupo de Windows que desea asignar al rol. Haga clic en **Aceptar**.

Si es necesario, asigne más usuarios o grupos al rol, según se describe en los pasos 5 y 6.

4.1.3 Borrar roles

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar roles**, seleccione el rol que desea eliminar y haga clic en **Borrar**.

Nota
El rol preconfigurado Administrador del sistema no se puede eliminar.

4.1.4 Editar roles

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar roles**, seleccione el rol que desea editar y haga clic en **Editar**.
   Aparece el cuadro de diálogo **Editar rol**.
3. En el panel **Permisos**, elimine permisos existentes o asigne permisos nuevos al rol.
4. En el panel **Usuarios y grupos**, añada usuarios o grupos al rol o elimine los existentes.

4.1.5 Otorgar permisos a un rol

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar roles**, seleccione el rol que desea eliminar y haga clic en **Editar**.
   Aparece el cuadro de diálogo **Editar rol**.
3. En el panel **Permisos**, en la lista **Permisos disponibles**, seleccione un permiso y haga clic en **Añadir**.

4.1.6 Crear subentornos

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar subentornos**, haga clic en **Crear**.
   Aparece el cuadro de diálogo, **Crear subentorno**.
3. En el campo **Nombre del subentorno**, escriba un nombre para el subentorno.
4. En el panel de **Grupos de Enterprise Console**, seleccione los grupos que desea añadir al subentorno.
5. En el panel **Usuarios y grupos**, haga clic en **Añadir** para añadir usuarios o grupos de Windows al subentorno.

4.1.7 Cambiar el subentorno activo

Los usuarios con más de un subentorno asignado pueden elegir qué subentorno ver al abrir Enterprise Console, o pasar desde un subentorno a otro.

Sólo se puede tener abierto un subentorno. Al cambiar el subentorno activo, Enterprise Console carga el subentorno nuevo.

Para cambiar el subentorno activo:

1. En el menú **Herramientas**, haga clic en **Seleccionar subentorno activo**.
2. En el cuadro de diálogo **Seleccionar subentorno activo**, seleccione el subentorno que desea abrir y haga clic en **Aceptar**.

4.1.8 Editar subentornos

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar subentornos**, seleccione el subentorno que desea editar y haga clic en **Editar**.
3. En el cuadro de diálogo **Editar subentorno**, cambie el nombre del subentorno, cambie los grupos de Enterprise Console incluidos o cambie qué usuarios y grupos de Windows tienen acceso al subentorno según sea necesario. Haga clic en **Aceptar**.

4.1.9 Copiar subentornos

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar subentornos**, seleccione el subentorno que desea copiar y haga clic en **Copiar**.
   Aparece una copia del subentorno en la lista.

3. Seleccione el subentorno recién creado y haga clic en **Editar**. Cambie el nombre del subentorno. Cambie los grupos incluidos en el subentorno o los usuarios y grupos de Windows que tienen acceso, si lo desea.

4.1.10 Borrar subentornos

Si ya utiliza la administración delegada, necesitará el permiso **Administración delegada** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, en la ficha **Administrar subentornos**, seleccione el subentorno que desea borrar y haga clic en **Borrar**.

   No es posible borrar el subentorno **predeterminado**.

4.1.11 Ver roles y subentornos de usuarios o grupos

Para ver los roles y subentornos a los que se ha asignado un usuario o grupo de Windows:

1. En el menú **Herramientas**, haga clic en **Administrar roles y subentornos**.
2. En el cuadro de diálogo **Administrar roles y subentornos**, abra la ficha **Ver usuarios y grupos**, y haga clic en el botón **Seleccionar**.
3. En el cuadro de diálogo **Seleccionar Usuarios o Grupos**, seleccione un usuario o grupo cuyos roles o subentornos desee ver y haga clic en **Aceptar**.

4.1.12 Qué tareas autoriza cada permiso

Nota
En función de su licencia, es posible que algunos de los derechos no apliquen.

Permiso	Tareas
Auditoría	Activar la auditoría, desactivar la auditoría

Permiso	Tareas
Búsqueda de ordenadores, protección y grupos	Iniciar y detener una búsqueda, y buscar dominios para búsquedas en la red, búsquedas por rango IP y búsquedas en Active Directory Importar equipos y grupos de Active Directory; importar grupos de Active Directory Importar nombres de ordenadores Eliminar un ordenador Proteger un ordenador Sincronizar un grupo con Active Directory Cambiar propiedades de sincronización del grupo Eliminar sincronización del grupo Mover un ordenador Crear un grupo Cambiar el nombre de un grupo Mover un grupo Eliminar un grupo Asignar una política a un grupo
Personalización del control de datos	Crear reglas de control de datos Modificar reglas de control de datos Copiar reglas de control de datos Eliminar reglas de control de datos Excluir archivos del escaneado de control de datos Crear listas de control de contenido Editar listas de control de contenido Copiar listas de control de contenido Eliminar listas de control de contenido
Eventos del control de datos	Visualizador de eventos del control de datos Eventos del control de datos en los detalles del ordenador
Configuración de políticas: antivirus y HIPS	Crear políticas antivirus y HIPS Duplicar políticas antivirus y HIPS Cambiar el nombre de políticas antivirus y HIPS Editar políticas antivirus y HIPS Restaurar la configuración predeterminada de políticas antivirus y HIPS Eliminar políticas antivirus y HIPS Añadir o eliminar entradas de la lista de amenazas

Permiso	Tareas
Configuración de políticas: restricción de aplicaciones	Crear políticas de restricción de aplicaciones Duplicar políticas de restricción de aplicaciones Cambiar el nombre de políticas de restricción de aplicaciones Modificar políticas de restricción de aplicaciones Restaurar la configuración predeterminada de la restricción de aplicaciones Eliminar políticas de restricción de aplicaciones
Configuración de políticas: control de datos	Crear políticas de control de datos Duplicar políticas de control de datos Cambiar el nombre de políticas de control de datos Modificar políticas de control de datos Restaurar la configuración predeterminada del control de datos Eliminar políticas de control de datos
Configuración de políticas: control de dispositivos	Crear políticas de control de dispositivos Duplicar políticas de control de dispositivos Cambiar el nombre de políticas de control de dispositivos Modificar políticas de control de dispositivos Restaurar la configuración predeterminada del control de dispositivos Eliminar políticas de control de dispositivos
Configuración de políticas: cortafuegos	Crear políticas cortafuegos Duplicar políticas cortafuegos Cambiar el nombre de políticas cortafuegos Modificar políticas cortafuegos Restaurar la configuración predeterminada del cortafuegos Eliminar políticas cortafuegos
Configuración de políticas: parches	Crear políticas de parches Duplicar políticas de parches Cambiar el nombre de políticas de parches Modificar políticas de parches Restaurar la configuración predeterminada de parches Eliminar políticas de parches

Permiso	Tareas
Configuración de políticas: protección contra manipulaciones	Crear políticas de protección contra manipulaciones Duplicar políticas de protección contra manipulaciones Cambiar el nombre de políticas de protección contra manipulaciones Editar políticas de protección contra manipulaciones Restaurar la configuración de la protección contra manipulaciones Eliminar políticas de protección contra manipulaciones
Configuración de políticas: actualización	Crear políticas de actualización Duplicar políticas de actualización Cambiar el nombre de políticas de actualización Editar políticas de actualización Restaurar la configuración de la actualización predeterminada Eliminar políticas de actualización Crear suscripciones Editar suscripciones Cambiar el nombre de suscripciones Duplicar suscripciones Eliminar suscripciones Configurar gestores de actualización
Configuración de políticas: control web	Crear políticas de control web Duplicar políticas de control web Cambiar el nombre de políticas de control web Modificar políticas de control web Restaurar la configuración predeterminada del control web Eliminar políticas de control web
Configuración de políticas: prevención de vulnerabilidades	Crear una política de prevención de vulnerabilidades Duplicar una política de prevención de vulnerabilidades Cambiar el nombre de una política de prevención de vulnerabilidades Editar una política de prevención de vulnerabilidades Añadir una exclusión de prevención de vulnerabilidades Eliminar una exclusión de prevención de vulnerabilidades Restablecer una política de prevención de vulnerabilidades Eliminar una política de prevención de vulnerabilidades

Permiso	Tareas
Remediación: limpieza	Limpiar elementos detectados Quitar alertas Quitar errores
Remediación: actualización y escaneado	Actualizar ordenadores al instante Realizar escaneados remotos Imponer la política del grupo a equipos Hacer que el gestor cumpla con la configuración Hacer que el gestor de actualice de forma inmediata
Configuración de informes	Crear, editar y borrar informes
Administración delegada	Crear roles Cambiar el nombre de roles Borrar roles Modificar permisos de roles Añadir usuarios o grupos a roles Eliminar usuarios o grupos de roles Administración de subentornos: crear subentornos, cambiar el nombre de subentornos; eliminar subentornos; añadir grupos raíz de subentornos; eliminar grupos raíz de subentornos; añadir usuarios o grupos a subentornos; eliminar usuarios o grupos de subentornos
Configuración del sistema	Modificar y probar la configuración del servidor SMTP; modificar los destinatarios de alertas de email Configurar los niveles de aviso y críticos del panel de control Configurar informes: configurar el purgado de alertas de la base de datos, configurar el nombre de la empresa que aparece en los informes Configurar los informes para Sophos: activar o desactivar los informes para Sophos; modificar el nombre de usuario; modificar la dirección de email de contacto Configurar el uso de los paquetes de software de versión fija
Eventos web	Visualizador de eventos web Eventos web en los detalles del ordenador

4.1.13 Uso de Enterprise Console por otro usuario

Los miembros del grupo Full Administrators de Sophos tienen acceso total a Enterprise Console.

Si lo desea, puede permitir que otros usuarios utilicen Enterprise Console. Para abrir Enterprise Console, los usuarios deben:

- pertenecer al grupo Sophos Console Administrators,
- estar asignados, como mínimo, a un rol de Enterprise Console,
- estar asignados, como mínimo, a un subentorno de Enterprise Console.

Si desea asignar a un usuario al grupo Sophos Console Administrators, utilice las herramientas de Windows para añadirlo al grupo.

Para asignar a un usuario a un rol de Enterprise Console o subentorno, en el menú **Herramientas**, haga clic en **Administrar roles y subentornos**. Para más información sobre roles y subentornos, consulte Administrar roles y subentornos (página 13).

Para utilizar una Enterprise Console adicional o remota, los usuarios deben:

- Pertenecer al grupo Sophos Console Administrators en el servidor en el que está instalado el servidor de administración de Enterprise Console.
- Pertenecer al grupo Distributed COM Users en el servidor en el que está instalado el servidor de administración de Enterprise Console. (El grupo Distributed COM Users está ubicado en el contenedor Builtin de la herramienta Usuarios y equipos de Active Directory.)
- estar asignados, como mínimo, a un rol de Enterprise Console,
- estar asignados, como mínimo, a un subentorno de Enterprise Console.

4.2 Crear y usar grupos

Debe crear grupos y adjudicarles ordenadores antes de proteger y administrar los equipos.

4.2.1 Para qué son los grupos

El uso de grupos le permitirá:

- Actualizar ordenadores de grupos diferentes desde fuentes diferentes o a diferentes horas.
- Usar políticas antivirus y HIPS, de restricción de aplicaciones, cortafuegos y otras políticas para diferentes grupos.
- Administrar sus estaciones de forma más sencilla.

Sugerencia
Puede crear grupos dentro de otros grupos y aplicar un grupo de políticas diferente a cada grupo o subgrupo.

4.2.2 Qué es un grupo

Un grupo

es una carpeta que contiene cierto número de ordenadores.

Los grupos se pueden crear o importar desde los contenedores de Active Directory, con o sin equipos, para utilizarlos como grupos de equipos de Enterprise Console. También puede configurar

la sincronización con Active Directory para que los equipos y contenedores nuevos, además de cualquier otro cambio en Active Directory, se copien en Enterprise Console de forma automática.

Cada grupo puede disponer de su propia configuración antivirus y HIPS, de actualización, cortafuegos, etc. Generalmente, todos los ordenadores de un grupo usan estos parámetros de configuración, que constituyen una "política".

Un grupo puede contener subgrupos.

4.2.3 Qué hay en el grupo No asignados

El grupo **No asignados** es donde Enterprise Console pone los ordenadores antes de que los asigne a los grupos.

No es posible:

- Aplicar políticas al grupo **No asignados**.
- Crear subgrupos en el grupo **No asignados**.
- Mover o borrar el grupo **No asignados**.

4.2.4 Crear un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para crear un grupo nuevo de equipos:

1. En el panel **Grupos** de la vista **Estaciones**, en la parte lateral izquierda, seleccione dónde desea crear el grupo.

   Haga clic en el ordenador en la parte superior si desea crear un grupo en el nivel más alto. Haga clic en un grupo existente si desea crear un subgrupo.
2. En la barra de herramientas, haga clic en el icono **Crear grupo**.
   Un "Nuevo grupo" se añadirá a la lista y se destacará su nombre.
3. Escriba un nombre para el grupo.

Las políticas de actualización, antivirus y HIPS, restricción de aplicaciones, cortafuegos, parchers, control de datos, control de dispositivos, protección contra manipulaciones y control web se aplican al grupo nuevo de forma automática. Puede editar estas políticas o aplicar otras políticas. Consulte Editar políticas (página 30) o Asignar una política a un grupo (página 30).

Nota
Los subgrupos tomarán inicialmente la configuración del grupo al que pertenecen.

4.2.5 Añadir ordenadores a un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Seleccione los ordenadores que desea añadir al grupo. Por ejemplo, abra el grupo **No asignados** y seleccione los ordenadores que desee.
2. Arrastre los ordenadores hasta el nuevo grupo.

Si mueve ordenadores no protegidos desde el grupo **No asignados** a un grupo con actualización automática, se iniciará un asistente para la protección de los nuevos ordenadores.

Si cambia ordenadores de grupo, utilizarán las mismas políticas que los ordenadores incluidos en el nuevo grupo.

4.2.6 Borrar ordenadores de un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede eliminar ordenadores de un grupo, por ejemplo, si desea eliminar entradas de equipos que ya no están en la red.

Importante
Si borra ordenadores que todavía están en la red, ya no aparecerán en la consola ni serán administrados por ella.

Si se ha actualizado desde una versión anterior de Enterprise Console y tiene ordenadores que están cifrados con el cifrado completo de discos administrado por Enterprise Console heredado, no elimine estos ordenadores de la consola. La recuperación del cifrado puede no ser posible en este caso.

Para borrar ordenadores:

1. Seleccione los ordenadores que desee borrar.
2. Haga clic con el botón derecho del ratón y seleccione **Borrar**.

Si desea ver los equipos otra vez, haga clic en el icono de **Detectar ordenadores** de la barra de herramientas. Estos ordenadores no aparecerán como gestionados hasta que se reinicien.

4.2.7 Cortar y pegar grupos

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Seleccione el grupo que desea mover. Seleccione **Cortar** en el menú **Edición**.
2. Seleccione la ubicación donde desea ponerlo. Seleccione **Pegar** en el menú **Edición**.

4.2.8 Eliminar un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Los ordenadores que formaban parte de un grupo borrado serán colocados en el grupo **No asignados.**

1. Seleccione el grupo que desee borrar.
2. Haga clic con el botón derecho del ratón y seleccione **Borrar**. Cuando se le pida, confirme que desea eliminar el grupo y los subgrupos, si existen.

4.2.9 Cambiar el nombre de un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Seleccione el grupo que desee modificar.
2. Haga clic con el botón derecho del ratón y seleccione **Cambiar nombre**.

4.2.10 Comprobar qué políticas usa un grupo

Para ver qué políticas se han asignado a un grupo:

- En el panel **Grupos**, haga clic con el botón derecho del ratón en el grupo. Seleccione **Ver/editar políticas del grupo**.

  En el cuadro de diálogo de detalles del grupo, verá las políticas que están siendo utilizadas.

4.3 Crear y usar políticas

Una política es el conjunto de normas y opciones de configuración que rigen cada grupo.

Al instalar Enterprise Console, se crean políticas predeterminadas que proporcionan un nivel básico de seguridad. Estas políticas se aplican a cada grupo nuevo. Es posible modificar las políticas predeterminadas o crear políticas nuevas.

Nota
Las funciones que no se incluyan en su licencia no estarán disponibles.

Puede crear más de una política de cada tipo.

Puede aplicar la misma política a más de un grupo.

4.3.1 ¿Qué políticas están disponibles?

Nota
Las funciones que no se incluyan en su licencia no estarán disponibles.

- La política de **actualización** define la configuración de actualización de nuevo software de seguridad.
- La política **antivirus y HIPS** especifica las opciones de escaneado y limpieza de virus, troyanos, gusanos, programas espía y publicitarios, aplicaciones no deseadas, y comportamientos y archivos sospechosos.
- La política de **restricción de aplicaciones** permite especificar los tipos de aplicaciones que desea bloquear en su red.
- La política **cortafuegos** establece la configuración del cortafuegos en las estaciones de la red.

- La política de **control de datos** especifica reglas para el control o restricción de la transferencia de archivos según el contenido, nombre o tipo de archivo.
- La política de **control de dispositivos** especifica qué dispositivos de almacenamiento y red no están autorizados para el uso en las estaciones.
- La política de **parches** indica la frecuencia con la que se comprueba los parches instalados en las estaciones.
- La política de **protección contra manipulaciones** especifica la contraseña que permite a los usuarios autorizados modificar la configuración, desactivar o desinstalar el software de seguridad de Sophos.
- La política de **control web** permite restringir los sitios web a los que se permite el acceso. El usuario recibirá un mensaje de notificación ante sitios web bloqueados o no recomendados.
- La política **Prevención de vulnerabilidades** especifica las aplicaciones, las funciones y los procesos que están protegidos contra la explotación de vulnerabilidades, como la protección de archivos de documentos del ransomware (CryptoGuard) o la protección de funciones críticas de los navegadores web (Navegación segura).

4.3.2 Políticas predeterminadas

Cuando instale Enterprise Console, se crearán políticas predeterminadas.

Nota
Las funciones que no se incluyan en su licencia no estarán disponibles.

Política de actualización

La política de actualización predeterminada en una instalación nueva de Enterprise Console proporciona:

- Actualización automática de los equipos cada 10 minutos desde la ubicación predeterminada. La ubicación predeterminada es una unidad compartida UNC `\\<ordenador>\SophosUpdate`, siendo éste el equipo en el que está instalado el gestor de actualización.

Política antivirus y HIPS

La política antivirus y HIPS predeterminada en una instalación nueva de Enterprise Console proporciona:

- Escaneado en acceso de virus, troyanos, gusanos, programas espía y otras aplicaciones potencialmente no deseadas (pero no archivos sospechosos).
- Detección de desbordamientos de búfer, comportamientos maliciosos y sospechosos de programas en ejecución en el sistema y tráfico de red malicioso.
- Bloqueo de sitios web que albergan programas maliciosos.
- Escaneado de contenidos descargados de Internet.
- Alertas de seguridad en el escritorio del ordenador afectado y entrada correspondiente en el registro de sucesos.

Para la lista completa de la configuración predeterminada de la política antivirus y HIPS en una instalación nueva de Enterprise Console, consulte el artículo 27267 de la base de conocimiento.

Política de restricción de aplicaciones

Por defecto no se bloquea ninguna aplicación. El escaneado en acceso de aplicaciones que desea restringir en la red está desactivado.

Política cortafuegos

Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Antes de utilizarlo en la red, configúrelo para permitir las aplicaciones que desea utilizar. Consulte Configurar una política básica del cortafuegos (página 106).

Para ver la lista completa de configuración predeterminada del cortafuegos, vea el artículo 57757 en la base de conocimiento de Sophos.

Política de control de datos

Por defecto, el control de datos está desactivado y no existen reglas para el control o para la restricción de transferencias de archivos a través de Internet o a dispositivos de almacenamiento.

Política de control de dispositivos

Por defecto, el control de dispositivos está desactivado y se permiten todos los dispositivos.

Política de parches

Por defecto, el control de parches se encuentra desactivado. En políticas nuevas, el control de parches se encuentra activado. Al activar el control de parches en las estaciones, se realiza de inmediato la comprobación inicial, para luego realizar comprobaciones periódicas según el intervalo establecido (por defecto, a diario).

Política de protección contra manipulaciones

Por defecto, la protección contra manipulaciones se encuentra desactivada y no se requiere una contraseña adicional para que los usuarios autorizados puedan modificar la configuración, desactivar y desinstalar el software de seguridad de Sophos.

Política de control web

Por defecto, el control web se encuentra desactivado, por lo que se permite el acceso a todos los sitios web que no estén restringidos en Enterprise Console. Consulte Protección web (página 95).

Política de prevención de vulnerabilidades

Por defecto, la prevención de vulnerabilidades está activada. Consulte Política de prevención de vulnerabilidades (página 172).

4.3.3 ¿Es necesario crear políticas propias?

Cuando instale Enterprise Console, se crearán políticas "predeterminadas". Estas políticas se aplican a cada grupo nuevo.

Las políticas predeterminadas ofrecen un nivel básico de seguridad, pero es necesario crear políticas nuevas o cambiar las políticas predeterminadas para poder utilizar funciones como el control de acceso a la red o la restricción de aplicaciones.

Nota
Cuando modifica la política predeterminada, el cambio se aplica a las políticas nuevas que cree.

Nota
Si utiliza administración delegada, necesitará el permiso de **Configuración de políticas** correspondiente para crear o editar una política. Por ejemplo, para crear o editar una política antivirus y HIPS, es necesario tener el derecho **Configuración de políticas: antivirus y HIPS**. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Política de actualización

La política de actualización predeterminada hace que las estaciones actualicen la suscripción recomendada del software cada 10 minutos desde la ubicación de actualización compartida predeterminada. Para modificar la suscripción, ubicación de actualización u otras opciones de configuración, consulte Configurar la política de actualización (página 65).

Antivirus y HIPS

La política antivirus y HIPS predeterminada protege los equipos contra virus y otros programas maliciosos. Sin embargo, debe crear nuevas políticas, o modificar la predeterminada, para detectar aplicaciones no deseadas o elementos sospechosos. Consulte Política antivirus y HIPS (página 75).

Restricción de aplicaciones

Para definir las aplicaciones no autorizadas, configure políticas de restricción de aplicaciones como se describe en Política de restricción de aplicaciones (página 135).

Política cortafuegos

Para permitir el acceso a aplicaciones a la red, configure políticas cortafuegos como se describe en Política cortafuegos (página 106).

Control de datos

Por defecto, el control de datos está desactivado. Para evitar la salida accidental de datos, configure políticas de control de datos como se describe en Política de control de datos (página 138).

Control de dispositivos

Por defecto, el control de dispositivos está desactivado. Para controlar el uso de dispositivos, configure políticas de control de dispositivos como se describe en Política de control de dispositivos (página 153).

Parches

Por defecto, el control de parches se encuentra desactivado. En políticas nuevas, el control de parches se encuentra activado. Al activar el control de parches en las estaciones, se realiza de inmediato la comprobación inicial, para luego realizar comprobaciones periódicas según el intervalo establecido (por defecto, a diario). Para activar o desactivar el control de parches, o modificar el intervalo de comprobación, configure la política de parches como se describe en Política de parches (página 163).

Protección contra manipulaciones

Por defecto, la protección contra manipulaciones está desactivada. Para disponer de protección contra manipulaciones, configure políticas de protección contra manipulaciones como se describe en Política de protección contra manipulaciones (página 160).

Control web

Por defecto, el control web está desactivado. Para ver cómo activarlo y configurarlo, consulte Política de control web (página 165).

Prevención de vulnerabilidades

Por defecto, la prevención de vulnerabilidades está activada. Para configurar políticas de prevención de vulnerabilidades, consulte Política de prevención de vulnerabilidades (página 172).

4.3.4 Crear políticas

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para crear una política:

1. En el panel **Políticas** de la vista **Estaciones**, haga clic con el botón derecho en el tipo de política que desea crear, por ejemplo, "Actualización" y seleccione **Crear política**.
   Una "Nueva política" se añadirá a la lista y se destacará su nombre.
2. Escriba un nombre para la política.
3. Haga doble clic en la nueva política. Introduzca los parámetros que desee.

   Para más información sobre qué configuración elegir, consulte la sección sobre la configuración de la política correspondiente.

Ha creado una política y ya puede ser aplicada a un grupo.

4.3.5 Asignar una política a un grupo

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En el panel **Políticas**, seleccione la política.
2. Haga clic en la política y arrástrela al grupo al que desea aplicar la política. Confirme que desea continuar.

Nota
Si lo prefiere, haga clic con el botón derecho del ratón en el grupo y seleccione **Ver/editar políticas del grupo**. A continuación, puede seleccionar las políticas para ese grupo desde los menús desplegables.

4.3.6 Editar políticas

Si utiliza administración delegada:

- Necesitará el permiso **Configuración de políticas** correspondiente para realizar esta tarea.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para editar una política de un grupo:

1. En el panel **Políticas**, haga doble clic sobre la política que desea modificar.
2. Edite los parámetros de configuración.

Para más información sobre cómo configurar diferentes políticas, consulte las secciones correspondientes.

4.3.7 Cambiar el nombre de una política

Si utiliza administración delegada:

- Necesitará el permiso **Configuración de políticas** correspondiente para realizar esta tarea.
- No es posible cambiar el nombre de las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Nota
No puede cambiar el nombre de una política "Predeterminada".

Para cambiar el nombre de una política:

1. En el panel **Políticas**, seleccione la política cuyo nombre desea cambiar.
2. Haga clic con el botón derecho y seleccione **Cambiar nombre de la política**.

4.3.8 Borrar políticas

Si utiliza administración delegada:

- Necesitará el permiso **Configuración de políticas** correspondiente para realizar esta tarea.
- No es posible borrar políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Nota
No puede borrar una política "Predeterminada".

Para borrar una política:

1. En el panel **Políticas**, haga clic con el botón derecho en la política que desea borrar y seleccione **Borrar política**.
2. Cualquier grupo que use la política que ha borrado pasará a utilizar la política predeterminada.

4.3.9 Comprobar qué grupos utilizan una política

Para comprobar qué grupos comparten la misma política:

- En el panel **Políticas**, haga clic con el botón derecho del ratón en la política y seleccione **Ver grupos con esta política**.

  Aparecerá una lista con los grupos que utilizan esa política.

4.3.10 Comprobar que los ordenadores utilizan la política del grupo

Si lo desea, puede comprobar si todos los equipos de un grupo cumplen las políticas del mismo.

1. Seleccione el grupo que desea comprobar.
2. En la vista **Estaciones** de la lista de ordenadores, en la ficha **Estado**, observe la columna **Cumplimiento de políticas**.
   - Los equipos que indican "Igual que la política" cumplen las políticas del grupo.
   - Si aparece un icono de aviso amarillo que indica "Diferente de la política", el equipo no utiliza la misma política que el resto de equipos del grupo.

   Para más información sobre el estado de las funciones de seguridad del equipo y las políticas aplicadas, consulte la ficha correspondiente de la vista **Estaciones**, por ejemplo, la ficha **Detalles antivirus**.

Si quiere que los equipos cumplan las políticas de los grupos a los que pertenecen, consulte Imponer el uso de la política del grupo (página 32).

4.3.11 Imponer el uso de la política del grupo

Si utiliza administración delegada, necesitará el permiso **Remediación: actualización y escaneado** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si encuentra equipos que no cumplen las políticas del grupo, puede aplicárselas.

1. Seleccione los ordenadores que no cumplen la política del grupo.
2. Haga clic con el botón derecho del ratón y seleccione **Cumplir con**. Después, seleccione el tipo de política adecuado, por ejemplo, **Política antivirus y HIPS del grupo**.

4.4 Detectar ordenadores en la red

Para administrar los equipos de la red desde Enterprise Console, primero debe añadirlos a Enterprise Console. Puede utilizar las opciones de la función "Detectar ordenadores" para buscar ordenadores en red y añadirlos a Enterprise Console. Existen varias opciones:

- Importar contenedores y equipos de Active Directory (página 32)
- Detectar ordenadores en Active Directory (página 33)
- Detectar ordenadores en la red (página 33)
- Detectar ordenadores en un rango IP (página 34)
- Importar nombres de ordenadores (página 34)

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para añadir equipos a la consola. Para obtener más información, consulte Administrar roles y subentornos (página 13).

4.4.1 Importar contenedores y equipos de Active Directory

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Al importar grupos de Active Directory se obtiene la estructura de contenedores de Active Directory y se copia en Enterprise Console como una estructura de grupos de ordenadores. Si lo desea, puede importar sólo la estructura de grupos o también los ordenadores en cada grupo. Si opta por la segunda opción, los ordenadores encontrados en Active Directory se colocan en su grupo correspondiente, en lugar de colocarse en el grupo **No asignados**.

Enterprise Console podrá disponer tanto de grupos importados desde Active Directory como de los grupos creados de forma manual. Los grupos importados desde Active Directory también se pueden sincronizar.

Para importar grupos desde Active Directory:

1. En la barra de herramientas, haga clic en **Detectar ordenadores**.
2. En el cuadro de diálogo **Detectar ordenadores**, en el panel **Importar desde Active Directory**, seleccione **Importar** y haga clic en **Aceptar**.

   Si lo prefiere, seleccione un grupo al que quiera importar los contenedores de Active Directory, haga clic con el botón derecho y seleccione **Importar desde Active Directory**.

Se iniciará el **Asistente para importar desde Active Directory**.

3. Siga las instrucciones del asistente. En la página para seleccionar qué importar, seleccione **Ordenadores y contenedores** o **Sólo contenedores**, dependiendo de lo que desee importar.

Tras importar los contenedores de Active Directory, aplique las políticas correspondientes. Consulte ¿Qué políticas están disponibles? (página 25).

Tras aplicar las políticas a los grupos, podrá sincronizar los grupos con Active Directory. Para más información, consulte Sincronizar con Active Directory (página 35).

4.4.2 Detectar ordenadores en Active Directory

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede usar Active Directory para buscar ordenadores y añadirlos al grupo **No asignados**.

1. En la barra de herramientas, haga clic en **Detectar ordenadores**.
2. En el cuadro de diálogo **Detectar ordenadores**, seleccione **Detectar en Active Directory** y haga clic en **Aceptar**.
3. Deberá introducir un nombre de usuario y una contraseña. Esto será necesario si dispone de ordenadores que requieren cuenta de acceso (por ejemplo, Windows XP Service Pack 2).

   La cuenta debe ser de administrador de dominio o debe disponer de todos los derechos administrativos sobre los equipos XP.

   Si utiliza una cuenta de dominio, *debe* introducir el nombre de usuario en la forma dominio\usuario.
4. En el cuadro de diálogo **Detectar ordenadores**, seleccione los dominios en los que desea realizar la búsqueda. Haga clic en **Aceptar**.
5. Haga clic en el grupo **No asignados** para ver los ordenadores localizados.

Para administrar dichos ordenadores, ubíquelos en algún grupo (puede hacerlo con "arrastrar y soltar").

4.4.3 Detectar ordenadores en la red

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para añadir al grupo **No asignados** una lista de los ordenadores encontrados en los dominios y grupos de trabajo de Windows:

1. En la barra de herramientas, haga clic en **Detectar ordenadores**.
2. En el cuadro de diálogo **Detectar ordenadores**, seleccione **Detectar en la red** y haga clic en **Aceptar**.
3. En el cuadro de diálogo **Credenciales**, introduzca el nombre de usuario y la contraseña de una cuenta con permisos suficientes para obtener información de equipos.

   La cuenta debe ser de administrador de dominio o debe disponer de todos los derechos administrativos sobre los equipos. Si utiliza una cuenta de dominio, *debe* introducir el nombre de usuario en la forma dominio\usuario.

   Si puede acceder a los ordenadores sin datos de cuenta, ignore este paso.
4. En el cuadro de diálogo **Detectar ordenadores**, seleccione los dominios o grupos de trabajo en los que desea realizar la búsqueda. Haga clic en **Aceptar**.

5. Haga clic en el grupo **No asignados** para ver los ordenadores localizados.

Para administrar dichos ordenadores, ubíquelos en algún grupo (puede hacerlo con "arrastrar y soltar").

4.4.4 Detectar ordenadores en un rango IP

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede usar un rango de direcciones IP para buscar ordenadores y añadirlos al grupo **No asignados**.

Nota
No es posible utilizar direcciones IPv6.

1. En la barra de herramientas, haga clic en **Detectar ordenadores**.
2. En el cuadro de diálogo **Detectar ordenadores**, seleccione **Detectar en un rango IP** y haga clic en **Aceptar**.
3. En el cuadro de diálogo **Credenciales**, deberá introducir un nombre de usuario y una contraseña. Esto será necesario si dispone de ordenadores que requieren cuenta de acceso (por ejemplo, Windows XP Service Pack 2).

   La cuenta debe ser de administrador de dominio o debe disponer de todos los derechos administrativos sobre los equipos XP.

   Si utiliza una cuenta de dominio, *debe* introducir el nombre de usuario en la forma dominio\usuario.

   En el panel **SNMP**, introduzca el nombre de la comunidad SNMP.
4. En el cuadro de diálogo **Detectar ordenadores**, introduzca el **Inicio del rango IP** y el **Fin del rango IP**. Haga clic en **Aceptar**.
5. Haga clic en el grupo **No asignados** para ver los ordenadores localizados.

Para administrar dichos ordenadores, ubíquelos en algún grupo (puede hacerlo con "arrastrar y soltar").

4.4.5 Importar nombres de ordenadores

Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para que Enterprise Console muestre sus ordenadores, puede importar los nombre de los ordenadores desde un archivo. Puede crear el archivo usando entradas de la siguiente manera:

```
[Grupo1]
 Dominio1|Windows7|Equipo1
 Dominio1|Windows2008ServerR2|Equipo2
```

Nota
No es necesario especificar en qué grupo se colocarán los ordenadores. Si utiliza [ ] (sin espacio entre los corchetes) como nombre del grupo, los equipos se colocarán en el grupo **No asignados**.

Los nombres de sistema operativo válidos son: WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, Windows2008ServerR2, Windows8, WindowsServer2012, Windows81, WindowsServer2012R2, Windows10, WindowsServer2016, MACOSX, Linux, y Unix.

El nombre de dominio y el sistema operativo son opcionales. De modo que una entrada puede tener este aspecto:

```
[Grupo1]
 Equipo1
```

Puede importar nombres de ordenadores de la siguiente manera:

1. En el menú **Archivo**, haga clic en **Importar nombres de ordenadores**.
2. En la ventana de examinar, seleccione el archivo.
3. Haga clic en el grupo **No asignados** para ver los ordenadores localizados.
4. Para administrar dichos ordenadores, ubíquelos en algún grupo (puede hacerlo con "arrastrar y soltar").

4.5 Sincronizar con Active Directory

En esta sección se describe la sincronización con Active Directory.

Ventajas de la sincronización con Active Directory

La sincronización con Active Directory permite mantener la estructura de los grupos de Enterprise Console según los contenedores de Active Directory. Los nuevos ordenadores y contenedores detectados en Active Directory se añadirán de forma automática a Enterprise Console. También es posible proteger de forma automática nuevos ordenadores Windows. De esta forma, los ordenadores estarán menos tiempo expuestos a infecciones y resultará más sencillo organizarlos y protegerlos.

Nota
No se protegerán de forma automática ordenadores con servidores Windows, Mac, Linux o UNIX. Deberá proteger estos ordenadores de forma manual.

Junto con la sincronización automática puede disponer de notificación por email de los nuevos ordenadores y contenedores añadidos durante cada sincronización. Si activa la protección automática de los grupos de Enterprise Console sincronizados, también puede recibir notificación ante fallos de protección.

Funcionamiento de la sincronización con Active Directory

En Enterprise Console puede disponer de grupos "normales" no sincronizados y grupos sincronizados con Active Directory.

Al crear la sincronización, deberá establecer un punto de sincronización en Enterprise Console y seleccionar el contenedor correspondiente de Active Directory. Todos los ordenadores y subgrupos en el contenedor de Active Directory se copiarán en Enterprise Console y se mantendrán sincronizados.

Nota
Para más información sobre los puntos de sincronización, consulte el apartado Punto de sincronización (página 37) Para más información sobre los grupos sincronizados, consulte el apartado Grupo sincronizado (página 37).

Enterprise Console mantendrá la estructura de grupos sincronizada con el contenedor de Active Directory. Esto quiere decir que:

- Si se añade un ordenador al contenedor de Active Directory, también aparecerá en Enterprise Console.
- Si se elimina o mueve un ordenador en Active Directory, el ordenador pasará al grupo **No asignados** de Enterprise Console.

Nota
Cuando un ordenador pasa al grupo **No asignados**, no recibirá nuevas políticas.

- Si un ordenador se mueve entre contenedores sincronizados, pasará al grupo correspondiente en Enterprise Console.
- Si algún ordenador ya existe en Enterprise Console y luego forma parte de un grupo sincronizado, el ordenador pasará al grupo sincronizado correspondiente.
- Cuando un ordenador cambia de grupo, se le aplicarán las políticas de dicho grupo.

Por defecto, la sincronización se realiza cada 60 minutos. Si lo desea, puede cambiar el intervalo de sincronización.

Planificar la sincronización

Debe decidir qué grupos desea sincronizar con Active Directory y cuántos puntos de sincronización quiere tener. Tendrá que tener en cuenta el tamaño de los grupos a sincronizar y cómo mejorar su administración. La implementación de software, el escaneado y la limpieza de equipos debe resultar sencilla. Esto es importante, sobre todo, para la implementación inicial.

Nota
Si tiene un estructura de Active Directory compleja y desea sincronizar grupos locales del dominio o grupos de Active Directory anidados, consulte el artículo de la base de conocimiento 122529 para obtener información sobre cómo activar esta función.

Se recomienda que:

1. Importe la estructura de grupos (sin los ordenadores), mediante la función **Importar desde Active Directory**. Para más información, vea el apartado Importar contenedores y equipos de Active Directory (página 32).
2. Revise la estructura y decida los puntos de sincronización.
3. Establezca las políticas de los grupos. Para más información, consulte Crear políticas (página 29) y Asignar una política a un grupo (página 30).

4. Sincronice los puntos de sincronización, de uno en uno, con Active Directory. Para más información, vea el apartado: Sincronizar con Active Directory (página 37).

4.5.1 Punto de sincronización

Un *punto de sincronización* es un grupo de Enterprise Console que coincide con un contenedor (o rama) de Active Directory. Un punto de sincronización puede contener grupos importados desde Active Directory.

En el panel **Grupos**, los puntos de sincronización se muestran de la siguiente manera:

Es *posible* mover, cambiar el nombre y borrar puntos de sincronización. También es posible modificar las políticas y opciones de sincronización de los puntos de sincronización.

No es posible crear o borrar subgrupos dentro de un punto de sincronización, ni mover aquí otros grupos. Tampoco se pueden mover ordenadores a o desde un punto de sincronización.

4.5.2 Grupo sincronizado

Un *grupo sincronizado* es un subgrupo de un punto de sincronización, importado desde Active Directory.

En el panel **Grupos**, los grupos sincronizados se muestran de la siguiente manera:

Es *posible* modificar las políticas asignadas a los grupos sincronizados.

No es posible cambiar ninguna otra opción de los grupos sincronizados. No se puede mover, cambiar el nombre ni borrar grupos sincronizados. Tampoco se pueden mover ordenadores o grupos a o desde los grupos sincronizados. No se pueden crear ni borrar subgrupos en los grupos sincronizados. Tampoco se pueden modificar las opciones de sincronización de los grupos sincronizados.

4.5.3 Sincronizar con Active Directory

Antes de realizar esta tarea:

- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos**. Para obtener más información, consulte Administrar roles y subentornos (página 13).
- Si desea proteger de forma automática los ordenadores que se añadan a los grupos sincronizados, prepare los ordenadores como se describe en Preparar la instalación del software de seguridad (página 42).
- Si tiene un estructura de Active Directory compleja y desea sincronizar grupos locales del dominio o grupos de Active Directory anidados, active esta función como se describe en el artículo de la base de datos 122529.

Para sincronizar con Active Directory:

1. Seleccione el grupo que será el punto de actualización, haga clic con el botón derecho del ratón y seleccione **Sincronizar con Active Directory**.
   Se iniciará el **Asistente de sincronización con Active Directory**.

2. En la página **Resumen** del asistente, haga clic en **Siguiente**.
3. En la página **Seleccione un grupo de Sophos Enterprise Console**, seleccione o cree el grupo de Enterprise Console a sincronizar con Active Directory (punto de sincronización). Haga clic en **Siguiente**.
4. En la página **Seleccione un contenedor de Active Directory**, podrá especificar el contenedor de Active Directory desde el que desea sincronizar ordenadores y subgrupos. Escriba el nombre del contenedor (por ejemplo, LDAP://CN=ordenador,DC=dominio,DC=local) o haga clic en **Examinar** para localizar el contenedor deseado en Active Directory. Haga clic en **Siguiente**.

   Importante
   Si algún ordenador pertenece a más de un contenedor de Active Directory sincronizado, causará problemas y se sucederán los mensajes entre el ordenador y Enterprise Console. Cada ordenador sólo debe aparecer una vez en Enterprise Console.

5. Si desea proteger de forma automática nuevas estaciones con Windows, en la página **Proteger ordenadores automáticamente**, active la opción **Instalar automáticamente el software de Sophos** y seleccione el software que desea instalar.

   Nota
   Consulte la página de requisitos del sistema en el sitio web de Sophos (http://www.sophos.com/es-es/products/all-system-requirements.aspx).

   - Antes de instalar el **cortafuegos** en los equipos, configure el cortafuegos para permitir el tráfico, las aplicaciones y los procesos necesarios. Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Consulte Política cortafuegos (página 106).
   - Deje seleccionada la opción **Eliminar software de seguridad de terceros** si quiere que se eliminen automáticamente los programas de terceros. Si necesita eliminar alguna herramienta de actualización de terceros, vea Eliminar software de seguridad de terceros (página 42).

   Todas las estaciones con Windows que se encuentren durante ésta y posteriores sincronizaciones se protegerán de forma automática, de acuerdo a las respectivas políticas de grupo.

   Importante
   No se protegerán de forma automática ordenadores con servidores Windows, Mac, Linux o UNIX. Proteja dichos ordenadores de forma manual según se describe en la *Guía avanzada de inicio de Sophos Enterprise Console*.

   Nota
   Puede activar o desactivar la protección automática más tarde en el cuadro de diálogo **Opciones de sincronización**. Para más información, consulte Opciones de sincronización (página 40).

   Haga clic en **Siguiente**.
6. Si activó la opción de protección automática, en la página **Introduzca las credenciales de Active Directory**, especifique una cuenta con derechos de administrador que permita instalar el software en los ordenadores de la red. Haga clic en **Siguiente**.
7. En la página **Seleccione el intervalo de sincronización**, indique la frecuencia de las sincronizaciones del grupo de Enterprise Console con el contenedor de Active Directory. Por defecto será cada 60 minutos.

Nota
Puede cambiar el intervalo de sincronización más tarde en el cuadro de diálogo **Opciones de sincronización**. Para más información, consulte Opciones de sincronización (página 40).

8. En la página **Confirme sus opciones**, compruebe los detalles de importación y haga clic en **Siguiente**.
9. Finalmente se mostrará un resumen de los grupos y ordenadores sincronizados.

   Si lo desea, puede recibir notificación por email de los nuevos ordenadores y grupos en cada sincronización. Si activa la protección automática de nuevos ordenadores sincronizados, también puede recibir notificación ante fallos de protección. Para abrir el cuadro de diálogo **Configuración de alertas por email** tras hacer clic en **Finalizar**, active la opción correspondiente en la última página del asistente. Para más información, consulte Alertas por email sobre la sincronización con Active Directory (página 183).

   Haga clic en **Finalizar** para salir del asistente.

4.5.4 Usar la sincronización para proteger ordenadores

Antes de realizar esta tarea:

- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos**. Para obtener más información, consulte Administrar roles y subentornos (página 13).
- Prepare los ordenadores para la instalación automática del software de seguridad como se describe en Preparar la instalación del software de seguridad (página 42).

Las estaciones Windows se pueden proteger de forma automática durante la sincronización con Active Directory.

Importante
No se protegerán de forma automática ordenadores con servidores Windows, Mac, Linux o UNIX. Proteja dichos ordenadores de forma manual según se describe en la *Guía avanzada de inicio de Sophos Enterprise Console*.

Los ordenadores de grupos sincronizados se pueden proteger de forma automática al configurar la sincronización (consulte Sincronizar con Active Directory (página 37)) o modificando las opciones de sincronización más adelante.

Estas instrucciones describen cómo proteger los ordenadores editando las opciones de sincronización.

1. En el panel **Grupos**, seleccione el grupo (punto de sincronización) en el que desea disponer de protección automática de nuevos ordenadores. Haga clic con el botón derecho del ratón y seleccione **Opciones de sincronización**.
2. En el cuadro de diálogo **Opciones de sincronización**, active la opción **Instalar automáticamente el software de Sophos** y seleccione el software que desea instalar.
   - Antes de instalar el **cortafuegos** en los equipos, configure el cortafuegos para permitir el tráfico, las aplicaciones y los procesos necesarios. Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Consulte Política cortafuegos (página 106).
   - Deje seleccionada la opción **Eliminar software de seguridad de terceros** si quiere que se eliminen automáticamente los programas de terceros. Si necesita eliminar alguna herramienta de actualización de terceros, vea Eliminar software de seguridad de terceros (página 42).

3. Especifique una cuenta de usuario con permisos para instalar el software en los ordenadores de la red. Haga clic en **Aceptar**.

Si desea desactivar la protección automática, en el cuadro de diálogo **Opciones de sincronización**, desactive la opción **Instalar automáticamente el software de Sophos**.

4.5.5 Opciones de sincronización

Antes de realizar esta tarea:

- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos**. Para obtener más información, consulte Administrar roles y subentornos (página 13).
- Si desea proteger de forma automática los ordenadores que se añadan a los grupos sincronizados, prepare los ordenadores como se describe en Preparar la instalación del software de seguridad (página 42).
- Si tiene un estructura de Active Directory compleja y desea sincronizar grupos locales del dominio o grupos de Active Directory anidados, active esta función como se describe en el artículo de la base de datos 122529.

Para ver y editar las propiedades de sincronización:

1. En el panel **Grupos**, seleccione el grupo (punto de sincronización) en el que desea ver las opciones de sincronización. Haga clic con el botón derecho del ratón y seleccione **Opciones de sincronización**.
   Aparece el cuadro de diálogo **Opciones de sincronización**.
2. En el campo **Contenedor de Active Directory**, aparece el contenedor con el que está sincronizado el grupo. Si desea sincronizar el grupo con otro contenedor, elimine la sincronización y utilice de nuevo el **Asistente de sincronización con Active Directory**. Consulte Activar o desactivar la sincronización (página 41) y Sincronizar con Active Directory (página 37).
3. En el campo **Intervalo de sincronización**, configure la frecuencia de las sincronizaciones. Por defecto será cada 60 minutos. El mínimo es 5 minutos.
4. Seleccione la casilla **Instalar automáticamente el software de Sophos** si desea proteger de forma automática todas las estaciones nuevas con Windows que se encuentren, de acuerdo con las políticas de sus respectivos grupos. La protección antivirus está seleccionada por defecto en la sección **Funciones**. Si desea instalar otros programas de seguridad de Sophos, active las casillas correspondientes. Especifique una cuenta de usuario con permisos para instalar el software en los ordenadores de la red.

Nota
Sólo las estaciones con Windows se pueden proteger de forma automática. No se protegerán de forma automática ordenadores con servidores Windows, Mac, Linux o UNIX. Proteja dichos ordenadores de forma manual según se describe en la *Guía avanzada de inicio de Sophos Enterprise Console*.

4.5.6 Sincronizar con Active Directory de forma inmediata

Antes de realizar esta tarea:

- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos**. Para obtener más información, consulte Administrar roles y subentornos (página 13).

- Si desea proteger de forma automática los ordenadores que se añadan a los grupos sincronizados, prepare los ordenadores como se describe en Preparar la instalación del software de seguridad (página 42).
- Si tiene un estructura de Active Directory compleja y desea sincronizar grupos locales del dominio o grupos de Active Directory anidados, active esta función como se describe en el artículo de la base de datos 122529.

Si lo desea, puede sincronizar los grupos de Enterprise Console con los contenedores de Active Directory de forma inmediata, sin esperar a la siguiente sincronización programada.

Para sincronizar con Active Directory de forma inmediata:

1. En el panel **Grupos**, seleccione el grupo que desea sincronizar con Active Directory. Haga clic con el botón derecho del ratón y seleccione **Opciones de sincronización**.
2. En el cuadro de diálogo **Opciones de sincronización**, seleccione las opciones necesarias y haga clic en **Aceptar**.

4.5.7 Activar o desactivar la sincronización

Antes de realizar esta tarea:

- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos**. Para obtener más información, consulte Administrar roles y subentornos (página 13).
- Si desea proteger de forma automática los ordenadores que se añadan a los grupos sincronizados, prepare los ordenadores como se describe en Preparar la instalación del software de seguridad (página 42).
- Si tiene un estructura de Active Directory compleja y desea sincronizar grupos locales del dominio o grupos de Active Directory anidados, active esta función como se describe en el artículo de la base de datos 122529.

Para activar o desactivar la sincronización con Active Directory:

- Para activar la sincronización, utilice el **Asistente de sincronización con Active Directory** como se describe en la sección Sincronizar con Active Directory (página 37).
- Para desactivar la sincronización, seleccione el grupo (punto de sincronización) en el que desee desactivar la sincronización con Active Directory, haga clic con el botón derecho del ratón y seleccione **Eliminar sincronización**. Haga clic en **Sí** para confirmar.

4.6 Configurar URL Sophos Mobile

Sophos Mobile es una solución de administración de dispositivos para dispositivos móviles como teléfonos inteligentes y tabletas. Sophos Mobile ayuda a mantener los datos corporativos seguros administrando las aplicaciones y la configuración de seguridad.

La consola web de Sophos Mobile se abre en Enterprise Console haciendo clic en el botón **Sophos Mobile** en la barra de herramientas. Para ello es necesario configurar primero la URL de Sophos Mobile.

1. En el menú **Herramientas**, haga clic en **Configurar dirección de Sophos Mobile**.
2. En el cuadro de diálogo de **URL Sophos Mobile**, introduzca la URL de la consola web de Sophos Mobile y haga clic en **Aceptar**.

5 Proteger ordenadores

Puede instalar el software de seguridad de Sophos de las siguientes formas:

- Mediante el asistente automático de protección en Enterprise Console, consulte Proteger ordenadores de forma automática (página 43).
- También puede disponer de sincronización automática con Active Directory, consulte Sincronizar con Active Directory (página 35).
- Manual en cada equipo. En Enterprise Console podrá ver la ubicación del software, consulte Ubicación de los archivos para la protección manual (página 45). A continuación, vaya al ordenador correspondiente e instale el software de seguridad manualmente.

5.1 Preparar la instalación del software de seguridad

Además de asegurarse de que los ordenadores cumplen los requisitos generales del sistema, es necesario realizar algunos pasos más para instalar el software de forma automática.

Nota
No es posible realizar la instalación automática en ordenadores Mac, Linux ni UNIX.

Si utiliza Active Directory, puede prepara las estaciones mediante objetos de directiva de grupo (GPO). Si utiliza grupos de trabajo, debe configurar las estaciones de forma local.

Para más información, consulte la *Guía de distribución de Sophos*. Para ver vídeos de despliegue, consulte el artículo de la base de conocimiento 111180.

5.2 Eliminar software de seguridad de terceros

Si desea eliminar el software de seguridad instalado previamente, siga estos pasos ANTES de seleccionar la opción **Third-Party Security Software Detection** en el **Asistente para proteger ordenadores**:

- Si los equipos cuentan con software de otros proveedores, compruebe que la interfaz está cerrada.
- Si los equipos cuentan con un cortafuegos o un producto HIPS de otro proveedor, compruebe que está desactivado o que permite la ejecución del programa de instalación de Sophos.
- Si desea desinstalar además alguna herramienta de actualización (para que no vuelva a instalar el software de forma automática), vea los pasos a continuación. Si no dispone de herramienta de actualización, puede ignorar estos pasos.

Nota
Debe reiniciar las estaciones, desde cada equipo, en las que se eliminen programas antivirus de terceros.

Nota
Es posible que HitmanPro.Alert ya esté instalado como producto independiente o desde Sophos Central. Debe eliminar HitmanPro.Alert antes de aplicar la administración local desde Sophos Enterprise Console.

Si lo equipos tienen una herramienta de actualización de otro proveedor instalada y desea eliminarla, deberá modificar el archivo de configuración antes de seleccionar la opción **Third-Party Security Software Detection** en el **Asistente para proteger ordenadores**:

Nota
Si las estaciones utilizan algún producto cortafuegos o HIPS, es posible que tenga que dejar la herramienta de actualización intacta. Vea la documentación de dicho producto para más información.

Para modificar el archivo de configuración:

1. En el directorio de instalación central, localice el archivo data.zip.
2. Extraiga el archivo crt.cfg.
3. Edite el archivo crt.cfg para cambiar la línea "RemoveUpdateTools=0" a "RemoveUpdateTools=1".
4. Guarde los cambios y copie el archivo crt.cfg donde se encuentre data.zip. No vuelva a insertar el archivo crt.cfg dentro de data.zip o perderá los cambios en la próxima actualización.

Al ejecutar el **Asistente para proteger ordenadores** y seleccionar el opción **Third-Party Security Software Detection**, se eliminarán también las herramientas de actualización del software de seguridad de terceros.

5.3 Proteger ordenadores de forma automática

Antes de proteger ordenadores desde la consola:

- Para poder proteger los ordenadores de un grupo, es necesario aplicar al grupo una política de actualización.
- Prepare los ordenadores para la instalación automática del software de seguridad como se describe en Preparar la instalación del software de seguridad (página 42).
- Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para proteger ordenadores. Para obtener más información, consulte Administrar roles y subentornos (página 13).

No es posible realizar la instalación automática en ordenadores Mac, Linux ni UNIX. Vea cómo realizar la instalación manual. Para más información, consulte la *Guía avanzada de inicio de Sophos Enterprise Console*.

Si decide sincronizar con Active Directory y proteger los ordenadores automáticamente, *no* es necesario que siga estos pasos. Para más información, consulte Sincronizar con Active Directory (página 35) y temas relacionados.

Para proteger los ordenadores de forma automática:

1. Dependiendo de si los ordenadores que desea proteger pertenecen ya a un grupo o no, siga uno de estos procedimientos:
    - Si los ordenadores que desea proteger están en la carpeta **No asignados**, arrástrelos a un grupo.

- Si los ordenadores que desea proteger ya están en un grupo, selecciónelos, haga clic con el botón derecho del ratón y seleccione **Proteger ordenadores**.

Se inicia el **Asistente para proteger ordenadores**. Siga las instrucciones del asistente.

2. En el cuadro **Seleccionar funciones**, seleccione las funciones que desee.

Nota
Consulte la página de requisitos del sistema en el sitio web de Sophos (http://www.sophos.com/es-es/products/all-system-requirements).

La protección antivirus está seleccionada por defecto y no se puede desactivar. También puede instalar las siguientes funciones: Algunas funciones sólo están disponibles si dispone de la licencia correspondiente.

- **Firewall**

  Antes de instalar el cortafuegos en los equipos, configure el cortafuegos para permitir el tráfico, las aplicaciones y los procesos necesarios. Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Consulte Política cortafuegos (página 106).

- **Patch**

- **Exploit Prevention, Sophos Clean**

  Ofrece protección contra ransomware y vulnerabilidades de seguridad. Esta opción está seleccionada por defecto si su licencia incluye esta función.

  Nota
  Si actualiza su licencia para que incluya la prevención de vulnerabilidades (con Sophos Clean), no se instala automáticamente en los equipos que ya gestiona. Necesita volver a proteger los equipos para instalarla.

- **Third-Party Security Software Detection**

  Deje seleccionada la opción **Third-Party Security Software Detection** si quiere que se eliminen automáticamente los programas de terceros. Sólo se eliminarán productos de terceros con las funciones de los productos que se dispone a instalar. Si necesita eliminar alguna herramienta de actualización de terceros, vea Eliminar software de seguridad de terceros (página 42).

3. En la página **Resumen de protección**, cualquier problema con la instalación aparecerá en la columna **Problemas de protección**. Solucione los problemas de instalación (consulte Error en la instalación de Sophos Endpoint Security and Control (página 212)) o realice la instalación de forma manual en dichos equipos (consulte la *Guía avanzada de inicio de Sophos Enterprise Console*). Haga clic en **Siguiente**.
4. En la página **Credenciales**, introduzca los datos de una cuenta que pueda utilizarse para instalar software.

   Esta cuenta suele ser una cuenta de administración de dominio. Deberá:

   - Tener derechos de administrador local para los equipos que desee proteger.
   - Poder iniciar sesión en los equipos en los que instaló el servidor de administración.
   - Derecho de lectura al **servidor primario** especificado en la política de actualización. Consulte Configurar servidores de actualización (página 66).

Nota
Si utiliza una cuenta de dominio, *debe* introducir el nombre de usuario en la forma `dominio\usuario`.

Si los equipos pertenecen a dominios diferentes dentro del mismo esquema de Active Directory, utilice la cuenta de administrador de Active Directory.

5.4 Ubicación de los archivos para la protección manual

Si Enterprise Console no puede instalar el software antivirus, el cortafuegos o el control de parches de forma automática en ciertos equipos, podrá hacerlo de forma manual.

Para ubicar los programas de instalación:

1. En el menú **Ver**, haga clic en **Ubicación de archivos de inicio**.
2. En el cuadro de diálogo **Ubicación de archivos de inicio**, aparecen las ubicaciones que contienen los programas de instalación de cada suscripción de software, además de las plataformas compatibles y las versiones del software. Anote la ubicación del programa de instalación que necesite.

Para más información sobre la instalación manual del software de seguridad en diferentes sistemas operativos, consulte la *Guía avanzada de inicio de Sophos Enterprise Console*.

5.5 Comprobar la protección de la red

Para obtener una vista general del estado de seguridad de la red, utilice el Panel de control. Para más información, consulte Paneles de control (página 4) y Configuración del panel de control (página 45).

Utilice la lista de ordenadores y sus filtros para identificar ordenadores con problemas. Por ejemplo, puede ver qué ordenadores no tienen el cortafuegos o el gestor de parches instalado, o tienen alertas que solucionar. Para más información, consulte Comprobar que los ordenadores están protegidos (página 46), Comprobar que los equipos están actualizados (página 46), y Buscar ordenadores con problemas (página 47).

También puede comprobar si los equipos de un grupo cumplen con las políticas del mismo, según se describe en Comprobar que los ordenadores utilizan la política del grupo (página 31).

5.5.1 Configuración del panel de control

Si utiliza administración delegada, necesitará el permiso **Configuración del sistema** para configurar el Panel de control. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El panel de control muestra avisos y alertas según el porcentaje de ordenadores administrados con alertas o errores, o según el tiempo desde la última actualización desde Sophos.

Puede configurar los umbrales de aviso y críticos que desee utilizar.

1. En el menú **Herramientas**, haga clic en **Configurar panel de control**.

2. En el cuadro de diálogo **Configuración del panel de control**, cambie los valores de los cuadros **Umbral de aviso** y **Umbral crítico** según se describe a continuación.

   a) En **Ordenadores con alertas**, **Ordenadores con errores en productos de Sophos** y **Protección y políticas**, introduzca el porcentaje de equipos administrados afectados por un problema concreto que provoque el cambio del indicador correspondiente de "aviso" a "crítico".

   b) En **Ordenadores con eventos**, introduzca el número de eventos ocurridos en un período de una semana que provocarán la aparición de la alerta en el Panel de control.

   c) En **Protección desde Sophos**, introduzca el tiempo transcurrido en horas desde la última actualización de Sophos que provoque el cambio del indicador de "Actualización" de "aviso" a "crítico". Haga clic en **Aceptar**.

   Si utiliza el valor cero, los avisos se generarán en cuanto se reciba la primera alerta.

Podrá disponer de alertas por email para las situaciones en las que se supere el umbral de aviso o crítico. Para más información, consulte Configurar los mensajes de alerta (página 176).

5.5.2 Comprobar que los ordenadores están protegidos

Los ordenadores están protegidos si tienen activado el escaneado en acceso y el cortafuegos (si lo ha instalado). Para una protección completa, el software debe estar actualizado.

Nota
Puede haber elegido no disponer de escaneado en acceso en ciertos ordenadores, por ejemplo en los servidores. En este caso, debería asegurarse de que disponen de escaneado programado y que están actualizados.

Para comprobar que los ordenadores están protegidos:

1. Seleccione el grupo de ordenadores que desea comprobar.
2. Si desea comprobar ordenadores en subgrupos, seleccione **A este nivel y por debajo** en la lista desplegable.
3. En la ficha **Estado** de la lista de ordenadores, observe la columna **En acceso**.
   Si aparece "Activo", el equipo dispone de escaneado en acceso. Si aparece un escudo gris y el texto "Inactivo", el escaneado en acceso no está funcionando en ese equipo.
4. Si instaló el cortafuegos, compruebe la columna **Cortafuegos activado**.
   Si aparece “Sí,” el cortafuegos se encuentra activado. Se se muestra un icono gris del cortafuegos junto a “No”, el cortafuegos se encuentra activado.
5. Si utiliza otras funciones, como la restricción de aplicaciones, el control de datos o el control de parches, revise el estado de cada una en la columna correspondiente.

Para más información sobre cómo comprobar que los equipos están actualizados, consulte Comprobar que los equipos están actualizados (página 46).

Para más información sobre cómo encontrar equipos con problemas mediante la lista de ordenadores, consulte Buscar ordenadores con problemas (página 47).

5.5.3 Comprobar que los equipos están actualizados

Si configuró Enterprise Console de la forma recomendada, las estaciones recibirán las actualizaciones de forma automática.

Para comprobar que los equipos están actualizados:

1. Seleccione el grupo de ordenadores que desea comprobar.
2. Si desea comprobar ordenadores en subgrupos, seleccione **A este nivel y por debajo** en la lista desplegable.
3. En la ficha **Estado**, observe la columna **Actualizado** o vaya a la ficha **Detalles de actualización**.
   - Si la columna **Detalles de actualización** indica "Sí", el ordenador está actualizado.
   - De lo contrario, el equipo no estará actualizado. Se indicará el tiempo que lleva sin actualizarse.

Para más información sobre la actualización de los ordenadores no actualizados, consulte Actualizar ordenadores con protección obsoleta (página 74).

5.5.4 Buscar ordenadores con problemas

Para ver una lista de los equipos que no están protegidos adecuadamente o que tienen problemas relacionados con la protección:

1. Seleccione el grupo de ordenadores que desea comprobar.
2. En la lista **Ver**, seleccione qué equipos quiere buscar, por ejemplo, **Ordenadores con posibles problemas**.

   También puede seleccionar una subentrada de una entrada para ver los equipos afectados por un problema concreto (por ejemplo, equipos que no cumplen la política del grupo, equipos con alertas pendientes o equipos en los que se ha producido un error durante la instalación).
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel** o **A este nivel y por debajo**. En la lista aparecerán los ordenadores que tengan problemas de protección.

También se puede filtrar la lista de ordenadores por el nombre del elemento detectado, como p. ej., programa malicioso, aplicación potencialmente no deseada o archivo sospechoso. Para obtener más información, consulte Filtrar ordenadores por el nombre de un elemento detectado (página 8).

Para más información sobre cómo solucionar problemas de protección, consulte El escaneado en acceso no se ejecuta en ciertos equipos (página 210) y el resto de apartados en la sección Solución de problemas (página 210).

5.6 Alertas y errores

Si se detecta un elemento sospechoso, un programa publicitario u otra aplicación no deseada, aparecen iconos de alerta en la ficha **Estado** de la vista **Estaciones**.

Para ver una explicación de los iconos de alerta, consulte Significado de los iconos de alerta (página 48) El resto de temas de esta sección explican qué hacer con las alertas.

Nota
También se mostrarán avisos en la consola si el programa está desactivado u obsoleto. Para más información, consulte Comprobar la protección de la red (página 45).

Para más información sobre cualquier alerta, por ejemplo, el nombre del elemento detectado, haga clic en la ficha **Detalles de alertas y errores**.

Para más información sobre las alertas de los gestores de actualización, consulte Monitorizar el gestor de actualización (página 72).

5.6.1 Significado de los iconos de alerta

Icono	Significado
	La detección de virus, gusanos, troyanos, programas espía o comportamientos sospechosos se indica mediante iconos de aviso rojos en la columna **Alertas y errores**.
	Un icono de aviso amarillo en la columna **Alertas y errores** indica alguno de los problemas siguientes: • Se ha detectado un archivo sospechoso. • Se ha detectado un programa publicitario o aplicación no deseada. • Se ha producido algún error. Los iconos de aviso amarillos que aparecen en la columna **Cumplimiento de políticas** indican que el equipo no utiliza las mismas políticas que el resto de equipos del grupo.

Si existen varias alertas o errores en un equipo, el icono de la alerta más importante aparecerá en la columna **Alertas y errores**. A continuación se enumeran los tipos de alertas en orden descendente de prioridad.

1. Alertas de virus y programas espía
2. Alertas de comportamientos sospechosos
3. Alertas de archivos sospechosos
4. Alertas de programas publicitarios y otras aplicaciones no deseadas
5. Errores del software (por ejemplo, errores de instalación)

5.6.2 Alertas sobre elementos detectados

Si utiliza administración delegada, necesitará el permiso **Remediación: limpieza** para limpiar elementos detectados o eliminar alertas de la consola. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para solucionar las alertas que aparecen en la consola:

1. En la vista **Estaciones**, seleccione los ordenadores cuyas alertas desee ver. Haga clic con el botón derecho del ratón y seleccione **Resolver alertas y errores**.
   Se abre el cuadro de diálogo **Resolver alertas y errores**.
2. La solución a la alerta depende del estado de limpieza de la misma. Consulte la columna **Estado de la limpieza** y decida qué hacer.

Sugerencia
Para ordenar las alertas, haga clic en el encabezado de la columna. Por ejemplo, para ordenar las alertas según el estado de la limpieza, haga clic en el encabezado de la columna **Estado de la limpieza**.

Estado de la limpieza	Descripción y solución
Se puede limpiar	Elimine el elemento. Para ello, seleccione las alertas y haga clic en **Limpiar**.
Imposible limpiar este tipo de amenaza	Este tipo de elemento detectado, por ejemplo, un archivo o un comportamiento sospechoso, o tráfico de red malicioso, no se puede limpiar desde la consola. Decida si desea permitirlo o bloquearlo. Si el elemento no es de confianza, puede enviarlo a Sophos para que lo analicemos. Para obtener más información, consulte Información sobre elementos detectados (página 49).
Imposible limpiar	El elemento no se puede limpiar desde la consola. Para más información sobre el elemento y cómo solucionarlo, consulte Información sobre elementos detectados (página 49).
Requiere escaneado completo	Es posible que el elemento se pueda limpiar, pero es necesario realizar un escaneado completo del equipo para poder limpiarlo. Para más información, consulte Escaneado remoto (página 51).
Requiere reiniciar	El elemento se ha eliminado de forma parcial, pero es necesario reiniciar el equipo para que finalice la limpieza. **Nota** Las estaciones se deben reiniciar desde el propio equipo, no desde Enterprise Console.
Falló la limpieza	No se pudo eliminar el elemento. Puede que sea necesario realizar una limpieza manual. Para obtener más información, consulte Realizar una limpieza inmediata (página 51).
Limpieza en progreso (iniciada <hora>)	Se está realizando la limpieza.
Tiempo agotado de limpieza (iniciado <hora>)	Se ha agotado el tiempo de la limpieza. Puede que no se haya limpiado el elemento. Esto puede ocurrir, por ejemplo, si la estación no está conectada a la red o si la red está ocupada. Intente limpiarlo más tarde.

Si decide permitir algún elemento, consulte Autorizar programas publicitarios y otras aplicaciones no deseadas (página 102) o Autorizar elementos sospechosos (página 104).

5.6.3 Información sobre elementos detectados

Si necesita más información sobre una amenaza u otro elemento detectado en una estación o desea saber qué hacer para solucionarlo, siga estos pasos:

1. En la lista de ordenadores de la vista **Estaciones**, haga doble clic en el equipo afectado.
2. En el cuadro de diálogo **Detalles del ordenador**, vaya a la sección **Alertas y errores pendientes**. En la lista de elementos detectados, haga clic en el nombre del elemento correspondiente. Se abrirá el sitio web de Sophos, donde encontrará una descripción del elemento y qué hacer para solucionar el problema.

Nota
También puede visitar la página de **análisis de seguridad** en el sitio web de Sophos (http://www.sophos.com/es-es/threat-center/threat-analyses/viruses-and-spyware.aspx), seleccionar el tipo de elemento que busca y escribir el nombre del elemento en el cuadro de búsqueda.

5.6.4 Alertas sobre ransomware

Si utiliza administración delegada, necesitará el permiso **Remediación: limpieza** para limpiar elementos detectados o eliminar alertas de la consola. Para obtener más información, consulte Administrar roles y subentornos (página 13).

CryptoGuard bloquea el proceso en la estación de trabajo que ha generado la alerta de ransomware. El bloqueo solo se elimina cuando se quita la alerta.

Nota
Si se reinicia la estación de trabajo, se elimina el bloqueo. Se genera una nueva alerta de ransomware si se reinicia el proceso infectado.

Recuerde
Debe ejecutar de forma manual Sophos Clean en el equipo que desencadena la detección. De lo contrario, el equipo desencadenará la alerta y el proceso se volverá a bloquear cada vez que se ejecute.

Para solucionar las alertas de ransomware que aparecen en la consola:

1. En la vista **Estaciones**, seleccione los ordenadores cuyas alertas desee ver. Haga clic con el botón derecho del ratón y seleccione **Resolver alertas y errores**.
   Se abre el cuadro de diálogo **Resolver alertas y errores**.
2. Seleccione las alertas de ransomware que desee borrar y haga clic en **Quitar**.
   Las alertas reconocidas dejan de mostrarse en la consola. Con esto se desbloquea el proceso.

5.6.5 Borrar alertas y errores de las estaciones en la consola

Si utiliza administración delegada, necesitará el permiso **Remediación: limpieza** para eliminar alertas o errores de la consola. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Una vez resuelto el problema que hubiera causado la alarma ya puede borrarla de la consola.

Nota
No se pueden borrar alertas sobre errores de instalación. Estas alertas solamente se borrarán cuando Sophos Endpoint Security and Control se instale de forma satisfactoria en el ordenador.

1. En la vista **Estaciones**, seleccione los ordenadores cuyas alertas desee borrar. Haga clic con el botón derecho del ratón y seleccione **Resolver alertas y errores**.
   Se abre el cuadro de diálogo **Resolver alertas y errores**.
2. Para borrar alertas o errores de los productos de Sophos en la consola, vaya a la ficha Alertas o Errores, respectivamente, seleccione los que desee eliminar y haga clic en **Quitar**.
   Las alertas reconocidas dejan de mostrarse en la consola.

Para ver cómo quitar alertas del gestor de actualización en la consola, consulte Quitar alertas del gestor de actualización en la consola (página 73).

5.7 Escaneado y limpieza de ordenadores

5.7.1 Escaneado remoto

Puede escanear ordenadores de forma inmediata sin necesidad de esperar hasta el siguiente escaneado programado.

Si utiliza administración delegada, necesitará el permiso **Remediación: actualización y escaneado** para escanear ordenadores. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Nota
Los equipos Windows, Linux y UNIX son los únicos que pueden realizar escaneados completos del sistema originados desde la consola.

Para escanear equipos de forma inmediata:

1. Seleccione los ordenadores en la lista de ordenadores o un grupo en el panel **Grupos**. Haga clic con el botón derecho y seleccione **Escaneado remoto**.

   Si lo prefiere, en el menú **Acciones**, seleccione **Escaneado remoto**.
2. Para iniciar el escaneado, en el cuadro de diálogo **Escaneado remoto**, compruebe la lista de ordenadores a escanear y haga clic en **Aceptar**.

Nota
Si se detecta alguna amenaza en la memoria, el escaneado se detiene y se envía una alerta a Enterprise Console. Esto se debe a que si se continua con el escaneado, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneado.

5.7.2 Realizar una limpieza inmediata

Podrá limpiar de forma remota las estaciones Windows y Mac afectados por virus o aplicaciones no deseadas.

Si utiliza administración delegada, necesitará el permiso **Remediación: limpieza** para limpiar ordenadores. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Nota
Para limpiar equipos Linux o UNIX, puede configurar la limpieza automática desde la consola (consulte Configurar la limpieza automática del escaneado en acceso (página 79)) o limpiar los equipos por separado como se describe en Eliminar elementos detectados si falla la limpieza (página 52).

Si un elemento, como un troyano o una aplicación no deseada, se ha "detectado parcialmente", antes de limpiar el equipo afectado, deberá realizar un escaneado completo para buscar todos los componentes del elemento detectado de forma parcial. En la lista de ordenadores, en la vista **Estaciones**, haga clic con el botón derecho en el equipo afectado y haga clic en **Escaneado**

remoto. Para obtener más información, consulte Elemento detectado de forma parcial (página 214).

Para limpiar los ordenadores de forma inmediata:

1. En la vista **Estaciones** de la lista de ordenadores, haga clic con el botón derecho del ratón en el equipo que desea limpiar y seleccione **Resolver alertas y errores**.
2. En el cuadro de diálogo **Resolver alertas y errores**, en la ficha **Alertas**, active las casillas de los elementos que desea limpiar o haga clic en **Seleccionar todo**. Haga clic en **Limpiar**.

Si la limpieza se realiza de forma satisfactoria, las alertas que se muestran en la lista de ordenadores desaparecerán.

Si alguna alerta permanece en la lista, debería limpiar los ordenadores de forma manual. Consulte Eliminar elementos detectados si falla la limpieza (página 52).

Nota
La limpieza de ciertos virus requiere un escaneado completo del sistema, durante el que se intentarán limpiar *todos* los virus. Esto puede tardar bastante. Las alertas se actualizan al finalizar el escaneado.

5.7.3 Eliminar elementos detectados si falla la limpieza

Si no puede limpiar ordenadores desde la consola, puede proceder a la limpieza manual.

1. En la lista de ordenadores, haga doble clic en el equipo infectado.
2. En el cuadro de diálogo **Detalles del ordenador**, vaya a la sección **Alertas y errores pendientes**. En la lista de elementos detectados, haga clic en el elemento que desea eliminar del ordenador. Se abrirá el sitio web de Sophos para que pueda informarse sobre cómo limpiar el ordenador.
3. Proceda a la limpieza manual en cada ordenador.

Nota
En la web de Sophos se ofrecen herramientas para la desinfección automática de ciertos virus y gusanos.

6 Actualizar ordenadores

6.1 Configurar el gestor de actualización

El gestor de actualización permite configurar la actualización automática del software de seguridad de Sophos. Los gestores de actualización se instalan y administran con Enterprise Console.

Si lo desea, puede instalar gestores de actualización adicionales. Por ejemplo, si cuenta con una red compleja con varias ubicaciones, puede instalar un gestor de actualización adicional en una ubicación remota. Para más información, consulte Añadir gestores de actualización adicionales (página 59).

6.1.1 Funcionamiento de los gestores de actualización

El gestor de actualización, una vez configurado:

- Conecta de forma periódica con un almacén de distribución de datos de Sophos o de la red.
- Descarga actualizaciones de los datos de detección de amenazas y actualizaciones del software de seguridad a los que se haya suscrito el administrador.
- Coloca el software actualizado en las unidades compartidas de red para su instalación en las estaciones.

Los equipos se actualizan de forma automática desde las unidades compartidas, siempre y cuando el software de Sophos instalado se haya configurado correctamente, por ejemplo, aplicando una política de actualización.

6.1.2 Ver o editar la configuración del gestor de actualización

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores, seleccione el gestor de actualización cuya configuración desee ver o modificar. Haga clic con el botón derecho del ratón y seleccione **Ver/editar configuración**.

   Nota
   Si lo prefiere, seleccione el gestor de actualización, vaya al menú **Acciones**, señale **Gestor de actualización** y haga clic en **Ver/editar configuración**.

   Se abrirá el cuadro de diálogo **Configuración del gestor de actualización**.
3. Modifique la configuración según se describe en las secciones siguientes:
   - Seleccionar fuentes de actualización para el gestor de actualización (página 54).
   - Seleccionar el software a descargar (página 55).
   - Especificar la ubicación del software (página 56).

- Crear o editar una actualización programada (página 56).
- Configurar el registro del gestor de actualización (página 57).
- Configurar la autoactualización del gestor de actualización (página 58).

Para ver cómo quitar alertas del gestor de actualización en la consola, consulte Quitar alertas del gestor de actualización en la consola (página 73).

Tras configurar el gestor de actualización, debe configurar las políticas de actualización que aplicará a las estaciones.

6.1.3 Seleccionar fuentes de actualización para el gestor de actualización

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Es necesario seleccionar una fuente de actualización desde la que el gestor descargará el software de seguridad y las actualizaciones para su distribución en la red.

Es posible seleccionar más de una fuente. Debe existir una fuente primaria. El resto de las fuentes se utilizarán, en el orden especificado, si no es posible acceder a la fuente anterior.

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea seleccionar una fuente de actualización. Haga clic con el botón derecho del ratón y seleccione **Ver/editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
4. En el cuadro de diálogo **Detalles de la fuente**, en el campo **Dirección**, escriba la dirección de la fuente. Puede utilizar una dirección UNC o HTTP.

   Seleccione **Sophos** si desea descargar el software directamente desde Sophos.
5. Si es necesario, los campos **Nombre de usuario** y **Contraseña** deben especificar las credenciales de la cuenta necesaria para acceder a la fuente de actualización.
   - Si la fuente es Sophos, utilice las credenciales suministradas por Sophos.
   - Si la fuente es una unidad compartida predeterminada mantenida por otro gestor de actualización a un nivel superior en la jerarquía de actualización, el **Nombre de usuario** y **Contraseña** se completarán de forma automática.

     Por defecto, la unidad compartida UNC para las actualizaciones es `\\<ordenador>\SophosUpdate`, siendo éste el ordenador con el gestor de actualización.
   - Si se trata de una fuente no predeterminada en su red, utilice una cuenta con acceso de lectura. Si el **Nombre de usuario** tiene que indicar el dominio para su validación, use la forma dominio\usuario.
6. Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Especifique la **Dirección** y **Puerto** a utilizar. Introduzca el **Nombre de usuario** y la **Contraseña** de acceso al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario. Haga clic en Aceptar.
   La nueva fuente aparecerá en el cuadro de diálogo **Configuración del gestor de actualización**.

Si ya ha instalado un gestor de actualización en otro equipo, la unidad compartida desde la que el gestor de actualización descarga software y actualizaciones aparecerá en la lista de direcciones.

Si lo desea, puede seleccionar dicha unidad como fuente de actualización. A continuación, puede mover a la parte superior de la lista la dirección que desea que sea la primaria utilizando los botones **Subir** y **Bajar** situados a la derecha de la lista.

6.1.4 Seleccionar el software a descargar

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Seleccione las suscripciones que el gestor de actualización mantendrá actualizadas.

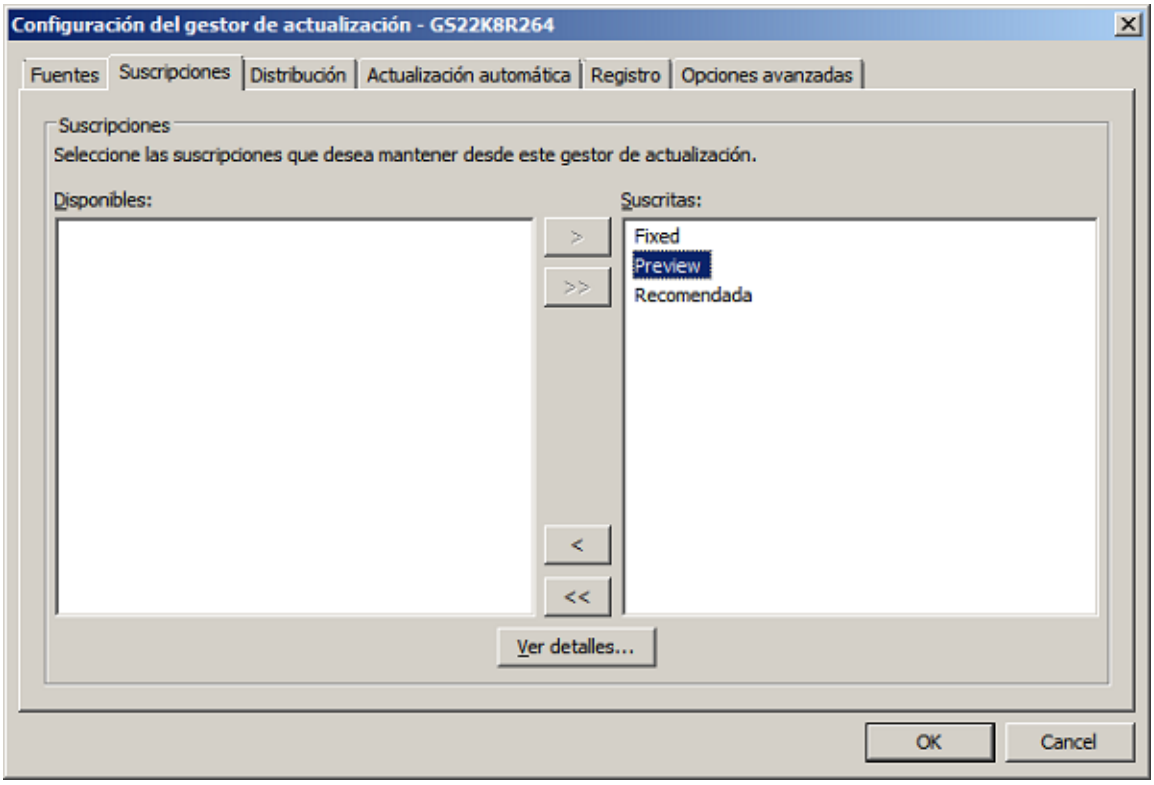
1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea seleccionar el software que descargar. Haga clic con el botón derecho del ratón y seleccione **Ver/ editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Suscripciones**, seleccione una suscripción de la lista de suscripciones disponibles.

   Para ver más información sobre la suscripción, por ejemplo, qué software incluye, haga clic en **Ver detalles**.
4. Para mover la suscripción a la columna “Suscrito”, haga clic en el botón “Añadir”.

   Para mover todas las suscripciones a la lista "Suscrito", haga clic en el botón "Añadir todas".



6.1.5 Especificar la ubicación del software

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Tras seleccionar el software a descargar, debe especificar la ubicación desde la que se ofrecerá al resto de la red. Por defecto, el software se descarga a la unidad compartida UNC `\\<ordenador>\SophosUpdate`, donde ordenador es el ordenador con el gestor de actualización.

El software descargado se puede distribuir desde otras unidades compartidas en la red. Para ello, añada una unidad compartida de red existente a la lista de unidades compartidas disponibles y muévala a la lista de unidades compartidas de actualización como se describe a continuación. Asegúrese de que la cuenta de Update Manager (**SophosUpdateMgr**) tiene permiso de lectura en las unidades compartidas.

Nota
La cuenta de Update Manager la creó antes de instalar Enterprise Console. Para más información, consulte la Guía de inicio de Enterprise Console.

Para especificar la ubicación del software:

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea seleccionar unidades compartidas de red para la distribución de software. Haga clic con el botón derecho del ratón y seleccione **Ver/editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Distribución**, seleccione la suscripción en la lista.
4. Seleccione una unidad compartida en la lista de unidades compartidas "Disponibles" y muévala a la lista "Actualizar en" haciendo clic en el botón "Añadir" (>).

   La unidad compartida predeterminada `\\<ordenador>\SophosUpdate` siempre aparece en la lista "Actualizar en". No es posible eliminar esta entrada.

   Entre las unidades compartidas disponibles se incluyen las conocidas por Enterprise Console y que no se utilizan en ningún otro gestor de actualización.

   Puede añadir una unidad compartida existente o eliminar otras de la lista "Disponibles", utilizando los botones "Añadir" (>) o "Eliminar" (<).
5. Haga clic en **Configurar** si desea indicar una descripción o las credenciales adecuadas para una unidad compartida. En el cuadro de diálogo **Gestor de unidades compartidas**, escriba la descripción y las credenciales.

   Si desea utilizar las mismas credenciales para varias unidades compartidas, selecciónelas en la lista "Actualizar en" y haga clic en **Configurar**. En el cuadro de diálogo **Gestor de unidades compartidas**, escriba las credenciales que se utilizarán para escribir en las unidades compartidas.

6.1.6 Crear o editar una actualización programada

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, los gestores de actualización comprueban la presencia de **actualizaciones de detección** cada 10 minutos.

Si lo desea, puede modificar este intervalo. El intervalo mínimo es de 5 minutos y el máximo de 1440 minutos (24 horas). Se recomienda un intervalo de 10 minutos para que su protección esté constantemente actualizada.

Por defecto, los gestores de actualización comprueban la presencia de **actualizaciones del software** cada 60 minutos.

Si lo desea, puede modificar este intervalo. El intervalo mínimo es de 10 minutos y el máximo de 1440 minutos (24 horas).

Para la actualización del software, puede especificar intervalos horarios o diarios, o una combinación de horas y días.

Nota
Puede crear una programación diferente para cada día de la semana. Sólo puede asignar una programación a cada día de la semana.

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea crear una actualización programada. Haga clic con el botón derecho del ratón y seleccione **Ver/ editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Programación**, introduzca el intervalo entre las actualizaciones de los datos de detección de amenazas.
4. Introduzca el intervalo entre las actualizaciones del software.
   - Si desea especificar un intervalo que se utilice cada hora todos los días, active la opción **Comprobar actualizaciones cada n minutos** e introduzca el intervalo en minutos.
   - Si desea crear una programación más sofisticada o diferentes programaciones para cada día de la semana, active la opción **Configurar y gestionar actualizaciones programadas** y haga clic en **Añadir**.

     En el cuadro de diálogo **Actualización programada**, escriba el nombre de la actualización, y seleccione los días de la semana y los intervalos.

6.1.7 Configurar el registro del gestor de actualización

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea configurar el registro. Haga clic con el botón derecho del ratón y seleccione **Ver/editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Registro**, seleccione el número de días que desea conservar el registro y el tamaño máximo.

6.1.8 Configurar la autoactualización del gestor de actualización

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización para el que desea configurar la autoactualización. Haga clic con el botón derecho del ratón y seleccione **Ver/editar configuración**.
3. En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Opciones avanzadas**, seleccione la versión con la que quiere mantener actualizado el gestor de actualización.
   Por ejemplo, si selecciona "recomendado", el gestor de actualización se actualizará siempre con la versión clasificada por Sophos como tal. La versión del gestor de actualización irá cambiando.

6.1.9 Forzar la actualización de un gestor

Si utiliza administración delegada, necesitará el permiso **Remediación: actualización y escaneado** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Una vez configurado, el gestor de actualización busca actualizaciones y las descarga desde la fuente de actualización a las unidades compartidas que mantiene de forma automática según la programación especificada. Si desea que un gestor de actualización busque y descargue actualizaciones de los datos de detección de amenazas, y actualizaciones del software para las estaciones y para el propio gestor, siga estos pasos:

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualizaciones que desea actualizar. Haga clic con el botón derecho y seleccione **Actualizar ahora**.

6.1.10 Hacer que un gestor cumpla con la configuración

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para configurar un gestor de actualización. Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, seleccione el gestor de actualización que quiere que cumpla las opciones de configuración. Haga clic con el botón derecho y seleccione **Cumplir con la configuración**.

6.1.11 Añadir gestores de actualización adicionales

Sophos Update Manager (SUM) se instala siempre en el mismo equipo que Enterprise Console. Si seleccionó la **Configuración personalizada** durante la instalación, el equipo será en el que instaló el servidor de administración.

Si lo desea, puede añadir gestores de actualización adicionales a la red para reducir la carga del gestor ya instalado y distribuir las actualizaciones de forma más eficaz. Instale los gestores de actualización adicionales en equipos que aún no tengan ningún gestor de actualización instalado.

Importante
No elimine el gestor de actualización instalado en el servidor de administración de Enterprise Console. Enterprise Console no podrá proteger correctamente la red hasta que este gestor de actualización no disponga de una fuente de actualización. Esto permitirá a Enterprise Console recibir las actualizaciones necesarias (por ejemplo, información sobre la versión del software de seguridad para las estaciones, nuevas listas de control de datos o la lista de aplicaciones y dispositivos restringidos).

Para permitir que otro gestor de actualizaciones descargue software de seguridad desde Sophos o desde otro gestor a través de HTTP, abra el puerto TCP 80 (saliente) del equipo en el que desea instalar el gestor de actualizaciones adicional. Para permitir que el gestor de actualización descargue el software de seguridad desde otro gestor de actualización mediante una ruta UNC, abra los siguientes puertos de salida del ordenador: puerto UDP 137, puerto UDP 138, puerto TCP 139 y puerto TCP 445.

Si la versión de Windows del equipo incluye la función Detección de redes y está desactivada, actívela y reinicie el equipo.

Desactive el Control de cuentas de usuario si se encuentra activado y reinicie el equipo. Puede volver a activarlo después de instalar el gestor de actualización y suscribirse a las actualizaciones de Sophos.

Si el ordenador se encuentra en un dominio, inicie la sesión como administrador del dominio.

Si el ordenador se encuentra en un grupo de trabajo, inicie la sesión como administrador local.

El programa de instalación del gestor de actualización está ubicado en el mismo equipo que el servidor de administración de Enterprise Console, en la carpeta compartida `\\servidor\SUMInstallSet`. Para ver la ubicación del programa de instalación, vaya al menú **Ver** y haga clic en **Ubicación del instalador de Sophos Update Manager**.

Para instalar Sophos Update Manager puede utilizar el Escritorio remoto de Windows.

Para instalar un gestor de actualización adicional:

1. Ejecute el instalador de Sophos Update Manager **Setup.exe**.
   A continuación se abrirá el asistente de instalación.
2. En la página inicial, haga clic en **Siguiente**.
3. En el cuadro de diálogo **Acuerdo de licencia**, haga clic en **Acepto los términos del acuerdo de licencia** para continuar. Haga clic en **Siguiente**.
4. En el cuadro de diálogo **Carpeta de destino**, acepte la ubicación predeterminada o haga clic en **Cambiar** e introduzca otra alternativa. Haga clic en **Siguiente**.
5. En la página **Cuenta de Sophos Update Manager**, seleccione la cuenta que las estaciones de la red utilizarán al acceder a la ubicación desde la que se ofrezcan las actualizaciones. (Por defecto, la unidad compartida para las actualizaciones es `\\<ordenador>\SophosUpdate`, siendo éste

el ordenador con el gestor de actualización.) Esta cuenta no requiere derechos de administrador, tan sólo de lectura en la unidad compartida.

Puede dejar el usuario predeterminado, seleccionar otro usuario o crear uno nuevo.

Por defecto, el programa de instalación creará la cuenta **SophosUpdateMgr** con permiso de lectura en la unidad compartida y sin inicio de sesión interactivo.

Si desea añadir otras unidades compartidas, seleccione una cuenta existente, o cree una cuenta nueva, con permiso de lectura en dichas unidades compartidas. Asegúrese de que la cuenta **SophosUpdateMgr** tiene permiso de lectura en las unidades compartidas.

6. En la página **Datos de cuenta de Sophos Update Manager**, según la opción seleccionada anteriormente, especifique una contraseña para el usuario predeterminado, seleccione otro usuario o introduzca los datos para crear uno nuevo.

   La contraseña debe ajustarse a la política establecida en su red.
7. En la página **Preparado para instalar el programa**, haga clic en **Instalar**.
8. Al completarse la instalación, haga clic en **Finalizar**.

Este ordenador con Sophos Update Manager debe aparecer ahora en Enterprise Console, en la vista **Gestores de actualización**. (En el menú **Ver**, seleccione **Gestores de actualización**.)

Para configurar el gestor de actualización, selecciónelo, haga clic con el botón derecho y seleccione **Ver/editar configuración**.

6.1.12 Publicar el software de seguridad en un servidor web

Si lo desea, puede publicar el software de seguridad de Sophos en un servidor web para los equipos que acceden a través de HTTP.

Para publicar el software de seguridad en un servidor web:

1. Para averiguar la ruta a la carpeta compartida en la que se ha descargado el software de seguridad, conocida como ubicación de archivos de inicio:

   a) En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**. En el cuadro de diálogo **Ubicación de archivos de inicio**, la columna **Ubicación** muestra la ubicación de los archivos de inicio de cada plataforma.

   b) Anote la ruta sin incluir la carpeta de los `CID`. Por ejemplo: `\\servidor\SophosUpdate`
2. Permita que la ubicación de los archivos de inicio, incluidas las subcarpetas, estén disponibles desde el servidor web. Para más información, consulte el artículo 38238 de la base de conocimiento de Sophos.

6.2 Configurar suscripciones de software

Mediante las suscripciones de software se especifica la versión del producto de Sophos que se utilizará en las estaciones de trabajo.

El **Asistente para descargar el software** configura una suscripción predeterminada con las versiones recomendadas del software seleccionado.

Si desea añadir software a su suscripción o suscribirse a otra versión que no sea la recomendada, configure su suscripción según se describe en Suscribirse a software de seguridad (página 63).

Si no ha completado todos los pasos del asistente después de instalar Enterprise Console, consulte Ejecutar el Asistente para descargar el software de seguridad (página 64).

6.2.1 ¿Qué tipos de actualización hay disponibles?

Para cada plataforma (p. ej., Windows), hay disponibles distintos paquetes de software con distintos tipos de actualización y que incluyen distintas versiones de software para estaciones. Puede seleccionar qué paquete de software descargar desde Sophos para su implementación en las estaciones de trabajo seleccionando uno de los siguientes tipos de actualización en la suscripción.

Tipo de actualización	Descripción
Versión Recomendada	Este es el paquete predeterminado. Al usar este paquete Sophos actualiza su software regularmente (normalmente cada mes) con: • Parches para problemas detectados por los clientes. • Nuevas funciones listas para su distribución. Si la primera vez que instala Enterprise Console acepta la configuración predeterminada, esta es la versión que utilizará.
Versión previa	Este paquete está dirigido a administradores de TI y seguridad. Al usar esta versión se obtienen las funciones nuevas antes de que se distribuyan con la versión recomendada. Esto significa que puede probar y evaluar las funciones nuevas, p. ej., en una red, antes de que estén disponibles para el público en general. **Nota** Ocasionalmente el software del paquete de la versión previa y de la versión recomendada es el mismo. Esto sucede cuando no hay funciones nuevas lista para ser probadas en el entorno operativo de nuetros clientes.
Versión ampliada	La versión ampliada esta dirigida a clientes que aplican procesos estrictos o conservadores al instalar actualizaciones de software en su red. Al usar esta versión se reciben las mismas actualizaciones que a través del canal recomendado, pero con un retraso de varios meses. Esto significa que cualquier problema que pueda presentar el producto ya se haya detectado y rectificado antes de que se instale en su red.
Versión recomendada anterior	La versión anterior del paquete actualmente recomendado. Esta versión puede ser útil si necesita algo más de tiempo para probar el nuevo software antes de implementarlo en su red.
Versión ampliada anterior	La versión anterior del paquete ampliado actual. Esta versión puede ser útil si necesita algo más de tiempo para probar el nuevo software antes de implementarlo en su red.
Versiones fijas	Consulte Paquetes de software de versión fija (página 62).

Nota
Es posible que en el futuro cambiemos los paquetes. Para más información sobre los paquetes de software disponibles actualmente, consulte el artículo 119216 de la base de conocimiento de Sophos.

El **Asistente para descargar el software** configura una suscripción que especifica las versiones recomendadas del software seleccionado.

Las versiones que se descargan en la práctica suelen cambiar todos los meses. Para comprobar qué versiones de software se van a descargar, en la casilla **Suscripción de software**, seleccione el paquete que desea comprobar y haga clic en **Detalles**.

6.2.2 Paquetes de software de versión fija

Una **versión fija** es una versión que se actualiza con los datos para la detección de amenazas nuevas, pero no con la versión más reciente del software cada mes. Un ejemplo de versión fija de Sophos Endpoint Security and Control para Windows es "10.3.15 VE3.60.0". Compuesto por un identificador de versión compuesto por tres partes: un identificador de versión principal (10), un identificador de versión secundario (3) y un identificador de actualización (15), y la versión de motor de detección de amenazas (VE3.60.0).

Uso de paquetes fijos

De manera predeterminada, el uso de paquetes de software de versión fija está desactivado (en **Herramientas > Configurar Uso de paquetes fijos**). No se muestran en el cuadro de diálogo **Suscripciones de software** y no es posible suscribirse a ellos.

Sugerencia
Si está suscrito a una versión fija de software, recomendamos que para obtener la mejor protección posible cambie su suscripción a una suscripción "recomendada". Para más información sobre paquetes de software, consulte ¿Qué tipos de actualización hay disponibles? (página 61).

Si no ha utilizado paquetes de software de versión fija anteriormente pero desea hacerlo, puede activar su uso en **Herramientas > Configurar Uso de paquetes fijos**. Cuando se activa el uso de los paquetes fijos, se muestran en el cuadro de diálogo **Suscripciones de software** y puede suscribirse a ellos.

Nota
Si utiliza la administración basada en roles, necesitará el permiso **Configuración del sistema** para configurar el uso de los paquetes fijos.

Si desactiva el uso de paquetes fijos mientras aún está suscrito a un paquete fijo, seguirá suscrito a este paquete y seguirá descargándose hasta que anule la suscripción. Sin embargo, no podrá ver ni volver a suscribirse a otro paquete fijo.

Si tiene consolas remotas, cambiar esta opción de configuración en una de ellas surtirá efecto en todas las consolas. Si ha activado el uso de paquetes fijos en el registro tal como se describe en el artículo de la base de datos de Sophos 117348, la configuración del registro surtirá efecto solo en el ordenador en el que se haya establecido, y tendrá preferencia sobre la configuración de la consola.

Ciclo de vida de los paquetes fijos

Las versiones fijas se descargan siempre y cuando estén disponibles. Si una versión se va a retirar, aparecerá una alerta en la vista **Gestores de actualización** junto al gestor de actualización que descargue esa versión. Si están configuradas las alertas por email, el administrador también recibirá una notificación.

Cuando se retira una versión fija que se utiliza en una suscripción, si no modifica su suscripción antes de que finalice el soporte, se le suscribirá automáticamente a un paquete ampliado fijo más reciente. Para más información, consulte el artículo de la base de conocimiento de Sophos 121139.

Para más información sobre la política del ciclo de vida de Sophos Endpoint, consulte el artículo de la base de conocimiento de Sophos 112580 .

6.2.3 Suscribirse a software de seguridad

Si utiliza administración delegada:

- Para modificar suscripciones de software, es necesario tener el permiso **Configuración de políticas: actualización**.
- No es posible editar las suscripciones aplicadas a políticas de actualización de otro subentorno que no sea el activo.

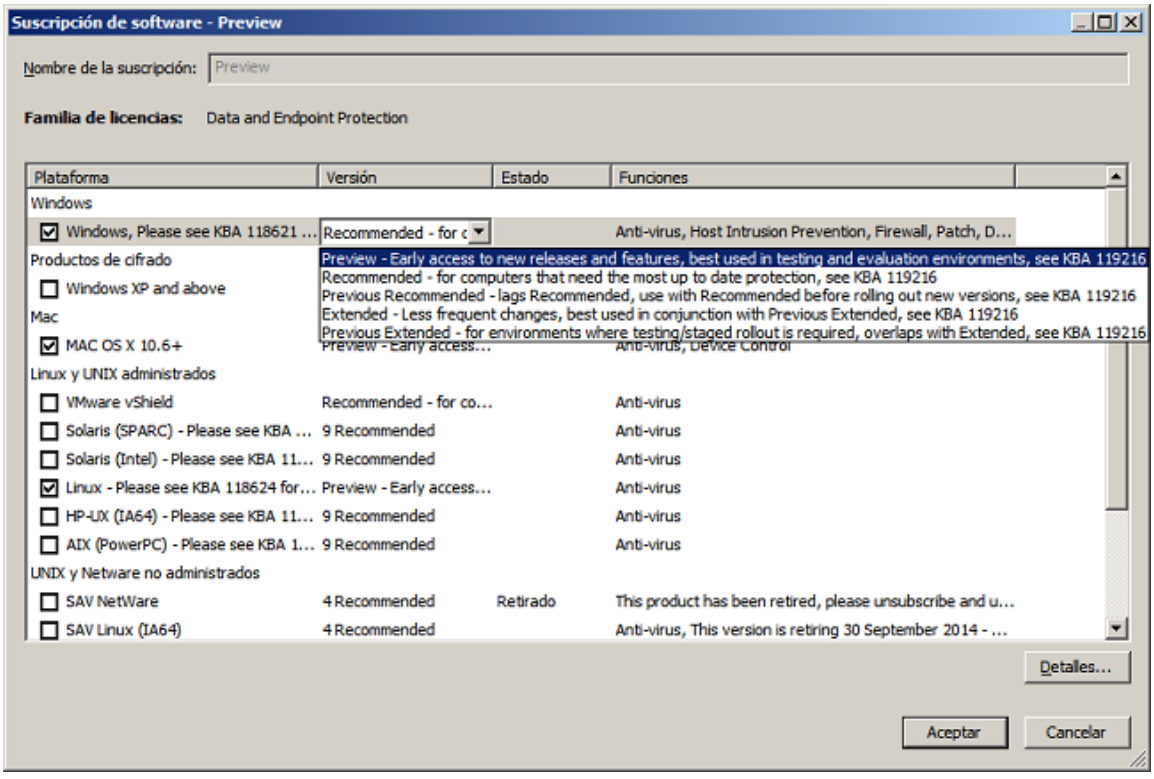
Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para suscribirse a software de seguridad:

1. En el menú **Ver**, seleccione **Gestores de actualización**.
2. En el panel **Suscripciones**, haga doble clic en la suscripción que desee modificar o haga clic en el botón **Añadir** en la parte superior del panel.

   Se abrirá el cuadro de diálogo **Suscripción de software**.

   Si desea crear una copia de una suscripción existente, haga clic con el botón derecho del ratón en la suscripción deseada y seleccione **Duplicar suscripción**. Indique el nombre para la suscripción y haga doble clic para abrir el cuadro de diálogo **Suscripción de software**.
3. En el cuadro de diálogo **Suscripción de software**, puede cambiar el nombre si lo desea.
4. Seleccione las plataformas para las que desea descargar el software.
5. Por defecto, está suscrito a un paquete "Recomendado". También es posible seleccionar un paquete distinto (p. ej., si desea probar funciones nuevas). Para ello haga clic en el campo de **Versión** junto a la plataforma para la que quiere cambiar el paquete y haga clic de nuevo. En la lista desplegable con las versiones disponibles, seleccione la versión que desea descargar (p. ej., versión de avance).



Para informarse sobre los paquetes de actualización disponibles, consulte ¿Qué tipos de actualización hay disponibles? (página 61)

Tras suscribirse al software de seguridad, puede recibir alertas por email referentes a las suscripciones. Para más información consulte Configurar alertas de suscripciones (página 176).

Si ha creado una suscripción nueva, configure el gestor de actualización para su mantenimiento, como se describe en Ver o editar la configuración del gestor de actualización (página 53).

6.2.4 Ejecutar el Asistente para descargar el software de seguridad

Si utiliza administración delegada, necesitará el permiso **Configuración de políticas: actualización** para ejecutar el **Asistente para descargar el software de seguridad**. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si no ha completado todos los pasos del **Asistente para descargar el software de seguridad** después de instalar Enterprise Console:

- En el menú **Acciones**, haga clic en **Iniciar el asistente para descargar el software de seguridad**.

  El **Asistente para descargar el software de seguridad** sirve de guía en la selección y descarga de software.

Nota
Una vez completado correctamente el asistente, la opción **Ejecutar el Asistente para descargar el software de seguridad** desaparece del menú **Acciones**.

6.2.5 Ver las políticas de actualización que utilizan las suscripciones

Para ver qué políticas de actualización utilizan determinadas suscripciones:

- Seleccione la suscripción, haga clic con el botón derecho del ratón y seleccione **Ver uso de la suscripción**.

  En el cuadro de diálogo **Uso de la suscripción de software**, verá una lista de las políticas de actualización que utilizan la suscripción.

6.3 Configurar la política de actualización

Las políticas de actualización permiten mantener los equipos actualizados con el software de seguridad elegido. Enterprise Console busca actualizaciones y actualiza los equipos, si es necesario, cada cierto tiempo.

La política de actualización predeterminada utiliza la suscripción "Recomendada" del software.

Si desea cambiar la política de actualización predeterminada o crear una política de actualización nueva, siga las instrucciones de las secciones siguientes:

- Seleccionar suscripciones (página 65)
- Configurar servidores de actualización (página 66)
- Programar las actualizaciones (página 71)
- Seleccionar una fuente alternativa para la instalación inicial (página 71)
- Registro de actualizaciones (página 72)

Nota
Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

6.3.1 Seleccionar suscripciones

Si utiliza administración delegada:

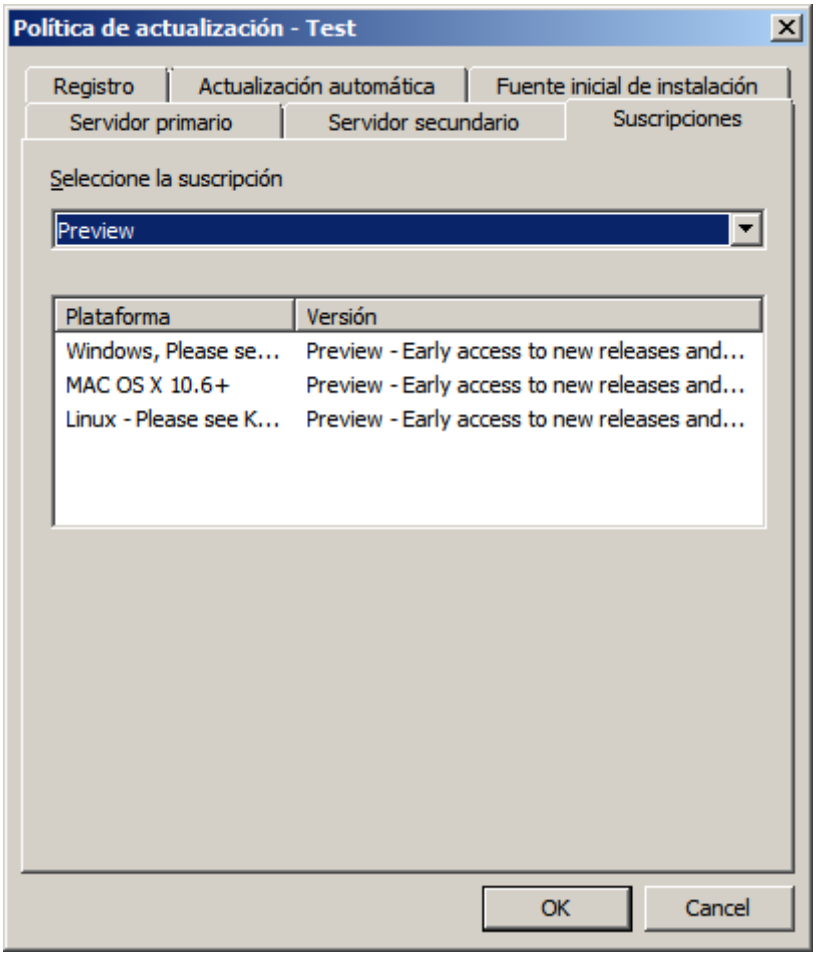
- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Las suscripciones especifican la versión del software descargada desde Sophos para cada plataforma. La suscripción predeterminada incluye el software más reciente para Windows.

Para seleccionar una suscripción:

1. Compruebe qué política de actualización usa el grupo de ordenadores que desea configurar. Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de actualización**, abra la ficha **Suscripciones** y seleccione la suscripción del software que quiere mantener actualizado.



6.3.2 Configurar servidores de actualización

Por defecto, las estaciones se actualizan desde la fuente primaria de actualización en `\\<ordenador>\SophosUpdate`, donde `<ordenador>` es el nombre del equipo con Update Manager. También es posible establecer una fuente secundaria alternativa para las actualizaciones, activar la itinerancia y activar la limitación del ancho de banda.

Cuando una estación no puede conectar con la fuente primaria, intentará la actualización desde la fuente secundaria (si se ha especificado). Siempre se recomienda especificar una fuente secundaria de actualización.

Tanto la fuente primaria como la secundaria pueden indicarse como unidad compartida UNC o dirección HTTP. Si lo prefiere, puede establecer Sophos como la fuente secundaria de actualización a través de Internet.

Nota
Los gestores de actualización pueden disponer de diferentes unidades compartidas de actualización, según su configuración.

Servidor primario

El servidor primario se configura automáticamente con la ubicación del servidor primario predeterminado. Por defecto, las estaciones se actualizan desde la fuente primaria de actualización en `\\<ordenador>\SophosUpdate`, donde `<ordenador>` es el nombre del equipo con Sophos Update Manager.

Para acceder al recurso de red, los ordenadores utilizan las credenciales de Sophos Update Manager que especificó durante la instalación de Enterprise Console. Si ha seguido las recomendaciones de la guía de inicio de Enterprise Console, la cuenta tiene el nombre «SophosUpdateMgr».

Si necesita cambiar las credenciales, consulte Cambiar las credenciales del servidor primario (página 69).

Si accede a la fuente de actualización a través de un servidor proxy, haga clic en **Detalles del proxy** e introduzca los detalles del servidor proxy.

Si desea activar la itinerancia, consulte Itinerancia en portátiles (página 67).

También puede activar la limitación del ancho de banda para restringir el ancho de banda que pueden utilizar los ordenadores al actualizarse. En la ficha **Servidor primario** de la política de actualización, haga clic en el botón **Avanzadas**. En el cuadro de diálogo **Opciones avanzadas**, active la opción **Limitar el ancho de banda a utilizar** y utilice el selector para especificar el ancho de banda en Kbits/segundo.

Itinerancia en portátiles

Es habitual que los usuarios de portátiles trabajen desde diferentes ubicaciones. Si activa la opción de itinerancia en la política de actualización, los portátiles detectarán el servidor de actualización más cercano para optimizar la actualización de la protección.

La detección del servidor de actualización más cercano se realiza comprobando la fuente de actualización de las estaciones en la misma red. De las direcciones obtenidas, se utilizará la más cercana. Si no es posible realizar la actualización desde estas direcciones, se utilizará la ubicación primaria o secundaria especificadas en la política de actualización.

Nota
El intercambio de contraseñas con otras estaciones de realiza de forma segura y los datos se guardan cifrados. De cualquier modo, las cuentas que utilizan las estaciones para obtener las actualizaciones deberían ofrecer sólo acceso de lectura. Consulte Especificar la ubicación del software (página 56).

Para más información detallada sobre la itinerancia, consulte Cómo funciona la itinerancia (página 68).

Sólo se puede utilizar la opción de itinerancia cuando:

- Enterprise Console es común para las estaciones y los portátiles.

- Las estaciones y los portátiles utilizan la misma suscripción del software.
- Existe una ubicación primaria en la política de actualización de los portátiles.
- El cortafuegos está configurado para permitir la comunicación con otras estaciones. El puerto predeterminado es UDP 51235, aunque se puede configurar; para más información consulte el artículo 110371 en la base de conocimiento de Sophos.

La itinerancia se utiliza como una forma de especificar la fuente de actualizaciones. Sólo debe activar la itinerancia en equipos que se llevan de oficina a oficina. Para más información sobre cómo activar la itinerancia, consulte Cambiar las credenciales del servidor primario (página 69).

Para consultar dudas frecuentes sobre la itinerancia, vea el artículo 112830 en la base de conocimiento de Sophos.

Cómo funciona la itinerancia

La itinerancia es un método de actualización inteligente para portátiles que permite la actualización desde la ubicación más conveniente, independientemente de la ubicación de actualización especificada en la política del portátil.

Si activa la itinerancia:

1. Cuando un portátil cambia de ubicación, el componente Sophos AutoUpdate de Endpoint Security and Control detectará el cambio de red respecto a la última actualización. Se enviará una transmisión ICMP en la subred local a otras instalaciones de AutoUpdate, a través del puerto UDP 51235 por defecto.
2. Esto permitirá conocer la política de actualización local. Sólo se utilizará la ubicación primaria.

   Todas las instalaciones de Endpoint Security and Control reciben estas transmisiones aunque no tengan la itinerancia activada.

   La comunicación se realiza de forma cifrada y segura.

   Los mensajes de respuesta se realizan en intervalos de tiempo aleatorios para evitar una avalancha de mensajes. Las respuestas también se realizan mediante transmisiones ICMP para evitar respuestas duplicadas.
3. AutoUpdate elegirá la ubicación más conveniente y comprobará si el equipo que responde está administrado por el mismo Enterprise Console con la misma suscripción de software.

   La ubicación se elegirá según el número pasos intermedios para acceder a las actualizaciones.
4. Una vez elegida la ubicación, se realizará una actualización y, si se completa con éxito, se guardará para las actualizaciones posteriores.

   En el portátil se guardan hasta cuatro ubicaciones de actualización accesibles con el mismo ID de suscripción y el recuento de saltos más bajo (en el archivo `iustatus.xml` en la siguiente ubicación: `C:\Program Files\Sophos\AutoUpdate\data\status\iustatus.xml`).

   Estas ubicaciones se comprobarán en cada actualización.

   Nota
   Si desea volver a utilizar la ubicación en su política de actualización, desactive la itinerancia.

Activar la itinerancia

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Sólo debe activar la itinerancia en equipos que se llevan de oficina a oficina.

Para activar la itinerancia:

1. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política de actualización que desea modificar.
2. En el cuadro de diálogo **Política de actualización**, abra la ficha **Servidor primario** y active la opción **Permitir itinerancia**.
3. En el panel **Grupos**, seleccione un grupo que utilice la política de actualización que acaba de cambiar. Haga clic con el botón derecho y seleccione **Cumplir con**, **Política de actualización del grupo**.

   Repita este paso con todos los grupos que utilicen esta política de actualización.

Nota
Si desea volver a utilizar la ubicación en su política de actualización, desactive la itinerancia.

Cambiar las credenciales del servidor primario

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para cambiar las credenciales del servidor primario:

1. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política de actualización que desea modificar.
2. En el cuadro de diálogo **Política de actualización**, en la ficha **Servidor primario**, escriba las credenciales nuevas para acceder al servidor. Cambie otros datos, si lo desea.

   Nota
   Aunque la fuente de actualización primaria se encuentre en un servidor web con Internet Information Services (IIS) con autenticación anónima, tendrá que introducir credenciales en la ficha **Servidor primario**. Utilice las credenciales para la fuente inicial de instalación, aunque no sean necesarias para acceder al servidor web. Si deja vacíos los campos **Nombre de usuario** y **Contraseña** en la ficha **Servidor primmario**, no podrá proteger las estaciones desde la consola.

3. En el panel **Grupos**, seleccione un grupo que utilice la política de actualización que acaba de cambiar. Haga clic con el botón derecho y seleccione **Cumplir con**, **Política de actualización del grupo**.

   Repita este paso con todos los grupos que utilicen esta política de actualización.

Establecer el servidor de actualización secundario

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para establecer la ubicación secundaria de actualización:

1. Compruebe qué política de actualización usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Actualización** y, a continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de actualización**, abra la ficha **Servidor secundario** y active la opción **Utilizar servidor secundario**.
4. En el cuadro **Dirección (HTTP o UNC)**, puede:
   - Indicar la dirección HTTP o UNC al servidor de actualización.
   - Seleccionar **Sophos**.

   Importante
   Si especifica una fuente de actualización que no está gestionada mediante Update Manager, Enterprise Console no podrá comprobar si el software suscrito se encuentra disponible. Deberá asegurarse de forma manual de que la fuente de actualización contiene el software especificado en la suscripción.

5. Si la política incluye estaciones Mac y utiliza una ruta UNC como **Dirección**, seleccione el protocolo correspondiente en la sección **Protocolo para compartir archivos en Mac OS X**.
6. Si es necesario, escriba el **Nombre de usuario** de la cuenta que se utilizará para acceder al servidor y, a continuación, confirme la contraseña. Si selecciona Sophos como fuente de actualización, utilice las credenciales que se incluyen con su licencia.

   Esta cuenta debería disponer sólo de acceso de lectura a la unidad compartida especificada anteriormente.

   Nota
   Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario. Para más información sobre cómo comprobar cuentas de usuario de Windows, consulte el artículo 11637 de la base de conocimiento de Sophos.

7. Para limitar el ancho de banda a utilizar durante las actualizaciones, haga clic en **Avanzadas**. En el cuadro de diálogo **Opciones avanzadas**, active la opción **Limitar el ancho de banda a utilizar** y utilice el selector para especificar el ancho de banda en Kbits/segundo.
8. Si utiliza un servidor proxy para acceder a las actualizaciones, haga clic en **Detalles del proxy**. En el cuadro de diálogo **Detalles del proxy**, active la opción **Usar servidor proxy** y especifique la **Dirección** y **Puerto** correspondientes. Introduzca el **Nombre de usuario** y la **Contraseña** de acceso al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.

   Nota
   Algunos proveedores de acceso a Internet utilizan servidores proxy para conexiones HTTP.

9. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Política de actualización**.
10. En el panel **Grupos**, haga clic con el botón derecho sobre cada grupo que utilice esta política de actualización y seleccione **Cumplir con > Política de actualización del grupo**.

    Repita este paso con todos los grupos que utilicen esta política de actualización.

6.3.3 Programar las actualizaciones

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, los equipos intentan obtener actualizaciones cada 5 minutos.

Nota
Si las estaciones se actualizan directamente desde Sophos, no se aplica esta frecuencia. Los ordenadores con Sophos PureMessage se actualizarán cada 15 minutos. Los ordenadores sin Sophos PureMessage se actualizarán cada 60 minutos.

Para especificar el intervalo de actualización:

1. Compruebe qué política de actualización usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de actualización**, en la ficha **Programación**, deje la opción **Activar la actualización automática de Sophos en la red** activada. Introduzca el intervalo en minutos entre las actualizaciones.
4. Si los equipos utilizan una conexión telefónica a redes para actualizarse, active la opción **Usar también conexiones telefónicas**.
   Se comprobará si existe alguna actualización cada vez que se inicie la conexión a Internet.

6.3.4 Seleccionar una fuente alternativa para la instalación inicial

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, el software de seguridad se instala en los equipos y se mantiene actualizado desde la fuente especificada en la ficha **Servidor primario**. Puede especificar una fuente diferente para la instalación inicial.

Nota
Esta opción sólo se aplica a Windows.

Si su servidor primario tiene dirección HTTP y desea realizar la instalación desde la consola, deberá especificar una fuente inicial de instalación.

Para realizar la instalación inicial desde otra fuente:

1. Compruebe qué política de actualización usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de actualización**, en la ficha **Fuente inicial de instalación**, desactive la casilla **Usar el servidor primario**. Introduzca la dirección para la fuente inicial de instalación.

6.3.5 Registro de actualizaciones

Si utiliza administración delegada:

- Para configurar una política de actualización, es necesario contar con el permiso **Configuración de políticas: actualización**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, se crean registros de las actualizaciones de los equipos. El tamaño máximo predeterminado de cada registro es de 1 MB. El nivel normal de los registros es la opción predeterminada.

Para cambiar las opciones de registro:

1. Compruebe qué política de actualización usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Actualización**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de actualización**, en la ficha **Registro**, deje activada la opción **Registrar la actividad de Sophos AutoUpdate**. En el campo **Tamaño máximo**, especifique el tamaño máximo del registro en MB.
4. En el campo **Nivel del informe**, seleccione **Normal** o **Detallado**.
   El registro detallado ofrece más información por lo que el tamaño del archivo de registro se incrementará más rápidamente. Utilice esta opción sólo si existen problemas.

6.4 Monitorizar el gestor de actualización

Estado de los gestores de actualización en el panel de control

El estado de los gestores de actualización se muestra en la sección **Actualización** del **Panel de control**. Se indicará la hora de la última actualización desde Sophos y se mostrará un icono de alerta cuando se supere el umbral de aviso o crítico.

Nota
La sección **Actualización** en el panel de control no muestra ningún error ni alerta si algún gestor no se puede actualizar de forma temporal. Sólo se genera un error o alerta cuando el tiempo desde la última actualización supera los umbrales establecidos en Configuración del panel de control (página 45).

Alertas y errores de los gestores de actualización

Las alertas y errores de los gestores de actualización se muestran en la vista **Gestores de actualización**, en las columnas **Alertas** y **Errores**, respectivamente.

Si está suscrito a una versión fija del software, aparecerá una alerta cuando la versión esté a punto de retirarse o se haya retirado. También se mostrará una alerta si cambia de licencia.

Para ver las alertas y errores de los gestores de actualización:

1. En la vista **Estaciones**, haga clic en el botón **Gestores de actualización** de la barra de herramientas para ir a la vista **Gestores de actualización**.
2. En la lista de gestores de actualización, compruebe si existe algún problema en las columnas **Alertas** y **Errores**.
3. Si aparece una alerta o un error junto al gestor de actualización, haga clic con el botón derecho y seleccione **Ver gestor de actualización**.

   En el cuadro de diálogo **Detalles del gestor de actualización**, aparece la fecha de las últimas actualizaciones de datos de detección de amenazas y software, el estado de las suscripciones que actualiza el gestor y el estado del gestor de actualización.
4. Para obtener más información sobre el estado de un gestor de actualización determinado y solucionar problemas, siga el enlace de la columna **Descripción**.

Si necesita modificar o consultar la suscripción de software, por ejemplo, si algún producto se encuentra cercano a su retirada o si ha cambiado de licencia, consulte Suscribirse a software de seguridad (página 63).

Si el cambio de licencia proporciona nuevas funciones, tendrá que configurar las políticas correspondientes para hacer uso de dichas funciones.

Alertas por email

Si lo desea, puede recibir alertas por email cuando algún producto que utilice esté cercano a su retirada o cuando los productos de Sophos discrepen al cambiar de licencia. Para obtener más información, consulte Configurar alertas de suscripciones (página 176).

6.4.1 Quitar alertas del gestor de actualización en la consola

Si utiliza administración delegada, necesitará el permiso **Remediación: limpieza** para eliminar alertas de la consola. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para quitar alertas del gestor de actualización en la consola:

1. En la vista **Gestores de actualización**, seleccione los gestores cuyas alertas desee borrar. Haga clic con el botón derecho del ratón y seleccione **Quitar alertas**.
   Aparece el cuadro de diálogo **Alertas del gestor de actualización**.
2. Para quitar las alertas en la consola, seleccione las alertas necesarias y haga clic en **Quitar**.
   Las alertas reconocidas dejan de mostrarse en la consola.

6.5 Actualizar ordenadores con protección obsoleta

Si utiliza administración delegada, necesitará el permiso **Remediación: actualización y escaneado** para actualizar ordenadores. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Después de configurar y aplicar las políticas de actualización, los ordenadores se mantienen actualizados de forma automática. No es necesario actualizarlos de forma manual, a menos que se produzca un problema con la actualización.

Si en la lista de ordenadores de la vista **Estaciones** aparece un icono de un reloj junto a un ordenador en la columna **Actualizado** de la ficha **Estado**, el software de seguridad del equipo no está actualizado. Se indicará el tiempo que lleva sin actualizarse.

La protección de un ordenador puede estar obsoleta por dos razones:

- El ordenador no ha podido recoger una actualización desde el servidor.
- El servidor no dispone de las últimas actualizaciones del software de Sophos.

Para diagnosticar el problema y actualizar los ordenadores:

1. En la vista **Estaciones**, seleccione el grupo que contiene equipos no actualizados.
2. En la ficha **Estado**, haga clic en el encabezado de la columna **Actualizado** para ordenar los ordenadores por su estado de actualización.
3. Abra la ficha **Detalles de la actualización** y mire en la columna **Servidor primario**. Aquí se muestra el directorio que utiliza cada ordenador para actualizarse.
4. Observe los ordenadores que se actualizan desde un directorio en concreto.
   - *Si algunos de ellos tienen una protección obsoleta y otros no*, el problema radica en los equipos individuales. Selecciónelos, haga clic con el botón derecho y seleccione **Actualizar ordenadores ahora**.
   - *Si todos tienen una protección obsoleta*, el problema podría estar en el directorio. En el menú **Ver**, seleccione **Gestores de actualización**. Seleccione el gestor de actualización que mantiene el directorio que cree que no está actualizado, haga clic con el botón derecho y seleccione **Actualizar ahora**. Después, en el menú **Ver**, haga clic en **Estaciones**. Seleccione los ordenadores no actualizados, haga clic con el botón derecho del ratón y seleccione **Actualizar ordenadores ahora**.

   Si tiene varios gestores de actualización y no sabe cuál actualiza el directorio obsoleto, utilice el informe de jerarquía de actualización para ver qué gestores actualizan cada unidad compartida. Para ver el informe de jerarquía de actualización, en el menú **Herramientas**, haga clic en **Gestor de informes**. En el cuadro de diálogo **Gestor de informes**, seleccione **Jerarquía de actualización** y haga clic en **Crear**. Revise la sección del informe "Unidades compartidas administradas por gestores de actualización".

7 Configurar las políticas

7.1 Política antivirus y HIPS

Las políticas antivirus y HIPS permiten:

- Detectar virus, troyanos, gusanos y programas espía de forma automática tan pronto como un usuario intente copiar, mover o abrir un archivo infectado.
- Detectar programas publicitarios y otras aplicaciones no deseadas.
- Detectar archivos sospechosos y rootkits.
- Detectar tráfico malicioso, es decir, comunicaciones entre estaciones de trabajo y servidores de comando y control involucrados en ataques de redes de bots u otros ataques de programas maliciosos.
- Limpiar automáticamente elementos con virus u otras amenazas.

  Para más información sobre la limpieza automática, consulte Configurar la limpieza automática del escaneado en acceso (página 79).
- Analizar el comportamiento de los programas que se ejecutan en el sistema.

  Para obtener más información, consulte Control de comportamiento (página 89).
- Escanee los equipos a horas determinadas.

  Para obtener más información, consulte Crear un escaneado programado (página 83).

Podrá utilizar una configuración diferente para cada grupo de ordenadores. Para más información sobre la configuración del escaneado, vea las siguientes secciones:

- Configurar el escaneado en acceso (página 77)
- Configurar el escaneado programado (página 84)

Nota
El equipo de SophosLabs puede controlar de forma independiente los archivos que se escanean. Puede añadir o eliminar el escaneado de determinados tipos de archivos para ofrecer la mejor protección.

Para más información sobre las opciones de escaneado y limpieza que no son compatibles en Mac, Linux o UNIX, consulte Opciones que no se aplican a Mac, Linux o UNIX (página 75).

Para información sobre las opciones de escaneado y desinfección que no aplican a Sophos Anti-Virus para VMware vShield, consulte el artículo 121745 de la base de conocimiento de Sophos. En el caso de Sophos Anti-Virus para VMware vShield, versión 2.x, consulte también la *guía de configuración de Sophos Anti-Virus para VMware vShield* disponible en www.sophos.com/es-es/support/documentation/sophos-anti-virus-for-vmware-vshield.

7.1.1 Opciones que no se aplican a Mac, Linux o UNIX

Todas las opciones de escaneado y limpieza en Windows se pueden administrar desde Enterprise Console, sin embargo, algunas de estas opcines no se aplican a Mac, Linux o UNIX.

Mac OS X

Para más información sobre la configuración de la política antivirus y HIPS que aplica en equipos Mac, consulte el artículo 118859 en la base de conocimiento de Sophos.

Linux

Las siguientes opciones de limpieza automática no se aplican a equipos Linux.

Opciones de limpieza automática para el escaneado en acceso:

- **Denegar acceso y mover a la carpeta predeterminada**
- **Denegar acceso y mover a**

Opciones de limpieza automática para el escaneado programado:

- **Mover a la carpeta predeterminada**
- **Mover a**

Para más información sobre la limpieza automática, consulte Configurar la limpieza automática en el escaneado programado (página 86) y Limpieza automática para el escaneado programado (página 86).

Para más información sobre la configuración de la política antivirus y HIPS que aplica en equipos Linux, consulte el artículo 117344 en la base de conocimiento de Sophos.

UNIX

- Enterprise Console no puede realizar escaneados en acceso en equipos UNIX.

  Puede configurar el escaneado programado, las alertas, el registro y la actualización de forma centralizada desde Enterprise Console.

  Nota
  Ciertos parámetros no se pueden configurar desde Enterprise Console. Utilice la línea de comandos de Sophos Anti-Virus en cada estación UNIX para configurar estos parámetros de forma local. Enterprise Console ignora estos parámetros.

  El escaneado en demanda también se puede configura desde la línea de comandos de Sophos Anti-Virus en cada estación UNIX.

  Para más información sobre la configuración adicional local de Sophos Anti-Virus para UNIX, consulte la *Guía de configuración de Sophos Anti-Virus para UNIX*.
- Las siguientes opciones de limpieza automática para el escaneado programado no se aplican a equipos UNIX.
  - **Mover a la carpeta predeterminada**
  - **Mover a**

  Para más información sobre la limpieza automática en el escaneado programado, consulte Limpieza automática para el escaneado programado (página 86).

Para más información sobre la configuración de la política antivirus y HIPS que aplica en equipos UNIX, consulte el artículo 117344 en la base de conocimiento de Sophos.

7.1.2 Escaneado en acceso

Recomendaciones para el escaneado en acceso

Esta sección contiene recomendaciones para sacar el mayor provecho del escaneado en acceso.

Se recomienda usar la configuración predeterminada del escaneado en acceso, ya que ofrece el mejor equilibrio entre protección y consumo de recursos. Para más información sobre la configuración recomendada del escaneado en acceso, vea el artículo 114345 en la base de conocimiento de Sophos (http://www.sophos.com/es-es/support/knowledgebase/114345.aspx).

Se recomienda consultar la *Guía de configuración de políticas de Sophos Enterprise Console* para conocer el uso y administración recomendados para el software de seguridad de Sophos. La documentación de Sophos se encuentra en http://www.sophos.com/es-es/support/documentation.

Configurar el escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Atención
El escaneado en acceso no puede escanear elementos cifrados. Modifique el proceso de inicio del sistema para que los archivos se puedan escanear cuando se active el escaneado en acceso. Para más información sobre cómo utilizar la política Antivirus y HIPS en sistemas con encriptación, consulte el artículo 12790 de la base de conocimiento de Sophos.

Para configurar el escaneado en acceso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, junto a la opción **Activar el escaneado en acceso**, haga clic en **Configurar**.
5. Para cambiar cuándo ocurre el escaneado en acceso, en la sección **Comprobar archivos al**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Leer	• Se escanean los archivos que se copian, mueven o abren. • Se escanean los programas que se ejecutan.

Opción	Descripción
Cambiar nombre	Se escanean los archivos que se cambian de nombre.
Escribir	Se escanean los archivos que se crean o guardan.

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

Opción	Descripción
Adware y PUA	• Los programas publicitarios muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. • Las aplicaciones no deseadas (PUA, Potentially Unwanted Applications) no son maliciosas, pero se consideran inapropiadas en redes corporativas..
Archivos sospechosos	Los archivos sospechosos contienen ciertas características habituales en los programas maliciosos (por ejemplo, código de descompresión dinámica). Sin embargo, sólo con estas características no es posible identificar un archivo como malicioso. **Nota** Esta opción sólo está disponible en Sophos Endpoint Security and Control para Windows.

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

Opción	Descripción
Permitir el acceso a unidades con sectores de arranque infectados	Permite el acceso a unidades externas como CD-ROM, disquetes o unidades USB que tengan el sector de arranque infectado. Sólo debería utilizar esta opción bajo las indicaciones del soporte técnico de Sophos.
Escanear archivos comprimidos	Escanea el contenido de archivos comprimidos al descargarlos o enviarlos por email. Se recomienda **desactivar** esta opción ya que puede ralentizar el escaneado. El contenido de los archivos comprimidos se escanea: • Cuando se realiza la extracción.

Opción	Descripción
	• Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.
Escanear memoria del sistema	Realiza un escaneado en segundo plano cada hora para detectar amenazas en la memoria del sistema.

Activar o desactivar el escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, Sophos Endpoint Security and Control escanea archivos antes de su uso y deniega el acceso a menos que el archivo esté limpio.

Es probable que decida desactivar el escaneado en acceso en servidores Exchange u otros servidores en los que el rendimiento pueda verse afectado. En este caso, coloque los servidores en un grupo especial y cambie la política antivirus y HIPS para el grupo tal como se describe más abajo.

Para activar o desactivar el escaneado en acceso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**. A continuación, haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
3. En el panel **Escaneado en acceso**, utilice la opción **Activar el escaneado en acceso**.

Importante
Si desactiva el escaneado en acceso en un servidor, recomendamos que configure escaneados programados en los ordenadores pertinentes. Para más información, consulte Crear un escaneado programado (página 83).

Configurar la limpieza automática del escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, Sophos Endpoint Security and Control realiza la limpieza automática al detectar virus u otras amenazas. Para modificar la limpieza automática del escaneado en acceso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.

Consulte Comprobar qué políticas usa un grupo (página 25).

2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, junto a la opción **Activar el escaneado en acceso**, haga clic en **Configurar**.
5. En el cuadro de diálogo **Configuración del escaneado en acceso**, abra la ficha **Limpieza**.
6. Las opciones disponibles se describen en Limpieza automática para el escaneado en acceso (página 80).

Limpieza automática para el escaneado en acceso

Virus/spyware

Utilice la opción **Limpiar automáticamente elementos con virus/spyware**.

También puede especificar qué hacer con los elementos si la limpieza falla:

- **Sólo denegar acceso**
- **Borrar**
- **Denegar acceso y mover a la carpeta predeterminada**
- **Denegar acceso y mover a <ruta UNC>**

Nota
Las opciones **Denegar acceso y mover a la carpeta predeterminada** y **Denegar acceso y mover a** no son compatibles con Linux o UNIX y se ignorarán.

Archivos sospechosos

Nota
Estas opciones sólo son compatibles con Windows.

Especifique qué hacer con los archivos sospechosos detectados:

- **Sólo denegar acceso**
- **Borrar**
- **Denegar acceso y mover a la carpeta predeterminada**
- **Denegar acceso y mover a <ruta UNC>**

Especificar extensiones de archivo del escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, junto a la opción **Activar el escaneado en acceso**, haga clic en **Configurar**.
5. Abra la ficha **Extensiones** y configure las opciones según se describe a continuación.

Opción	Descripción
Escanear todos los archivos	Se escanean todos los archivos independientemente de la extensión. Si activa esta opción, se desactivan el resto de opciones en la ficha **Extensiones**. Sólo se recomienda utilizar esta opción en un escaneado semanal, ya que puede afectar al rendimiento del sistema.
Escanear sólo los archivos ejecutables o vulnerables	• Se escanean todos los archivos ejecutables (por ejemplo, .exe, .bat, .pif) o archivos que se pueden infectar (por ejemplo, .doc, .chm, .pdf). • Se comprueba la estructura de todos los archivos y se escanean aquellos que pueden ser ejecutables.
Extensiones adicionales a escanear	Para escanear tipos de archivo adicionales, haga clic en **Añadir** y escriba la nueva extensión, como PDF, en el campo **Extensión**. Puede utilizar el comodín ? para indicar cualquier carácter posible. Para quitar alguna extensión, selecciónela y haga clic en **Eliminar**. Para modificar alguna extensión, selecciónela y haga clic en **Editar**.
Escanear archivos sin extensión	Archivos sin extensión pueden pertenecer a programas maliciosos, por lo que se recomienda activar esta opción.
Excluir	Para excluir tipos de archivo del escaneado en acceso, haga clic en **Añadir** y escriba la extensión, como PDF, en el campo **Extensión**. Para quitar alguna extensión, selecciónela y haga clic en **Eliminar**. Para modificar alguna extensión, selecciónela y haga clic en **Editar**.

Excluir elementos del escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Es posible excluir elementos del escaneado en acceso.

Nota
Estas opciones sólo se aplican a Windows, Mac OS X y Linux.

Enterprise Console no puede realizar escaneados en acceso en equipos UNIX.

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**. A continuación, haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
3. En el panel **Escaneado en acceso**, haga clic en el botón **Configurar**.
4. Seleccione **Exclusiones de Windows**, **Exclusiones de Mac** o **Exclusiones de Linux/UNIX**. Para agregar elementos a la lista, haga clic en **Añadir** y escriba la ruta completa al elemento en el cuadro de diálogo **Exclusión de elementos**.

   Los elementos que puede excluir del escaneado difieren según el sistema operativo. Consulte Elementos que pueden excluirse del escaneado (página 98).

   Para excluir archivos que no se encuentren en los discos duros locales, seleccione la opción **Excluir archivos remotos**. Seleccione esta opción si desea incrementar la velocidad de acceso a archivos remotos en ubicaciones seguras.

Importante
Si selecciona la opción **Excluir archivos remotos** en la ficha **Exclusiones de Windows**, el control de datos no comprobará los archivos utilizados desde unidades compartidas en la red. Esto se debe a que el control de datos utiliza el mismo conjunto de exclusiones que el escaneado en acceso de Sophos Anti-Virus (InterCheck ™). Si se desactiva el escaneado de archivos remotos, no se enviará ningún archivo remoto para una comprobación del control de datos. Esta restricción no afecta a unidades de almacenamiento.

Es posible exportar e importar la lista de exclusiones de Windows. Para obtener más información, consulte Importar y exportar exclusiones del escaneado en acceso (página 82).

Importar y exportar exclusiones del escaneado en acceso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Es posible exportar e importar la lista de exclusiones de Windows en el escaneado en acceso.

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, junto a la opción **Activar el escaneado en acceso**, haga clic en **Configurar**.
5. En la ficha **Exclusiones de Windows**, haga clic en **Exportar** o **Importar**.

7.1.3 Escaneado en demanda y programado

En el panel **Escaneado en demanda** de la política **Antivirus y HIPS**, puede:

- Configurar escaneados programados.
- Configure las opciones de escaneado como las extensiones y exclusiones para todos los tipos de escaneado en demanda: los escaneados programados, el escaneado completo del sistema y los escaneados en demanda predeterminados en ordenadores individuales.

Crear un escaneado programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Utilice un escaneado programado para que Sophos Endpoint Security and Control compruebe el sistema a las horas establecidas.

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en demanda**, en **Configurar y gestionar escaneados programados**, haga clic en **Añadir**.
   Aparece el cuadro de diálogo **Configuración del escaneado programado**.
5. En el cuadro de texto **Nombre del escaneado**, indique un nombre descriptivo para el nuevo escaneado.
6. En la sección **Escanear**, seleccione los elementos a escanear. Por defecto se escanearán los discos duros locales y las unidades montadas en UNIX.
7. En la sección **Horario de escaneado**, seleccione los días de escaneado.
8. Para especificar las horas de escaneado, haga clic en **Añadir**.
   - Para modificar una hora establecida, selecciónela en la lista **Horas de escaneado** y haga clic en **Editar**.
   - Para borrar una hora establecida, selecciónela en la lista **Horas de escaneado** y haga clic en **Eliminar**.

Nota
Si se detecta alguna amenaza en la memoria, y no tiene activada la limpieza automática, el escaneado se detiene y se envía una alerta a Enterprise Console. Esto se debe a que si se continua con el escaneado, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneado.

Para configurar las opciones de escaneado y limpieza, vea las siguientes secciones:

- Configurar el escaneado programado (página 84)
- Configurar la limpieza automática del escaneado en acceso (página 79)

Configurar el escaneado programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para configurar el escaneado programado:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En la lista **Configurar y gestionar escaneados programados**, seleccione el escaneado y haga clic en **Editar**.
5. En el cuadro de diálogo **Configuración del escaneado programado**, haga clic en **Configurar**.
6. En la sección **Detectar**, seleccione las opciones correspondientes según se describe a continuación.

Opción	Descripción
Adware y PUA	• Los programas publicitarios muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. • Las aplicaciones no deseadas (PUA, Potentially Unwanted Applications) no son maliciosas, pero se consideran inapropiadas en redes corporativas..
Archivos sospechosos	Los archivos sospechosos contienen ciertas características habituales en los programas maliciosos (por ejemplo, código de descompresión dinámica). Sin embargo, sólo con estas características no es posible identificar un archivo como malicioso.

Opción	Descripción
	Nota Esta opción sólo está disponible en Sophos Endpoint Security and Control para Windows.
Rootkits	Los rootkits son troyanos o tecnología que se utiliza para ocultar la presencia de un objeto malicioso (proceso, archivo, clave del registro o puerto de red) ante el usuario o el administrador.

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

Opción	Descripción
Escanear archivos comprimidos	Permite escanear el contenido de archivos comprimidos. No se recomienda utilizar esta opción en escaneados programados ya que puede incrementar notablemente el tiempo de escaneado. En su lugar, utilice el escaneado en acceso (de lectura y escritura) para proteger la red. De esta forma, el contenido de los archivos comprimidos se comprobará cuando se abran. Si desea escanear archivos comprimidos en ciertos equipos mediante escaneados programados, se recomienda lo siguiente: • Cree un escaneado programado nuevo. • En el cuadro de diálogo **Configurar > Configuración del escaneado en demanda**, en la ficha **Extensiones**, añada solo las extensiones de archivos comprimidos a la lista de extensiones que se escanearán. • Desactive la opción **Escanear todos los archivos**. De esta forma se comprobarán los archivos comprimidos en el menor tiempo posible.
Escanear memoria del sistema	Realiza un escaneado en segundo plano cada hora para detectar amenazas en la memoria del sistema.
Ejecutar escaneado con baja prioridad	En Windows Vista y posterior, realiza los escaneados programados en baja prioridad

Opción	Descripción
	para minimizar el impacto en los recursos del sistema.

Para más información sobre la configuración del escaneado programado, vea el artículo 63985 en la base de conocimiento de Sophos.

Configurar la limpieza automática en el escaneado programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, Sophos Endpoint Security and Control realiza la limpieza automática al detectar virus u otras amenazas. Para modificar la limpieza automática del escaneado en acceso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En la lista **Configurar y gestionar escaneados programados**, seleccione el escaneado y haga clic en **Editar**.
5. Junto a **Opciones de escaneado y desinfección**, haga clic en **Configurar**.
   Se mostrará el cuadro de diálogo **Configuración de escaneado y limpieza**.
6. Abra la ficha **Limpieza**.
7. Las opciones disponibles se describen en Limpieza automática para el escaneado en acceso (página 80).

Limpieza automática para el escaneado programado

Virus/spyware

Utilice la opción **Limpiar automáticamente elementos con virus/spyware**.

También puede especificar qué hacer con los elementos si la limpieza falla:

- **Sólo registrar**
- **Borrar**
- **Mover a la carpeta predeterminada**
- **Mover a <ruta UNC>**

Notas

- Mover un archivo ejecutable reduce la probabilidad de activarlo.
- No es posible mover de forma automática componentes de una infección múltiple.

Adware y PUA

Utilice la opción **Limpiar automáticamente elementos con adware/PUA**.

Nota

- Esta opción sólo se aplica a Windows.

Archivos sospechosos

Especifique qué hacer con los archivos sospechosos detectados:

- **Sólo registrar**
- **Borrar**
- **Mover a la carpeta predeterminada**
- **Mover a <ruta UNC>**

Notas

- Estas opciones sólo son compatibles con Windows.
- Mover un archivo ejecutable reduce la probabilidad de activarlo.
- No es posible mover de forma automática componentes de una infección múltiple.

Especificar extensiones de archivo del escaneado en demanda y programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en demanda**, haga clic en **Configurar**.
   Aparece el cuadro de diálogo **Configuración del escaneado en demanda**.
5. En la ficha **Extensiones**, configure las opciones según se describe a continuación.

Opción	Descripción
Escanear todos los archivos	Se escanean todos los archivos independientemente de la extensión. Si activa esta opción, se desactivan el resto de opciones en la ficha **Extensiones**.

Opción	Descripción
	Sólo se recomienda utilizar esta opción en un escaneado semanal, ya que puede afectar al rendimiento del sistema.
Escanear sólo los archivos ejecutables o vulnerables	• Se escanean todos los archivos ejecutables (por ejemplo, .exe, .bat, .pif) o archivos que se pueden infectar (por ejemplo, .doc, .chm, .pdf). • Se comprueba la estructura de todos los archivos y se escanean aquellos que pueden ser ejecutables.
Extensiones adicionales a escanear	Para escanear tipos de archivo adicionales, haga clic en **Añadir** y escriba la nueva extensión, como PDF, en el campo **Extensión**. Puede utilizar el comodín ? para indicar cualquier carácter posible. Para quitar alguna extensión, selecciónela y haga clic en **Eliminar**. Para modificar alguna extensión, selecciónela y haga clic en **Editar**.
Escanear archivos sin extensión	Archivos sin extensión pueden pertenecer a programas maliciosos, por lo que se recomienda activar esta opción.
Excluir	Para excluir tipos de archivo del escaneado programado, haga clic en **Añadir** y escriba la extensión, como PDF, en el campo **Extensión**. Para quitar alguna extensión, selecciónela y haga clic en **Eliminar**. Para modificar alguna extensión, selecciónela y haga clic en **Editar**.

Para más información sobre la configuración de extensiones del escaneado programado, vea el artículo 63985 en la base de conocimiento de Sophos.

Excluir elementos del escaneado en demanda y programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede excluir elementos del escaneado en demanda y programado.

Nota
La exclusión de elementos de los escaneados programados también se aplica a los escaneados remotos ejecutados desde la consola y a los escaneados individuales ejecutados en cada ordenador de la red. Consulte Escaneado remoto (página 51).

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**. A continuación, haga doble clic en la política que desee modificar.
3. Aparece el cuadro de diálogo **Política antivirus y HIPS**. En el panel **Escaneado en demanda**, haga clic en **Configurar**.
4. Abra las fichas **Exclusiones de Windows**, **Exclusiones de Linux/UNIX** o **Exclusiones de Mac**. Para agregar elementos a la lista, haga clic en **Añadir** y escriba la ruta completa al elemento en el cuadro de diálogo **Exclusión de elementos**.
   Los elementos que puede excluir del escaneado difieren según el sistema operativo. Consulte Elementos que pueden excluirse del escaneado (página 98).

Es posible exportar e importar la lista de exclusiones de Windows. Para obtener más información, consulte Importar y exportar exclusiones del escaneado en acceso (página 82).

Importar y exportar exclusiones de Windows del escaneado en demanda y programado

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede exportar la lista de exclusiones de Windows para el escaneado en demanda y programado a un archivo y luego importarlo a otra política.

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en demanda**, haga clic en **Configurar**.
5. En la ficha **Exclusiones de Windows**, haga clic en **Exportar** o **Importar**.

7.1.4 Control de comportamiento

Integrado en el escaneado en acceso, el sistema de control de comportamiento de Sophos protege equipos Windows contra amenazas desconocidas y comportamiento sospechoso.

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

- Detección de comportamiento malicioso o sospechoso

- Detección de tráfico malicioso
- Detección de desbordamiento del búfer

Detección de comportamiento malicioso o sospechoso

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

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

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

Detección de tráfico malicioso

La detección de tráfico malicioso detecta las comunicaciones entre ordenadores y servidores de comando y control utilizados en un ataque de bots u otros ataques maliciosos.

Nota
La detección de tráfico malicioso requiere que Sophos Live Protection esté activado a fin de de realizar búsquedas y obtener los datos. (Por defecto, la protección activa de Sophos está activada.)

Detección de desbordamiento del búfer

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

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

Activar o desactivar control de comportamiento

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, el control de comportamiento está activado.

Para activar o desactivar el control de comportamiento:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar. Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.

3. Haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, active o desactive la opción **Activar el control de comportamiento**.

Detectar comportamiento malicioso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Por defecto, la detección de comportamiento malicioso está activada.

Para configurar el sistema de detección de comportamiento malicioso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, asegúrese de que la opción **Activar el control de comportamiento** está marcada.
5. Junto a **Activar el control de comportamiento**, haga clic en **Configurar**.
6. En el cuadro de diálogo **Configuración del control de comportamiento**:
   - Para detectar y alertar ante comportamiento malicioso, seleccione la opción **Detectar comportamiento malicioso**.
   - Para desactivar la detección de comportamiento malicioso, desactive la opción **Detectar comportamiento malicioso**.

     Nota
     Al desactivar la detección de comportamiento malicioso, también se desactiva la detección de comportamiento sospechoso. Tenga en cuenta que la detección de tráfico malicioso **no** se desactivará.

Detectar tráfico malicioso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

  Para obtener más información, consulte Administrar roles y subentornos (página 13).
- La detección de tráfico malicioso requiere que Sophos Live Protection esté activado. (Por defecto, la protección activa de Sophos está activada.)

La detección de tráfico malicioso detecta las comunicaciones entre ordenadores y servidores de comando y control utilizados en un ataque de bots u otros ataques maliciosos.

Nota
La detección de tráfico malicioso utiliza el mismo conjunto de exclusiones que el escaneado en acceso del Anti-Virus de Sophos (InterCheck ™). Para más información sobre las exclusiones del escaneado en acceso, consulte Excluir elementos del escaneado en acceso (página 82).

Por defecto, la detección de tráfico malicioso está activada en las instalaciones nuevas de Enterprise Console 5.3 o posterior. En caso de actualizar desde una versión anterior de Enterprise Console, es necesario activar la detección de tráfico malicioso para poder aprovechar esta función.

Para cambiar la configuración de la detección de tráfico malicioso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, asegúrese de que la opción **Activar el control de comportamiento** está marcada.
5. Junto a **Activar el control de comportamiento**, haga clic en **Configurar**.
6. En el cuadro de diálogo **Configuración del control de comportamiento** asegúrese de que la opción **Detectar comportamiento malicioso** está activada.
7. Para activar o desactivar la detección de tráfico malicioso, active o desactive la opción **Detectar tráfico malicioso**.

Detectar comportamiento sospechoso

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Por defecto, el comportamiento sospechoso se detecta y notifica, pero no se bloquea.

Para configurar el sistema de detección de comportamiento sospechoso:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, asegúrese de que la opción **Activar el control de comportamiento** está marcada.
5. Junto a **Activar el control de comportamiento**, haga clic en **Configurar**.
6. En el cuadro de diálogo **Configuración del control de comportamiento**, asegúrese de que la opción **Detectar comportamiento malicioso** está marcada.

- Para alertar al administrador y bloquear procesos sospechosos, utilice la opción **Detectar comportamiento sospechoso** y desactive la opción **Sólo alertar ante comportamiento sospechoso**.
- Para alertar al administrador, pero no bloquear procesos sospechosos, utilice la opción **Detectar comportamiento sospechoso** y active la opción **Sólo alertar ante comportamiento sospechoso**.

Para una protección más completa, se recomienda detectar comportamiento sospechoso. Consulte Configurar el escaneado en acceso (página 77).

Detectar desbordamientos del búfer

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Por defecto, los desbordamientos de búfer se detectan y bloquean.

Para configurar el sistema de detección de desbordamiento búfer:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política antivirus y HIPS**.
4. En el panel **Escaneado en acceso**, asegúrese de que la opción **Activar el control de comportamiento** está marcada.
5. Junto a **Activar el control de comportamiento**, haga clic en **Configurar**. En el cuadro de diálogo **Configuración del control de comportamiento**:
   - Para detectar y alertar ante el desbordamiento del búfer, utilice la opción **Detectar desbordamiento del búfer** y desactive la opción **Sólo alertar**.
   - Para alertar pero no bloquear ante el desbordamiento del búfer, utilice la opción **Detectar desbordamiento del búfer** y active la opción **Sólo alertar**.

7.1.5 Protección activa de Sophos

La protección activa de Sophos utiliza la conexión a Internet para comprobar archivos sospechosos.

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

Para sacar el mayor partido de la protección activa debe seleccionar las siguientes opciones.

- **Activar la protección activa**

  Si el escaneado en acceso en una estación de trabajo detecta algún archivo sospechoso pero no consigue identificarlo con los datos de identidad de amenazas (IDE) de dicha estación, se enviarán determinados datos del archivo, como la suma de comprobación, a Sophos para

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

Importante
Las funciones Detección de tráfico malicioso y Reputación de descargas requieren que la protección activa esté activada para poder realizar búsquedas instantáneas en la base de datos online de SophosLabs y obtener los últimos datos de reputación o amenazas.

- **Activar protección activa para el escaneado en demanda**

  Si desea que los escaneados en demanda utilicen la misma comprobación en la nube que el escaneado en acceso, seleccione esta opción.

- **Enviar automáticamente muestras de archivos a Sophos**

  Si algún archivo sospechoso no se puede identificar mediante los datos iniciales, la protección activa permite enviar una muestra del mismo a Sophos. Cuando la protección activa está activada, si activa esta opción y Sophos no dispone todavía de una muestra del archivo, este se enviará de forma automática.

  De esta forma Sophos podrá mejorar la detección de amenazas.

Nota
El tamaño máximo de cada muestra es 10 MB. El tiempo de espera para la carga de muestras es 30 segundos. No se recomienda enviar muestras de forma automática con conexiones lentas (menos de 56 Kbps).

Importante
Debe asegurarse de que el dominio Sophos es un sitio de confianza en su filtrado web para poder enviar los datos necesarios. Para más información, consulte el artículo 62637 de la base de conocimiento (http://www.sophos.com/es-es/support/knowledgebase/62637.aspx).

Si utiliza los productos de filtrado web de Sophos, por ejemplo WS1000 Web Appliance, el dominio Sophos ya se considera de confianza.

Activar o desactivar la protección activa de Sophos

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Sophos Live Protection compara los archivos sospechosos con la información más reciente de la base de datos de SophosLabs.

Por defecto, Live Protection envía a Sophos datos de archivos como sumas de verificación para su comprobación, pero no envía archivos de muestra para el análisis. Para sacar el máximo partido de Live Protection, es recomendable seleccionar la opción de enviar archivos de muestra.

Para activar o desactivar la protección activa:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.

Consulte Comprobar qué políticas usa un grupo (página 25).

2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en el botón **Protección activa de Sophos**.
4. En el cuadro de diálogo **Protección activa de Sophos**:

   - Marque o desmarque la casilla **Activar la protección activa** Esto activa o desactiva la protección activa para el escaneado en acceso.

     Importante
     Las funciones Detección de tráfico malicioso y Reputación de descargas requieren que la protección activa esté activada para poder realizar búsquedas instantáneas en la base de datos online de SophosLabs y obtener los últimos datos de reputación o amenazas.

   - Marque o desmarque la casilla **Activar protección activa para el escaneado en demanda**. Esto activa o desactiva la protección activa para el escaneado en en demanda.
   - Marque o desmarque la casilla **Enviar automáticamente muestras de archivos a Sophos**.

     Las muestras solo se pueden enviar si está activada la protección activa.

     Nota
     Cuando se envía una muestra de archivo a Sophos para el escaneado online, los datos de archivo (como la suma de verificación) se envían siempre con la muestra.

7.1.6 Protección web

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

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

Filtrado activo de direcciones web

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

Nota
Para un mayor control sobre los sitos web que se permiten visitar, utilice la función de control web. Para obtener más información, consulte Política de control web (página 165).

Escaneado de contenido

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

Reputación de descarga

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

Nota
La reputación de descarga solo es compatible en Windows 7 o posterior.

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

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

Para más información sobre la reputación de descargas, consulte el artículo de la base de conocimiento 121319.

Opciones de configuración de la protección web

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

Para más información sobre las opciones de configuración de la protección web y cómo cambiarlas, consulte Configurar las opciones de protección web (página 97).

Navegadores de Internet compatibles

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

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

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

Eventos de la protección web

Cuando se bloquea el acceso a un sitio web malicioso, se registra un evento que se puede consultar mediante el Visualizador de eventos web o en el cuadro de **Detalles del ordenador**. Si utiliza la función de control web, los eventos de la protección web y del control web aparecen en el Visualizador de eventos web y en **Detalles del ordenador**. Consulte Visualizar eventos del control web (página 192) y Visualizar los eventos del control web más recientes (página 193).

Configurar las opciones de protección web

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para activar o desactivar la protección web:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
4. En el cuadro de diálogo de la política **Antivirus y HIPS**, haga clic en el botón **Protección web**.
5. En el cuadro de diálogo **Protección web**, en **Protección contra aplicaciones maliciosas**, junto a **Bloquear acceso a sitios web maliciosos**, seleccione **Sí** o **No** para bloquear o desbloquear el acceso a sitios web maliciosos. Esta opción está activada por defecto.
   Para más información sobre cómo autorizar sitios web específicos, consulte Autorizar sitios web (página 105).
6. Para activar o desactivar escaneado de datos y archivos descargados, junto a **Escaneado de contenido**, seleccione **Como en acceso**, **Sí**, o **No**.
   La opción predeterminada es **Como en acceso**, es decir, se ajusta al estado del escaneado en acceso.
7. Para cambiar lo que ocurre cuando un usuario intenta descargar un archivo con una reputación baja o desconocida, en **Reputación de descarga**, junto a **Acción**, seleccione **Preguntar al usuario** (predeterminado) o **Solo registrar**.

   Nota
   La reputación de descarga requiere que Sophos Live Protection esté activado. (Por defecto, la protección activa de Sophos está activada.)

   - Si se selecciona **Preguntar al usuario**, cada vez que un usuario intente descargar un archivo de baja reputación, se mostrará una alerta preguntando si se desea bloquear o permitir la descarga. Recomendamos que los usuarios no descarguen este tipo de archivos. Si confían en la fuente y el editor del archivo, tienen la opción de descargar el archivo. La decisión de bloquear o permitir la descarga y la URL del archivo se registrarán en el registro de escaneado y como evento web en Enterprise Console.
   - Si selecciona **Solo registrar**, no se mostrará ninguna alerta; se permitirá la descarga y se registrará en el registro de escaneado y como evento web en Enterprise Console.

8. Para seleccionar el nivel de rigurosidad del escaneado de reputación, junto a **Umbral**, seleccione **Recomendado** (predeterminado) o **Estricto**.
   - Si selecciona **Recomendado**, se mostrará una alerta y/o se creará un registro o un evento cada vez que un usuario intente descargar un archivo con una reputación baja o desconocida.
   - Con **Estricto**, se mostrará una alerta y/o se creará un registro o un evento cada vez que un usuario intente descargar un archivo con una reputación baja, desconocida o media.

7.1.7 Tipos de archivos escaneados y exclusiones

Por defecto, Sophos Endpoint Security and Control escanea los tipos de archivo que pueden contener virus. La lista predeterminada de tipos de archivo a escanear varía según el sistema operativo y se actualiza con el producto.

Para ver la lista de tipos de archivo, vaya a un equipo con el sistema operativo correspondiente, abra Sophos Endpoint Security and Control o Sophos Anti-Virus y vea el cuadro de configuración de extensiones.

Se pueden escanear tipos de archivo adicionales o excluir algunos del escaneado.

Windows

Para ver la lista de los tipos de archivo escaneados en Windows:

1. Abra Sophos Endpoint Security and Control.
2. En **Antivirus y HIPS**, haga clic en **Configurar el antivirus y HIPS** y seleccione **Extensiones y exclusiones en demanda**.

Para más información sobre extensiones y exclusiones del escaneado en Windows, vea las siguientes secciones:

- Especificar extensiones de archivo del escaneado en acceso (página 80)
- Especificar extensiones de archivo del escaneado en demanda y programado (página 87)

Mac OS X

Sophos Anti-Virus para Mac OS X analiza todos los tipos de archivo durante el scanedo en acceso. Para cambiar las opciones del escaneado programado, consulte Especificar extensiones de archivo del escaneado en demanda y programado (página 87).

Linux o UNIX

En equipos Linux, utilice el comando `savconfig` y `savscan` como se describe en la *Guía de configuración de Sophos Anti-Virus para Linux*.

En equipos UNIX, utilice el comando `savscan` como se describe en la *Guía de configuración de Sophos Anti-Virus para UNIX*.

Elementos que pueden excluirse del escaneado

Los elementos que se pueden excluir del escaneado varían según el sistema operativo.

Windows

En Windows, puede excluir unidades, carpetas, archivos y procesos.

Se permite el uso de los caracteres comodín * y ?

El 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 un 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.

Mac OS X

En Mac OS X, se pueden excluir volúmenes, carpetas y archivos.

Se pueden especificar los ítems a excluir colocando delante o detrás de la exclusión una barra inclinada o una doble barra inclinada.

Para más información, consulte la *Ayuda de Sophos Anti-Virus para Mac OS X*.

Linux o UNIX

En Linux y UNIX, se pueden excluir directorios y archivos.

Puede indicar una ruta de acceso POSIX tanto para archivos como para carpetas, por ejemplo, /carpeta/archivo. Se permite el uso de los caracteres comodín ? y *.

Nota
Enterprise Console sólo permite exclusiones Linux y UNIX mediante ruta de acceso. En las estaciones podrá establecer otro tipo de exclusiones para poder utilizar expresiones normales y excluir tipos y sistemas de archivos. Para más información sobre cómo hacerlo, consulte la *Guía de configuración de Sophos Anti-Virus para Linux* o la *Guía de configuración de Sophos Anti-Virus para UNIX*.

Si configura otra exclusión mediante rutas de acceso en un ordenador Linux o UNIX administrado, la consola recibirá un informe sobre las diferencias de dicho ordenador con la política del grupo.

Para más información sobre las exclusiones del escaneado, vea las siguientes secciones:

- Excluir elementos del escaneado en acceso (página 82)
- Excluir elementos del escaneado en demanda y programado (página 88)

Especificar exclusiones de escaneado en Windows

Nomenclatura estándar

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

Archivos con múltiples extensiones

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

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

Excluir archivos, carpetas o unidades específicos

Tipo de exclusión	Descripción	Ejemplos	Comentarios

Archivo específico	Para excluir un archivo, debe especificar el nombre y la ruta de acceso. La ruta de acceso puede incluir una letra de unidad o un nombre de recurso compartido de red.	`C:\Documentos \CV.doc`
		`\\servidor \Usuarios \Documentos \CV.doc`
			Para asegurar que la exclusión se aplica siempre correctamente, añada tanto el nombre largo como en formato 8.3:
			`C:\Archivos de programa \Sophos \Sophos Anti-Virus`
			`C: \Archiv~1\Sophos \Sophos~1`
			Para más información, vea el artículo 13045 en la base de conocimiento.

Todos los archivos con el mismo nombre	Especifique un nombre de archivo sin una ruta de acceso para excluir todos los archivos con ese nombre independientemente de su ubicación en el sistema de archivos.	`spacer.gif`	

Tipo de exclusión	Descripción	Ejemplos	Comentarios
Todos los elementos de una unidad o un recurso compartido de red	Especifique una letra de unidad o un nombre de recurso compartido de red para excluir todos los elementos de esa unidad o recurso compartido de red.	`D:` `\\Servidor\<Unidad compartida>\`	Cuando especifique un recurso compartido de red, incluya una barra diagonal al final del nombre del recurso compartido.
Carpeta específica	Especifique la ruta de acceso de la carpeta incluida la letra de unidad o el nombre de recurso compartido de red para excluir todos los elementos de esa carpeta y niveles inferiores.	`D:\Herramientas\registros\`	Incluya una barra diagonal al final del nombre de la carpeta.
Todas las carpetas con el mismo nombre	Para excluir todas las carpetas con el mismo nombre en **cualquier** unidad local o compartida, indique el nombre de la carpeta sin la unidad.	`\Herramientas\registros\` (excluye las siguientes carpetas: `C:\Herramientas\registros\`, `\\servidor\Herramientas\registros\`)	Debe especificar la ruta de acceso sin la unidad, local o compartida. En este ejemplo, si se especifica `\registros\`, no se excluirá ningún archivo.

Caracteres comodín

Puede utilizar los caracteres comodín ? y *.

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

Al final de un nombre o extensión de archivo, el comodín ? puede sustituir un carácter o ninguno. Por ejemplo, `archivo??.txt` incluiría `archivo.txt`, `archivo1.txt` y `archivo12.txt`, pero no `archivo123.txt`.

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

Uso correcto

`archivo.*`

`*.txt`

Uso incorrecto

```
archivo.txt*
archivo.*txt
```

También se pueden excluir archivos que empiecen de forma concreta y tengan una extensión específica:

```
archivo*.txt
```

El ejemplo anterior excluye los archivos siguientes del escaneado:

```
archivo.txt
archivo1.txt
archivo12.txt
archivo.1.txt
archivo.12.txt
archivo12.12.txt
```

Los archivos siguientes no se excluyen al aplicar la exclusión definida arriba:

```
archivo.1txt
archivo.12txt
archivo.txt1
archivo.txt12
1archivo.txt
1archivo.txt1
```

7.1.8 Autorizar el uso de elementos

Autorizar programas publicitarios y otras aplicaciones no deseadas

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si ha activado Sophos Endpoint Security and Control para detectar programas publicitarios y aplicaciones no deseadas (PUA), es posible que le impida usar una aplicación que desea.

Para autorizar programas publicitarios y otras aplicaciones no deseadas:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. Haga clic en **Gestor de autorización**.
   Se abrirá el cuadro de diálogo **Gestor de autorización**.
5. En la ficha **Adware/PUA**, en la lista **Adware/PUA conocidos**, seleccione la aplicación que desea autorizar.

Si no encuentra la aplicación que desea autorizar, puede añadirla a la lista de forma manual. Para más información sobre cómo hacerlo, consulte Preautorizar programas publicitarios y otras aplicaciones no deseadas (página 103).

6. Haga clic en **Añadir**.

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

Preautorizar programas publicitarios y otras aplicaciones no deseadas

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si desea permitir alguna aplicación que Sophos Endpoint Security and Control todavía no clasifica como programa publicitario o aplicación no deseada, puede preautorizarlo.

1. Visite la página web de **Programas no deseados** en la web de Sophos (http://www.sophos.com/es-es/threat-center/threat-analyses/adware-and-puas.aspx).
2. Localice y copie la aplicación que desea preautorizar.
3. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
4. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
5. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
6. Haga clic en **Gestor de autorización**.
   Se abrirá el cuadro de diálogo **Gestor de autorización**.
7. En la ficha **Adware/PUA**, haga clic en **Nuevo**.
8. En el cuadro de diálogo **Nuevo adware/PUA**, copie el nombre de la aplicación que desea preautorizar.

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

Si ha cometido un error o simplemente desea eliminar una aplicación del **Gestor de autorización**, elimínela de la lista de adware/PUA conocidos:

1. En la lista **Adware/PUA autorizados**, seleccione la aplicación que desea eliminar.
2. Haga clic en **Quitar**.
3. En la lista **Adware/PUA conocidos**, seleccione la aplicación que desea eliminar.
4. Haga clic en **Borrar**.

Bloquear aplicaciones no deseadas y programas publicitarios autorizados

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en el botón **Gestor de autorización**.
4. En la ficha **Adware/PUA**, en la lista **Adware/PUA autorizados**, seleccione el programa que desea bloquear.
5. Haga clic en **Quitar**.

Autorizar elementos sospechosos

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si ha activado una o más opciones de HIPS (como la detección de comportamiento sospechoso, desbordamiento del búfer o archivos sospechosos), pero desea utilizar algunos de los elementos detectados, puede autorizarlos de la forma siguiente:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. Haga clic en **Gestor de autorización**.
   Se abrirá el cuadro de diálogo **Gestor de autorización**.
5. Abra la ficha del tipo de comportamiento detectado.
   En este ejemplo se utiliza **Desbordamiento del búfer**.
6. En la lista de **Aplicaciones conocidas**, seleccione la aplicación a autorizar.
   Si no encuentra la aplicación que desea autorizar, puede añadirla a la lista de forma manual. Para más información sobre cómo hacerlo, consulte Preautorizar programas publicitarios y otras aplicaciones no deseadas (página 103).
7. Haga clic en **Añadir**.

El elemento sospechoso aparece en la lista **Aplicaciones autorizadas**.

Preautorizar elementos sospechosos

Si desea permitir alguna aplicación que Sophos Endpoint Security and Control todavía no clasifica como sospechoso, puede preautorizarlo.

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. Haga clic en **Gestor de autorización**.

Se abrirá el cuadro de diálogo **Gestor de autorización**.

5. Abra la ficha del tipo de comportamiento detectado.
   En este ejemplo se utiliza **Desbordamiento del búfer**.
6. Haga clic en **Nuevo**.
   Se abrirá el cuadro de diálogo **Abrir**.
7. Haga doble clic en la aplicación.

El elemento sospechoso aparece en la lista **Aplicaciones autorizadas**.

Si desea eliminar alguna aplicación de la lista:

1. En el cuadro de diálogo **Gestor de autorización**, abra la ficha del tipo de comportamiento detectado.

   En este ejemplo se utiliza **Archivos sospechosos**.
2. En la lista **Archivos autorizados**, seleccione el archivo.
3. Haga clic en **Quitar**.
4. En la lista **Archivos conocidos**, seleccione el archivo.
5. Haga clic en **Borrar**.

Autorizar sitios web

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

Para autorizar un sitio web:

1. Compruebe qué política antivirus y HIPS usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
3. Haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política antivirus y HIPS**.
4. Haga clic en **Gestor de autorización**.
   Se abrirá el cuadro de diálogo **Gestor de autorización**.
5. En la ficha **Sitios web**, haga clic en **Añadir**.
   - Para modificar una entrada, selecciónela en la lista **Sitios web autorizados** y haga clic en **Editar**.
   - Para borrar una entrada, selecciónela en la lista **Sitios web autorizados** y haga clic en **Eliminar**.

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

Notas

- Al tener el escaneado de descargas activado e intentar visitar un sitio web que contenga una amenaza, se bloqueará el acceso aunque el sitio web esté incluido en la lista de sitios autorizados.
- Si utiliza la función de control web, si autoriza un sitio web que se bloquea en la política de **Control web**, dicho sitio web seguirá bloqueado. Para permitir el acceso deberá crear una excepción en el control web además de autorizar el sitio web en la política Antivirus y HIPS. Para más información sobre el control web, consulte Política de control web (página 165).

7.2 Política cortafuegos

La política **cortafuegos** establece la configuración del cortafuegos en las estaciones de la red.

Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Antes de utilizarlo en la red, configúrelo para permitir las aplicaciones que desea utilizar. Consulte Configurar una política básica del cortafuegos (página 106).

Para ver la lista completa de configuración predeterminada del cortafuegos, vea el artículo 57757 en la base de conocimiento de Sophos.

Nota
Se han eliminado una serie de funciones de Sophos Client Firewall 3.0 para Windows 8 y posterior y solo están disponibles para ordenadores que ejecuten Windows 7 o anterior. Estas funciones son:

- Modo interactivo
- Detección de procesos ocultos
- Detección de memoria modificada
- Aplicaciones de bajo nivel (las conexiones de bajo nivel se tratan igual que otras conexiones)
- Reglas estáticas
- La opción **Conexiones simultáneas** para reglas TCP
- La opción **Puerto local igual al puerto remoto**

7.2.1 Configuración básica del cortafuegos

Configurar una política básica del cortafuegos

Por defecto, el cortafuegos se encuentra activado y bloqueará todas las conexiones no esenciales. Deberá configurar el cortafuegos para permitir el tráfico de las aplicaciones necesarias y hacer las pruebas necesarias antes de instalarlo en toda la red. Encontrará información detallada en la *Guía de configuración de políticas de Sophos Enterprise Console*.

Para más información sobre la configuración predeterminada del cortafuegos, vea el artículo 57757 en la base de conocimiento de Sophos.

Para más información sobre cómo impedir los puentes de red, consulte Política de control de dispositivos (página 153).

Importante
Al aplicar una política nueva o actualizada a los equipos, las aplicaciones permitidas en la política antigua pueden quedar bloqueadas hasta que la política nueva se aplique por completo. Debería avisar a los usuarios ante esta posibilidad cuando vaya a aplicar una política nueva.

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para configurar una política básica del cortafuegos:

1. En el panel **Políticas**, haga doble clic en **Cortafuegos**.
2. Haga doble clic en la política **Predeterminada** para editarla.
   Se iniciará el **Asistente de políticas del cortafuegos**. Siga las instrucciones en pantalla. A continuación se ofrece información adicional sobre algunas de las opciones.
3. En la página de **Configuración del cortafuegos**, seleccione el tipo de ubicación:
   - Seleccione **Ubicación única** para los equipos que estén siempre en la red, como los ordenadores de escritorio.
   - Seleccione **Ubicación dual** si desea que el cortafuegos utilice una configuración diferente según la ubicación de los equipos, por ejemplo, en la oficina o fuera de ella. La ubicación dual es aconsejable para los equipos portátiles.
4. En el cuadro de diálogo **Modo de funcionamiento**, especifique el comportamiento del cortafuegos ante el tráfico entrante y saliente:

Modo	Descripción
Bloquear el tráfico de entrada y el de salida	• Nivel predeterminado. Ofrece la máxima seguridad. • Sólo permite el paso a través del cortafuegos del tráfico esencial y autentica la identidad de las aplicaciones que utilizan sumas de verificación. • Para permitir que las aplicaciones utilizadas habitualmente en la empresa se puedan comunicar a través del cortafuegos, haga clic en **Confianzas**. Para obtener más información, consulte Aplicaciones de confianza (página 114).
Bloquear el tráfico de entrada y permitir el de salida	• Ofrece un nivel de seguridad más bajo que **Bloquear el tráfico de entrada y el de salida**. • Permite a los equipos acceder a la red y a Internet sin necesidad de crear reglas especiales.

Modo	Descripción
	• Todas las aplicaciones tienen permiso para comunicarse a través del cortafuegos.
Monitorizar	• Aplica al tráfico de red las reglas configuradas. Si no existe ninguna regla que coincida con el tráfico, se informa a la consola y sólo se permite si es saliente. • De esta forma, podrá obtener información sobre el uso de aplicaciones en su red para crear las reglas apropiadas antes de imponer el cortafuegos en todas las estaciones. Para obtener más información, consulte Modo de control (página 108).

5. En la página **Uso compartido de archivos e impresoras**, seleccione **Permitir el uso compartido de archivos e impresoras** si desea que los usuarios puedan acceder a las impresoras y unidades compartidas en la red.

Tras configurar el cortafuegos, puede utilizar el **Visualizador de eventos del cortafuegos** para monitorizar el comportamiento (por ejemplo, aplicaciones bloqueadas por el cortafuegos). Para más información, vea Visualizar eventos del cortafuegos (página 188).

El número de equipos con eventos que superen un umbral determinado durante la última semana también aparece en el Panel de control.

Modo de control

Puede activar el modo de control en ordenadores de prueba para luego revisar el visualizador de eventos del cortafuegos para entender el tráfico, aplicaciones y procesos en la red.

A continuación cree las reglas apropiadas para permitir o bloquear el tráfico, aplicaciones o procesos, como se describe en Crear reglas de eventos del cortafuegos (página 111).

Nota
Tras crear una regla desde el visualizador de eventos del cortafuegos y aplicarla a la política, el modo del cortafuegos cambiará de **Monitorizar** a **Personalizar**.

Si desea bloquear el tráfico desconocido por defecto, puede utilizar el *modo interactivo*.

En modo interactivo, el cortafuegos pide al usuario que permita o bloquee las aplicaciones y el tráfico para los que no cuenta con una regla. Para más información, vea Modo interactivo (página 113).

Añadir aplicaciones de confianza

Las aplicaciones de confianza tienen permiso completo e incondicional de acceso a la red, incluido acceso a Internet.

Para añadir una aplicación de confianza al cortafuegos:

1. En la página **Modo de funcionamiento** del asistente **Política cortafuegos**, haga clic en **Confianzas**.
   Se abrirá el cuadro de diálogo **Política cortafuegos**.
2. Haga clic en **Añadir**.

Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir aplicación de confianza**.

3. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos de aplicaciones que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
4. Si desea visualizar eventos de aplicaciones de algún tipo, en el campo **Tipo de evento**, abra la lista desplegable y seleccione el tipo.
5. Si desea visualizar eventos de una aplicación determinada, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todas las aplicaciones.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
6. Haga clic en **Buscar** para mostrar la lista de eventos de aplicaciones.
7. Seleccione una aplicación y haga clic en **Aceptar**.

La aplicación aparecerá en la política del cortafuegos como **De confianza**.

Administración delegada

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Permitir todo el tráfico en la red local

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

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
3. En la página **Uso compartido de archivos e impresoras** en el asistente **Política cortafuegos**, seleccione **Usar configuración personalizada** y haga clic en **Personalizar**.
4. En la ficha **Red local**, active la opción **De confianza** en la red deseada.

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

Administración delegada

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Permitir el uso compartido de archivos e impresoras

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

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
3. En la página **Uso compartido de archivos e impresoras** del asistente **Política cortafuegos**, seleccione **Permitir el uso compartido de archivos e impresoras**.

Administración delegada

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Control flexible del uso compartido de archivos e impresoras

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

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

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

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
3. En la página **Uso compartido de archivos e impresoras** en el asistente **Política cortafuegos**, seleccione **Usar configuración personalizada** y haga clic en **Personalizar**.

4. Desactive la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**.

Administración delegada

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Bloquear el uso compartido de archivos e impresoras

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
3. En la página **Uso compartido de archivos e impresoras** en el asistente **Política cortafuegos**, seleccione **Usar configuración personalizada** y haga clic en **Personalizar**.
4. Active la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**.

Crear reglas de eventos del cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede crear reglas para todos los eventos del cortafuegos, menos para los eventos de “memoria modificada”.

Para crear reglas de eventos del cortafuegos:

1. En el menú **Eventos**, haga clic en **Eventos del cortafuegos**.
2. En el cuadro de diálogo **Visualizador de eventos del cortafuegos**, seleccione un evento de la aplicación para la que desea crear una regla y haga clic en **Crear regla**.

3. En el cuadro de diálogo que aparece, seleccione la opción que desee aplicar a la aplicación.
4. Seleccione la ubicación a la que desea aplicar la regla (primaria, secundaria o ambas). Si selecciona la ubicación secundaria o ambas, la regla se añadirá sólo a las políticas con ubicación secundaria. Haga clic en **Aceptar**.

   Nota
   Los eventos “nueva aplicación” y “aplicación modificada” no dependen de la ubicación (utilizan sumas de verificación que se comparten en ambas ubicaciones). No podrá seleccionar la ubicación para estos eventos.

5. En la lista de políticas del cortafuegos, seleccione las políticas a las que desea aplicar la regla. Haga clic en **Aceptar**.

   Nota
   No podrá añadir una regla a una política aplicada fuera del subentorno activo.

Nota
Si desea crear una regla de aplicación desde las opciones avanzada en el asistente de configuración del cortafuegos, consulte Crear una regla de aplicación desde la política cortafuegos (página 127).

Desactivar el cortafuegos temporalmente

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, el cortafuegos está activado. En momentos puntuales, es posible que tenga que desactivarlo para realizar tareas de mantenimiento o para solucionar algún problema.

Para desactivar el cortafuegos en un grupo de ordenadores:

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos**. A continuación, haga doble clic en la política que desee modificar.
   Se iniciará el **Asistente de políticas del cortafuegos**.
3. En la página de inicio del asistente, elija una de estas opciones:
   - Si desea desactivar el cortafuegos para todas las ubicaciones (primaria y secundaria, si la tiene configurada), haga clic en **Siguiente**. En la página **Configuración del cortafuegos**, seleccione **Permitir todo el tráfico (cortafuegos desactivado)**. Finalice el asistente.
   - Si sólo desea desactivar el cortafuegos para una de las ubicaciones (primaria o secundaria), haga clic en el botón **Opciones avanzadas**. En el cuadro de diálogo **Política cortafuegos**, seleccione **Permitir todo el tráfico** junto a la **Ubicación primaria** o **Ubicación secundaria**. Haga clic en **Aceptar**. Complete el **Asistente de políticas del cortafuegos**.

Si desactiva el cortafuegos, los ordenadores estarán desprotegidos. Para activar el cortafuegos de nuevo, desactive la opción **Permitir todo el tráfico**.

7.2.2 Configuración avanzada del cortafuegos

Opciones avanzadas del cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si desea un mayor control sobre la configuración del cortafuegos y la posibilidad de ajustes más precisos, puede utilizar las opciones avanzadas de configuración del cortafuegos.

Para acceder a las opciones avanzadas del cortafuegos:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.

Modo interactivo

En ordenadores que ejecutan Windows 7 y versiones anteriores, puede activar el modo interactivo. Después el cortafuegos muestra en las estaciones de trabajo un cuadro de diálogo de aprendizaje cada vez que una aplicación o servicio desconocido solicita acceso a la red. Se preguntará al usuario si desea permitir o bloquear el tráfico, o si desea crear una regla para este tipo de tráfico.

Nota
El modo interactivo no está disponible en Windows 8 y posterior. Debe añadir reglas específicas para autorizar o bloquear aplicaciones. Puede utilizar **Visualizador de eventos del cortafuegos** para administrar las reglas de aplicaciones de forma interactiva, tal como se describe en Crear reglas de eventos del cortafuegos (página 111).

Activar el modo interactivo

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

El cortafuegos puede funcionar en modo interactivo y pedir confirmación al usuario sobre qué hacer con el tráfico detectado. Para obtener más información, consulte Modo interactivo (página 113).

Para activar el modo interactivo del cortafuegos en un grupo de ordenadores:

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
4. En la ficha **General**, en **Modo de funcionamiento**, haga clic en **Interactivo**.

Cambiar a modo no interactivo

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Existen dos opciones para el modo no interactivo:

- Permitir por defecto
- Bloquear por defecto

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

Para cambiar a un modo no interactivo en un grupo de ordenadores:

1. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
4. Abra la ficha **General**.
5. En **Modo de funcionamiento**, seleccione **Permitir por defecto** o **Bloquear por defecto**.

Configurar el cortafuegos

Aplicaciones de confianza

Para proteger los equipos, el cortafuegos bloquea el tráfico de aplicaciones desconocidas. Sin embargo, ciertas aplicaciones de uso común en su red pueden verse bloqueadas, lo que afectaría a la productividad de los usuarios.

Para que puedan comunicarse a través del cortafuegos, dichas aplicaciones deben ser *de confianza*. Las aplicaciones de confianza tienen acceso total e incondicional a la red y a Internet.

Nota
Para mayor seguridad, puede aplicar una o más reglas de aplicaciones y especificar las condiciones bajo las cuales se puede ejecutar la aplicación. Para más información sobre cómo hacerlo, consulte Crear una regla de aplicación desde la política cortafuegos (página 127).

Añadir aplicaciones a la política del cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para añadir aplicaciones a la política del cortafuegos:

1. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
2. Abra la ficha **Aplicaciones**.
3. Haga clic en **Añadir**.
   Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir aplicación**.
4. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos de aplicaciones que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
5. Si desea visualizar eventos de aplicaciones de algún tipo, en el campo **Tipo de evento**, abra la lista desplegable y seleccione el tipo.
6. Si desea visualizar eventos de una aplicación determinada, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todas las aplicaciones.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
7. Haga clic en **Buscar** para mostrar la lista de eventos de aplicaciones.
8. Seleccione una aplicación y haga clic en **Aceptar**.

- La aplicación aparecerá en la política del cortafuegos como **De confianza**.
- Para su identificación posterior, se realizará una suma de verificación.

Eliminar una aplicación de una política cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para eliminar una aplicación de una política cortafuegos:

1. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
2. Abra la ficha **Aplicaciones**.
3. Seleccione la aplicación en la lista y haga clic en **Eliminar**.

Añadir aplicaciones de confianza

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para añadir una aplicación de confianza en un grupo de ordenadores:

1. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
2. Abra la ficha **Aplicaciones**.
   Si la aplicación que desea bloquear no aparece en la lista, siga las instrucciones en Añadir aplicaciones a la política del cortafuegos (página 115).
3. Seleccione la aplicación en la lista y haga clic en **Confiar**.

- La aplicación aparecerá en la política del cortafuegos como **De confianza**.
- Para su identificación posterior, se realizará una suma de verificación.

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

- Crear una regla de aplicaciones (página 126)
- Aplicar reglas de aplicaciones predefinidas (página 129)

Añadir una aplicación de confianza desde el visualizador de eventos del cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si el cortafuegos notifica alguna aplicación desconocida o bloquea alguna aplicación en su red, el evento aparecerá en el visualizador de eventos del cortafuegos. A continuación se describe cómo añadir aplicaciones de confianza desde el visualizador de eventos y aplicar la regla a las políticas necesarias.

Para acceder al visualizador de eventos del cortafuegos y establecer confianzas o crear una regla nueva:

1. En el menú **Eventos**, haga clic en **Eventos del cortafuegos**.
2. En el cuadro de diálogo **Visualizador de eventos del cortafuegos**, seleccione la entrada de la aplicación para la que desea crear una regla o añadir a la lista de confianzas y haga clic en **Crear regla**.
3. En el cuadro de diálogo que aparece, seleccione si desea hacer la aplicación de confianza o crear una regla para que utilice una configuración existente.
4. Desde la lista de políticas del cortafuegos, seleccione las políticas a las que desea aplicar la regla. Para aplicar la regla a todas las políticas, haga clic en **Seleccionar todo** y haga clic en **Aceptar**.

- Si utiliza sumas de verificación, puede que tenga que añadir la suma de verificación de la aplicación a la lista. Consulte Añadir sumas de verificación de aplicaciones (página 119).
- También puede añadir una aplicación de confianza mediante la configuración avanzada del cortafuegos. Consulte Crear una regla de aplicación desde la política cortafuegos (página 127).

Bloquear una aplicación

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para bloquear una aplicación en un grupo de ordenadores:

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política que desee modificar.
3. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
4. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
5. Abra la ficha **Aplicaciones**.
   Si la aplicación que desea bloquear no aparece en la lista, siga las instrucciones en Añadir aplicaciones a la política del cortafuegos (página 115).
6. Seleccione la aplicación en la lista y haga clic en **Bloquear**.

Permitir que las aplicaciones inicien procesos ocultos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

Para permitir que las aplicaciones inicien procesos ocultos, siga estos pasos:

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

1. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
2. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
3. Abra la ficha **Procesos**.
4. En la parte superior, haga clic en **Añadir**.

Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir aplicación**.

5. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos de aplicaciones que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
6. Si desea visualizar eventos de una aplicación determinada, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todas las aplicaciones.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
7. Haga clic en **Buscar** para mostrar la lista de eventos de aplicaciones.
8. Seleccione una aplicación y haga clic en **Aceptar**.

Si activa el modo interactivo, el cortafuegos puede mostrar en las estaciones un cuadro de diálogo de aprendizaje si se detecta una aplicación nueva. Para más información, vea Activar el modo interactivo (página 113). El modo interactivo no está disponible en Windows 8 y posterior.

Permitir que las aplicaciones utilicen conexiones de bajo nivel

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

Para permitir que las aplicaciones accedan a la red mediante conexiones de bajo nivel, siga estos pasos:

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Procesos**.
5. En la parte inferior, haga clic en **Añadir**.
   Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir aplicación**.
6. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos de aplicaciones que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
7. Si desea visualizar eventos de una aplicación determinada, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todas las aplicaciones.

Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.

8. Haga clic en **Buscar** para mostrar la lista de eventos de aplicaciones.
9. Seleccione una aplicación y haga clic en **Aceptar**.

Si activa el modo interactivo, el cortafuegos puede mostrar en las estaciones un cuadro de diálogo de aprendizaje si se detecta alguna conexión de bajo nivel. Para más información, vea Activar el modo interactivo (página 113).

Añadir sumas de verificación de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Por defecto, el cortafuegos comprueba todas las sumas de verificación de las aplicaciones que se ejecutan. Si la suma de verificación es desconocida o ha cambiado, el cortafuegos bloqueará la aplicación.

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. Abra la ficha **Sumas de verificación**.
4. Haga clic en **Añadir**.
   Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir suma de verificación de la aplicación**.
5. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos de aplicaciones que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
6. En el cuadro de lista desplegable **Tipo de evento**, seleccione si la suma de verificación es para una nueva aplicación o para una aplicación modificada.
7. Si desea visualizar eventos de una aplicación determinada, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todas las aplicaciones.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
8. Haga clic en **Buscar** para mostrar la lista de eventos de aplicaciones.
9. Seleccione la aplicación para la que desea añadir la suma de verificación y haga clic en **Aceptar**.

La suma de verificación para dicha aplicación se añadirá a la lista en el cuadro de diálogo **Política cortafuegos**.

Si activa el modo interactivo, el cortafuegos puede mostrar en las estaciones un cuadro de diálogo de aprendizaje si se detecta una aplicación nueva o modificada. Para más información, vea Activar el modo interactivo (página 113).

Activar o desactivar el bloqueo de procesos modificados

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

Para activar o desactivar el bloqueo de procesos modificados:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. En la ficha **General**, en la sección **Bloqueo**, desactive la opción **Bloquear procesos si otro programa modifica la memoria** para desactivar el bloqueo de procesos modificados.
   Para activar el bloqueo de procesos modificados, active la opción.

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

Notas

- No es aconsejable desactivar el bloqueo de procesos modificados de forma permanente. Sólo debe desactivarlo cuando sea estrictamente necesario.
- El bloqueo de procesos modificados no es compatible con versiones de 64 bits de Windows ni con Windows 8 y posterior. En Windows 8 y posterior, la tecnología de antivirus y HIPS de Sophos se hace cargo de ello automáticamente.
- Sólo se bloquea el proceso modificado. No se impide el acceso a la red al programa que lo ha bloqueado.

Activar o desactivar el uso de sumas de verificación

De forma predeterminada, el cortafuegos utiliza sumas de verificación para autenticar las aplicaciones. Cuando se confía en aplicaciones o se bloquean, se identifican por sus sumas de verificación automáticamente (también puede añadir sumas de verificación manualmente). Si la aplicación difiere de la suma de verificación, será bloqueada.

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

Para activar o desactivar el uso de sumas de verificación:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. En la ficha **General**, en **Bloqueo**, marque o desmarque la casilla **Autenticar aplicaciones mediante sumas de verificación**.

Permitir o bloquear paquetes IPv6

Para permitir o bloquear paquetes IPv6:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. En la ficha **General**, en **Bloqueo**, marque o desmarque la casilla **Bloquear paquetes IPv6**.

Filtrar mensajes ICMP

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

No se recomienda filtrar los mensajes ICMP a menos que conozca bien los protocolos de red. Para más información sobre los tipos de mensajes ICMP, consulte Explicación de los tipos de mensajes ICMP (página 121).

Para filtrar mensajes ICMP:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. En la ficha **ICMP**, active las casillas **Entrada** o **Salida** para permitir los mensajes entrantes o salientes de cada tipo.

Explicación de los tipos de mensajes ICMP

Petición eco, Respuesta eco	Se utilizan para probar la accesibilidad y el estado de los destinos. El host envía una **Petición eco** y espera la **Respuesta eco** correspondiente. La operación suele llevarse a cabo con el comando `ping`.
Destino no alcanzado, Respuesta eco	Enviado por un router cuando no puede entregar un datagrama IP. Los datagramas son las unidades de datos o paquetes transmitidos en una red TCP/IP.
Acallar fuente	Enviado por un host o router si recibe datos demasiado rápido. El mensaje solicita a la fuente que reduzca la velocidad de transmisión de datagramas.
Mensaje de redirección	Enviado por un router si recibe un datagrama que se debería haber enviado a otro router. El mensaje contiene la dirección a la que la fuente debería enviar datagramas en el futuro. Se utiliza para optimizar el enrutado del tráfico de red.
Anuncio de router, Solicitud de router	Permite al host descubrir la existencia de routers. Los routers retransmiten de forma periódica las direcciones IP mediante mensajes **Anuncio de router**. Los hosts también pueden solicitar

	la dirección de un router retransmitiendo un mensaje **Solicitud de router** al que responderá el router con un **Anuncio de router**.
Tiempo agotado	Enviado por un router cuando el datagrama alcanza el número máximo de routers por los que puede pasar.
Problema de parámetro	Enviado por un router si se produce un problema durante la transmisión de un datagrama que impide finalizar el proceso. Los encabezados incorrectos de los datagramas suelen provocar este problema.
Petición de sincronización, Respuesta timestamp	Se utiliza para sincronizar los relojes entre los hosts para calcular el tiempo de tránsito.
Solicitar información, Respuesta de información	Obsoletos. Los hosts utilizaban estos mensajes para determinar las direcciones entre redes, pero ya no deberían utilizarse.
Petición de máscara de red, Respuesta de máscara de red	Se utiliza para encontrar la máscara de la subred (es decir, las partes de la dirección que definen la red). Un host envía una **Petición de máscara de red** a un router y recibe una **Respuesta de máscara de red**.

Reglas del cortafuegos

Reglas globales

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

Reglas de aplicaciones

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

Para más información sobre la configuración de estas reglas, consulte el artículo 57757 en la base de conocimiento de Sophos.

Orden de aplicación de las reglas

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

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

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

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

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

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

1. Para el tráfico **NetBIOS** no autorizado en la ficha **Red local** se aplica la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**:
   - Si activa esta opción, se bloqueará el tráfico.
   - Si desactiva esta opción, se aplicarán las reglas restantes.
2. Se comprueban las reglas globales con alta prioridad en el orden especificado.
3. Si aún no se ha aplicado ninguna regla a la conexión, se comprueban las reglas de aplicaciones.
4. Si la conexión no dispone de reglas, se comprueban las reglas globales de prioridad normal en el orden en que aparecen en la lista.
5. Si la conexión no dispone de reglas:
   - En el modo **Permitir por defecto**, el tráfico está permitido (si es de salida).
   - En el modo **Bloquear por defecto**, el tráfico está bloqueado.
   - En el modo **Interactivo**, se pide confirmación al usuario. Este modo no está disponible en Windows 8 o posterior.

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

Detección de la red local

Nota
Esta función no está disponible en Windows 8 y posterior.

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

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

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

Reglas globales

Crear reglas globales

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

Para crear una regla global:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Reglas globales**.
5. Haga clic en **Añadir**.
6. En **Nombre de la regla**, escriba un nombre para la regla.

   El nombre debe ser exclusivo en la lista de reglas. No pueden existir dos reglas globales con el mismo nombre.
7. Para aplicar la regla antes que otras reglas de aplicaciones o reglas globales de prioridad normal, active la opción **Alta prioridad**.

   Para más información sobre el orden de aplicación de las reglas, consulte Orden de aplicación de las reglas (página 122).
8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
9. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
10. Escoja una de las siguientes opciones:
    - Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**.

      Nota
      Esta opción sólo está disponible para reglas TCP, por defecto con filtrado dinámico.

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

      Nota
      Esta opción solo está disponible para reglas IP y UDP.

Nota
Estas opciones no son aplicables en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.

11. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP dinámico**, se abre el cuadro de diálogo **Seleccionar protocolo**.

Editar reglas globales

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Para editar una regla global:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Reglas globales**.
5. En la lista **Regla**, seleccione la regla que desea cambiar.
6. Haga clic en el botón **Editar**.

   Para más información sobre la configuración de reglas globales, consulte el artículo 57757 de la base de conocimiento de Sophos.

Copiar una regla global

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Reglas globales**.
5. En la lista **Regla**, seleccione la regla que desea copiar.
6. Haga clic en **Copiar**.

Eliminar una regla global

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Reglas globales**.
5. En la lista **Regla**, seleccione la regla que desea eliminar.
6. Haga clic en **Quitar**.

Cambiar el orden de aplicación de las reglas globales

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Para cambiar el orden de aplicación de las reglas globales:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Reglas globales**.
5. En la lista **Regla**, seleccione la regla que desea subir o bajar en la lista.
6. Haga clic en **Arriba** o **Abajo**.

Reglas de aplicaciones

Crear una regla de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
6. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Añadir**.
7. En **Nombre de la regla**, escriba un nombre para la regla.

   El nombre debe ser exclusivo en la lista de reglas. No puede haber dos reglas con el mismo nombre, pero dos aplicaciones distintas pueden tener una regla que se llame igual.
8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
9. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
10. Escoja una de las siguientes opciones:

    - Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**.

      Nota
      Esta opción sólo está disponible para reglas TCP, por defecto con filtrado dinámico.

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

      Nota
      Esta opción solo está disponible para reglas IP y UDP.

    Nota
    Estas opciones no son aplicables en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.

11. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP dinámico**, se abre el cuadro de diálogo **Seleccionar protocolo**.

Crear una regla de aplicación desde la política cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede crear una regla de aplicación desde las opciones avanzada en el asistente de configuración del cortafuegos.

Para crear una regla de aplicación desde la política cortafuegos:

1. Haga doble clic en la política que desee modificar.

2. En la página de inicio del **Asistente de políticas del cortafuegos**, haga clic en **Opciones avanzadas**.
3. En el cuadro de diálogo **Política cortafuegos**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Escoja una de las siguientes opciones:
   - Si desea añadir una aplicación a la política cortafuegos, abra la ficha **Aplicaciones** y haga clic en **Añadir**.
   - Si desea permitir a alguna aplicación iniciar procesos ocultos, abra la ficha **Procesos** y haga clic en **Añadir** en la parte superior.
   - Si desea permitir a alguna aplicación el acceso a bajo nivel, abra la ficha **Procesos** y haga clic en **Añadir** en la parte inferior.

   Se abrirá el cuadro de diálogo **Política cortafuegos - Añadir aplicación**.
5. Si está añadiendo una aplicación, en el cuadro de lista desplegable **Tipo de evento**, seleccione si desea añadir una aplicación modificada, una aplicación nueva o una aplicación sin regla.
6. A continuación, seleccione la entrada con la aplicación y haga clic en **Aceptar**.
   La aplicación se añadirá a la política del cortafuegos.

Si añadió una aplicación desde la ficha **Aplicaciones**, la aplicación se añadirá como de confianza. Si lo desea, puede bloquearla o crear una regla de personalizada.

Editar reglas de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
6. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Editar**.
7. En **Nombre de la regla**, escriba un nombre para la regla.

   El nombre debe ser exclusivo en la lista de reglas. No puede haber dos reglas con el mismo nombre, pero dos aplicaciones distintas pueden tener una regla que se llame igual.
8. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
9. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
10. Escoja una de las siguientes opciones:
    - Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**.

      Nota
      Esta opción sólo está disponible para reglas TCP, por defecto con filtrado dinámico.

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

  Nota
  Esta opción solo está disponible para reglas IP y UDP.

Nota
Estas opciones no son aplicables en Windows 8 y posterior porque se utiliza siempre el **Filtrado dinámico** y no se permiten **Conexiones concurrentes**.

11. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP dinámico**, se abre el cuadro de diálogo **Seleccionar protocolo**.

Aplicar reglas de aplicaciones predefinidas

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
6. Señale **Predefinidas** y haga clic en una regla predefinida.

Copiar reglas de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.

6. En el cuadro de diálogo **Reglas de aplicaciones**, seleccione la regla que desea copiar y haga clic en **Copiar**.

Eliminar reglas de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
6. En el cuadro de diálogo **Reglas de aplicaciones**, seleccione la regla que desea eliminar y haga clic en **Eliminar**.

Cambiar el orden de aplicación de las reglas de aplicaciones

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

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

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Aplicaciones**.
5. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
6. En el cuadro de diálogo **Reglas de aplicaciones**, en la lista **Regla**, seleccione la regla que desea subir o bajar en la lista.
7. Haga clic en **Arriba** o **Abajo**.

Detección de la ubicación

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

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

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

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

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

Configurar la detección de la ubicación

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

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

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

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

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

Definir las ubicaciones primarias

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **Detección de ubicación**.
5. En la sección **Método de detección**, haga clic en **Configurar** junto al método que desea utilizar para definir las ubicaciones primarias:

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

6. Siga las instrucciones en pantalla.

Crear una configuración secundaria

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Active la opción **Configurar una ubicación secundaria**.

Configure las opciones de la configuración secundaria. Para más información sobre cómo hacerlo, consulte Opciones avanzadas del cortafuegos (página 113).

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

Seleccionar la configuración que se aplica

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. En la ficha **General**, en la sección **Ubicación actual**, seleccione una de las siguientes opciones:

Opción	Descripción
Ubicación detectada	El cortafuegos aplica la configuración primaria o secundaria según la conexión detectada (establecida en Configurar la detección de la ubicación (página 131)).
Ubicación primaria	El cortafuegos aplica la configuración primaria.
Ubicación secundaria	El cortafuegos aplica la configuración secundaria.

Informes del cortafuegos

Por defecto, el cortafuegos en las estaciones informa a Enterprise Console sobre cambios en el estado, eventos y errores.

Cambios en el estado del cortafuegos

El cortafuegos considera como tales los cambios de estado siguientes:

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

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

Para obtener más información, consulte Activar o desactivar notificación de cambios locales (página 133).

Eventos del cortafuegos

Se produce un *evento* cuando una aplicación desconocida o sistema operativo de un equipo intentan comunicarse con otro equipo mediante una conexión de red.

Si lo desea, puede impedir que el cortafuegos envíe informes sobre los eventos a Enterprise Console.

Para obtener más información, consulte Desactivar la notificación de tráfico desconocido (página 134).

Activar o desactivar notificación de cambios locales

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

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

Nota
Esta opción no es compatible con Windows 8 y posterior.

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

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

Para desactivar la notificación de cambios locales:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **General**.
5. En la sección **Notificación**, siga uno de los procedimientos siguientes
   - Para activar la notificación de cambios locales, active la opción **Enviar una alerta a la consola de administración si se modifica alguna regla global, aplicación, proceso o suma de verificación**.
   - Para activar la notificación de cambios locales, desactive la opción **Enviar una alerta a la consola de administración si se modifica alguna regla global, aplicación, proceso o suma de verificación**.

Desactivar la notificación de tráfico desconocido

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, puede impedir que el cortafuegos en las estaciones envíe notificación a Enterprise Console en relación con tráfico de red desconocido. El tráfico desconocido es el que no dispone de una regla.

Para impedir que el cortafuegos en las estaciones envíe notificación a Enterprise Console en relación con tráfico de red desconocido.

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **General**.
5. En la sección **Bloqueo**, active la opción **Autenticar aplicaciones mediante sumas de verificación**.
6. En la sección **Notificación**, desactive la opción **Notificar aplicaciones y tráfico desconocidos a la consola de administración**.

Desactivar la notificación de errores del cortafuegos

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

Para impedir que el cortafuegos en las estaciones envíe notificación de errores a Enterprise Console:

1. Haga doble clic en la política del cortafuegos que desea modificar.
2. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
3. En la sección **Configuración**, haga clic en **Configurar** junto a la ubicación que desea modificar.
4. Abra la ficha **General**.
5. En la sección **Notificación**, desactive la opción **Notificar errores a la consola de administración**.

Importar y exportar la configuración del cortafuegos

Nota
Si utiliza administración delegada:

- Para configurar la política cortafuegos, es necesario contar con el permiso **Configuración de políticas: cortafuegos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Es posible importar y exportar las reglas y la configuración general del cortafuegos en un archivo de configuración (*.conf). Utilice esta función para:

- Crear una copia de seguridad y restaurar la configuración del cortafuegos.
- Importar reglas de aplicaciones en ordenadores que utilicen las mismas aplicaciones.
- Aunar la configuración de diferentes ordenadores para crear una política de grupo.

Para importar y exportar la configuración del cortafuegos:

1. Compruebe qué política cortafuegos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Cortafuegos** y, a continuación, haga doble clic en la política correspondiente.
3. En la página de **inicio** del asistente **Política cortafuegos**, haga clic en **Opciones avanzadas**.
4. En el cuadro de diálogo **Política cortafuegos**, en la ficha **General**, en la sección **Opciones de configuración**, haga clic en **Importar** o **Exportar**.

7.3 Política de restricción de aplicaciones

Enterprise Console permite detectar y bloquear "aplicaciones restringidas", es decir, aplicaciones legítimas que no suponen una amenaza para la seguridad, pero cuyo uso no considere adecuado en el entorno empresarial. Entre estas aplicaciones se incluyen programas de mensajería instantánea, de voz sobre IP (VoIP), de fotografía digital, reproductores multimedia o complementos del navegador.

Nota
Esta opción sólo está disponible en Sophos Endpoint Security and Control para Windows.

Podrá bloquear o autorizar aplicaciones para diferentes grupos de usuarios con total flexibilidad. Por ejemplo, las aplicaciones de voz sobre IP pueden desactivarse para los ordenadores internos, pero autorizarse para los equipos remotos.

Sophos actualiza la lista de aplicaciones restringidas de forma regular. No es posible añadir aplicaciones a la lista, pero puede enviar una solicitud a Sophos para que incluya una aplicación legítima nueva que desee restringir en su red.

Para más información, vea el artículo 63656 en la base de conocimiento de Sophos.

En esta sección se explica cómo seleccionar las aplicaciones que desea restringir en la red y cómo configurar la detección de aplicaciones restringidas.

Nota
Si utiliza administración delegada:

- Para configurar una política de restricción de aplicaciones, es necesario contar con el permiso **Configuración de políticas: restricción de aplicaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Eventos de la restricción de aplicaciones

Cuando se produce un evento de la restricción de aplicaciones, por ejemplo cuando se detecta una aplicación restringida en la red, el evento se escribe en el registro de eventos de la restricción de aplicaciones para poder visualizarlo en Enterprise Console. Para más información, vea Visualizar eventos de la restricción de aplicaciones (página 186).

El número de equipos con eventos que superen un umbral determinado durante la última semana aparece en el Panel de control.

También puede configurar alertas que se envíen a determinados destinatarios cuando se produzca un evento de la restricción de aplicaciones. Para más información, vea Alertas y mensajes de aplicaciones restringidas (página 179).

7.3.1 Seleccionar las aplicaciones que desea restringir

Si utiliza administración delegada:

- Para configurar una política de restricción de aplicaciones, es necesario contar con el permiso **Configuración de políticas: restricción de aplicaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, todas las aplicaciones están permitidas. Para seleccionar las aplicaciones que desea restringir:

1. Compruebe qué política de restricción de aplicaciones usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Restricción de aplicaciones**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de restricción de aplicaciones**, abra la ficha **Autorización**.
4. Seleccione un **Tipo de aplicación**, por ejemplo, **Intercammbio de archivos**.

   La lista **Autorizadas** de la parte inferior contiene todas las aplicaciones incluidas en el grupo.

   - Para bloquear una aplicación, selecciónela y muévala a la lista **Bloqueadas** haciendo clic en el botón "Añadir".

   - Para bloquear todas las aplicaciones nuevas que Sophos añada a ese tipo en lo sucesivo, mueva **Todas las añadidas por Sophos en el futuro** a la lista **Bloqueadas**.
   - Para bloquear todas las aplicaciones de ese tipo, muévalas todas desde la lista **Autorizadas** a la lista **Bloqueadas** haciendo clic en el botón "Añadir todas".

5. En la ficha **Escaneado** del cuadro de diálogo **Política de restricción de aplicaciones**, compruebe que la opción de detección de aplicaciones restringidas está seleccionada (consulte Detectar aplicaciones restringidas (página 137) para más información.) Haga clic en **Aceptar**.

7.3.2 Detectar aplicaciones restringidas

Si utiliza administración delegada:

- Para configurar una política de restricción de aplicaciones, es necesario contar con el permiso **Configuración de políticas: restricción de aplicaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Puede configurar Sophos Endpoint Security and Control para detectar aplicaciones cuyo uso desea restringir en su red.

1. Compruebe qué política de restricción de aplicaciones usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Restricción de aplicaciones**. A continuación, haga doble clic en la política que desee modificar.
   Se mostrará el cuadro de diálogo **Política de restricción de aplicaciones**.
3. En la ficha **Escaneado**, configure las opciones de la forma siguiente:
   - Para activar el escaneado en acceso, active la casilla **Activar el escaneado en acceso**. Si no desea bloquear las aplicaciones detectadas, active la opción **Detectar pero permitir ejecución**.
   - Para activar los escaneados en demanda y programado, active la casilla **Activar el escaneado en demanda y programado**.

   Nota
   La política antivirus y HIPS determina los archivos a escanear (extensiones y exclusiones).

Si desea eliminar aplicaciones restringidas de los ordenadores en red, siga las instrucciones del apartado Desinstalar aplicaciones restringidas (página 137).

Si lo desea, podrá recibir alertas ante la detección de aplicaciones restringidas. Para más información, consulte Alertas y mensajes de aplicaciones restringidas (página 179).

7.3.3 Desinstalar aplicaciones restringidas

Antes de desinstalar aplicaciones restringidas, desactive el escaneado en acceso de las mismas. Este tipo de escaneado bloquea los programas que se utilizan para instalar y desinstalar aplicaciones, por lo que puede interferir con la desinstalación.

Para eliminar una aplicación:

- Ejecute el programa de desinstalación del producto en cada ordenador. También puede hacerlo desde el Panel de control de Windows, con la función Agregar o quitar programas.
- En el servidor, utilice el script o herramienta de administración habituales para ejecutar el programa de desinstalación del producto en sus equipos en red.

Ahora ya puede activar el escaneado en acceso de aplicaciones restringidas.

7.4 Política de control de datos

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

El control de datos permite reducir las fugas accidentales de datos de las estaciones mediante el control y la restricción de las transferencias de archivos que contengan datos delicados. Para ello, se crean reglas de control de datos y se añaden a las políticas de **Control de datos**.

Es posible controlar las transferencias de archivos a dispositivos de almacenamiento determinados (unidades extraíbles u ópticas) o mediante aplicaciones específicas (programas de correo o navegador de Internet).

Para que pueda definir y distribuir rápidamente una política de control de datos, SophosLabs mantiene una biblioteca de definiciones de datos delicados (Listas de control de contenido). La biblioteca contiene principalmente información personal, pero también abarca ciertas estructuras habituales de datos. Utilice las listas de control de contenido de Enterprise Console, como se describe más adelante en esta sección.

7.4.1 Cómo funciona el control de datos

El control de datos identifica fugas de datos accidentales que suelen producirse por descuidos de los usuarios en el trato de datos delicados. Por ejemplo, un usuario puede enviar un archivo con datos confidenciales a su casa a través de un programa de correo electrónico de Internet.

El control de datos permite controlar las transferencias de archivos a dispositivos de almacenamiento o mediante aplicaciones conectadas a Internet.

- **Dispositivo de almacenamiento:** El control de datos intercepta todos los archivos que se copian en dispositivos de almacenamiento controlados mediante el Explorador de Windows (incluido el Escritorio). Sin embargo, no se interceptan los archivos que se guardan desde aplicaciones, como Microsoft Word, o mediante transferencias desde la línea de comandos.

  Las acciones **Pedir confirmación al usuario y registrar evento** y **Bloquear transferencia y registrar evento** permiten hacer que el uso del Explorador de Windows sea obligatorio para todas las transferencias a dispositivos de almacenamiento controlados. En ambos casos, el control de datos impide la transferencia de archivos desde la línea de comandos o que se guarden directamente desde una aplicación, y aparece una alerta para que el usuario utilice el Explorador de Windows.

  Cuando las políticas de control de datos sólo contienen reglas para la acción **Permitir transferencia y registrar evento**, es posible guardar archivos directamente desde aplicaciones y realizar transferencias desde la línea de comandos. Esta configuración permite que los usuarios utilicen dispositivos de almacenamiento libremente. Sin embargo, se siguen registrando eventos de control de datos de las transferencias realizadas mediante el Explorador de Windows.

  Nota
  Esta restricción no afecta al control de aplicaciones.

- **Aplicaciones:** Para garantizar que sólo se controlan los archivos cargados por los usuarios, ciertas carpetas del sistema están excluidas del control de datos. De esta forma se minimiza el número de falsas alarmas cuando la aplicación carga archivos de configuración.

Importante
Si se generan falsas alarmas al utilizar alguna aplicación, pruebe a excluir la carpeta de la aplicación o haga las reglas menos restrictivas. Para más información, consulte el artículo 113024 de la base de conocimiento de Sophos.

Nota
Las exclusiones del escaneado en acceso no se aplican siempre al control de datos.

¿Cuándo utiliza el control de datos las exclusiones del escaneado en acceso?

En función de cómo y dónde copie o mueva archivos, el control de datos puede o no tener en cuenta las exclusiones del escaneado en acceso que haya definido en la política antivirus y HIPS.

El control de datos **utiliza** las exclusiones del escaneado en acceso cuando los archivos se cargan o se adjuntan mediante una aplicación supervisada, por ejemplo, un cliente de correo electrónico, un navegador web o un cliente de mensajería instantánea (IM). Para más información sobre las exclusiones del escaneado en acceso, consulte Excluir elementos del escaneado en acceso (página 82).

Importante
Si ha excluido archivos remotos del escaneado en acceso, el control de datos no escaneará los archivos que cargue o adjunte desde una ubicación de red a una aplicación supervisada, por ejemplo, de correo electrónico o un navegador web. Consulte también El control de datos no detecta archivos cargados o adjuntos (página 217).

El control de datos **no utiliza** las exclusiones del escaneado en acceso cuando los archivos se copian o mueven con Internet Explorer. Por tanto, las exclusiones no funcionarán, por ejemplo, si copia archivos a un dispositivo de almacenamiento como USB o si copia o mueve archivos a una ubicación de red. Se escanearán todos los archivos, aunque haya excluido los archivos remotos del escaneado en acceso.

Nota
Si copia o mueve archivos **comprimidos** a una ubicación de red, el proceso puede llevar algún tiempo, por ejemplo, más de un minuto por 100 MB de datos, en función de su conexión de red. Esto se debe a que el escaneado de los archivos comprimidos tarda más tiempo que el escaneado de los archivos no comprimidos.

Políticas de control de datos

El control de datos permite controlar las transferencias de datos mediante la definición de políticas que se aplican a los grupos de ordenadores de la red.

Importante
El control de datos no es compatible con Windows 2008 Server Core y debe desactivarlo para dicho sistema. Para excluir el control de datos en ordenadores con Windows 2008 Server Core, póngalos en un grupo y desactive el escaneado de control de datos. Para más información, vea Activar o desactivar el control de datos (página 143).

Las políticas de control de datos incluyen una o más reglas que especifican las condiciones y las acciones que se llevarán a cabo si se cumplen esas reglas. Una misma regla de control de datos puede incluirse en varias políticas.

Cuando una política de control de datos contiene varias reglas, cualquier archivo que cumpla *cualquiera* de ellas estará violando la política.

Condiciones de las reglas de control de datos

Las condiciones de las reglas de control de datos incluyen el destino, el nombre y la extensión del archivo, el tipo de archivo o el contenido.

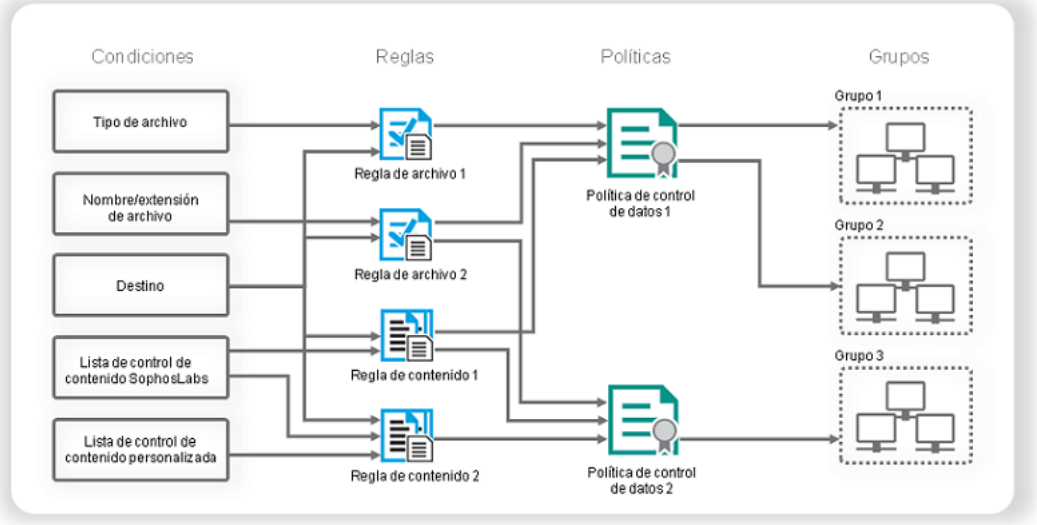
El destino puede ser un dispositivo (por ejemplo, dispositivos de almacenamiento extraíbles, como una unidad de memoria USB) o una aplicación (por ejemplo, navegadores de Internet o programas de correo electrónico).

El contenido identificable del archivo se define mediante las listas de control de contenido, que son descripciones XML de datos estructurados. SophosLabs proporciona una amplia colección de listas de control del contenido que pueden utilizarse con las reglas de control de datos.

Para más información sobre las reglas de control de datos y condiciones aplicadas a los archivos, consulte Acerca de las reglas de control de datos (página 141).

Para más información sobre las listas de control del contenido, consulte Acerca de las listas de control de contenido (página 142).

Control de datos



Acciones de las reglas de control de datos

Cuando el control de datos detecta todas las condiciones especificadas en una regla, la regla se cumple, y el control de datos lleva a cabo las acciones especificadas y registra el evento. Puede especificar una de las acciones siguientes:

- Permitir transferencia y registrar evento
- Pedir confirmación al usuario y registrar evento
- Bloquear transferencia y registrar evento

Si un archivo cumple dos reglas del control de datos que especifican acciones diferentes, se aplicará la regla que especifique la acción más restrictiva. Las reglas de control de datos que bloquean la transferencia de archivos tienen prioridad sobre las reglas que permiten la transferencia de archivos cuando el usuario las acepta. Las reglas que permiten la transferencia tras la confirmación del usuario tienen prioridad sobre las reglas que permiten la transferencia de archivos.

Por defecto, cuando se cumple la regla y se bloquea la transferencia de archivos o se pide la confirmación del usuario, aparece un mensaje en el equipo. El mensaje indica que se ha cumplido una regla. Si lo desea, puede añadir mensajes personalizados a los mensajes estándar para la confirmación y el bloqueo de las transferencias. Para obtener más información, consulte Alertas y mensajes del control de datos (página 180).

7.4.2 Acerca de las reglas de control de datos

Las reglas de control de datos especifican las condiciones que detecta el control de datos, las acciones que se llevan a cabo cuando se detectan estas condiciones y los archivos que se desean excluir del escaneado del control de datos.

Puede crear reglas propias o utilizar las reglas de muestra proporcionadas. Sophos ofrece una serie de reglas de control de datos preconfiguradas, que puede utilizar en cuanto lo desee o ajustarlas a sus necesidades. Dichas reglas se ofrecen como ejemplo y no se actualizan.

Existen dos tipos de reglas de control de datos: *reglas de archivo* y *reglas de contenido*.

Reglas de archivos

Las *reglas de archivos* especifican las acciones que se llevan a cabo cuando el usuario intenta transferir un archivo con el nombre o del tipo especificado (categoría de archivo, por ejemplo, una hoja de cálculo) a un destino específico, por ejemplo, bloquear la transferencia de bases de datos a dispositivos de almacenamiento extraíbles.

El control de datos incluye definiciones de más de 150 formatos de archivo. Sophos puede añadir más tipos de archivos en el futuro. Estos nuevos tipos se añadirán de forma automática a las reglas de control de datos que utilizan las categorías de archivos correspondientes.

Los tipos de archivo que no pertenezcan a ninguna definición pueden identificarse mediante sus extensiones.

Reglas de contenido

Las *reglas de contenido* contienen una o más listas de control de contenido y especifican las acciones que se llevan a cabo cuando el usuario intenta transferir datos que coinciden con la lista de control a un destino determinado.

7.4.3 Acerca de las listas de control de contenido

Una *lista de control de contenido* es un conjunto de condiciones que describen contenido estructurado de archivos. Las listas de control de contenido pueden describir un solo tipo de datos (por ejemplo, una dirección de correos o un número de la seguridad social) o una combinación de tipos de datos (por ejemplo, el nombre de un proyecto junto al término "confidencial").

Puede utilizar las *listas de control del contenido de SophosLabs* proporcionadas por Sophos o crear las suyas propias.

Las listas de control del contenido de SophosLabs contienen definiciones de tipos de datos personales y económicos habituales, por ejemplo, números de tarjetas de crédito, números de la seguridad social, direcciones postales o de correo electrónico. Las listas de control del contenido de SophosLabs utilizan técnicas avanzadas, como sumas de verificación, para aumentar la exactitud de la detección de datos delicados.

Las listas de control de contenido de SophosLabs no se pueden modificar, pero puede enviar una solicitud a Sophos para que cree una lista nueva. Para obtener más información, consulte el artículo 51976 de la base de conocimiento de Sophos.

Nota
El uso de caracteres de doble byte (por ejemplo, los utilizados en japonés y chino) no cuenta con soporte oficial en la versión actual de las listas de control de contenido. De cualquier modo, sí es posible utilizar caracteres de doble byte desde el editor de listas de control de contenido.

Configurar la cantidad de listas de control del contenido de SophosLabs

La mayoría de listas de control del contenido de SophosLabs tienen una *cantidad* asignada.

La *cantidad* es el volumen de los tipos de datos clave de la lista de control de contenido que deben aparecer en un archivo para que se detecte. La cantidad de las listas de control de contenido de SophosLabs se puede modificar en la regla de contenido que incluya esa lista.

Mediante la cantidad, se pueden ajustar las reglas de control de datos para impedir que se bloqueen documentos que no contengan información confidencial (por ejemplo, un documento que contenga una dirección o uno o dos números de teléfono, probablemente en la cabecera, el pie o la firma de una carta). Si busca una sola dirección de correo, pueden existir miles de documentos que coincidan con la regla y provocar un evento del control de datos. Sin embargo, si no quiere perder una lista de clientes, puede detectar sólo la transferencia de documentos que contengan, por ejemplo, más de 50 direcciones. En otros casos, puede ser preferible realizar una búsqueda del contenido específico, por ejemplo, un número de tarjeta de crédito.

7.4.4 Acerca de los eventos del control de datos

Cuando se produce un evento del control de datos, por ejemplo, la copia de un archivo con datos delicados en una unidad de memoria USB, el evento se envía a Enterprise Console y puede visualizarse en el **Visualizador de eventos del control de datos**. El evento se registra también de forma local en el equipo y puede visualizarse, con los permisos necesarios, en Sophos Endpoint Security and Control.

Nota
Las estaciones pueden enviar a Enterprise Console un máximo de 50 eventos del control de datos por hora. Todos los eventos se registran de forma local en el equipo.

En el cuadro de diálogo **Visualizador de eventos del control de datos**, utilice los filtros para mostrar sólo los eventos que le interesen. También puede exportar una lista de los eventos del control de datos. Para más información, consulte Acerca de los eventos del control de datos (página 143) y Exportar la lista de eventos a un archivo (página 194).

El número de equipos con eventos del control de datos que superen un umbral determinado en los últimos 7 días aparece en el Panel de control. Para más información sobre cómo configurar el umbral, consulte Paneles de control (página 4).

También puede configurar alertas que se envíen a determinados destinatarios cuando se produzca un evento del control de datos. Para más información, vea Alertas y mensajes del control de datos (página 180).

7.4.5 Activar o desactivar el control de datos

Si utiliza administración delegada:

- Para configurar las políticas de control de datos, es necesario contar con el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, el control de datos está desactivado y no hay reglas especificadas para controlar o restringir la transferencia de archivos en la red.

Para activar el control de datos:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
   Aparecerá el cuadro de diálogo **Política de control de datos**.
3. En la ficha **Reglas de la política**, active la opción **Activar escaneado de control de datos**.
4. Haga clic en el botón **Añadir regla**. En el cuadro de diálogo **Gestión de reglas de control de datos**, seleccione las reglas que desea añadir a la política y haga clic en **Aceptar**.

Importante
Hasta que no añada ninguna regla de control de datos, no se controlará ni se restringirá la transferencia de archivos.

Si desea desactivar el escaneado de control de datos más tarde, desactive la opción **Activar escaneado de control de datos**.

7.4.6 Crear reglas de identificación de archivos

Si utiliza administración delegada:

- Para crear o editar reglas de control de datos, es necesario contar con el permiso **Personalización del control de datos**.
- Para configurar políticas de control de datos, es necesario contar con el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

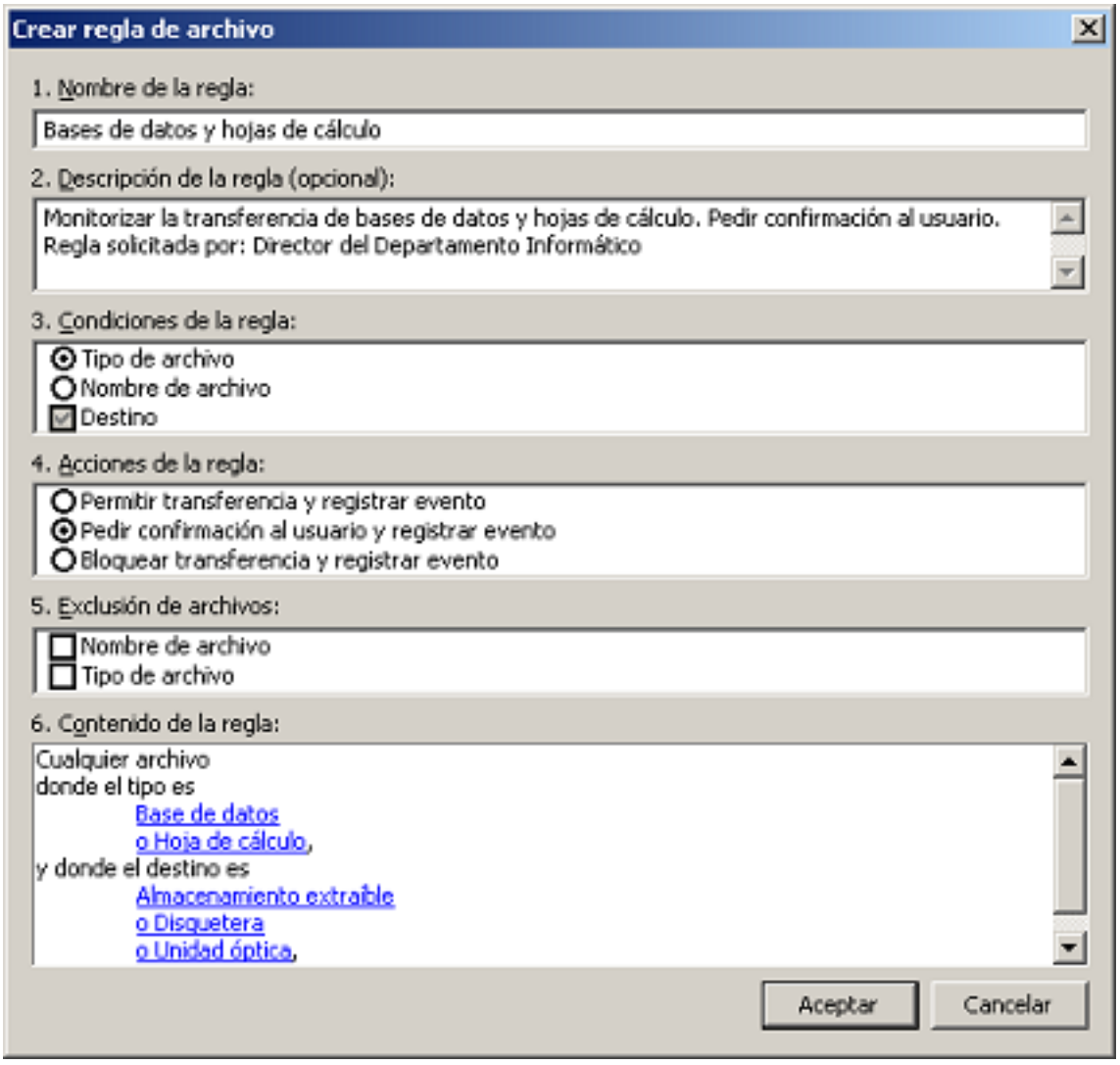
Para más información sobre las reglas de archivos, consulte Acerca de las reglas de control de datos (página 141).

Para crear una regla de identificación de archivos y añadirla a una política de control de datos:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
   También puede crear reglas desde el menú **Herramientas** y añadirlas a las políticas más tarde. En el menú **Herramientas**, señale **Administrar el control de datos**, haga clic en **Reglas de control de datos** y realice los pasos del 4 al 10.
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de datos**, en la ficha **Reglas de la política**, compruebe que la opción **Activar escaneado de control de datos** está activada y haga clic en **Gestor de reglas**.
4. En el cuadro de diálogo **Gestión de reglas de control de datos**, haga clic en el botón **Añadir regla de archivos**.
5. En el cuadro de diálogo **Crear regla de archivo**, en la sección **Nombre de la regla**, escriba un nombre para la regla.
6. En **Descripción de la regla (opcional)** puede escribir una descripción sobre la regla.
7. En **Condiciones de la regla**, seleccione condiciones para la regla.
   La condición de destino está preseleccionada y debe incluirse en la regla.
   Por defecto, se escanean todos los tipos de archivos. Si desea escanear sólo ciertos tipos de archivos, active la casilla **Tipo de archivo**. Después, puede configurar esta condición según se describe en el paso 10.
8. En **Acciones de la regla**, seleccione la acción que se llevará a cabo si la regla se cumple.
9. Si desea excluir ciertos archivos del escaneado de control de datos, en **Exclusión de archivos**, active la opción **Nombre de archivo** o **Tipo de archivo**.
10. En **Contenido de la regla**, haga clic en los valores subrayados y configure las condiciones de la regla.

Por ejemplo, si hace clic en **Seleccione destino**, se abre el cuadro de diálogo **Condición de tipo de destino**, en el que puede seleccionar los dispositivos o aplicaciones para los que desea restringir la transferencia de datos.

Seleccione o introduzca condiciones para cada valor subrayado.



Haga clic en **Aceptar**.

La regla nueva aparece en el cuadro de diálogo **Gestión de reglas de control de datos**.

11. Para añadir la regla a la política, active la casilla situada junto al nombre de la regla y haga clic en **Aceptar**.
    La regla se añade a la política de control de datos.

Puede configurar alertas y mensajes que se enviarán al usuario cuando se cumpla una regla de la política de control de datos. Consulte Alertas y mensajes del control de datos (página 180).

7.4.7 Crear reglas de contenido

Si utiliza administración delegada:

- Para crear o editar reglas de control de datos y listas de control del contenido, es necesario contar con el permiso **Personalización del control de datos**.

- Para configurar políticas de control de datos, es necesario contar con el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para ver una descripción completa de las reglas y listas de control del contenido, consulte Acerca de las reglas de control de datos (página 141).

Para crear una regla de contenido y añadirla a una política de control de datos:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).

   También puede crear reglas desde el menú **Herramientas** y añadirlas a las políticas más tarde. En el menú **Herramientas**, señale **Administrar el control de datos**, haga clic en **Reglas de control de datos** y realice los pasos del 4 al 13.
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de datos**, en la ficha **Reglas de la política**, compruebe que la opción **Activar escaneado de control de datos** está activada y haga clic en **Gestor de reglas**.
4. En el cuadro de diálogo **Gestión de reglas de control de datos**, haga clic en el botón **Añadir regla de contenido**.
5. En el cuadro de diálogo **Crear reglas de contenido**, en la sección **Nombre de la regla**, escriba un nombre para la regla.
6. En **Descripción de la regla (opcional)** puede escribir una descripción sobre la regla.
7. En **Condiciones de la regla**, las condiciones de destino y contenido del archivo ya están seleccionadas. Es necesario configurar ambas condiciones para las reglas de contenido.
8. En **Acciones de la regla**, seleccione la acción que se llevará a cabo si la regla se cumple.
9. Si desea excluir ciertos archivos del escaneado de control de datos, en **Exclusión de archivos**, active la opción **Nombre de archivo** o **Tipo de archivo**.
10. En **Contenido de la regla**, haga clic en el valor subrayado para seleccionar el contenido del archivo.
11. En el cuadro de diálogo **Gestión de listas de control de contenido**, seleccione las listas de control de contenido que desea incluir en la regla.

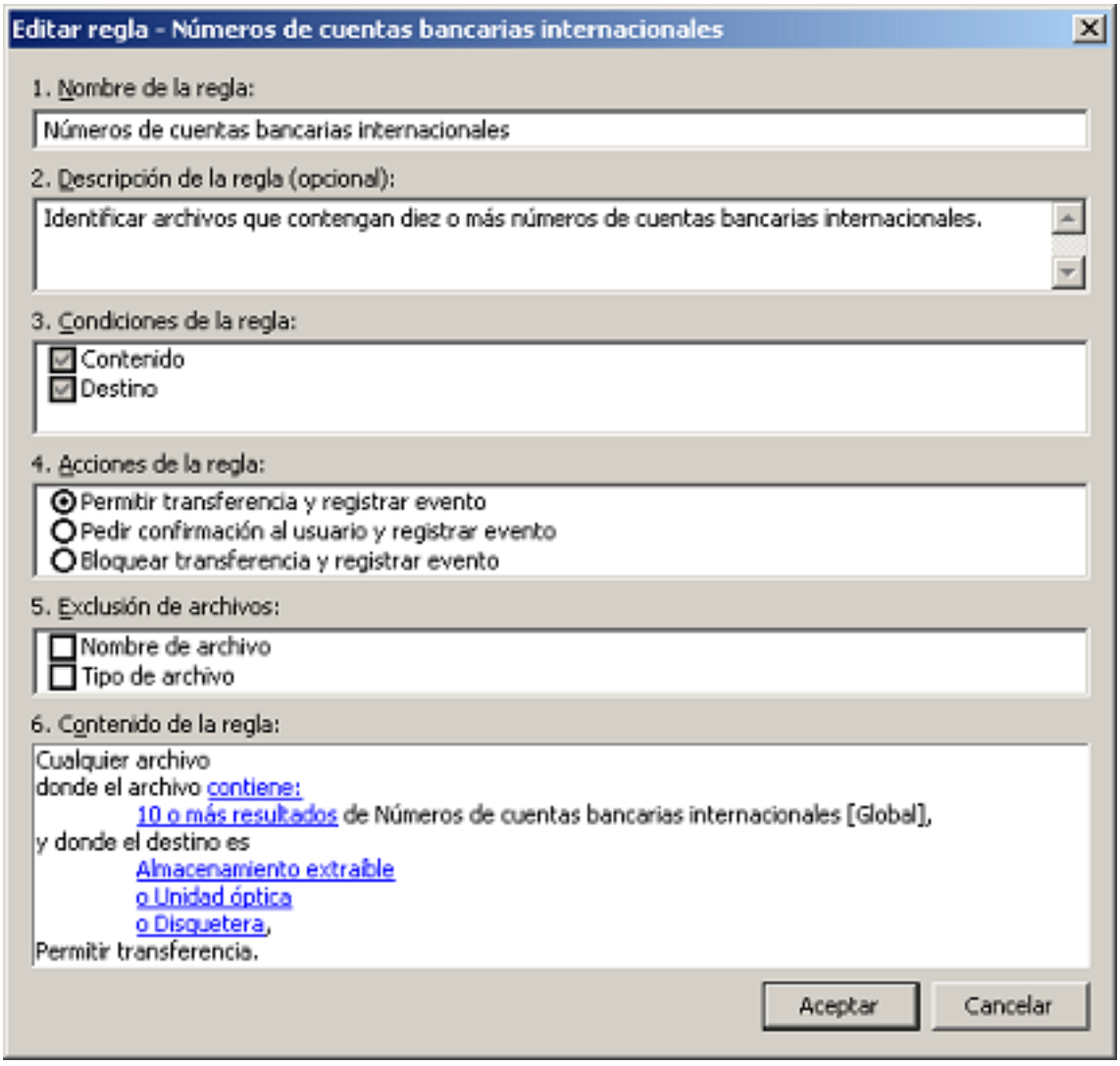
    Si desea añadir listas de control de contenido de SophosLabs, seleccione una para cada país necesario.

    Sugerencia
    No seleccione una lista de control de contenido global si no requiere soporte para todos los países. En lugar de ello, seleccione listas de control de contenido solo para aquellos países que sean necesarios. Así se reducirá notablemente el tiempo de escaneado, además del riesgo de coincidencias fortuitas y no deseadas.

    Si desea crear una lista de control de contenido, consulte Crear o editar listas de control de contenido sencillas (página 149) o Crear o editar una lista avanzada de control de contenido (página 150).

    Haga clic en **Aceptar**.
12. Si desea cambiar la cantidad asignada a la lista de control de contenido de SophosLabs, en **Contenido de la regla**, haga clic en el valor subrayado ("*n* o más resultados") que desea modificar. En el cuadro de diálogo **Editor de cantidad**, introduzca una cantidad nueva. Para obtener más información, consulte Acerca de las listas de control de contenido (página 142).

13. En **Contenido de la regla**, seleccione o introduzca las condiciones para el resto de valores subrayados.



Haga clic en **Aceptar**.

La regla nueva aparece en el cuadro de diálogo **Gestión de reglas de control de datos**.

14. Para añadir la regla a la política, active la casilla situada junto al nombre de la regla y haga clic en **Aceptar**.
La regla se añade a la política de control de datos.

Puede configurar alertas y mensajes que se enviarán al usuario cuando se cumpla una regla de la política de control de datos. Consulte Alertas y mensajes del control de datos (página 180).

7.4.8 Añadir reglas de control de datos a políticas

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para añadir una regla de control de datos a una política:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
   Aparecerá el cuadro de diálogo **Política de control de datos**.
3. En la ficha **Reglas de la política**, haga clic en **Añadir regla**.
   Aparecerá el cuadro de diálogo **Gestión de reglas de control de datos**.
4. Seleccione las reglas que desea añadir a la política y haga clic en **Aceptar**.

7.4.9 Eliminar reglas de control de datos de políticas

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para eliminar una regla de control de datos de una política:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
   Aparecerá el cuadro de diálogo **Política de control de datos**.
3. En la ficha **Reglas de la política**, seleccione la regla que desea eliminar y haga clic en **Eliminar regla**.

7.4.10 Excluir archivos o tipos de archivos del control de datos

Si utiliza administración delegada, necesitará el permiso **Personalización del control de datos** para excluir archivos del control de datos. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Los archivos y tipos de archivos se excluyen del control de datos mediante la configuración de exclusiones en la regla de control de datos.

Para excluir un archivo o tipo de archivo del control de datos, exclúyalo en una regla con la máxima prioridad (es decir, con la acción más restrictiva).

Para excluir archivos o tipos de archivos del control de datos:

1. En el menú **Herramientas**, señale **Administrar el control de datos** y haga clic en **Reglas de control de datos**.
2. En el cuadro de diálogo **Gestión de reglas de control de datos**, seleccione la regla que desea modificar y haga clic en **Editar**, o cree una regla nueva haciendo clic en los botones **Añadir regla de archivo** o **Añadir regla de contenido**.
3. Para excluir archivos del control de datos, en el cuadro de diálogo **Editor de reglas**, en **Exclusión de archivos**, active la opción **Nombre de archivo**.
4. En **Contenido de la regla**, haga clic en el valor subrayado para especificar nombres de archivos excluidos.
5. En el cuadro de diálogo **Exclusión de archivos por nombre**, haga clic en **Añadir** y especifique los nombres de los archivos que desea excluir.

   Se permite el uso de los caracteres comodín * y ?

El 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 un 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.

6. Para excluir tipos de archivo del control de datos, en el cuadro de diálogo **Editor de reglas**, en **Exclusión de archivos**, active la opción **Tipo de archivo**.
7. En **Contenido de la regla**, haga clic en el valor subrayado para especificar tipos de archivos excluidos.
8. En el cuadro de diálogo **Exclusión de archivos por tipo**, seleccione los tipos de archivo que desea excluir y haga clic en **Aceptar**.

7.4.11 Importar o exportar reglas de control de datos

Si utiliza administración delegada, necesitará el permiso **Personalización del control de datos** para importar o exportar una regla de control de datos. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Las reglas de control de datos se pueden importar o exportar desde Enterprise Console como archivos XML.

Para importar o exportar reglas de control de datos:

1. En el menú **Herramientas**, señale **Administrar el control de datos** y haga clic en **Reglas de control de datos**.
2. En el cuadro de diálogo **Gestión de reglas de control de datos**, haga clic en **Importar** o **Exportar**.
   - Si desea importar una regla, en el cuadro de diálogo **Importar**, vaya a la regla que desea importar, selecciónela y haga clic en **Abrir**.
   - Si desea exportar una regla, en el cuadro de diálogo **Exportar**, seleccione un destino para el archivo, escriba un nombre para el archivo y haga clic en **Guardar**.

7.4.12 Crear o editar listas de control de contenido sencillas

Si utiliza administración delegada, necesitará el permiso **Personalización del control de datos** para crear un lista de control de contenido. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para ver una descripción completa de las listas de control del contenido, consulte Acerca de las listas de control de contenido (página 142).

Para crear o editar una lista de control de contenido:

1. En el menú **Herramientas**, señale **Administrar el control de datos** y haga clic en **Listas de control de contenido**.
2. En el cuadro de diálogo **Gestión de listas de control de contenido**, haga clic en **Añadir** para crear una lista de control de contenido nueva, o seleccione una existente y haga clic en **Editar**.
3. En el cuadro de diálogo **Lista de control de contenido** en el campo **Nombre**, escriba un nombre para la lista de control de contenido.
4. En el campo **Descripción**, escriba una descripción para la lista de control de contenido, si lo desea.

5. Si desea añadir etiquetas o modificar las etiquetas ya asignadas a la lista, haga clic en **Cambiar** junto al campo **Etiquetas**.

   Si lo desea, puede etiquetar la lista de control del contenido para saber a qué tipo y región hace referencia.
6. En el cuadro de diálogo **Etiquetas de listas de control de contenido**, en la lista **Etiquetas disponibles**, seleccione las etiquetas que desea asignar y muévalas a la lista **Etiquetas seleccionadas**. Haga clic en **Aceptar**.
7. En la sección **Escaneado de contenido**, seleccione una condición de búsqueda ("Cualquiera de estos términos", "Todos estos términos" o "Esta frase exacta") e introduzca los términos de búsqueda que desea encontrar en los documentos, separados por espacios. Haga clic en **Aceptar**.

   Nota
   La búsqueda diferencia entre mayúsculas y minúsculas.

   Las comillas no están permitidas en las listas de control del contenido sencillas. Utilice la condición "Esta frase exacta" para buscar frases exactas.

   Para crear expresiones más complejas, utilice el editor avanzado de listas de control de contenido, según se describe en Crear o editar una lista avanzada de control de contenido (página 150).

La nueva lista de control de contenido aparece en el cuadro de diálogo **Gestión de listas de control de contenido**.

Ejemplos

Condición de búsqueda	Ejemplo	Descripción
Cualquiera de estos términos	confidencial secreto	Busca documentos que contengan "confidencial" o "secreto".
Todos estos términos	proyecto confidencial	Busca documentos que contengan "proyecto" y "confidencial".
Esta frase exacta	sólo para uso interno	Busca documentos que contengan la frase "sólo para uso interno".

Si lo desea, añada la nueva lista de control de contenido a una regla de contenido.

7.4.13 Crear o editar una lista avanzada de control de contenido

Si utiliza administración delegada, necesitará el permiso **Personalización del control de datos** para crear un lista de control de contenido. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para ver una descripción completa de las listas de control del contenido, consulte Acerca de las listas de control de contenido (página 142).

Las listas de control de contenido pueden estar compuestas por una o más expresiones regulares y una puntuación límite. Para ello, utilice el editor avanzado.

Para crear o editar una lista de control de contenido con el editor avanzado:

1. En el menú **Herramientas**, señale **Administrar el control de datos** y haga clic en **Listas de control de contenido**.
2. En el cuadro de diálogo **Gestión de listas de control de contenido**, haga clic en **Añadir** para crear una lista de control de contenido nueva, o seleccione una existente y haga clic en **Editar**.
3. En el cuadro de diálogo **Lista de control de contenido** en el campo **Nombre**, escriba un nombre para la lista de control de contenido.
4. En el campo **Descripción**, escriba una descripción para la lista de control de contenido, si lo desea.
5. Si desea añadir etiquetas o modificar las etiquetas ya asignadas a la lista, haga clic en **Cambiar** junto al campo **Etiquetas**.

   Si lo desea, puede etiquetar la lista de control del contenido para saber a qué tipo y región hace referencia.
6. En el cuadro de diálogo **Etiquetas de listas de control de contenido**, en la lista **Etiquetas disponibles**, seleccione las etiquetas que desea asignar y muévalas a la lista **Etiquetas seleccionadas**. Haga clic en **Aceptar**.
7. Haga clic en el botón **Avanzadas**.
8. En el panel **Avanzadas**, haga clic en **Crear** para crear una expresión nueva, o seleccione una expresión existente y haga clic en **Editar**.
9. En el cuadro de diálogo **Lista de control de contenido - Opciones avanzadas**, escriba una expresión regular de Perl 5.

   Para ver una descripción de las expresiones regulares de Perl 5, consulte la documentación de Perl o visite http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html.
10. En el campo **Puntuación de la expresión**, introduzca el número que se añadirá a la puntuación total de la lista de control de contenido cuando se cumpla la expresión regular.
11. En el campo **Número máximo**, escriba el número máximo de coincidencias de la expresión regular que se pueden tener en cuenta para la puntuación total.
    Por ejemplo, una expresión con una puntuación de 5 y el número máximo de 2, puede aportar un máximo de 10 a la puntuación total de la lista de control de contenido. Si la expresión aparece 3 veces, seguirá contando como 10 en la puntuación total.

    Haga clic en **Aceptar**.
12. Repita los pasos del 5 al 11 para añadir más expresiones regulares a la lista de control de contenido.
13. En el campo **Puntuación límite**, escriba el número de veces que debe aparecer una expresión para cumplir la lista de control de contenido.

    Por ejemplo, una lista de control de contenido con la puntuación límite de 6 formada por 3 expresiones (A, B y C) con las puntuaciones y números máximos siguientes:

Expresión	Puntuación	Número máximo
Expresión A	5	2
Expresión B	3	1
Expresión C	1	5

    La lista de control de contenido se cumple si el control de datos encuentra 2 ejemplos de la expresión A o 1 ejemplo de la expresión A y 1 de la expresión B, o 1 ejemplo de la expresión B y 5 ejemplos de la expresión C.

    Haga clic en **Aceptar**.

La nueva lista de control de contenido aparece en el cuadro de diálogo **Gestión de listas de control de contenido**.

Ejemplo de expresión regular

```
(?i)\b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?
[abcd]?\b
```

Esta expresión regular representa números de la seguridad social en el Reino Unido, por ejemplo, AA 11 11 11 A.

(?i)	No diferencia entre mayúsculas y minúsculas.
\b	Representa un límite entre letras y otros caracteres.
[a-ceghj-npr-tw-z]	Representa cualquier carácter individual del rango de caracteres (A a C E G H J a N P R a T W a Z).
?	Representa la ocurrencia del elemento anterior una vez o ninguna.
\s?	Representa un o ningún espacio.
\d{2}	Representa dos dígitos.
[abcd]	Representa cualquier carácter individual de la lista (A, B, C o D).

Si lo desea, añada la nueva lista de control de contenido a una regla de contenido.

7.4.14 Importar o exportar listas de control de contenido

Si utiliza administración delegada, necesitará el permiso **Personalización del control de datos** para importar o exportar una lista de control de contenido. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Las listas de control del contenido se pueden importar o exportar desde Enterprise Console como archivos XML. Las listas de control del contenido se pueden compartir entre los productos de Sophos que sean compatibles.

Nota
Las listas de control del contenido de SophosLabs no se pueden exportar.

Para importar o exportar listas de control de contenido:

1. En el menú **Herramientas**, señale **Administrar el control de datos** y haga clic en **Listas de control de contenido**.
2. En el cuadro de diálogo **Gestión de listas de control de contenido**, haga clic en **Importar** o **Exportar**.
   - Si desea importar una lista de control de contenido, en el cuadro de diálogo **Importar**, vaya a la lista de control de contenido que desea importar, selecciónela y haga clic en **Abrir**.
   - Si desea exportar una lista de control de contenido, en el cuadro de diálogo **Exportar**, seleccione un destino para el archivo, escriba un nombre para el archivo y haga clic en **Guardar**.

7.5 Política de control de dispositivos

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

Importante
No debe utilizar el control de dispositivos de Sophos junto con otros programas de terceros para el mismo propósito.

El control de dispositivos permite impedir el uso de dispositivos de hardware externos no autorizados, medios de almacenamiento extraíbles y tecnologías de conexión inalámbrica en los equipos. Esto puede reducir de forma significativa el riesgo de pérdida accidental de datos y la entrada de programas externos.

Los dispositivos de almacenamiento extraíbles, unidades ópticas y disquetes también se pueden configurar para permitir acceso de sólo lectura.

Mediante el control de dispositivos, es posible reducir de forma significativa el riesgo de puentes de red entre redes corporativas y no corporativas. El modo **Bloquear puente** está disponible tanto para módems como dispositivos inalámbricos. Este modo funciona desactivando el adaptador de red inalámbrico o módem cuando una estación está conectada a una red física (normalmente, mediante una conexión Ethernet). Cuando el ordenador se desconecta de la red de la empresa, podrá volver a utilizar los dispositivos inalámbricos o módem.

Por defecto, el control de dispositivos está desactivado y se permiten todos los dispositivos.

Si desea activar el control de dispositivos por primera vez, se recomienda:

- Seleccionar los tipos de dispositivo que desea controlar.
- Detectar los dispositivos pero sin bloquearlos.
- Utilice los eventos del control de dispositivos para decidir qué tipos de dispositivos bloquear y cuáles dejar exentos.
- Detectar y bloquear, o permitir sólo la lectura de dispositivos de almacenamiento.

Para más información sobre la configuración recomendada para el control de dispositivos, consulte la *Guía de configuración de políticas de Sophos Enterprise Console*.

Nota
Si utiliza administración delegada:

- Para configurar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

7.5.1 Acerca de los eventos del control de dispositivos

Cuando se produce un evento del control de dispositivos, por ejemplo, si se bloquea un dispositivo de almacenamiento extraíble, el evento se envía a Enterprise Console y se puede visualizar en el cuadro de diálogo **Visualizador de eventos del control de dispositivos**.

Nota
Si define unidades ópticas como de "Sólo lectura", los eventos de estas unidades no se envían a Enterprise Console ni se registran de forma local. Esto impide la generación no deseada de informes de eventos.

En el cuadro de diálogo **Visualizador de eventos del control de dispositivos**, utilice los filtros para mostrar sólo los eventos que le interesen. También puede exportar una lista de los eventos del control de dispositivos. Para más información, consulte Acerca de los eventos del control de dispositivos (página 154) y Exportar la lista de eventos a un archivo (página 194).

Los eventos del control de dispositivos pueden utilizarse para añadir excepciones para determinados dispositivos o modelos a las políticas de control de dispositivos. Para más información sobre las excepciones de dispositivos, consulte Excluir dispositivos de una sola política (página 158) o Excluir un dispositivo de todas las políticas (página 157).

El número de equipos con eventos del control de dispositivos que superen un umbral determinado en los últimos 7 días aparece en el Panel de control. Para más información sobre cómo configurar el umbral, consulte Configuración del panel de control (página 45).

También puede configurar alertas que se envíen a determinados destinatarios cuando se produzca un evento del control de dispositivos. Para más información, vea Alertas y mensajes del control de dispositivos (página 181).

7.5.2 Tipos de dispositivos que se pueden controlar

El control de dispositivos le permite bloquear los siguientes tipos de dispositivo: *almacenamiento*, *red*, *corto alcance* y *medios*.

Almacenamiento

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

Para ver la lista de los dispositivos de almacenamiento seguro compatibles, consulte el artículo 63102 de la base de conocimiento de Sophos.

Sugerencia
Mediante la categoría de dispositivos seguros de almacenamiento extraíbles, puede permitir el uso de dispositivos compatibles, a la vez que bloquea otros dispositivos de almacenamiento extraíbles.

Red

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

Para las interfaces de red, también puede seleccionar el modo **Bloquear puente**, que ayuda de forma significativa a reducir el riesgo de puentes de red entre redes corporativas y no corporativas. Este modo funciona desactivando el adaptador de red inalámbrico o módem cuando una estación está conectada a una red física (normalmente, mediante una conexión Ethernet). Cuando el ordenador se desconecta de la red de la empresa, podrá volver a utilizar los dispositivos inalámbricos o módem.

Corto alcance

- Bluetooth
- Infrarrojos (IrDA)

El control se extiende tanto a dispositivos internos como externos. Por ejemplo, una política que bloquea interfaces Bluetooth bloqueará:

- La interfaz Bluetooth integrada en el ordenador
- Cualquier dispositivo Bluetooth USB que se conecte

Medios

- MTP/PTP

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

7.5.3 Seleccionar tipos de dispositivos

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Importante
No debe bloquear la conexión inalámbrica en los ordenadores administrados por Enterprise Console a través de este tipo de conexión.

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Configuración**, en **Almacenamiento**, seleccione el tipo de dispositivo de almacenamiento que desea controlar.
4. Haga clic en la columna **Estado** junto al tipo de dispositivo y abra la lista desplegable que aparece. Seleccione el tipo de acceso que desea permitir.

   Por defecto, los dispositivos tienen acceso total. Para los dispositivos de almacenamiento extraíbles, unidades ópticas y disquetes, puede cambiarlo por "Bloqueado" o "Sólo lectura". Para los dispositivos seguros de almacenamiento extraíbles, puede cambiarlo por "Bloqueado".
5. En **Red**, seleccione el tipo de dispositivo de red que desea bloquear.
6. Haga clic en la columna **Estado** junto al tipo de dispositivo de red y abra la lista desplegable que aparece.
   - Selecione "Bloqueado" si desea bloquear los dispositivos de ese tipo.
   - Seleccione "Bloquear puente" si desea impedir los puentes de red entre redes corporativas y no corporativas. Los dispositivos de ese tipo se bloquearán cuando la estación esté conectada a una red física (normalmente, a través de una conexión Ethernet). Cuando la estación se desconecte de la red física, se desbloquearán los dispositivos de ese tipo.
7. En la sección **Corto alcance**, seleccione el tipo de dispositivo de corto alcance que desea bloquear. En la columna **Estado**, junto al tipo de dispositivos, seleccione "Bloqueado".

   Haga clic en **Aceptar**.
8. Para bloquear dispositivos multimedia que se conectan a un ordenador utilizando el protocolo de transferencia multimedia (MTP) o el protocolo de transferencia de imágenes (PTP), como teléfonos móviles, tabletas, cámaras digitales o reproductores multimedia, en **Medios**, seleccione **MTP/PTP**. En la columna **Estado** seleccione "Bloqueado".

7.5.4 Detectar dispositivos sin bloquearlos

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, puede detectar dispositivos sin bloquearlos. Por ejemplo, si tiene intención de bloquear dispositivos más adelante, pero quiere detectar y excluir los que necesite.

Para detectar dispositivos sin bloquearlos, active el escaneado para el control de dispositivos en una política de control de dispositivos y active el modo de *sólo detección*. Cambie el estado de los dispositivos que desea detectar por "Bloqueado". Se crearán eventos sobre los dispositivos utilizados en estaciones cuando se infrinja la política, pero no se bloquearán los dispositivos.

Para más información sobre cómo visualizar los eventos del control de dispositivos, consulte Acerca de los eventos del control de dispositivos (página 154).

Para detectar dispositivos sin bloquearlos:

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Configuración**, active la opción **Activar el control de dispositivos**.
4. Active la opción **Detectar pero no bloquear**.
5. Si aún no lo ha cambiado, modifique el estado de los dispositivos que desea detectar por "Bloqueado". (Para saber cómo hacerlo, consulte Seleccionar tipos de dispositivos (página 155).)

   Haga clic en **Aceptar**.

7.5.5 Detectar y bloquear dispositivos

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Configuración**, active la opción **Activar el control de dispositivos**.
4. Desactive la opción **Detectar pero no bloquear**.
5. Si aún no lo ha cambiado, modifique el estado de los dispositivos que desea bloquear por "Bloqueado". (Para saber cómo hacerlo, consulte Seleccionar las aplicaciones que desea restringir (página 136).)

   Haga clic en **Aceptar**.

7.5.6 Excluir un dispositivo de todas las políticas

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, puede excluir un dispositivo de todas las políticas, incluida la predeterminada. Dicha excepción se añadirá a todas las políticas nuevas que cree.

Puede excluir un dispositivo determinado ("sólo este dispositivo") o un modelo de dispositivo específico ("todos los dispositivos con este identificador de modelo"). No configure excepciones múltiples para el mismo dispositivo definiendo a la vez el identificador y el dispositivo. Si se definen ambas, la excepción del dispositivo determinado tendrá preferencia.

Para excluir un dispositivo de todas las políticas de control de dispositivos:

1. En el menú **Eventos**, haga clic en **Eventos del control de dispositivos**.
   Aparece el cuadro de diálogo **Visualizador de eventos del control de dispositivos**.
2. Si sólo desea mostrar ciertos eventos, en el panel **Criterio de búsqueda**, configure los filtros que necesite y haga clic en **Buscar** para mostrar los eventos.

   Para obtener más información, consulte Acerca de los eventos del control de dispositivos (página 154).
3. Seleccione la entrada del dispositivo que desea excluir de las políticas y haga clic en **Excepciones**.

   Aparece el cuadro de diálogo **Excepción de dispositivos**. En **Detalles del dispositivo**, aparece el tipo, el ID de modelo y el ID de dispositivo del dispositivo. En **Detalles de la excepción**, **Ámbito**, se puede leer "Todas las políticas".

   Nota
   Si no existe un evento del dispositivo que desea excluir, por ejemplo, una unidad de CD-ROM o DVD en una estación, vaya al equipo que contiene el dispositivo y actívelo en el Administrador de dispositivos. (Para acceder al Administrador de dispositivos, haga clic con el botón derecho en **Mi PC**, haga clic en **Administrar** y haga clic en **Administrador de dispositivos**.) Se creará un evento nuevo que aparecerá en el cuadro de diálogo **Visualizador de eventos del control de dispositivos**. Después, puede excluir el dispositivo según lo descrito en este paso.

4. Excluya sólo este dispositivo o todos los dispositivos de este ID de modelo.
5. Permita el acceso total al dispositivo o acceso de sólo lectura.
6. En el campo **Comentario**, escriba un comentario, si lo desea. Por ejemplo, puede especificar quién solicitó la exención del dispositivo.
7. Haga clic en **Aceptar**.

7.5.7 Excluir dispositivos de una sola política

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, puede excluir un dispositivo determinado de una política de control de dispositivos.

Puede excluir un dispositivo determinado ("sólo este dispositivo") o un modelo de dispositivo específico ("todos los dispositivos con este identificador de modelo"). No configure excepciones múltiples para el mismo dispositivo definiendo a la vez el identificador y el dispositivo. Si se definen ambas, la excepción del dispositivo determinado tendrá preferencia.

Para excluir dispositivos de políticas:

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

Consulte Comprobar qué políticas usa un grupo (página 25).

2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Configuración**, haga clic en **Añadir excepción**.
   Aparece el cuadro de diálogo **Visualizador de eventos del control de dispositivos**.
4. Si sólo desea mostrar ciertos eventos, en el panel **Criterio de búsqueda**, configure los filtros que necesite y haga clic en **Buscar** para mostrar los eventos.

   Para obtener más información, consulte Acerca de los eventos del control de dispositivos (página 154).
5. Seleccione la entrada del dispositivo que desea excluir de la política y haga clic en **Excepciones**.

   Aparece el cuadro de diálogo **Excepción de dispositivos**. En **Detalles del dispositivo**, aparece el tipo, el ID de modelo y el ID de dispositivo del dispositivo. En **Detalles de la excepción**, **Ámbito**, se puede leer "Sólo esta política".

   Nota
   Si no existe un evento del dispositivo que desea excluir, por ejemplo, una unidad de CD-ROM o DVD en una estación, vaya al equipo que contiene el dispositivo y actívelo en el Administrador de dispositivos. (Para acceder al Administrador de dispositivos, haga clic con el botón derecho en **Mi PC**, haga clic en **Administrar** y haga clic en **Administrador de dispositivos**.) Se creará un evento nuevo que aparecerá en el cuadro de diálogo **Visualizador de eventos del control de dispositivos**. Después, puede excluir el dispositivo según lo descrito en este paso.

6. Excluya sólo este dispositivo o todos los dispositivos de este ID de modelo.
7. Permita el acceso total al dispositivo o acceso de sólo lectura.
8. En el campo **Comentario**, escriba un comentario, si lo desea. Por ejemplo, puede especificar quién solicitó la exención del dispositivo.
9. Haga clic en **Aceptar**.

7.5.8 Ver o editar la lista de dispositivos excluidos

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para ver o editar la lista de dispositivos excluidos:

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Configuración**, seleccione el tipo de dispositivo del que desea visualizar las excepciones, por ejemplo, una unidad óptica. Haga clic en **Ver excepciones**.
   Aparece el cuadro de diálogo **Excepciones de <tipo de dispositivo>**. Si una excepción afecta a todos los dispositivos con ese identificador de modelo, el campo **Identificador** está vacío.

4. Si desea editar la lista de dispositivos excluidos:
   - Si desea añadir una excepción, haga clic en **Añadir**. Para obtener más información, consulte Excluir dispositivos de una sola política (página 158).
   - Si desea editar una excepción, selecciónela y haga clic en **Editar**. Cambie la configuración según sea necesario en el cuadro de diálogo **Excepción de dispositivos**.
   - Si desea eliminar una excepción, seleccione el dispositivo exento y haga clic en **Eliminar**.

     Se eliminará el dispositivo exento de la política modificada. Si desea eliminar el dispositivo de otras políticas, repita estos pasos en cada una de ellas.

7.6 Política de protección contra manipulaciones

La protección contra manipulaciones permite evitar que programas maliciosos o usuarios no autorizados (administradores locales o usuarios con conocimientos limitados) puedan desinstalar el software de seguridad de Sophos o desactivarlo desde Sophos Endpoint Security and Control.

Nota
Esta protección puede no ser efectiva ante usuarios con amplios conocimientos técnicos. También podría ser ineficaz ante programas maliciosos diseñados específicamente para realizar ciertos cambios en el funcionamiento del sistema operativo. Este tipo de programas maliciosos se detecta mediante el escaneado de amenazas y comportamientos sospechosos. (Para más información, consulte Política antivirus y HIPS (página 75).)

Después de activar y crear una contraseña para la protección contra manipulaciones, los usuarios que pertenezcan al grupo SophosAdministrator de la estación y no la conozcan, no podrán:

- Cambiar la configuración del escaneado en acceso ni de la detección de comportamientos sospechosos de Sophos Endpoint Security and Control.
- Desactivar la protección contra manipulaciones.
- Desinstalar los componentes de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate y Sophos Remote Management System).

Si desea que los usuarios que pertenecen a SophosAdministrators puedan realizar estas tareas, proporcióneles la contraseña para que se puedan autenticar.

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

Nota
Si utiliza administración delegada:

- Para configurar la política de protección contra manipulaciones, es necesario contar con el permiso **Configuración de políticas: protección contra manipulaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Eventos de la protección contra manipulaciones

Cuando se produce algún evento de la protección contra manipulaciones, por ejemplo, cuando se detecta un intento no autorizado de desinstalar Sophos Anti-Virus, quedará registrado en Enterprise Console. Para más información, vea Visualizar eventos de la protección contra manipulaciones (página 189).

Existen dos tipos de eventos de la protección contra manipulaciones:

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

7.6.1 Activar o desactivar la protección contra manipulaciones

Si utiliza administración delegada:

- Para configurar la política de protección contra manipulaciones, es necesario contar con el permiso **Configuración de políticas: protección contra manipulaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para activar o desactivar la protección contra manipulaciones:

1. Compruebe qué política de protección contra manipulaciones usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Protección contra manipulaciones**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de protección contra manipulaciones**, utilice la opción **Activar la protección contra manipulaciones**.

   Si desea activar la protección contra manipulaciones por primera vez, haga clic en **Establecer** debajo del cuadro de texto **Contraseña**. En el cuadro de diálogo **Contraseña de la protección contra manipulaciones**, introduzca y confirme una contraseña.

   Sugerencia
   Se recomienda que la contraseña contenga al menos ocho caracteres, incluyendo mayúsculas, minúsculas y números.

7.6.2 Cambiar la contraseña de la protección contra manipulaciones

Para cambiar la contraseña de la protección contra manipulaciones:

1. Compruebe qué política de protección contra manipulaciones usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Protección contra manipulaciones**. A continuación, haga doble clic en la política que desee modificar.

3. En el cuadro de diálogo **Política de protección contra manipulaciones**, haga clic en **Cambiar** debajo del cuadro de texto **Contraseña**. En el cuadro de diálogo **Contraseña de la protección contra manipulaciones**, introduzca y confirme la nueva contraseña.

   Sugerencia
   La contraseña debería contener al menos ocho caracteres, incluyendo mayúsculas, minúsculas y números.

7.6.3 Acerca de la protección contra manipulaciones mejorada

La protección contra manipulaciones mejorada se basa en la función de la protección contra manipulaciones. Si la protección contra manipulaciones mejorada está activada, se bloquean las acciones siguientes para Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System y Sophos Endpoint Defense:

- Detener servicios de la IU Servicios
- Terminar servicios de la IU Administrador de tareas
- Cambiar la configuración de servicios de la IU Servicios
- Detener servicios o editar la configuración de servicios desde la línea de comandos
- Desinstalando
- Volver a instalar
- Terminar procesos de la IU Administrador de tareas
- Eliminar o modificar archivos o carpetas protegidos
- Eliminar o modificar claves del registro protegidas

Importante
Para habilitar la protección contra manipulaciones mejorada, debe estar activada la protección contra manipulaciones. Si la protección contra manipulaciones está desactivada, la protección contra manipulaciones mejorada se desactivará de forma automática.

7.6.4 Configuración de la protección contra manipulaciones mejorada

1. En el panel **Políticas**, haga doble clic en **Protección contra manipulaciones**. A continuación, haga doble clic en la política que desee modificar.
2. En el cuadro de diálogo **Política de protección contra manipulaciones**, asegúrese de que la casilla **Activar la protección contra manipulaciones** está activada y, a continuación, seleccione la casilla **Activar la protección contra manipulaciones mejorada**.
3. Si se trata de una nueva instalación o actualización, en el cuadro de diálogo **Política de protección contra manipulaciones**, haga clic en **Establecer** debajo del cuadro de texto **Contraseña**.

   Si la protección contra manipulaciones ya está activada, haga clic en **Cambiar** debajo del cuadro de texto **Contraseña**. En el cuadro de diálogo **Contraseña de la protección contra manipulaciones**, introduzca y confirme una contraseña.

Nota
Se utiliza la misma contraseña para la protección contra manipulaciones y la protección contra manipulaciones mejorada. Cuando la protección contra manipulaciones mejorada está habilitada, anula la protección contra manipulaciones. Esta es la razón por la que debe cambiarse la contraseña cuando ya se ha definido la contraseña de la protección contra manipulaciones.

Recomendamos usar una contraseña distinta para cada política.

7.7 Política de parches

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

Enterprise Console permite comprobar que los equipos tienen instalados los parches de seguridad más recientes.

El nivel de gravedad permite identificar los problemas de seguridad más críticos relacionados con los parches para resolverlos con prontitud. Para establecer el nivel de gravedad, SophosLabs tiene en cuenta las amenazas más recientes que se aprovechan de agujeros de seguridad.

Para poder hacer uso del sistema de control de parches, debe instalar el agente de parches en las estaciones de la red, que se gestiona desde Enterprise Console. Para ello, puede utilizar el **Asistente para proteger ordenadores**. Consulte Proteger ordenadores de forma automática (página 43).

En esta sección, se da por supuesto que tiene instalado el agente de parches.

Nota
Si utiliza administración delegada:

- Para configurar la política de parches, es necesario contar con el permiso **Configuración de políticas: parches**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

7.7.1 Cómo funciona el control de parches

El control de parches no se encuentra activado en la política predeterminada. Al activar el control de parches en las estaciones, se realiza la comprobación inicial. Puede tardar unos minutos. Las comprobaciones posteriores se realizan con la frecuencia establecida (por defecto, a diario).

Nota
Si las estaciones realizan la comprobación antes de que Enterprise Console haya descargado los datos de parches desde Sophos, el visualizador de eventos de parches no mostrará nada. La descarga inicial puede tardar varias horas. Para comprobar si se ha completado la descarga, vea el campo **Actualización de parches** en el **Visualizador de eventos del control de parches**.

Si el agente de parches no se puede actualizar desde Enterprise Console, seguirá utilizando la lista de parches más reciente.

Sólo se evalúan los parches de seguridad del software instalado en cada equipo. Si se publica un parche que sustituye a otro, la evaluación del anterior se sustituye por la evaluación del más reciente. Sólo se comprueba el parche nuevo.

Parches reemplazados

En ocasiones, puede ocurrir que ciertos parches se actualicen con versiones más recientes. El parches reemplazado será sustituido.

Sophos recomienda actualizar los parches reemplazados para mantener los equipos actualizados.

Ejemplo: Si en una búsqueda muestra el parche P01 reemplazado por el parche P02, Sophos recomienda instalar P02.

7.7.2 Acerca de los eventos del control de parches

Cuando se produce un evento del control de parches, por ejemplo, si a alguna estación le falta algún parche, el evento se envía a Enterprise Console y se puede visualizar en el **Visualizador de eventos del control de parches**.

En el **Visualizador de eventos del control de parches**, utilice los filtros para mostrar solo los eventos que le interesen. También puede exportar una lista de los eventos del control de parches. Para más información, consulte Eventos del control de parches (página 189) y Exportar la lista de eventos a un archivo (página 194).

7.7.3 Activar o desactivar el control de parches

Si utiliza administración delegada:

- Para configurar la política de parches, es necesario contar con el permiso **Configuración de políticas: parches**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para activar o desactivar el control de parches:

1. Compruebe qué política de parches usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Parches**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de parches**, active o desactive la opción **Activar el control de parches** y haga clic en **Aceptar**.

7.7.4 Establecer el intervalo de control de parches

Si utiliza administración delegada:

- Para configurar la política de parches, es necesario contar con el permiso **Configuración de políticas: parches**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para establecer el intervalo de comprobación de parches:

1. Compruebe qué política de parches usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Parches**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de parches**, seleccione el intervalo de comprobación en el cuadro de lista desplegable **Comprobar parches**. Haga clic en **Aceptar**.
   Para disponer de control de parches, debe activarlo en la política.

7.8 Política de control web

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

Por defecto, el control web se encuentra desactivado en Enterprise Console. Active la opción **Activar el control web** para disponer de las siguientes opciones:

- **Control de sitios web inapropiados**: Este control web básico incluye 14 categorías. Esta función permite evitar el acceso a sitios web que pueden afectar legalmente a la empresa. Para obtener más información, consulte Control de sitios web inapropiados (página 166).
- **Control web completo**: Esta opción incluye políticas de acceso para más de 50 categorías de sitios web. Para sincronizarla con las estaciones y distribuir actualizaciones de la política o recoger datos sobre las actividades en Internet, es necesario un dispositivo Sophos Web Appliance, Sophos Management Appliance o Sophos UTM (versión 9.2 o posterior). Para obtener más información, consulte Control web completo (página 170).

Para disponer de control web, ajuste la política existente o cree una política nueva. Para obtener más información, consulte Crear políticas (página 29). Las acciones para las diferentes categorías son: «Bloquear», «Avisar» y «Permitir». En Enterprise Console podrá ver el estado del control web y los eventos web. Para más información sobre los eventos web, consulte Visualizar eventos del control web (página 192).

En cambio, si utiliza la política de control web completo, Enterprise Console necesita la ubicación del dispositivo (Web, UTM o Management) en el que se ha configurado la política completa de filtrado web, así como una clave compartida para proteger las comunicaciones entre el dispositivo y Enterprise Console. Al seleccionar la política de control web completo, la mayor parte de las tareas de informes y vigilancia se realizan desde el dispositivo; sin embargo, los sitios web escaneados y evaluados con el filtrado activo de direcciones web (Protección web (página 95)) de Sophos Endpoint Security and Control aparecen como eventos web en Enterprise Console.

Para obtener más información sobre el control web, consulte la *Guía de introducción al control web*.

Nota
Si utiliza administración delegada:

- Para modificar las políticas de control web, es necesario contar con el permiso **Configuración de políticas: control web**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

7.8.1 Control de sitios web inapropiados

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

Este control web básico permite filtrar la navegación por Internet según 14 categorías. Para cada categoría (descritas en Acerca de las categorías de sitios web (página 167)) puede establecer una acción determinada, como se describe en Seleccionar la acción para las categorías web (página 169).

Podrá bloquear el acceso a sitios web restringidos. Se avisa al usuario y se envía notificación a Enterprise Console.

También se puede avisar al usuario; en cualquier caso se envía notificación. Si el usuario procede al sitio web a pesar del aviso, se envía una nueva notificación a Enterprise Console.

Nota
El tipo de notificación difiere de sitios web HTTP a HTTPS. Para sitios HTTP, se muestra el «bloqueo» o «aviso» según las categorías establecidas. Para sitios HTTPS, sólo se muestra el «bloqueo» en un mensaje del icono de la bandeja del sistema. Para sitios HTTPS no se muestran ni se registran avisos. En Enterprise Console, el evento se registra como la acción «proceder».

Si seleccione la acción «permitir», no se bloquearán los sitios web en esa categoría a menos que especifique alguna excepción. Esta acción no se registra si activa la opción **Control de sitios web inapropiados**.

Nota
Los sitios permitidos siguen escaneándose y evaluándose mediante la función de filtrado activo de direcciones web (protección web) de Sophos Endpoint Security and Control.

Activar el control de sitios web inapropiados

Siga los pasos que se indican a continuación para activar el control web en Enterprise Console y utilizar el control de sitios web inapropiados.

Nota
Si utiliza administración delegada:

- Para modificar las políticas de control web, es necesario contar con el permiso **Configuración de políticas: control web**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para activar el control de sitios web inapropiados:

1. Compruebe qué política web usa el grupo de ordenadores que desea configurar. Para obtener más información, consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control web**. A continuación, haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política de control web**.
3. En la ficha **General**, seleccione la opción **Activar el control web**.
   Se muestra la política **Control de sitios web inapropiados**. Puede establecer la acción deseada para cada una de las 14 categorías. Para obtener más información, consulte Seleccionar la acción para las categorías web (página 169).

Acerca de las categorías de sitios web

La opción **Control de sitios web inapropiados** permite configurar 14 categorías de sitios web. Para obtener más información, consulte Control de sitios web inapropiados (página 166).

A continuación se describe el contenido de cada categoría. Entre paréntesis se indica la acción predeterminada. Las acciones disponibles para cada categoría son: **Bloquear**, **Avisar** y **Permitir**. La acción **Permitir** da acceso a todos los sitios web en esa categoría. Para cambiar la acción, consulte Seleccionar la acción para las categorías web (página 169).

- **Adulto sexualmente explícito (bloquear)**: Esta categoría incluye sitios web con productos para adultos, incluyendo sexo o desnudez erótica total o parcial, descripciones o imágenes de actos sexuales, incluido el uso de objetos inanimados de manera sexual; relatos eróticos y descripciones textuales de actos sexuales; texto o gráficos sobre violencia o explotación sexual; ataduras, fetiches y perforación (piercing) en los genitales; productos para adultos como juguetes sexuales, CD-ROM y vídeos sobre sexo; servicios para adultos como videoconferencias, servicios de acompañante y clubes de desnudismo; animaciones y caricaturas explícitas.

  Nota
  No se incluyen sitios web de salud sexual, cáncer de mama o enfermedades de transmisión sexual (excepto en casos de ejemplos gráficos).

- **Alcohol y tabaco (avisar)**: Esta categoría incluye sitios web que promueven o distribuyen alcohol o tabaco de forma gratuita o previo pago.
- **Proxy de anonimato (bloquear)**: Esta categoría incluye sitios web con servidores proxy remotos o navegación anónima, caché de buscadores o traducción web para evitar filtrado.
- **Actividad criminal (bloquear)**: Esta categoría incluye sitios web para abogar, dar instrucciones o aconsejar sobre la realización de actos ilegales tales como robo de servicio telefónico, evadir el cumplimiento de la ley, forzar cerraduras, fraude, plagio/estafa y técnicas de robo con allanamiento de morada.

- **Juegos de azar (avisar)**: Esta categoría incluye sitios web de apuestas o lotería que incitan al uso de dinero real, casinos virtuales y apuestas en alta mar, ligas deportivas virtuales y grupos de apuestas y pronósticos deportivos.
- **Hackers (bloquear)**: Esta categoría incluye sitios web de promoción, instrucción o consejos sobre el uso ilegal o cuestionable de equipos o software con el fin de piratear contraseñas, crear virus y obtener acceso a otras computadoras o sistemas informáticos de comunicación; sitios que ofrecen formas de evitar nuestro software de filtrado; software pirateado; sitios de descargas de software pirateado; sitios de descargas de archivos multimedia pirateados.
- **Drogas ilegales (bloquear)**: Esta categoría incluye sitios web de recetas, instrucciones o kits para fabricar o cultivar sustancias ilegales para fines diferentes del uso industrial; hacer atractivo, alentar o instruir el consumo o esconder el consumo de alcohol, tabaco, drogas ilegales u otras sustancias ilegales para menores; sitios; información sobre sustancias psicotrópicas legales: aspirar pegamento, mal uso de medicamentos recetados o abuso de otras sustancias legales; distribución de alcohol, drogas ilegales de forma gratuita o previo pago; exhibición, venta o descripción detallada del uso de parafernalia de drogas.
- **Intolerancia y odio (bloquear)**: Esta categoría incluye sitios web que abogan o incitan a la degradación o ataque de poblaciones o instituciones específicas en base a asociaciones tales como religión, raza, nacionalidad, sexo, edad, discapacidad u orientación sexual; promoción de una agenda social o política que sostengan en su naturaleza la supremacía de un grupo y la exclusión de otros por su raza, religión, nacionalidad, sexo, edad, discapacidad u orientación sexual; sitios revisionistas o negadores del holocausto; coerción o reclutamiento para afiliarse a una pandilla[1] o culto[2]; militancia, extremismo.

  Nota
  No se incluyen las noticias ni incidentes históricos o de prensa que puedan incluir los criterios antes mencionados (excepto en los ejemplos gráficos).

  [1] Una pandilla se define como un grupo cuya actividad principal es la perpetración de actos delictivos, que tiene un nombre común o signo o símbolo identificatorio y cuyos miembros, de forma individual o colectiva, se involucran en actividades delictivas en nombre del grupo.

  [2] Un culto se define como un grupo cuyos seguidores han sido reclutados y retenidos de manera engañosa o manipuladora a través de influencia indebida de manera tal que la personalidad y el comportamiento de los seguidores se ven alteradas. El liderazgo es todopoderoso, la ideología es totalitaria y la voluntad del individuo está subordinada a la del grupo. Se aparta de la sociedad.
- **Pesca de información y fraude (bloquear)**: Esta categoría incluye sitios web de phishing (suplantación de identidad), consejos de robo mediante servicio telefónico; plagio & copia, incluida la venta de artículos de investigación.
- **Direcciones en correo no deseado (bloquear)**: Esta categoría incluye sitios web que aparecen en spam, como en estos temas: informática, finanzas y acciones, entretenimiento, juegos, salud y medicina, humor y novedades, anuncios personales y citas, productos y servicios, compras o viajes.
- **Programas espía (bloquear)**: Esta categoría incluye sitios web que ofrecen o promueven la recolección o el rastreo de información sin que el usuario final o la organización lo conozca o haya otorgado su consentimiento explícito; sitios que contienen archivos ejecutables maliciosos o virus; software de monitoreo de terceros y otro software comercial no solicitado; destinos de spyware y malware de "llamadas al hogar".
- **Contenido ofensivo (avisar)**: Esta categoría incluye sitios web con lenguaje ofensivo o violento, incluidas bromas, historietas o sátiras; uso excesivo de blasfemias o gestos obscenos.

- **Violencia (avisar)**: Esta categoría incluye sitios web con representaciones, descripciones o apología del ataque físico contra humanos, animales o instituciones; descripciones de torturas, mutilaciones, masacres o muertes horrorosas. Apología del suicidio o la automutilación; instrucciones, recetas o kits para fabricar bombas u otros dispositivos dañinos o destructivos; uso excesivo de blasfemias o gestos obscenos.

  Nota
  No bloqueamos las noticias ni incidentes históricos o de prensa que puedan incluir los criterios antes mencionados (excepto en los ejemplos gráficos).

- **Armas (avisar)**: Esta categoría incluye sitios web de compra o solicitud de información por Internet, incluidas listas de precios y direcciones de distribuidores; cualquier página o sitio que contenga predominantemente contenidos relacionados con la venta de pistolas, armas, municiones o sustancias venenosas o en la cual haya vínculos relacionados con alguna de estas cosas; exhibición o descripción del uso de pistolas, armas, municiones o sustancias venenosas.

  Nota
  Un arma es cualquier objeto (como un garrote, un cuchillo o una pistola) que se utiliza para herir, derrotar o destruir.

Seleccionar la acción para las categorías web

Tras activar el control web con la opción **Control de sitios web inapropiados** puede establecer la acción para cada categoría. También puede crear una política nueva a partir de la predeterminada. Para obtener más información, consulte Crear políticas (página 29).

Para seleccionar la acción en cada categoría web:

1. En la ficha **General**, junto a las categorías que desee configurar, seleccione:
   - **Bloquear**: No permite el acceso a sitios web en las categorías seleccionadas. Para sitios web HTTP, se muestra un mensaje de notificación para el usuario. Para sitios web HTTPS, se notifica al usuario con un mensaje del icono de la bandeja del sistema.
   - **Avisar**: Notifica al usuario del posible peligro si se visita el sitio web solicitado, pero se da la opción se proseguir. Para sitios web HTTP, se muestra un mensaje de aviso para el usuario. Para sitios web HTTPS, no se notifica al usuario y se permite el acceso. En Enterprise Console, el evento se registra como la acción «proceder».
   - **Permitir**: Permite el acceso a sitios web en las categorías seleccionadas. Esta acción no se registra.
2. Haga clic en **Aceptar**.

Gestionar las excepciones web

Si selecciona la opción **Control de sitios web inapropiados**, puede crear excepciones para las reglas «Bloquear» y «Avisar». Para añadir excepciones, utilice los cuadros «Sitios web autorizados» y «Sitios web bloqueados». Puede utilizar la dirección IP o el nombre de dominio. Los sitios web en la lista se pueden modificar o eliminar si es necesario.

Nota
Si existe algún conflicto entre las listas 'Bloquear' y 'Permitir', la de bloquear siempre tiene preferencia. Por ejemplo, si añade la misma dirección IP en las listas Bloquear y Permitir, dicha dirección será bloqueada. Además, si un dominio se encuentra en la lista Bloquear, también se bloquearán los subdominios aunque se encuentren en la lista Permitir.

Para añadir una excepción web:

1. En la ficha **Excepciones web**, haga clic en **Añadir** junto a **Sitios web autorizados** o **Sitios web bloqueados**.
2. En el cuadro de diálogo **Añadir sitio web a autorizar**, haga clic en **Nombre de dominio**, **Dirección IP con máscara subred** o **Dirección IP**. Sobre el cuadro de entrada se muestra un ejemplo en cada caso.
3. Introduzca la excepción según el tipo seleccionado.
4. Haga clic en **Aceptar**.

Si desea modificar o eliminar algún sitio web de la lista, selecciónelo y haga clic en **Editar** o **Eliminar**, respectivamente.

7.8.2 Control web completo

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte: http://www.sophos.com/es-es/products/complete/comparison.aspx.

Si utiliza un dispositivo Sophos Web Appliance, Sophos Management Appliance o Sophos UTM (versión 9.2 o posterior), puede distribuir una política web a los usuarios a través de Enterprise Console.

Las estaciones se comunican con Enterprise Console del mismo modo que cuando está seleccionada la política de control de sitios web inapropiados, pero las reglas de filtrado web y los registros de la navegación por Internet se sincronizan con el dispositivo especificado. La política se almacena en los equipos.

Según la política, se puede bloquear, avisar o permitir el acceso a diferentes sitios web. Para ver datos de las actividades de los usuarios, utilice las funciones de **Informes** y **Búsqueda** de los dispositivos Dispositivo web o Dispositivo de gestión, o la opción **Logging & Reporting > Web Protection** del dispositivo de UTM. Todos los eventos del control web se registran en el dispositivo; sin embargo, los sitios escaneados y evaluados con el filtrado activo de direcciones web (protección web) de Sophos Endpoint Security and Control se registran como eventos web en Enterprise Console.

Nota
Los sitios, tanto HTTP como HTTPS, se filtran en todos los navegadores web compatibles, pero las notificaciones en los dispositivos Sophos Web Appliance y Sophos Management Appliance son diferentes según el tipo de dirección web. Para sitios HTTP, se muestra el «bloqueo» o «aviso» según las categorías establecidas. Para sitios HTTPS, sólo se muestra el «bloqueo» en un mensaje del icono de la bandeja del sistema. Para sitios HTTPS no se muestran ni se registran avisos. En Dispositivo web o Dispositivo de gestión, el evento se registra como la acción «proceder».

El dispositivo de UTM utiliza un servicio central en la nube denominado Sophos LiveConnect para proteger y vigilar las estaciones. LiveConnect permite administrar todas las estaciones en todo momento, tanto si se encuentran en la red local como en oficinas remotas o con usuarios que se desplazan, las actualizaciones de las políticas se distribuyen a los usuarios y se cargan los datos de los informes sobre las estaciones incluso cuando los usuarios no están conectados a la red.

Al utilizar Dispositivo de gestión o Dispositivo web, las estaciones pueden comunicarse con el dispositivo tanto directamente como a través de Sophos LiveConnect.

La opción **Control web completo** permite aplicar una detallada política de acceso a Internet. En comparación con el control web básico, el control web completo ofrece las siguientes ventajas adicionales, según el dispositivo utilizado:

- Más de 50 categorías para clasificar los diferentes sitios web.
- Diferentes políticas según horario.
- Excepciones por usuario o grupo.
- Los registros e informes detallados están disponibles en Dispositivo web, Dispositivo de gestión y los dispositivos de UTM.
- La función LiveConnect permite la distribución de políticas y realizar el registro incluso cuando los usuarios no se conectan desde la red de la empresa.
- Permite la solicitud de acceso a sitios web por parte del usuario.
- Puede utilizar páginas de notificación personalizadas con su propio texto y logotipo. Para más información, consulte la documentación de Sophos Web Appliance.
- La función SafeSearch evita el acceso a sitios web no deseados desde motores de búsqueda.

Para más información sobre las opciones del control web de Dispositivo web, consulte la documentación de Sophos Web Appliance en http://wsa.sophos.com/docs/wsa/.

La documentación de los dispositivos de UTM está disponible en http://www.sophos.com/es-es/support/documentation/sophos-utm.aspx.

Activar el control web completo

Nota
En el procedimiento siguiente se da por hecho que tiene un dispositivo Sophos Web Appliance, Sophos Management Appliance o Sophos UTM (versión 9.2 o posterior) configurado y en pleno funcionamiento, y que utiliza Endpoint Web Control.

Por defecto, el control web se encuentra desactivado. Realice los siguientes pasos para activar la política de control web completo.

Nota
Si utiliza administración delegada:

- Para modificar las políticas de control web, es necesario contar con el permiso **Configuración de políticas: control web**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para activar el control web completo:

1. Compruebe qué política web usa el grupo de ordenadores que desea configurar. Para obtener más información, consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control web**. A continuación, haga doble clic en la política que desee modificar.
   Aparece el cuadro de diálogo **Política de control web**.
3. En la ficha **General**, seleccione la opción **Activar el control web**.
4. Seleccione **Control web completo**.
5. En el panel **Configuración**, introduzca el **Nombre del dispositivo** y la **Clave de seguridad para el intercambio de políticas**.
   - Para un Dispositivo web o Dispositivo de gestión, es necesario proporcionar el nombre de host completo. La clave de seguridad debe coincidir con la que aparece en la página de **Endpoint Web Control** del dispositivo.
   - Para UTM, introduzca el nombre del host y la clave compartida del agente de Sophos LiveConnect utilizado por UTM. Estos datos aparecen en la ficha **Endpoint Protection** > **Computer Management** > **Advanced**, en la sección **Sophos LiveConnect – Registration** de **SEC Information** de la interfaz de administración de UTM WebAdmin.

   Para obtener más información, consulte la documentación de Sophos Web Appliance disponible en http://wsa.sophos.com/docs/wsa/ o la documentación de los dispositivos de UTM disponible en http://www.sophos.com/es-es/support/documentation/sophos-utm.aspx.
6. Si lo desea, active la opción **Bloquear si no se puede determinar la categoría del sitio web**. Si no es posible obtener datos de categorización de sitios web, se bloqueará la navegación hasta que se restablezca el servicio.
   Por defecto, esta opción no se encuentra activada.
7. Haga clic en **Aceptar**.
   Enterprise Console reconfigura las estaciones para que se comuniquen con los dispositivos Dispositivo web o Dispositivo de gestión, o el agente de Sophos LiveConnect utilizado por UTM.

7.9 Política de prevención de vulnerabilidades

Nota
Esta función no se incluye en todas las licencias. Si desea utilizarla, deberá incorporarla a su licencia. Para más información, consulte http://www.sophos.com/es-es/products/complete/comparison.aspx.

La prevención de vulnerabilidades le permite:

- Proteger archivos de documentos de ransomware (CryptoGuard).
- Protegerse contra ataques al sector de arranque (WipeGuard).

  Importante
  En este momento, esta función no se encuentra disponible para servidores.

- Proteger funciones críticas en navegadores web (Navegación segura).
- Mitigar vulnerabilidades. Esta opción protege las aplicaciones más vulnerables a la explotación por parte de programas maliciosos, como las aplicaciones Java.
- Protegerse contra ataques de vaciado de procesos.
- Protegerse contra la carga de archivos .DLL por parte de carpetas que no son de confianza.

- Protegerse contra el seguimiento de bifurcaciones de procesador.

Por defecto, la prevención de vulnerabilidades y todas las opciones de prevención de vulnerabilidades están activadas.

Importante
Si actualiza su licencia para que incluya la prevención de vulnerabilidades, no se instala automáticamente en los equipos que ya gestiona. Necesita volver a proteger los equipos para instalarla. Consulte Proteger ordenadores de forma automática (página 43).

Puede excluir aplicaciones de la prevención de vulnerabilidades. Tenga en cuenta que seguirán protegidas por CryptoGuard y Navegación segura.

Para obtener más información sobre la configuración recomendada para la prevención de vulnerabilidades, consulte la Guía de configuración de políticas de Sophos Enterprise Console.

Nota
Si utiliza administración delegada:

- Para configurar una política de prevención de vulnerabilidades, es necesario contar con el permiso **Configuración de políticas: prevención de vulnerabilidades**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

HitmanPro.Alert y actualizaciones de políticas

HitmanPro.Alert detecta aplicaciones en estaciones de trabajo que necesitan protección. Informa de la aplicación detectada al servidor de Sophos Enterprise Console. El servidor recopila las aplicaciones que requieren protección y, cada 120 minutos, combina los nuevos datos de aplicaciones en la política. El servidor distribuye la política actualizada a las estaciones de trabajo y proporciona la lista de aplicaciones que deben protegerse.

7.9.1 Activar o desactivar la prevención de vulnerabilidades

Si utiliza administración delegada:

- Para configurar una política de prevención de vulnerabilidades, es necesario contar con el permiso **Configuración de políticas: prevención de vulnerabilidades**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Nota
Por defecto, la prevención de vulnerabilidades y todas las opciones de prevención de vulnerabilidades están activadas.

Para activar o desactivar la prevención de vulnerabilidades:

1. Compruebe qué política de prevención de vulnerabilidades usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).

2. En el panel **Políticas**, haga doble clic en **Prevención de vulnerabilidades**. A continuación, haga doble clic en la política que desee modificar.
3. En la ficha **Configuración de protección** del cuadro de diálogo **Política de prevención de vulnerabilidades**, marque o desmarque la casilla **Activar prevención de vulnerabilidades**.
4. Marque o desmarque la casilla **Proteger archivos de documentos de ransomware (CryptoGuard)**.

   También puede optar por proteger contra ransomware ejecutado remotamente (solo estaciones de trabajo de 64 bits).
5. Marque o desmarque la casilla **Protección del registro de arranque y disco (WipeGuard)**.
6. Marque o desmarque la casilla **Proteger funciones críticas en navegadores web (Navegación segura)**.
7. Marque o desmarque la casilla **Mitigar vulnerabilidades en aplicaciones vulnerables**.

   También puede elegir los tipos de aplicaciones que desea proteger contra la explotación de vulnerabilidades, por ejemplo, aplicaciones de Microsoft Office.
8. Marque o desmarque la casilla **Impedir ataques de vaciado de procesos**
9. Marque o desmarque la casilla **Impedir que se carguen archivos DLL de carpetas de no confianza**.
10. Marque o desmarque la casilla **Seguimiento de bifurcaciones de CPU**
11. Haga clic en **Aceptar**.

Puede excluir aplicaciones de la prevención de vulnerabilidades. Tenga en cuenta que seguirán protegidas por CryptoGuard y Navegación segura, si se seleccionan estas opciones. Consulte Excluir aplicaciones de la prevención de vulnerabilidades (página 174).

También puede excluir eventos de vulnerabilidad de la prevención de vulnerabilidades. Consulte Excluir eventos de vulnerabilidad de la prevención de vulnerabilidades (página 175).

7.9.2 Excluir aplicaciones de la prevención de vulnerabilidades

Si utiliza administración delegada:

- Para configurar una política de prevención de vulnerabilidades, es necesario contar con el permiso **Configuración de políticas: prevención de vulnerabilidades**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Importante
Las aplicaciones vulnerables están protegidas por defecto. Debe tener cuidado al excluir aplicaciones de la prevención de vulnerabilidades. Seguirán protegidas por CryptoGuard y Navegación segura. Consulte Activar o desactivar la prevención de vulnerabilidades (página 173).

Puede excluir aplicaciones de la prevención de vulnerabilidades. También puede proteger aplicaciones excluidas previamente.

Para excluir aplicaciones:

1. Compruebe qué política de prevención de vulnerabilidades usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Prevención de vulnerabilidades**. A continuación, haga doble clic en la política que desee modificar.

3. En la ficha **Exclusiones de aplicaciones** del cuadro de diálogo **Política de prevención de vulnerabilidades**, seleccione las aplicaciones que desee excluir en la lista **Aplicaciones protegidas** y haga clic en **Excluir**.
   Las aplicaciones seleccionadas se moverán a la lista **Aplicaciones excluidas**.
4. Para proteger aplicaciones que actualmente están excluidas de la verificación, vaya a la lista **Aplicaciones excluidas**, seleccione las aplicaciones y haga clic en **Incluir**.
5. Haga clic en **Aceptar**.

7.9.3 Excluir eventos de vulnerabilidad de la prevención de vulnerabilidades

Si utiliza administración delegada:

- Para configurar una política de prevención de vulnerabilidades, es necesario contar con el permiso **Configuración de políticas: prevención de vulnerabilidades**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Importante

- Cuando se excluye un evento de vulnerabilidad, solo se excluirá la vulnerabilidad concreta, no toda la aplicación.
- Si un evento de vulnerabilidad forma parte de una aplicación que ya se ha excluido, no es necesario excluirlo.

Puede excluir eventos de vulnerabilidad de la prevención de vulnerabilidades. También puede proteger eventos de vulnerabilidad excluidos previamente.

Para excluir eventos de vulnerabilidad:

1. Compruebe qué política de prevención de vulnerabilidades usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Prevención de vulnerabilidades**. A continuación, haga doble clic en la política que desee modificar.
3. En la ficha **Exclusiones de vulnerabilidades** del cuadro de diálogo **Política de prevención de vulnerabilidades**, seleccione los eventos de vulnerabilidad que desee excluir en la lista **Eventos de vulnerabilidad detectados** y haga clic en **Excluir**.
   Los eventos de vulnerabilidad seleccionados se moverán a la lista **Eventos de vulnerabilidad excluidos**.
4. Para proteger eventos de vulnerabilidad que actualmente están excluidos de la verificación, vaya a la lista **Eventos de vulnerabilidad excluidos**, seleccione los eventos y haga clic en **Incluir**.
5. Haga clic en **Aceptar**.

8 Configurar los mensajes de alerta

Enterprise Console utiliza diferentes tipos de notificaciones.

- **Notificaciones mostradas en la consola**

  Si aparece un elemento con problemas en un ordenador o se produce un error, Sophos Endpoint Security and Control envía un aviso a Enterprise Console. La notificación aparece en la lista de ordenadores. Para más información sobre dichas alertas, consulte Alertas sobre elementos detectados (página 48).

  Estas notificaciones se muestran siempre. No es necesario que las configure.

- **Eventos mostrados en la consola**

  Cuando se produce un evento de restricción de aplicaciones, control de parches, control web, control de datos o dispositivos, del cortafuegos o de la protección contra manipulaciones en una estación, por ejemplo, cuando el cortafuegos bloquea una aplicación, el evento se envía a Enterprise Console y se puede ver en el visualizador de eventos correspondiente.

- **Alertas y mensajes enviados desde la consola a destinatarios seleccionados**

  Por defecto, cuando se encuentra un elemento en un ordenador, aparece un mensaje en el escritorio de dicho ordenador y se añade una entrada en el registro de eventos de Windows. Cuando se produce un evento de la restricción de aplicaciones, o del control de datos o dispositivos, aparece un mensaje en el escritorio del equipo.

  Nota
  Los mensajes de escritorio definidos por el usuario opcionales no se muestran en ordenadores que ejecutan Windows 8 o posterior.

  También se pueden configurar alertas por email o mensajes SNMP para el administrador.

  Nota
  Si desea utilizar mensajes SMTP autenticados, consulte el artículo 113780 de la base de conocimiento de Sophos.

En esta sección, se explica cómo configurar las notificaciones que se enviarán a los destinatarios seleccionados.

8.1 Configurar alertas de suscripciones

Si utiliza administración delegada, necesitará el permiso **Configuración del sistema** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Enterprise Console muestra las alertas creadas por el gestor de actualización en la columna **Alertas** de la vista **Gestores de actualización**. Si está suscrito a una versión fija del software, aparecerá una alerta cuando la versión esté a punto de retirarse o se haya retirado. También se mostrará una alerta si cambia de licencia.

Si está suscrito a una versión fija y seleccionó la opción **Actualizar las versiones fijas obsoletas con la más antigua disponible**, la suscripción se actualizará de forma automática.

Si las suscripciones no se actualizan automáticamente, recibirá instrucciones para que cambie la suscripción.

Importante
El uso de software obsoleto no le protegerá contra nuevas amenazas de seguridad. Se recomienda actualizar los productos con las versiones más reciente lo antes posible.

También puede configurar el envío de alertas por email a los destinatarios seleccionados cuando la versión del producto al que están suscritos esté a punto de retirarse o se haya retirado.

1. En el menú **Herramientas**, seleccione **Configurar alertas por email**.
   Aparece el cuadro de diálogo **Configuración de alertas por email**.
2. Si no se han configurado las opciones de SMTP, o si desea verlas o cambiarlas, haga clic en **Configurar**.
   En el cuadro de diálogo **Configuración de correo SMTP**, seleccione las opciones correspondientes según se describe a continuación:
   a) En el cuadro de texto **Servidor**, escriba el nombre o la dirección IP del servidor de SMTP.
   b) En el cuadro de texto **Remitente**, escriba una dirección de email a la que se puedan enviar los mensajes devueltos o no entregados.
   c) Haga clic en **Probar** para verificar la conexión.
3. En el panel **Destinatarios**, haga clic en **Añadir**.
   Aparece el cuadro de diálogo **Añadir nuevo destinatario**.
4. En el campo **Email**, escriba la dirección del destinatario.
5. En el cuadro de lista desplegable **Idioma**, seleccione el idioma en el que se enviarán las alertas.
6. En el panel **Suscripciones**, seleccione las alertas por email que desea que se envíen a este destinatario. Es posible suscribirse a tres tipos de alertas:
   - La suscripción del software incluye una versión de algún producto que Sophos está a punto de retirar.
   - Alguna suscripción de software incluye algún producto que ya no está disponible.
     Esta alerta avisa de que algún producto al que está suscrito ha sido retirado o, debido a un cambio de licencia, ya no puede utilizarlo.
   - Cambios en la licencia de Sophos. Avisa de cambios en las características de los productos.

8.2 Alertas por email sobre antivirus y HIPS

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

El usuario puede recibir una notificación por email si se encuentra un virus, comportamientos sospechosos, una aplicación no deseada o algún problema en alguno de los ordenadores de un grupo.

Importante
Los ordenadores Mac OS X sólo pueden enviar alertas por email a una dirección electrónica.

1. En el panel **Políticas**, haga doble clic sobre la política antivirus y HIPS que desea modificar.
2. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Notificación**.
3. En el cuadro de diálogo **Notificación**, abra la ficha **Alerta por email** y seleccione **Activar alerta por email**.
4. En el panel **Notificar**, seleccione los eventos de los que desea que se envíen alertas.

   Nota
   Las opciones **Detección de comportamiento sospechoso**, **Detección de archivos sospechosos**, **Detección y limpieza de adware/PUA** y **Otros errores** sólo se aplican a estaciones Windows.

5. En el panel **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.

   Importante
   Desde ordenadores Mac OS X sólo se enviarán los mensajes al primer destinatario.

6. Haga clic en **Configurar correo SMTP** para cambiar la dirección de su servidor de correo SMTP y el idioma de las alertas.
7. En el cuadro de diálogo **Configuración de correo SMTP**, seleccione las opciones correspondientes según se describe a continuación:
   - En el cuadro de texto **Servidor SMTP**, escriba el nombre o la dirección IP del servidor de SMTP. Haga clic en **Probar** para enviar un mensaje de prueba.
   - En el cuadro de texto **Dirección remitente**, escriba una dirección de email a la que se puedan enviar los mensajes devueltos o no entregados.
   - En el cuadro de texto **Dirección de respuesta**, puede introducir una dirección de correo a la que se puedan enviar las respuestas a las alertas. Las alertas se envían desde un buzón desatendido.
   - En el panel **Idioma**, abra la lista desplegable y seleccione el idioma en el que desea que se envíen las alertas.

8.3 Alertas SNMP sobre antivirus y HIPS

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Es posible enviar mensajes SNMP si se encuentra un virus o algún problema en alguno de los ordenadores de un grupo.

Nota
Estas opciones sólo son compatibles con Windows.

1. En el panel **Políticas**, haga doble clic sobre la política antivirus y HIPS que desea modificar.
2. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Notificación**.
3. En el cuadro de diálogo **Notificación**, vaya a la ficha **Mensaje SNMP** y seleccione **Activar mensaje SNMP**.
4. En el panel **Notificar**, seleccione los tipos de eventos que desea que Sophos Endpoint Security and Control notifique mediante SNMP.
5. En el cuadro de texto **Destino SNMP**, escriba la dirección IP del destinatario.
6. En el cuadro de texto **Nombre de la comunidad SNMP**, escriba el nombre de la comunidad SNMP.

8.4 Alertas de escritorio sobre antivirus y HIPS

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, se mostrarán mensajes de escritorio en el ordenador en el que se ha detectado un virus, un elemento sospechoso o una aplicación no deseada. Estas notificaciones se pueden configurar.

1. En el panel **Políticas**, haga doble clic sobre la política antivirus y HIPS que desea modificar.
2. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Notificación**.
3. En el cuadro de diálogo **Notificación**, abra la ficha **Mensaje de escritorio**.
   Por defecto, **Activar mensaje de escritorio** y todas estas opciones del panel **Notificar** están seleccionadas. Si es necesario, modifique esta configuración.

   Nota
   Las opciones **Detección de comportamiento sospechoso**, **Detección de archivos sospechosos** y **Detección de adware/PUA** sólo se aplican a estaciones Windows.

4. En el cuadro **Mensaje personalizado**, puede escribir un mensaje que se añada al final del mensaje estándar para el usuario.

   Nota
   Los mensajes de escritorio definidos por el usuario no se muestran en ordenadores que ejecutan Windows 8 o posterior.

8.5 Alertas y mensajes de aplicaciones restringidas

Si utiliza administración delegada:

- Para configurar una política de restricción de aplicaciones, es necesario contar con el permiso **Configuración de políticas: restricción de aplicaciones**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Podrá recibir alertas cuando se detecten aplicaciones restringidas en la red.

1. En el panel **Políticas**, haga doble clic sobre la política de restricción de aplicaciones que desea modificar.
2. En el cuadro de diálogo **Política de restricción de aplicaciones**, abra la ficha **Notificación**.

   En el panel **Notificación**, la opción **Activar mensaje de escritorio** está activada por defecto. Permite informar al usuario mediante un mensaje de escritorio de la detección (y consiguiente bloqueo) de una aplicación restringida.
3. En el cuadro **Mensaje**, indique las instrucciones para el usuario.

   Nota
   Los mensajes de escritorio definidos por el usuario no se muestran en ordenadores que ejecutan Windows 8 o posterior.

4. Si desea enviar alertas sobre las aplicaciones restringidas detectadas, active la opción **Activar alerta por email**.
5. Active la opción **Activar mensaje SNMP** si desea enviar mensajes SNMP.

   Nota
   La política antivirus y HIPS determina los destinatarios de email y mensajes SNMP, y otras opciones de notificación. Para obtener más información, consulte Alertas SNMP sobre antivirus y HIPS (página 178).

8.6 Alertas y mensajes del control de datos

Si utiliza administración delegada:

- Para configurar las políticas de control de datos, es necesario contar con el permiso **Configuración de políticas: control de datos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Enterprise Console utiliza eventos y mensajes para informar sobre las detecciones y bloqueos de transferencias de datos delicados.

Para más información sobre cómo visualizar los eventos del control de dispositivos, consulte Política de control de datos (página 138).

Cuando el control de datos está activado, se registran o muestran por defecto estos eventos y mensajes:

- Los eventos del control de datos se registran en la estación.
- Los eventos del control de datos se envían a Enterprise Console y se pueden visualizar en el **Visualizador de eventos del control de datos**. (Para abrir el visualizador de eventos, en el menú **Eventos**, haga clic en **Eventos del control de datos**.)

Nota
Las estaciones pueden enviar a Enterprise Console un máximo de 50 eventos del control de datos por hora.

- El número de equipos con eventos del control de datos que superen un umbral determinado en los últimos 7 días aparece en el Panel de control.
- Los mensajes del escritorio se muestran en la estación.

También puede configurar Enterprise Console para enviar mensajes como:

Alertas por email	Se envía un mensaje de correo electrónico a los destinatarios especificados.
Mensajes SNMP	A los destinatarios indicados en la política antivirus y HIPS.

Para configurar los mensajes del control de datos:

1. Compruebe qué política de control de datos usa el grupo de ordenadores que desea configurar.
   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de datos**. A continuación, haga doble clic en la política que desee modificar.
   Aparecerá el cuadro de diálogo **Política de control de datos**.
3. En el cuadro de diálogo **Política de control de datos**, abra la ficha **Notificación**. Los mensajes de escritorio están activados por defecto y la opción **Incluir en el mensaje las reglas que se incumplen** activada.
4. Escriba mensajes que se añadirán a los mensajes estándar para que el usuario confirme la transferencia de los archivos o el bloqueo, si lo desea.
   Puede utilizar un máximo de 100 caracteres. El mensaje puede incluir enlaces HTML, por ejemplo, Acerca de Sophos.

   Nota
   Los mensajes de escritorio definidos por el usuario no se muestran en ordenadores que ejecutan Windows 8 o posterior.

5. Para activar las alertas, seleccione la opción **Activar alerta por email**. En el campo **Destinatarios**, escriba las direcciones de correo electrónico de los destinatarios. Utilice ; para separar las direcciones.
6. Para activar los mensajes SNMP, active la opción **Activar mensaje SNMP**.
   El servidor de email y el destino SNMP se configuran en la política antivirus y HIPS.

8.7 Alertas y mensajes del control de dispositivos

Si utiliza administración delegada:

- Para modificar las políticas de control de dispositivos, es necesario contar con el permiso **Configuración de políticas: control de dispositivos**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Enterprise Console utiliza eventos y mensajes para avisar cuando se ha detectado o bloqueado un dispositivo controlado.

Para más información sobre las políticas y eventos del control de dispositivos, consulte Política de control de dispositivos (página 153).

Cuando el control de dispositivos está activado, se registran o muestran por defecto estos eventos y mensajes:

- Los eventos del control de dispositivos se registran en la estación.
- Los eventos del control de dispositivos se envían a Enterprise Console y se pueden visualizar en el **Visualizador de eventos del control de dispositivos**. (Para abrir el visualizador de eventos, en el menú **Eventos**, haga clic en **Eventos del control de dispositivos**.)
- El número de equipos con eventos del control de dispositivos que superen un umbral determinado en los últimos 7 días aparece en el Panel de control.
- Los mensajes del escritorio se muestran en la estación.

También puede configurar Enterprise Console para enviar mensajes como:

Alertas por email	Se envía un mensaje de correo electrónico a los destinatarios especificados.
Mensajes SNMP	A los destinatarios indicados en la política antivirus y HIPS.

Para configurar los mensajes del control de dispositivos:

1. Compruebe qué política de control de dispositivos usa el grupo de ordenadores que desea configurar.

   Consulte Comprobar qué políticas usa un grupo (página 25).
2. En el panel **Políticas**, haga doble clic en **Control de dispositivos**. A continuación, haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política de control de dispositivos**, en la ficha **Notificación**, los mensajes de escritorio están activados por defecto. Si lo desea, puede configurar otras opciones de los mensajes:

   - *Para introducir texto en el mensaje de escritorio*, en el cuadro de texto **Mensaje**, escriba un mensaje que se añadirá al texto estándar.

     Puede utilizar un máximo de 100 caracteres. El mensaje puede incluir enlaces HTML, por ejemplo, Acerca de Sophos.

     Nota
     Los mensajes de escritorio definidos por el usuario no se muestran en ordenadores que ejecutan Windows 8 o posterior.

   - *Para activar las alertas*, seleccione la opción **Activar alerta por email**. En el campo **Destinatarios**, escriba las direcciones de correo electrónico de los destinatarios. Utilice ; para separar las direcciones.
   - *Para activar los mensajes SNMP*, active la opción **Activar mensaje SNMP**.

   El servidor de email y el destino SNMP se configuran en la política antivirus y HIPS.

8.8 Alertas por email sobre el estado de la red

Si utiliza administración delegada, necesitará el permiso **Configuración del sistema** para configurar las alertas sobre el estado de la red. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Podrá disponer de alertas por email para las situaciones en las que se supere el umbral de aviso o crítico en los elementos del panel de control de la consola.

1. En el menú **Herramientas**, seleccione **Configurar alertas por email**.
   Aparece el cuadro de diálogo **Configuración de alertas por email**.
2. Si no se han configurado las opciones de SMTP, o si desea verlas o cambiarlas, haga clic en **Configurar**. En el cuadro de diálogo **Configuración de correo SMTP**, seleccione las opciones correspondientes según se describe a continuación:
   a) En el cuadro de texto **Servidor**, escriba el nombre o la dirección IP del servidor de SMTP.
   b) En el cuadro de texto **Remitente**, escriba una dirección de email a la que se puedan enviar los mensajes devueltos o no entregados.
   c) Haga clic en **Probar** para verificar la conexión.
3. En el panel **Destinatarios**, haga clic en **Añadir**.
   Aparece el cuadro de diálogo **Añadir nuevo destinatario**.
4. En el campo **Email**, escriba la dirección del destinatario.
5. En el cuadro de lista desplegable **Idioma**, seleccione el idioma en el que se enviarán las alertas.
6. En el panel **Suscripciones**, seleccione los eventos que se notificarán dentro de las secciones "Superado el umbral de aviso" y "Superado el umbral crítico".

8.9 Alertas por email sobre la sincronización con Active Directory

Si utiliza administración delegada, necesitará el permiso **Configuración del sistema** para configurar las alertas de sincronización de Active Directory. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, también puede recibir notificación por email de los nuevos ordenadores y grupos en cada sincronización. Si activa la protección automática de nuevos ordenadores sincronizados, también puede recibir notificación ante fallos de protección.

1. En el menú **Herramientas**, seleccione **Configurar alertas por email**.
   Aparece el cuadro de diálogo **Configuración de alertas por email**.
2. Si no se han configurado las opciones de SMTP, o si desea verlas o cambiarlas, haga clic en **Configurar**.
   En el cuadro de diálogo **Configuración de correo SMTP**, seleccione las opciones correspondientes según se describe a continuación:
   a) En el cuadro de texto **Servidor**, escriba el nombre o la dirección IP del servidor de SMTP.
   b) En el cuadro de texto **Remitente**, escriba una dirección de email a la que se puedan enviar los mensajes devueltos o no entregados.
   c) Haga clic en **Probar** para verificar la conexión.
3. En el panel **Destinatarios**, haga clic en **Añadir**.
   Aparece el cuadro de diálogo **Añadir nuevo destinatario**.

4. En el campo **Email**, escriba la dirección del destinatario.
5. En el cuadro de lista desplegable **Idioma**, seleccione el idioma en el que se enviarán las alertas.
6. En el panel **Suscripciones**, seleccione los eventos que se notificarán dentro de las secciones "Sincronización con Active Directory".

   Notificaciones por email de "Sincronización con Active Directory":

   - Encontrados nuevos grupos
   - Encontrados nuevos ordenadores
   - Fallo en la protección automática de ordenadores

8.10 Configurar el registro de eventos de Windows

Si utiliza administración delegada:

- Para realizar esta tarea, es necesario contar con el permiso **Configuración de políticas: antivirus y HIPS**.
- No es posible modificar las políticas aplicadas fuera del subentorno activo.

Para obtener más información, consulte Administrar roles y subentornos (página 13).

Por defecto, Sophos Endpoint Security and Control añade alertas al registro de eventos de Windows cuando se detectan o se limpian virus, programas espía, adware o PUA, y cuando se detectan comportamientos o archivos sospechosos.

Para modificar estas opciones:

1. En el panel **Políticas**, haga doble clic sobre la política antivirus y HIPS que desea modificar.
2. En el cuadro de diálogo **Política antivirus y HIPS**, haga clic en **Notificación**.
3. En el cuadro de diálogo **Notificación**, abra la ficha **Registro de eventos**.

   Por defecto, el registro de eventos está activado. Modifique la configuración según sea necesario.

   Errores de escaneado incluye ocasiones en que Sophos Endpoint Security and Control no tiene acceso a algún elemento que intenta escanear.

8.11 Activar o desactivar la comunicación con Sophos

Si utiliza administración delegada, necesitará el permiso **Configuración del sistema** para activar o desactivar la comunicación con Sophos. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Enterprise Console enviará informes periódicamente a Sophos. Estos informes ayudarán a Sophos a comprender cómo se usan sus productos y a mejorar nuestros productos y servicios. Para obtener más información sobre el tipo de información recopilada y cómo se procesa, consulte el Acuerdo de Licencia de Usuario Final de Sophos (EULA) y la política de privacidad de Sophos que encontrará aquí: http://esp.sophos.com/legal.

Alguna de la información enviada es opcional y otra es obligatoria, según se describe en el EULA y la política de privacidad. Puede excluirse del envío de información opcional en cualquier momento modificando la configuración de **Comunicación con Sophos**.

Por defecto, la comunicación con Sophos está activada. Al instalar o actualizar la consola, puede desactivar esta opción en el asistente para la instalación de Sophos Enterprise Console.

Posteriormente, podrá activar la comunicación con Sophos de la siguiente manera:

1. En el menú **Herramientas**, haga clic en **Comunicación con Sophos**.
2. En el cuadro de diálogo **Comunicación con Sophos**, puede activar o desactivar esta opción.
   - *Si desea activar la comunicación con Sophos,* lea el acuerdo y seleccione la casilla **Sí, acepto** si está de acuerdo con las condiciones.
   - *Si desea desactivar la comunicación con Sophos,* desactive la casilla **Sí, acepto**.

9 Visualizar eventos

Cuando se produce un evento de control de aplicaciones, control de datos, control de dispositivos, firewall, evaluación de parches, protección contra manipulaciones, control web o prevención de vulnerabilidades en una estación de trabajo, por ejemplo, cuando el firewall bloquea una aplicación, el evento se envía a Enterprise Console y se puede ver en el visualizador de eventos correspondiente.

Utilice los visualizadores de eventos para investigar los eventos ocurridos en la red. También es posible generar una lista de eventos basados en un filtro configurado, por ejemplo, una lista de todos los eventos de control de datos en la última semana generados por un usuario concreto.

El número de equipos con eventos que superen un umbral determinado durante la última semana aparece en el Panel de control (excepto en el caso de eventos de la protección contra manipulaciones). Para más información sobre cómo configurar el umbral, consulte Configuración del panel de control (página 45).

También puede configurar alertas que se envíen a determinados destinatarios cuando se produzca un evento. Para obtener más información, consulte Administrar roles y subentornos (página 13).

9.1 Visualizar eventos de la restricción de aplicaciones

Para visualizar eventos de la restricción de aplicaciones:

1. En el menú **Eventos**, haga clic en **Eventos de la restricción de aplicaciones**.
   Aparece el cuadro de diálogo **Visualizador de eventos de la restricción de aplicaciones**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea ver los eventos de un usuario o equipo determinados, introduzca el nombre en el campo correspondiente.

   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios y equipos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
4. Si desea visualizar eventos de un tipo de aplicación determinado, en el campo **Tipo de aplicación**, abra la lista desplegable y seleccione el tipo de aplicación.

   Por defecto, el visualizador de eventos muestra eventos de todos los tipos de aplicaciones.
5. Haga clic en **Buscar** para mostrar la lista de eventos.

Si lo desea, puede exportar la lista de eventos de la restricción de aplicaciones a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.2 Visualizar eventos del control de datos

Nota
Esta función no está disponible si su licencia no incluye Control de datos.

Si utiliza administración delegada, necesitará el permiso **Eventos del control de datos** para ver los eventos del control de datos en Enterprise Console. Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para visualizar eventos del control de datos:

1. En el menú **Eventos**, haga clic en **Eventos del control de datos**.
   Aparece el cuadro de diálogo **Visualizador de eventos del control de datos**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea ver los eventos de un usuario, equipo o archivo determinados, introduzca el nombre en el campo correspondiente.

   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios, equipos y archivos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
4. Si desea ver los eventos de una regla determinada, en el campo **Regla**, abra la lista desplegable y seleccione el nombre de la regla.

   Por defecto, el visualizador de eventos muestra eventos de todas las reglas.
5. Si desea visualizar eventos de un tipo de archivos determinado, en el campo **Tipo de archivo**, abra la lista desplegable y seleccione el tipo de archivo.

   Por defecto, el visualizador de eventos muestra eventos de todos los tipos de archivos.
6. Haga clic en **Buscar** para mostrar la lista de eventos.

Si lo desea, puede exportar la lista de eventos del control de datos a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.3 Visualizar eventos del control de dispositivos

Para visualizar eventos del control de dispositivos:

1. En el menú **Eventos**, haga clic en **Eventos del control de dispositivos**.
   Aparece el cuadro de diálogo **Visualizador de eventos del control de dispositivos**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea visualizar eventos de un tipo de dispositivos determinado, en el campo **Tipo de dispositivo**, abra la lista desplegable y seleccione el tipo de dispositivo.

   Por defecto, el visualizador de eventos muestra eventos de todos los tipos de dispositivos.

Nota
Si define unidades ópticas como de "Sólo lectura", los eventos de estos dispositivos no se verán en el Visualizador de eventos.

4. Si desea ver los eventos de un usuario o equipo determinados, introduzca el nombre en el campo correspondiente.

   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios y equipos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
5. Haga clic en **Buscar** para mostrar la lista de eventos.

En el cuadro de diálogo **Visualizador de eventos del control de dispositivos**, puede excluir dispositivos de las políticas de control. Para más información, vea Excluir un dispositivo de todas las políticas (página 157).

Si lo desea, puede exportar la lista de eventos del control de dispositivos a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.4 Visualizar eventos del cortafuegos

Los eventos del cortafuegos sólo se envían una vez desde las estaciones a la consola. Los eventos del mismo tipo desde diferentes estaciones se agrupan en el **Visualizador de eventos del cortafuegos**. En la columna **Número** se indica la cantidad de eventos generadas desde diferentes estaciones.

Para ver eventos del cortafuegos:

1. En el menú **Eventos**, haga clic en **Eventos del cortafuegos**.
   Aparece el cuadro de diálogo **Visualizador de eventos del cortafuegos**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea visualizar eventos de un tipo determinado, en el campo **Tipo de evento**, abra la lista desplegable y seleccione el tipo.

   Por defecto, el visualizador de eventos muestra todos los tipos.
4. Si desea visualizar eventos de un archivo determinado, en el campo **Nombre del archivo**, escriba el nombre del archivo.

   Si deja el campo en blanco, se mostrarán los eventos de todos los archivos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
5. Haga clic en **Buscar** para mostrar la lista de eventos.

En el cuadro de diálogo **Visualizador de eventos del cortafuegos**, puede crear una regla del cortafuegos, como se describe en Crear reglas de eventos del cortafuegos (página 111).

Si lo desea, puede exportar la lista de eventos del cortafuegos a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.5 Visualizar eventos de la protección contra manipulaciones

Existen dos tipos de eventos de la protección contra manipulaciones:

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

Para visualizar eventos de la protección contra manipulaciones:

1. En el menú **Eventos**, haga clic en **Eventos de la protección contra manipulaciones**. Aparece el cuadro de diálogo **Visualizador de eventos de la protección contra manipulaciones**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea visualizar eventos de un tipo determinado, en el campo **Tipo de evento**, abra la lista desplegable y seleccione el tipo.

   Por defecto, el visualizador de eventos muestra eventos de todos los tipos.
4. Si desea ver los eventos de un usuario o equipo determinados, introduzca el nombre en el campo correspondiente.

   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios y equipos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
5. Haga clic en **Buscar** para mostrar la lista de eventos.

Si lo desea, puede exportar la lista de eventos a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.6 Eventos del control de parches

Nota
Esta función no está disponible si su licencia no incluye Control de parches.

El **Visualizador de eventos del control de parches** incluye información sobre los parches de seguridad y el resultado de la comprobación.

El campo **Estado de parches** muestra el estado de actualización de los parches. Los posibles valores son:

- **No disponible**, indica que no se ha descargado la información de parches o que no dispone de la licencia correspondiente para utilizar esta función.
- **Descargando** indica que se está realizando la descarga inicial tras la instalación.
- **Actualizado**, indica que la información de parches se encuentra actualizada.
- **Obsoleto,** indica que la información de parches no se ha actualizado en las últimas 72 horas. Esto puede ocurrir si existe algún problema de conexión de red. También se muestra si cambia a una

licencia que no incluya esta función. Este mensaje aparece incluso cuando se haya realizado una actualización parcial.

El **Visualizador de eventos del control de parches** incluye las siguientes fichas:

Parches

Esta ficha muestra los parches que no están instalados. Para cada parche se indica el número de ordenadores que no disponen de dicho parche y las amenazas relacionadas. Puede utilizar filtros para mostrar los parches según el número de ordenadores que no lo tienen instalado.

Ordenadores

Muestra el estado del control de parches por ordenador. Se mostrará cada parche que falte en cada estación. Los ordenadores a los que les falte más de un parche, aparecerán en más de una ocasión.

9.6.1 Visualizar eventos del control de parches

Para visualizar eventos del control de parches:

1. En el menú **Eventos**, seleccione **Eventos del control de parches**.
   Se abrirá el cuadro de diálogo **Visualizador de eventos del control de parches**.
2. Abra la ficha **Parches** u **Ordenadores**. Para obtener más información sobre las fichas, consulte Eventos del control de parches (página 189).
3. En el panel de búsqueda, si desea ver los eventos de un parche, equipo, amenaza o vulnerabilidad determinados, introduzca la información en el campo correspondiente. El criterio de búsqueda se ajusta a la ficha seleccionada.

   Si deja los campos vacíos, se mostrarán los eventos de todos los parches y equipos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
4. Para ajustar el resto de filtros, seleccione el valor correspondiente en cada cuadro de lista desplegable. El criterio de búsqueda se ajusta a la ficha seleccionada.

   Por defecto, se muestran los eventos sin filtrar.
5. Haga clic en **Buscar** para mostrar la lista de eventos del control de parches.
   Para más información sobre resultado de la búsqueda, consulte Categorías de búsqueda (página 191).

Puede hacer clic con el botón derecho del ratón en un enlace para copiar el nombre o utilizar la combinación de teclas Ctrl+C para copiar la fila del evento.

También puede exportar la lista de eventos del control de parches a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

Para ver información detallada, haga clic en el nombre del parche. Para obtener más información, consulte Ver detalles del parche, amenaza o vulnerabilidad (página 190).

9.6.2 Ver detalles del parche, amenaza o vulnerabilidad

Para ver detalles del parche, amenaza o vulnerabilidad:

1. En el menú **Eventos**, seleccione **Eventos del control de parches**.
   Se abrirá el cuadro de diálogo **Visualizador de eventos del control de parches**.

2. Abra la ficha **Parches** u **Ordenadores**, seleccione las opciones deseadas y haga clic en **Buscar**. Para más información sobre resultado de la búsqueda, consulte Categorías de búsqueda (página 191).
3. Haga clic en el nombre del parche para ver información detallada.
4. En el cuadro de diálogo **Detalles del parche** podrá ver información sobre el parche y las amenazas contra las que protege. Si lo desea:
   - Haga clic en el nombre del parche para acceder mediante su navegador web a la descripción del parche del propio fabricante.
   - Haga clic en el nombre de las amenazas para acceder mediante su navegador web a la descripción de la amenaza de Sophos.
   - Haga clic en el nombre de las vulnerabilidades para acceder mediante su navegador web a la descripción de la vulnerabilidad (CVE).
   - Haga clic en el nombre del parche en la columna **Antes corregido por** para ver en el navegador web información del fabricante sobre el parche al que sustituye.

La lista se muestra de forma alfabética por amenaza y por vulnerabilidad.

9.6.3 Categorías de búsqueda

El resultado de búsqueda se muestra por categorías:

- Parches (página 191)
- Ordenadores (página 192)

Parches

El resultado de la búsqueda se muestra según las siguientes categorías:

- **Amenazas**: Entre las amenazas se incluyen virus, troyanos, gusanos, programa espía, sitios web maliciosos, programas publicitarios y otras aplicaciones no deseadas. Haga clic en el nombre de la amenaza para ver el análisis detallado en la página web de Sophos.
- **Vulnerabilidades**: Agujeros de seguridad en el software que pueden facilitar ataques. El daño potencial de estos ataques dependen del tipo de vulnerabilidad y el software afectado. Los parches permiten tapar estos agujeros de seguridad. Haga clic en el nombre de la vulnerabilidad para ver el análisis detallado en la página web de Sophos.
- **Peligrosidad**: La peligrosidad la establece el laboratorio de Sophos.

  Nota
  Se recomienda aplicar los parches disponibles, independiente de la peligrosidad asociada.

  — **Crítica**: Es muy probable un ataque que aprovecha esta vulnerabilidad.
  — **Alta**: Es probable un ataque que aprovecha esta vulnerabilidad.
  — **Media**: Es posible un ataque que aprovecha esta vulnerabilidad.
  — **Baja**: Es improbable un ataque que aprovecha esta vulnerabilidad.
- **Nombre**: Muestra el nombre del parche. Haga clic en el nombre del parche para acceder mediante su navegador web a la descripción del parche del propio fabricante.
- **Fabricante**: Muestra el nombre del fabricante al que pertenece el parche.

- **Ordenadores**: Muestra el número de ordenadores afectados. Haga clic en el número para ver los detalles en la ficha **Ordenadores**. Si aparece "-", quiere decir que no se ha evaluado el parche.
- **Reemplazado por**: Muestra el nombre de parches de reemplazo. Haga clic en el nombre del parche si desea ver más información en el cuadro de diálogo **Detalles del parche**.
- **Fecha de edición**: Muestra la fecha de edición del parche.

Ordenadores

El resultado de la búsqueda se muestra según las siguientes categorías:

- **Ordenador**: Muestra los nombres de los ordenadores que no disponen del parche.
- **Peligrosidad**: La peligrosidad la establece el laboratorio de Sophos.

  Nota
  Se recomienda aplicar los parches disponibles, independiente de la peligrosidad asociada.

  — **Crítica**: Es muy probable un ataque que aprovecha esta vulnerabilidad.
  — **Alta**: Es probable un ataque que aprovecha esta vulnerabilidad.
  — **Media**: Es posible un ataque que aprovecha esta vulnerabilidad.
  — **Baja**: Es improbable un ataque que aprovecha esta vulnerabilidad.
- **Nombre**: Muestra el nombre del parche. Haga clic en el nombre del parche para acceder mediante su navegador web a la descripción del parche del propio fabricante.
- **Reemplazado por**: Muestra el nombre de parches de reemplazo. Haga clic en el nombre del parche si desea ver más información en el cuadro de diálogo **Detalles del parche**.
- **Última comprobación**: Muestra la fecha en la que se comprobaron los parches instalados.
- **Fabricante**: Muestra el nombre del fabricante al que pertenece el parche.
- **Fecha de edición**: Muestra la fecha de edición del parche.
- **Grupo**: Muestra el nombre del grupo al que pertenece el ordenador.

9.7 Visualizar eventos del control web

Nota
Esta función no está disponible si su licencia no incluye Control web.

Si utiliza administración delegada, necesitará el permiso **Eventos web** para ver los eventos web en Enterprise Console. Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

El Visualizador de eventos web le permitirá ver los siguientes tipos de eventos:

- Sitios web maliciosos bloqueados por la función de protección web en la política **Antivirus y HIPS**.
- Eventos del control web, si utiliza esta función.

Los eventos de control web dependen de la política web que utilice. Puede utilizar el Visualizador de eventos web para ambos, pero el contenido será diferente.

Si utiliza **Control de sitios web inapropiados**, podrá ver los eventos de «Bloqueo» y «Aviso». Los sitios web HTTPS bajo «aviso» se registran con la acción «proceder» (para más información consulte Control de sitios web inapropiados (página 166)).

Si utiliza **Control web completo**, los eventos se muestran en el dispositivo.

- Para monitorizar el acceso a Internet con Sophos Web Appliance o Management Appliance, puede utilizar las funciones **Informes** y **Búsqueda**. Se mostrarán todas las acciones. Los sitios web HTTPS bajo «aviso» se registran con la acción «proceder» (para más información consulte Control web completo (página 170)).
- Con UTM, utilice la página de informes del uso de Internet **Logging & Reporting** > **Web Protection** > **Web Usage Report**. En ella podrá ver, entre otros datos, los sitios web entregados al cliente o bloqueados por alguna regla de restricción de aplicaciones, o si algún usuario accedió a alguna página bloqueada utilizando la función de circunvalación del bloqueo.

Nota
Independientemente de la política seleccionada, los sitios web escaneados y evaluados con el filtrado activo de direcciones web de Sophos Endpoint Security and Control (Protección web (página 95)) se muestran como eventos en Enterprise Console.

Para ver eventos web:

1. En el menú **Eventos**, haga clic en **Eventos web**.
   Aparece el cuadro de diálogo **Visualizador de eventos del control web**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.
   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea ver los eventos de un **usuario** o **equipo** determinados, introduzca el nombre en el campo correspondiente.
   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios y equipos.
   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
4. Si desea visualizar eventos de un tipo de acción, en el campo **Acción**, abra la lista desplegable y seleccione el tipo.
5. Si desea visualizar eventos de algún dominio concreto, indíquelo en el campo **Dominio**.
6. Si desea visualizar eventos según la razón, selecciónelo en el cuadro de lista desplegable **Razón**.
7. Haga clic en **Buscar** para mostrar la lista de eventos.

Si lo desea, puede exportar la lista de eventos web a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).

9.7.1 Visualizar los eventos del control web más recientes

Puede ver los 10 eventos más recientes en las estaciones.

Para ver los eventos web más recientes:

1. En la vista **Estaciones**, en la lista de ordenadores, haga doble clic en el equipo del que desea ver los eventos.
2. En el cuadro de diálogo **Detalles del ordenador**, vaya a la sección **Eventos web más recientes**.

También puede generar un informe para ver el número de eventos web de un usuario determinado. Para obtener más información, consulte Configurar el informe de eventos por usuario (página 201).

9.8 Visualizar eventos de la prevención de vulnerabilidades

Nota
Esta función no está disponible si su licencia no incluye Prevención de vulnerabilidades.

Si utiliza la administración basada en roles, necesitará el permiso **Prevención de vulnerabilidades** para ver los eventos de prevención de vulnerabilidades en Enterprise Console. Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Para visualizar eventos de la prevención de vulnerabilidades:

1. En el menú **Eventos**, haga clic en **Prevención de vulnerabilidades**.
   Aparece el cuadro de diálogo **Prevención de vulnerabilidades - Visualizador de eventos**.
2. En el campo **Período de búsqueda**, abra la lista desplegable y seleccione el período de los eventos que desea ver.

   Puede seleccionar un período fijo, por ejemplo, **24 horas**, o seleccione **Personalizar** y especifique el período de tiempo que desee seleccionando las fechas de inicio y fin.
3. Si desea ver los eventos de un **usuario** o **equipo** determinados, introduzca el nombre en el campo correspondiente.

   Si deja los campos vacíos, se mostrarán los eventos de todos los usuarios y equipos.

   Puede utilizar caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres.
4. Si desea visualizar eventos asociados a un tipo determinado, en el campo **Tipo**, haga clic en la flecha desplegable y seleccione el tipo.
5. Haga clic en **Buscar** para mostrar la lista de eventos.

- Puede exportar la lista de eventos de la prevención de vulnerabilidades a un archivo. Para más información, vea Exportar la lista de eventos a un archivo (página 194).
- Puede excluir eventos de vulnerabilidad de la prevención de vulnerabilidades. Consulte Excluir eventos de la prevención de vulnerabilidades (página 195).

9.9 Exportar la lista de eventos a un archivo

Puede exportar la lista de eventos de control de aplicaciones, control de datos, control de dispositivos, firewall, evaluación de parches, protección contra manipulaciones, eventos web o prevención de vulnerabilidades en un archivo de valores separados por comas (CVS). También puede exportar la lista de eventos del control de parches en formato PDF.

1. En el menú **Eventos**, haga clic en una de las opciones de eventos, dependiendo de la lista de eventos que desee exportar.
   Aparece el cuadro de diálogo **Visualizador de eventos**.
2. Si sólo desea mostrar ciertos eventos, en el panel **Criterio de búsqueda**, configure los filtros que necesite y haga clic en **Buscar** para mostrar los eventos.

   Para más información, consulte:

- Visualizar eventos de la restricción de aplicaciones (página 186)
- Acerca de los eventos del control de datos (página 143)
- Acerca de los eventos del control de dispositivos (página 154)
- Visualizar eventos del cortafuegos (página 188)
- Eventos del control de parches (página 189)
- Visualizar eventos de la protección contra manipulaciones (página 189)
- Visualizar eventos del control web (página 192)
- Visualizar eventos de la prevención de vulnerabilidades (página 194)

3. Haga clic en **Exportar**.
4. En la ventana **Guardar como**, seleccione la ubicación, determine el tipo de archivo y escriba el nombre del archivo.
5. Haga clic en **Guardar**.

9.10 Excluir eventos de la prevención de vulnerabilidades

Para excluir aplicaciones y eventos de la prevención de vulnerabilidades, seleccione los eventos específicos del Visualizador de eventos.

1. En el menú **Eventos**, haga clic en **Eventos de prevención de vulnerabilidades**.
   Aparece el cuadro de diálogo **Visualizador de eventos**.
2. Si sólo desea mostrar ciertos eventos, en el panel **Criterio de búsqueda**, configure los filtros que necesite y haga clic en **Buscar** para mostrar los eventos.

   Para obtener más información, consulte Visualizar eventos de la prevención de vulnerabilidades (página 194).
3. Seleccione un evento y haga clic en **Excluir**.
   Aparece el cuadro de diálogo **Exclusiones de prevención de vulnerabilidades**.
4. Haga clic en la política que desee modificar. Para cambiar la configuración de todas las políticas, haga clic en **Seleccionar todo**.
5. En la sección **Evento de vulnerabilidad** o **Aplicación**, haga clic en **Excluir**
6. Haga clic en **Aceptar**.

El evento o aplicación se excluirá de la prevención de vulnerabilidades para las políticas seleccionadas.

10 Generar informes

Los informes ofrecen información en forma de tablas y gráficos sobre los diferentes aspectos de la seguridad en su red.

Los informes están disponibles mediante el **Gestor de informes**. Utilizando el **Gestor de informes**, es posible crear rápidamente un informe basado en una plantilla existente, cambiar la configuración de un informe existente y programar un informe para que se ejecute de forma regular y que los resultados se envíen a los destinatarios elegidos. También puede imprimir y exportar los informes en diferentes formatos.

Sophos proporciona diferentes informes predeterminados, pero puede ajustarlos a sus necesidades. Estos informes son:

- Historial de alertas y eventos
- Resumen de alertas
- Alertas y eventos por nombre
- Alertas y eventos por fecha
- Alertas y eventos por ubicación
- Incumplimiento de políticas
- Eventos por usuario
- Protección administrada
- Jerarquía de actualización

Informes y administración delegada

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para crear, editar o eliminar un informe. Sin este permiso, sólo es posible ejecutar informes. Para más información sobre la administración delegada, consulte Administrar roles y subentornos (página 13).

Los informes sólo pueden incluir datos del subentorno activo. No es posible compartir informes entre subentornos. Los informes predeterminados no se copian del subentorno **predeterminado** a los diferentes subentornos que cree.

Cuando elimine un subentorno, también se borrarán los informes asociados.

10.1 Crear informes nuevos

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para crear un informe:

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, haga clic en **Crear**.
3. En el cuadro de diálogo **Crear informe**, seleccione la plantilla de un informe y haga clic en **Aceptar**.

   El asistente le guiará en la creación del informe basado en la plantilla elegida.

Si no quiere utilizar el asistente, en el cuadro de diálogo **Crear informe**, desactive la opción **Usar asistente para crear el informe**. Así podrá configurar el informe nuevo en el cuadro de diálogo de propiedades. Para más información, consulte la sección sobre la configuración del informe correspondiente.

10.2 Configurar el informe del historial de alertas y eventos

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Historial de alertas y eventos** muestra alertas y eventos de los períodos de informes especificados.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Historial de alertas y eventos** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de historial de alertas y eventos**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.
   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.
      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.
   c) En el panel **Región del informe**, haga clic en **Grupo de ordenadores** u **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.
   d) En el panel **Tipos de alerta y evento a incluir**, seleccione los tipos de alertas y eventos que desea incluir en el informe.
      Por defecto, el informe muestra todos los tipos de alertas y eventos.
      Además, puede generar un informe en el que se muestren sólo los ordenadores o grupos en los que se hayan detectado determinadas alertas o eventos. Para especificar una alerta o evento determinado, haga clic en **Avanzadas** y haga clic en el nombre de la alerta o evento en la lista. Para especificar más de una alerta o evento, escriba el nombre utilizando caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres. Por ejemplo, W32/* incluye a todos los virus que comienzan con W32/.
4. En la ficha **Opciones de visualización**, seleccione cómo desea ordenar las alertas y eventos.
   Por defecto, los datos sobre las alertas y eventos se ordenan según el **Nombre de alerta y evento**. Seleccione otra opción si desea ordenarlos por **Nombre del ordenador**, **Nombre del grupo** o **Fecha y hora**.
5. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.3 Configurar el informe resumen de alertas

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Resumen de alertas** proporciona estadísticas sobre el estado general de la red.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Resumen de alertas** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de resumen de alertas**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.
   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.
      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.
4. En la ficha **Opciones de visualización**, en **Mostrar resultados por**, especifique cada cuánto tiempo se miden las infracciones, por ejemplo, cada hora o cada día, abra la lista desplegable y seleccione un intervalo.
5. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.4 Configurar el informe de alertas y eventos por nombre

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Alertas y eventos por nombre** proporciona estadísticas sobre las alertas y eventos de todos los equipos en un período determinado de tiempo, agrupadas por nombre.

Para configurar un informe:

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Alertas y eventos por nombre** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de alertas y eventos por nombre**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.
   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.
      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

c) En el panel **Región del informe**, haga clic en **Grupo de ordenadores** u **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.

d) En el panel **Tipos de alerta y evento a incluir**, seleccione los tipos de alertas y eventos que desea incluir en el informe.

Por defecto, el informe muestra todos los tipos de alertas y eventos.

4. En la ficha **Opciones de visualización**, en **Mostrar**, seleccione las alertas y eventos que quiere ver en el informe.

Por defecto, el informe mostrará todas las alertas y eventos, y el número de veces que se ha producido cada una.

También puede configurar el informe para que sólo muestre:

- las primeras *n* alertas y eventos (siendo *n* el número que usted especifique) o
- alertas y eventos con *m* o más ocurrencias (siendo *m* el número que usted especifique).

5. En **Ordenar por**, elija si prefiere ordenar las alertas y eventos por número o nombre.

Por defecto, el informe mostrará las alertas y eventos en orden descendente de número de veces que se han producido.

6. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.5 Configurar el informe de alertas y eventos por fecha

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Alertas y eventos por fecha** muestra las alertas y eventos de intervalos específicos.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Alertas y eventos por fecha** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de alertas y eventos por fecha**, en la ficha **Configuración**, configure las opciones que desee.

a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.

b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.

Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

c) En el panel **Región del informe**, haga clic en **Grupo de ordenadores** u **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.

d) En el panel **Tipos de alerta y evento a incluir**, seleccione los tipos de alertas y eventos que desea incluir en el informe.

Por defecto, el informe muestra todos los tipos de alertas y eventos.

Además, puede generar un informe en el que se muestren sólo los ordenadores o grupos en los que se hayan detectado determinadas alertas o eventos. Para especificar una alerta o

evento determinado, haga clic en **Avanzadas** y haga clic en el nombre de la alerta o evento en la lista. Para especificar más de una alerta o evento, escriba el nombre utilizando caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres. Por ejemplo, W32/* incluye a todos los virus que comienzan con W32/.

4. En la ficha **Opciones de visualización**, especifique cada cuánto tiempo se mide la tasa de alertas y eventos, por ejemplo, cada hora o cada día, abra la lista desplegable y seleccione un intervalo.
5. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.6 Configurar el informe de alertas y eventos por ubicación

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Alertas y eventos por ubicación** proporciona estadísticas sobre todas las alertas de todos los equipos en un período determinado de tiempo, agrupadas por ubicación.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Alertas y eventos por ubicación** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de alertas y eventos por ubicación**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.
   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.
      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.
   c) En el panel **Región del informe**, haga clic en **Ordenadores** para mostrar alertas por ordenador o **Grupos** para mostrar alertas por cada grupo de ordenadores.
   d) En el panel **Tipos de alerta y evento a incluir**, seleccione los tipos de alertas y eventos que desea incluir en el informe.
      Por defecto, el informe muestra todos los tipos de alertas y eventos.
      Además, puede generar un informe en el que se muestren sólo los ordenadores o grupos en los que se hayan detectado determinadas alertas o eventos. Para especificar una alerta o evento determinado, haga clic en **Avanzadas** y haga clic en el nombre de la alerta o evento en la lista. Para especificar más de una alerta o evento, escriba el nombre utilizando caracteres comodín. Use ? para sustituir un solo carácter y * para sustituir toda una cadena de caracteres. Por ejemplo, W32/* incluye a todos los virus que comienzan con W32/.
4. En la ficha **Opciones de visualización**, en **Mostrar**, seleccione las ubicaciones que quiere ver en el informe.

   Por defecto, el informe mostrará todos los ordenadores y grupos, y el número de veces que se ha producido cada una. Puede configurar el informe para mostrar sólo:

   - las primeras *n* entradas que hayan generado más alertas y eventos (siendo *n* el número que usted indique) o

- cada entrada con *m* o más ocurrencias (siendo *m* el número que usted indique).

5. En **Ordenar por**, seleccione si prefiere ordenar las ubicaciones por el número de elementos detectados o por nombre.

   Por defecto, el informe mostrará los ordenadores o grupos en orden decreciente de número de alertas y eventos. Seleccione **Ubicación** si desea la lista en orden alfabético.

6. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.7 Configurar el informe de incumplimiento de políticas

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Incumplimiento de políticas** muestra el porcentaje o el número de equipos que no cumplen con la política de su grupo a intervalos específicos.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Incumplimiento de políticas** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de Incumplimiento de políticas**, en la ficha **Configuración**, configure las opciones que desee.

   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.

   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.

      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

   c) En el panel **Mostrar**, seleccione las políticas que desea mostrar en el informe. Por defecto, sólo la política **Antivirus y HIPS** está seleccionada.

4. En la ficha **Opciones de visualización**, en **Mostrar resultados por**, especifique cada cuánto tiempo se miden las infracciones, por ejemplo, cada hora o cada día, abra la lista desplegable y seleccione un intervalo.
5. En **Mostrar resultados como**, elija si prefiere mostrar los resultados en porcentajes o números.
6. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.8 Configurar el informe de eventos por usuario

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Eventos por usuario** muestra eventos de la restricción de aplicaciones, del cortafuegos, del control de datos, dispositivos y web, agrupados por usuario.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Eventos por usuario** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de Eventos por usuario**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.
   b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.
      Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.
   c) En **Tipos de evento a incluir**, seleccione las funciones de las que desea mostrar eventos.
4. En la ficha **Opciones de visualización**, en **Mostrar**, seleccione los usuarios que quiere ver en el informe.
   Por defecto, el informe mostrará todos los usuarios y el número de eventos de cada uno. Puede configurar el informe para mostrar sólo:
   - los primeros *n* usuarios que hayan generado más eventos (siendo *n* el número que usted indique) o
   - los usuarios con *m* o más ocurrencias (siendo *m* el número que usted indique).
5. En **Ordenar por**, seleccione si prefiere ordenar los usuarios por el número de eventos o por nombre.
   Por defecto, el informe mostrará los usuarios en orden decreciente del número de eventos por usuario. Seleccione **Usuario** si desea la lista en orden alfabético.
6. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.9 Configurar el informe de protección administrada

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

El informe **Protección administrada** muestra el porcentaje o número de equipos protegidos en los intervalos especificados.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione **Protección administrada** y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades de protección administrada**, en la ficha **Configuración**, configure las opciones que desee.
   a) En el panel **Detalles del informe**, modifique el nombre y la descripción del informe, si lo desea.

b) En el panel **Periodo del informe**, en el cuadro de texto **Periodo**, abra la lista desplegable y seleccione un período de tiempo.

Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

c) En el panel **Mostrar**, seleccione las funciones que desea mostrar en el informe.

4. En la ficha **Opciones de visualización**, en **Mostrar resultados por**, especifique cada cuánto tiempo se miden las infracciones, por ejemplo, cada hora o cada día, abra la lista desplegable y seleccione un intervalo.
5. En **Mostrar resultados como**, elija si prefiere mostrar los resultados en porcentajes o números.
6. En la ficha **Programación**, seleccione **Programar este informe** si desea ejecutar el informe con cierta frecuencia y que los resultados se envíen a los destinatarios como adjuntos de correo. Introduzca la fecha de inicio y la frecuencia con la que desea que se generen los informes, especifique el formato y el idioma del archivo resultante, y escriba las direcciones de correo electrónico de los destinatarios.

10.10 Informe de jerarquía de actualización

El informe **Jerarquía de actualización** muestra los gestores de actualización de la red, las unidades compartidas de actualización que mantienen y el número de equipos que se actualizan desde estas unidades compartidas.

No es posible configurar el informe **Jerarquía de actualización**. Puede generar el informe según se describe en Generar un informe (página 203).

10.11 Programar un informe

Si utiliza administración delegada, necesitará el permiso **Configuración de informes** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Si lo desea, puede programar informes para que se ejecuten con determinada frecuencia y se envíen los resultados a los destinatarios elegidos como adjuntos de correo electrónico.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione el informe que desea programar y haga clic en **Programar**.
3. En el cuadro de diálogo que aparece, en la ficha **Programación**, seleccione **Programar este informe**.
4. Introduzca la fecha de inicio y la frecuencia con la que se generará el informe.
5. Especifique el formato y el idioma de los resultados del informe.
6. Introduzca las direcciones de correo electrónico de los destinatarios del informe.

10.12 Generar un informe

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione el informe que desea ejecutar y haga clic en **Ejecutar**.
   Aparece la ventana **Informes**, que muestra el informe.

Si lo desea, puede cambiar la distribución del informe, imprimirlo o exportarlo a un archivo.

10.13 Ver informes como tablas o gráficos

Algunos informes pueden verse como tablas o como gráficos. Cuando es posible, en la ventana **Informes** donde aparece el informe, podrá ver dos fichas, **Tabla** y **Gráfico**.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Gestor de informes**, seleccione el informe que desea ejecutar, por ejemplo **Alertas y eventos por ubicación** y haga clic en **Ejecutar**.
   Aparece la ventana **Informes**, que muestra el informe.
3. Para ver el informe como una tabla o como un gráfico, vaya a la ficha correspondiente.

10.14 Imprimir informes

Para imprimir un informe, haga clic en el icono **Imprimir** de la barra de herramientas al visualizar el informe.

10.15 Exportar informes

Para exportar un informe:

1. Haga clic en el icono **Exportar** en la barra de herramientas al visualizar el informe.

2. En el cuadro de diálogo **Exportar informe**, seleccione el formato en el que desea guardar el informe.

   Las opciones son:

   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Texto enriquecido (RTF)
   - Valores separados (CSV)
   - XML
3. Haga clic en el botón **Examinar**. Escriba un nombre. Haga clic en **Aceptar**.

10.16 Cambiar el diseño del informe

Puede cambiar el diseño de la página en la que se muestran los informes. Por ejemplo, puede mostrar los informes de forma apaisada.

1. Haga clic en el icono de diseño de página en la barra de herramientas al visualizar el informe.

2. En el cuadro de diálogo **Configurar página**, especifique el tamaño, orientación y los márgenes de la hoja. Haga clic en **Aceptar**.
   El informe se mostrará con la nueva configuración de página.

Esta configuración se utilizará también al imprimir o exportar el informe.

11 Auditoría

La auditoría permite monitorizar los cambios de configuración en Enterprise Console y otras acciones del usuario y del sistema. Puede utilizar esta información para el cumplimiento normativo y la solución de problemas, o como evidencia legar en caso de actividad maliciosa.

Por defecto, la auditoría está desactivada. Una vez activada, la base de datos de auditoría recogerá una entrada cada vez que cambien ciertas opciones de configuración o se realicen ciertas acciones.

Nota
Si utiliza administración delegada, necesitará el permiso **Auditoría** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

La entrada de auditoría incluye la siguiente información:

- Acción realizada
- Usuario que realizó la acción
- Equipo
- Subentorno del usuario
- Fecha y hora de la acción

Se registran tanto las acciones completadas como los intentos fallidos.

Las acciones recogidas en la auditoría incluyen:

Categoría	Acción
Acciones sobre ordenadores	Resolver o quitar alertas y errores, proteger ordenadores, actualizar ordenadores, quitar ordenadores, realizar escaneados remotos
Gestión de grupos de ordenadores	Crear grupos, eliminar grupos, mover grupos, cambiar de nombre, asignar un ordenador a un grupo
Gestión de políticas	Crear políticas, cambiar de nombre, publicar políticas, editar políticas, asignar una política a un ordenador, restaurar la configuración predeterminada de una política, eliminar políticas
Gestión de roles	Crear roles, eliminar roles, cambiar de nombre, duplicar roles, añadir un usuario a un rol, eliminar un usuario de un rol, añadir un derecho a un rol, eliminar un derecho de un rol
Gestión del gestor de actualización	Actualizar gestores de actualización, hacer que un gestor de actualización cumpla con la configuración, quitar alertas, eliminar gestores de actualización, configurar gestores de actualización, añadir suscripciones nuevas, eliminar suscripciones, cambiar el nombre de suscripciones, editar suscripciones, duplicar suscripciones
Eventos del sistema	Activar la auditoría, desactivar la auditoría

Puede utilizar aplicaciones de terceros, como Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services o Crystal Reports, para acceder y analizar las entradas de auditoría en la

base de datos. Para más información sobre cómo ver las entradas de la auditoría, consulte la Guía de usuario de auditoría *de Sophos Enterprise Console*.

11.1 Activar o desactivar la auditoría

Si utiliza administración delegada, necesitará el permiso **Auditoría** para realizar esta tarea. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Para activar o desactivar la auditoría:

1. En el menú **Herramientas**, haga clic en **Gestionar auditoría**.
2. En el cuadro de diálogo **Gestión de auditoría**, utilice la opción **Activar auditoría**. Esta opción está desactivada por defecto.

12 Copiar e imprimir datos de Enterprise Console

12.1 Copiar datos de la lista de ordenadores

Si lo desea, puede copiar información de la lista de equipos de la vista **Estaciones** en el portapapeles y pegarla en otro documento con campos separados por tabuladores.

1. En la vista **Estaciones**, en el panel **Grupos**, seleccione el grupo de equipos del que quiere copiar datos.
2. En la lista **Ver**, seleccione qué equipos quiere ver, por ejemplo, **Ordenadores con posibles problemas**.
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel** o **A este nivel y por debajo**.
4. En la lista de ordenadores, abra la ficha que quiere ver, por ejemplo **Detalles antivirus**.
5. Haga clic en cualquier parte de la lista de ordenadores.
6. En el menú **Edición**, haga clic en **Copiar** para copiar los datos del portapapeles.

12.2 Imprimir datos de la lista de ordenadores

Si lo desea, puede imprimir la información que aparece en la lista de ordenadores, en la vista **Estaciones**.

1. En la vista **Estaciones**, en el panel **Grupos**, seleccione el grupo de equipos del que quiere imprimir datos.
2. En la lista **Ver**, seleccione qué equipos quiere ver, por ejemplo, **Ordenadores con posibles problemas**.
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel** o **A este nivel y por debajo**.
4. En la lista de ordenadores, abra la ficha que quiere ver, por ejemplo **Detalles antivirus**.
5. Haga clic en cualquier parte de la lista de ordenadores.
6. En el menú **Archivo**, haga clic en **Imprimir**.

12.3 Copiar información de ordenadores

Si lo desea, puede copiar información del cuadro de diálogo **Detalles del ordenador** en el portapapeles para pegarlos en otro documento. La información incluye el nombre del equipo, el sistema operativo, las versiones del software de seguridad instalado, alertas y errores pendientes, el estado de las actualizaciones, etc.

1. En la vista **Estaciones**, en la lista de ordenadores, haga doble clic en el equipo del que desea copiar los datos.
2. En el cuadro de diálogo **Detalles del ordenador**, haga clic en **Copiar** para copiar los datos en el portapapeles.

12.4 Imprimir información de ordenadores

Si lo desea, puede imprimir la información del cuadro de diálogo **Detalles del ordenador**. La información incluye el nombre del equipo, el sistema operativo, las versiones del software de seguridad instalado, alertas y errores pendientes, el estado de las actualizaciones, etc.

1. En la vista **Estaciones**, en la lista de ordenadores, haga doble clic en el equipo del que desea imprimir los datos.
2. En el cuadro de diálogo **Detalles del ordenador**, haga clic en **Imprimir**.

13 Solución de problemas

Al ejecutar el asistente para proteger ordenadores, se pueden producir errores en la instalación del software de seguridad por diferentes motivos:

- No es posible llevar a cabo la instalación automática en ese sistema operativo. Realice la instalación de forma manual. Para más información sobre otros sistemas operativos (si su licencia lo incluye), consulte la Guía de inicio de para Linux y UNIX.
- No se puede determinar el sistema operativo. Esto puede ocurrir si, al buscar ordenadores, no introduce su nombre de usuario con el formato dominio\usuario.
- Las reglas con las que se ha configurado el Firewall están bloqueando el acceso necesario para implementar el software de seguridad.

13.1 El escaneado en acceso no se ejecuta en ciertos equipos

Si hay ordenadores que no tienen activado el escaneado en acceso:

1. Compruebe qué política antivirus y HIPS usan.

   Para más información, vea Comprobar qué políticas usa un grupo (página 25).
2. Compruebe que el escaneado en acceso está activado en esa política y que los equipos la cumplen.

   Para más información, consulte Activar o desactivar el escaneado en acceso (página 79) y Imponer el uso de la política del grupo (página 32).

13.2 El cortafuegos está desactivado

Si hay ordenadores con el cortafuegos desactivado:

1. Compruebe qué política cortafuegos usan.

   Para más información, vea Comprobar qué políticas usa un grupo (página 25).
2. Compruebe que el cortafuegos está activado en esa política y que los equipos la cumplen.

   Para más información, consulte Desactivar el cortafuegos temporalmente (página 112) y Imponer el uso de la política del grupo (página 32).

13.3 El cortafuegos no está instalado

Nota
Si utiliza administración delegada, necesitará el permiso **Búsqueda de ordenadores, protección y grupos** para instalar el cortafuegos. Para obtener más información, consulte Administrar roles y subentornos (página 13).

Antes de comenzar la instalación del cortafuegos en las estaciones, compruebe que utiliza sistemas operativos que no sean de servidor.

Nota
No es posible instalar el cortafuegos en equipos con sistemas operativos de servidor ni Windows Vista Starter.

Para las estaciones en las que desea instalar el cortafuegos:

1. Seleccione los equipos, haga clic con el botón derecho del ratón y seleccione **Proteger ordenadores**.
   Se abrirá el **Asistente para proteger ordenadores**. Haga clic en **Next**.
2. Cuando se le pida que seleccione las funciones, seleccione **Cortafuegos**. Finalice el asistente.

Si el problema persiste, póngase en contacto con el soporte técnico de Sophos.

13.4 Ordenadores con alertas pendientes

- Si hay ordenadores con un virus o una aplicación que no desea, consulte Realizar una limpieza inmediata (página 51).
- Si existen ordenadores con un programa publicitario u otra aplicación no deseada que *sí* quiera utilizar, consulte Autorizar programas publicitarios y otras aplicaciones no deseadas (página 102).
- Si tiene algún ordenador con protección obsoleta, vaya a Actualizar ordenadores con protección obsoleta (página 74) para saber cómo identificar y resolver el problema.

Nota
Una vez resuelto el problema, puede borrar la alerta. Seleccione los ordenadores con alertas, haga clic con el botón derecho y seleccione **Resolver alertas y errores**. Para quitar alertas y errores, es necesario contar con el permiso **Remediación: limpieza**.

13.5 Ordenadores no administrados por la consola

Los ordenadores Windows, Macintosh, Linux y UNIX deben gestionarse mediante Enterprise Console, de manera que puedan actualizarse y monitorizarse.

Nota
Recuerde que, a menos que utilice la sincronización con Active Directory (consulte Administrar roles y subentornos (página 13)), los ordenadores nuevos añadidos a la red no aparecerán en la consola ni serán administrados automáticamente. Haga clic en **Detectar ordenadores** en la barra de herramientas para buscarlos y colocarlos en el grupo **No asignados**.

Si algún ordenador no está administrado, las estaciones aparecerán en gris en la ficha **Estado**.

Para administrar ordenadores no administrados:

1. En la lista desplegable **Ver**, seleccione **Ordenadores no administrados**.
2. Escoja una de las siguientes opciones:
   - Si los ordenadores no administrados se encuentran en el grupo **No asignados**, arrástrelos al grupo desde el que desea administrarlos. Se iniciará el **Asistente para proteger ordenadores**.

- Si los ordenadores ya se encuentran en un grupo, haga clic en el botón derecho y seleccione **Proteger ordenadores**.

3. Si hay ordenadores en los que Enterprise Console no puede instalar Sophos Endpoint Security and Control de forma automática, realice una instalación manual.

   La instalación automática mediante el **Asistente para proteger ordenadores** sólo está disponible para ordenadores Windows. Si necesita proteger ordenadores Mac, Linux o UNIX, instale el software de forma manual.

   Para más información sobre la protección manual de ordenadores Mac o Windows, consulte la *Guía avanzada de inicio de Sophos Enterprise Console*.

   Para más información sobre la protección de ordenadores Linux y UNIX, consulte la *Guía de inicio de Sophos Enterprise Console para Linux y UNIX*.

13.6 No se pueden proteger los ordenadores en el grupo No asignados

El grupo **No asignados** no puede tener políticas asignadas, sólo contiene los ordenadores que aún no han sido adjudicados a ningún grupo. No podrá proteger ordenadores hasta que no los sitúe en un grupo.

13.7 Error en la instalación de Sophos Endpoint Security and Control

Si el **Asistente para proteger ordenadores** no es capaz de instalar Sophos Endpoint Security and Control en las estaciones, puede deberse a las siguientes razones:

- Enterprise Console desconoce el sistema operativo de los ordenadores. Esto puede deberse a que no introdujo su nombre de usuario en el formato dominio\usuario cuando buscó los ordenadores.
- No es posible llevar a cabo la instalación automática en ese sistema operativo. Realice la instalación de forma manual. Para más información, consulte la *Guía avanzada de inicio de Sophos Enterprise Console*.
- Los equipos tienen un cortafuegos activado.
- No se ha desactivado el uso compartido simple de archivos en los ordenadores con Windows XP.
- No se ha desactivado la opción “Usar el Asistente para compartir” en los equipos con Windows Vista.
- Ha seleccionado alguna función que no es compatible con el sistema operativo.

La lista completa de requisitos para Sophos Endpoint Security and Control está disponible en la web de Sophos (http://www.sophos.com/es-es/products/all-system-requirements).

13.8 Los ordenadores no se actualizan

Consulte Actualizar ordenadores con protección obsoleta (página 74) para saber cómo diagnosticar y solucionar el problema.

13.9 La configuración antivirus no se aplica a estaciones Macintosh

Ciertas opciones de configuración no son aplicables a sistemas Macintosh. En cada caso, verá una señal de aviso en el cuadro de configuración correspondiente.

Para más información sobre la configuración de la política antivirus y HIPS que aplica en equipos Mac, consulte el artículo 118859 en la base de conocimiento de Sophos.

13.10 La configuración antivirus no se aplica a estaciones Linux ni UNIX

Ciertas opciones de configuración no son aplicables a sistemas a Linux ni UNIX. En cada caso, verá una señal de aviso en el cuadro de configuración correspondiente.

Para sistemas Linux, utilice el comando `savconfig` y `savscan` como se describe en el *Guía de configuración de Sophos Anti-Virus para Linux*.

Para sistemas UNIX, utilice el comando `savscan` como se describe en el *Guía de configuración de Sophos Anti-Virus para UNIX*.

13.11 Los ordenadores Linux o UNIX no cumplen con la política

Si el directorio de instalación central para Linux utiliza un archivo central de configuración con opciones diferentes de las especificadas desde la consola, los ordenadores se mostrarán como que no cumplen con la política.

Seleccione la opción **Cumplir con política** para que el ordenador cumpla la política de forma temporal, hasta que se vuelva a aplicar la configuración basada en CID.

Para resolver el problema revise el archivo de configuración central o pase la administración a la consola.

13.12 Aparece un nuevo escaneado en Windows

Si abre Sophos Endpoint Security and Control en una estación con Windows, podría observar un nuevo escaneado en la lista, incluso si el usuario no lo ha creado.

Este nuevo escaneado será el escaneado que creó desde la consola. No debería borrarlo.

13.13 Problemas de conexión y tiempo de espera agotado

Cuando la comunicación entre Enterprise Console y un equipo de la red se vuelve lenta o el ordenador no responde, puede deberse a un problema de conectividad.

Consulte el informe de comunicaciones de red de Sophos que ofrece una descripción general del estado de la comunicación entre el equipo y Enterprise Console. Para ver el informe, vaya al equipo en el que se produjo el problema. En la barra de tareas, haga clic en el botón **Inicio**, seleccione **Programas > Sophos > Sophos Endpoint Security and Control** y haga clic en **Ver el informe del estado de la red de Sophos**.

El informe muestra áreas con posibles problemas y sugerencias para solucionarlos.

13.14 No se detectan programas publicitarios ni aplicaciones no deseadas

Si no se detectan programas publicitarios u otras aplicaciones no deseadas, compruebe lo siguiente:

- La detección está activada. Consulte Configurar el escaneado en acceso (página 77).
- Las aplicaciones se encuentran en un equipo con Windows.

13.15 Elemento detectado de forma parcial

Sophos Endpoint Security and Control puede informar sobre la "detección parcial" de un elemento, como un troyano o una aplicación no deseada. Esto significa que no ha identificado todos los componentes de la aplicación.

Para identificar el resto de componentes, será necesario realizar un escaneado exhaustivo del ordenador en cuestión. En ordenadores con Windows, lo podrá hacer desde la consola: seleccione el ordenador, haga clic con el botón derecho del ratón y seleccione **Escaneado remoto**. Puede hacerlo configurando un escaneado programado para detectar programas publicitarios y otras aplicaciones no deseadas. Consulte Configurar el escaneado en acceso (página 77) y Crear un escaneado programado (página 83).

Si la aplicación sigue siendo detectada de forma parcial, se puede deber a lo siguiente:

- no tiene suficientes derechos de acceso
- algunas unidades o carpetas del ordenador, que contienen los componentes de la aplicación, están excluidas del escaneado.

Si la segunda opción es el caso, compruebe la lista de elementos excluidos del escaneado (consulte Excluir elementos del escaneado en acceso (página 82)). Si la lista contiene varios elementos, bórrelos de la lista y vuelva a escanear el ordenador.

Es posible que Sophos Endpoint Security and Control no pueda detectar o eliminar completamente programas publicitarios y aplicaciones no deseadas con componentes instalados en unidades de red.

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

13.16 Alertas frecuentes de aplicaciones no deseadas

Es posible recibir gran cantidad de alertas de aplicaciones no deseadas, incluyendo múltiples informes de la misma aplicación.

Esto puede ocurrir porque algunos tipos de aplicaciones no deseadas "monitorizan" archivos para intentar acceder a ellos. Si tiene activado el escaneado en acceso, Sophos Endpoint Security and Control detectará cada uno de estos intentos y enviará una alerta.

Tiene varias opciones:

- Desactivar el escaneado en acceso de programas publicitarios y aplicaciones no deseadas. Puede utilizar en su lugar el escaneado programado.
- Autorizar la aplicación (si quiere que se ejecute en sus ordenadores). Consulte Autorizar programas publicitarios y otras aplicaciones no deseadas (página 102).
- Limpiar los ordenadores, eliminando así las aplicaciones que no ha autorizado. Consulte Realizar una limpieza inmediata (página 51).

13.17 Falló la limpieza

Si Sophos Endpoint Security and Control falla al intentar limpiar algún elemento ("Falló la limpieza"), puede deberse a varias razones:

- No ha identificado todos los componentes de un elemento multicomponente. Ejecute un escaneado exhaustivo del ordenador para identificar el resto de componentes. Consulte Escaneado remoto (página 51).
- Algunas unidades o carpetas que contienen componentes del elemento están excluidas del escaneado. Revise los elementos excluidos del escaneado (consulte Excluir elementos del escaneado en acceso (página 82)). Si hay elementos en la lista, elimínelos.
- No tiene suficientes derechos de acceso.
- No puede limpiar ese tipo de elemento.
- En vez de obtener una correspondencia exacta del virus, ha identificado sólo un fragmento de virus.
- El elemento está en un disquete o CD-ROM protegido contra escritura.
- El elemento está en un volumen NTFS protegido contra escritura (Windows).

13.18 Recuperación tras una infección

La limpieza puede eliminar un virus del ordenador, pero no siempre puede deshacer el daño que el virus haya podido causar.

Algunos virus no tienen efectos secundarios. Otros pueden realizar cambios o corromper datos en formas que son difíciles de detectar. Para saber qué hacer ante cada caso, deberá:

- En el menú **Ayuda**, seleccione **Ver información de seguridad**. Desde aquí será dirigido al sitio web de Sophos, donde podrá consultar el análisis del virus.

- Utilice copias de seguridad o copias originales de programas para sustituir programas infectados. Si no dispone de copias de seguridad, créelas para minimizar el impacto de una posible infección.

A veces es posible recuperar datos en discos dañados por un virus. Sophos proporciona herramientas para reparar el daño creado por ciertos virus. Póngase en contacto con el soporte técnico de Sophos si necesita ayuda.

13.19 Recuperación de los efectos secundarios de una aplicación

La limpieza puede eliminar aplicaciones no deseadas del ordenador, pero no siempre puede deshacer el daño que hayan podido causar.

Algunas aplicaciones modifican el sistema operativo, por ejemplo cambiando la configuración de la conexión a Internet. Sophos Endpoint Security and Control no siempre puede restaurar toda la configuración. Por ejemplo, si una aplicación ha cambiado la página de inicio del navegador web, Sophos Endpoint Security and Control no puede saber qué página de inicio estaba configurada previamente.

Algunas aplicaciones instalan herramientas, como archivos .dll o .ocx, en su ordenador. Si una herramienta es inofensiva (es decir, si no posee las cualidades de una aplicación no deseada), por ejemplo bibliotecas del programa, que no pertenecen a la aplicación en sí, es posible que Sophos Endpoint Security and Control no pueda detectarla como parte de una aplicación. En este caso, la limpieza no eliminará el archivo de su ordenador.

A menudo, una aplicación, como el adware, forma parte de un programa que ha instalado a propósito, y su presencia es necesaria para ejecutar el programa. Si elimina la aplicación, es posible que el programa deje de funcionar en su ordenador.

Haga lo siguiente:

- En el menú **Ayuda**, seleccione **Ver información de seguridad**. Desde aquí será dirigido al sitio web de Sophos, donde podrá consultar el análisis de la aplicación.
- Utilice copias de seguridad para recuperar la configuración de su sistema o los programas que desea usar. Si no dispone de copias de seguridad, créelas para minimizar el impacto de futuros incidentes.

Para obtener más información o recomendaciones sobre cómo recuperarse de los efectos secundarios de un programa publicitario o de una aplicación no deseada, póngase en contacto con el soporte técnico de Sophos.

13.20 El control de datos no detecta archivos cargados mediante navegadores integrados

El control de datos intercepta documentos que se cargan mediante navegadores web independientes. No intercepta documentos cargados mediante navegadores integrados en aplicaciones de terceros (como Lotus Notes). Si cuenta con aplicaciones de terceros con navegadores integrados y desea controlar todos los documentos cargados, deberá configurar la aplicación para que inicie un navegador externo.

13.21 El control de datos no detecta archivos cargados o adjuntos

Si el control de datos no detecta archivos utilizados desde una unidad compartida de red, puede deberse a que ha excluido el escaneado de archivos remotos en la política Antivirus y HIPS. En este caso, el control de datos utiliza las mismas exclusiones que el escaneado en acceso de Sophos Anti-Virus (InterCheck ™), de modo que, si se desactiva el escaneado de archivos remotos, no se enviará ningún archivo remoto para una comprobación del control de datos.

Para más información sobre las exclusiones del escaneado en acceso, consulte Excluir elementos del escaneado en acceso (página 82).

Nota
El control de datos no utiliza las exclusiones del escaneado en acceso cuando los archivos se copian o mueven con Internet Explorer. En este caso, el control de datos intercepta la transferencia de archivos a unidades de almacenamiento supervisadas desde una ubicación de red, por ejemplo, al copiar archivos a un dispositivo de almacenamiento extraíble o al grabar datos en una unidad óptica.

13.22 La consola sigue mostrando un gestor de actualización eliminado

Tras desinstalar algún gestor de actualización, es posible que se siga mostrando en Enterprise Console en la vista **Gestores de actualización**.

Para quitar algún gestor de actualización de la consola, haga clic con el botón derecho y seleccione **Borrar**.

14 Glosario

evento de sincronización con Active Directory	Evento que se produce durante la sincronización con Active Directory.
subentorno activo	Parte del entorno informático que se muestra en el panel Grupos.
editor avanzado de control de contenido	Editor que permite a los usuarios crear listas de control de contenido personalizadas formadas por una puntuación, un recuento máximo, una expresión regular y una puntuación límite que debe alcanzarse para coincidir con la lista de control de contenido.
gestor de aplicaciones	Cuadro de diálogo desde el que se pueden autorizar aplicaciones o crear reglas para aplicaciones que han sido bloqueadas por Sophos Client Firewall.
auditoría	Función que permite monitorizar los cambios de configuración en Enterprise Console y otras acciones del usuario y del sistema.
protección automática	Distribución automática del software de seguridad (instalación e imposición de políticas) a ordenadores nuevos que se incorporan a Active Directory.
categoría	Etiqueta específica que se utiliza para clasificar las listas de control de contenido de SophosLabs según el tipo, las normativas que definen el contenido o la región a la que hacen referencia.
lista de control de contenido (LCC)	Conjunto de condiciones que especifican el contenido de archivos, por ejemplo, números de tarjetas de crédito o datos bancarios, junto a otra información personal. Existen dos tipos de listas de control de contenido: las listas de control de contenido de SophosLabs y las personalizadas.
regla de contenido	Regla que contiene una o más listas de control de contenido y especifica la acción que se lleva a cabo si el usuario intenta transferir datos que coinciden con las listas de control de contenido de la regla al destino especificado.
aplicación restringida	Aplicación no maliciosa que las empresas desean detectar o bloquear por motivos de productividad.
datos restringidos	Archivos que cumplen las condiciones de control de datos.
dispositivo controlado	Dispositivo al que se aplica el control de dispositivos.
umbral crítico	Valor a partir del cual el estado de seguridad de un elemento se considera crítico.

lista de control de contenido personalizada	Lista de control de contenido creada por un cliente de Sophos. Las listas de control de contenido personalizadas se pueden crear de dos formas: mediante la creación de una lista de términos de búsqueda con una condición de búsqueda específica, como "cualquiera de estos términos" o mediante la utilización del editor avanzado de control de contenido.
Panel de control	El panel de control ofrece una visión general del estado de seguridad de la red.
evento del panel de control	Evento en el que un indicador del panel de control excede el nivel crítico. Cuando esto ocurre, el panel de control enviará un email de alerta.
control de datos	Sistema para prevenir la fuga accidental de datos en las estaciones. Se ejecuta cuando el usuario de una estación intenta transferir un archivo que cumple los criterios definidos en las reglas y políticas de control de datos. Por ejemplo, cuando un usuario intenta copiar una hoja de cálculo que contiene una lista de datos de clientes en un dispositivo de almacenamiento extraíble o cargar un documento marcado como confidencial en una cuenta de correo web, el control de datos bloquea la transferencia si está así configurado.
prevención de fugas de datos (DLP)	Consulte *control de datos*.
base de datos	Componente de Sophos Enterprise Console en el que se almacenan datos de los ordenadores de la red.
subentorno predeterminado	Subentorno inicial que muestra el directorio raíz del servidor y el grupo **No asignados**. Es el subentorno que aparece al abrir Enterprise Console por primera vez.
control de dispositivos	Sistema para prevenir la fuga accidental de datos en las estaciones y la entrada de software externo. Funciona limitando el uso de dispositivos de almacenamiento o red no autorizados.
reputación de descargas	Reputación de un archivo descargado de Internet. La reputación se calcula a partir de la antigüedad del archivo, el origen, la prevalencia, análisis de contenido profundo y otras características. Ayuda a establecer si el archivo es seguro o si representa un riesgo potencial que puede dañar el ordenador de un usuario si se descarga.
entorno	Vea *entorno informático*.
dispositivo exento	Dispositivo que se excluye del control de dispositivos.
expresión	Vea *expresión regular*.
regla de coincidencia de archivos	Regla que especifica la acción que se lleva a cabo si el usuario intenta transferir un archivo con el nombre de archivo o tipo especificados

	al destino especificado, como bloquear la transferencia de bases de datos a dispositivos de almacenamiento extraíbles.
grupo	Conjunto de ordenadores administrados definidos en Sophos Enterprise Console.
indicador de estado	Término genérico para los iconos que describen en el panel de control el estado de seguridad de las estaciones de la red.
HIPS (sistema de prevención contra intrusiones)	Tecnología de seguridad que protege los equipos contra archivos sospechosos, virus no identificados y comportamientos sospechosos.
entorno informático	El entorno informático de una empresa incluye ordenadores, redes, etc.
Detección de tráfico malicioso	Una función que detecta comunicaciones entre equipos secuestrados y los servidores de comando y control de atacantes.
ordenador administrado	Ordenador que dispone del sistema de administración remota (RMS) y en el que Sophos Enterprise Console puede instalar y actualizar software.
Consola de administración	Componente de Sophos Enterprise Console que permite proteger y administrar ordenadores.
servidor de administración	Componente de Sophos Enterprise Console que se encarga de la comunicación con los ordenadores de la red.
número máximo	Número máximo de coincidencias con una expresión regular que se pueden contabilizar en la puntuación total.
ordenador no actualizado	Ordenador que no dispone de las últimas actualizaciones de Sophos.
control de parches	Sistema para verificar la instalación de parches del sistema y aplicaciones.
política	Configuración establecida de forma centralizada, por ejemplo, de actualización, que se aplica a un grupo de ordenadores.
aplicaciones no deseadas (PUA)	Programa no malicioso en sí mismo, pero normalmente considerado inadecuado para la mayoría de redes empresariales.
cantidad	Volumen del tipo de datos clave de la lista de control de contenido que debe haber en un archivo para coincidir con la misma.
clave de cantidad	Tipo clave de datos definidos en la lista de control de contenido, al cual se aplica el valor de cantidad. Por ejemplo, en una lista de control de contenido que contiene números de tarjetas de crédito, la cantidad especifica cuántos números deben aparecer en un archivo para que coincida con la lista.

región	Alcance de una lista de control de contenido de SophosLabs. La región puede hacer referencia a un país (en listas por países) o ser "global" (en listas que afectan a todos los países).
expresión regular	Cadena de búsqueda que utiliza caracteres especiales para encontrar patrones de texto en un archivo. El control de datos utiliza sintaxis de expresiones regulares de Perl 5.
derecho	Conjunto de permisos que permiten realizar ciertas tareas en Enterprise Console.
rol	Conjunto de derechos que determinan el acceso a Enterprise Console.
administración delegada	Función que permite especificar los ordenadores y tareas a los que un usuario tiene acceso dependiendo de su rol.
rootkit	Troyano o tecnología que se utiliza para ocultar la presencia de un objeto malicioso (proceso, archivo, clave del registro o puerto de red) ante el usuario o el administrador.
regla	Regla que especifica la acción que se lleva a cabo si un archivo cumple determinadas condiciones. Existen dos tipos de reglas de control de datos: reglas de archivos y reglas de contenido.
puntuación	Número que se añade a la puntuación total de una lista de control de contenido cuando se cumple una expresión regular.
nodo raíz del servidor	Nodo superior que se muestra en el panel **Grupos**, que incluye el grupo **No asignados**.
Protección activa de Sophos	Función que utiliza la conexión a Internet para comprobar archivos sospechosos.
Sophos Update Manager (SUM)	Programa que descarga el software de seguridad de Sophos y las actualizaciones desde Sophos u otro servidor de actualización a los recursos compartidos de actualización.
regla definida de Sophos	Regla proporcionada por Sophos a modo de ejemplo. Sophos no actualiza dichas reglas.
lista de control de contenido de SophosLabs	Lista de control de contenido proporcionada y administrada por Sophos. Sophos puede actualizar las listas de control de contenido de SophosLabs o crear otras nuevas y publicarlas en Enterprise Console. El contenido de las listas de control de contenido de SophosLabs no se puede modificar. Pero se puede establecer la cantidad de dichas listas.
subentorno	Área definida del entorno informático que contiene ordenadores y grupos.

administración de subentorno	Función que permite restringir las posibles acciones sobre los ordenadores y grupos disponibles.
suscripción de software	Conjunto de versiones del software para diferentes plataformas que el usuario selecciona en Update Manager para su descarga y actualización. Se puede especificar una versión para cada plataforma (por ejemplo, “Recommended” para Windows).
detección de comportamiento sospechoso	Análisis dinámico del comportamiento de todos los programas para detectar y bloquear aquellos cuya actividad parezca maliciosa.
archivo sospechoso	Archivo con características habituales de virus, aunque no exclusivas.
intervalo de sincronización	Período tras el cual se realiza la sincronización de los grupos en Enterprise Console que se corresponden con un contenedor de Active Directory.
punto de sincronización (para un árbol de Active Directory)	Grupo en Enterprise Console que se corresponde con un contenedor de Active Directory (grupos y ordenadores, o sólo grupos) y su estructura.
sincronización con Active Directory	Sincronización de los grupos de Sophos Enterprise Console que se corresponden con contenedores de Active Directory.
grupo sincronizado	Grupos bajo un punto de sincronización.
Administrador del sistema	Usuario de Enterprise Console con derechos suficientes para administrar el software de seguridad de Sophos en la red y los derechos de usuarios. No es posible eliminar o modificar los permisos o el nombre del rol del administrador del sistema, ni eliminar el grupo de administradores totales de Sophos. El resto de usuarios y grupos se pueden añadir o eliminar del rol.
etiqueta	Identificador aplicado a una lista de control de contenido de SophosLabs para determinar el contenido o el alcance de la misma. Existen tres tipos de etiquetas: tipo, normativa y región.
protección contra manipulaciones	Función que evita que programas maliciosos o usuarios no autorizados puedan desinstalar el software de seguridad de Sophos o desactivarlo desde Sophos Endpoint Security and Control.
umbral	Valor a partir del cual el estado de seguridad de un elemento se considera de aviso o crítico.
puntuación total	Suma de las puntuaciones de una lista de control de contenido, en relación al contenido encontrado.

puntuación límite	Número de veces que debe cumplirse una expresión regular para coincidir con una lista de control de contenido.
tipo de archivo verdadero	Tipo de archivo establecido mediante el análisis de la estructura del archivo, en contraposición a la extensión del mismo. Este método es más fiable.
tipo	Criterio utilizado para la clasificación de las listas de control de contenido de SophosLabs, por ejemplo, las listas de control de contenido que definen datos de pasaportes, direcciones postales o direcciones de email pertenecen al tipo Información personal identificable.
gestor de actualización	Vea *Sophos Update Manager*.
umbral de aviso	Valor a partir del cual el estado de seguridad de un elemento se considera de aviso.
control web	Función que permite bloquear el acceso a sitios web no autorizados y generar informes del acceso a Internet desde las estaciones. Es posible bloquear, permitir o avisar cuando el usuario intente acceder a sitios web según ciertas categorías.
protección web	Función que permite detectar amenazas en páginas web. Es posible bloquear el acceso a sitios web con contenido malicioso así como descargas de este tipo. La protección web se incluye en la política antivirus y HIPS.

15 Soporte técnico

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

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

16 Aviso legal

Índice

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W