

Bitdefender® ENTERPRISE

BITDEFENDER SMALL OFFICE SECURITY

Guía del Informador >>

Bitdefender Small Office Security

Guía del Informador

fecha de publicación 2014.12.17

Copyright© 2014 Bitdefender

Advertencia legal

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La inclusión de breves citas en críticas sólo puede ser posible con la mención de la fuente citada. El contenido no puede ser modificado en forma alguna.

Advertencia y Renuncia de Responsabilidad. Este producto y su documentación están protegidos por los derechos de autor. La información en este documento se proporciona "tal cual", sin garantía. Aunque se han tomado todas las precauciones durante la preparación de este documento, los autores no tendrán responsabilidad alguna ante ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en el mismo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no se hace responsable por el contenido de ningún sitio enlazado. Si usted accede a sitios web de terceros listados en este documento, lo hará bajo su responsabilidad. Bitdefender proporciona estos vínculos solamente para su conveniencia, y la inclusión del enlace no implica la aprobación por parte de Bitdefender o aceptar responsabilidad alguna sobre el contenido del sitio de terceros.

Marcas Registradas. En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.

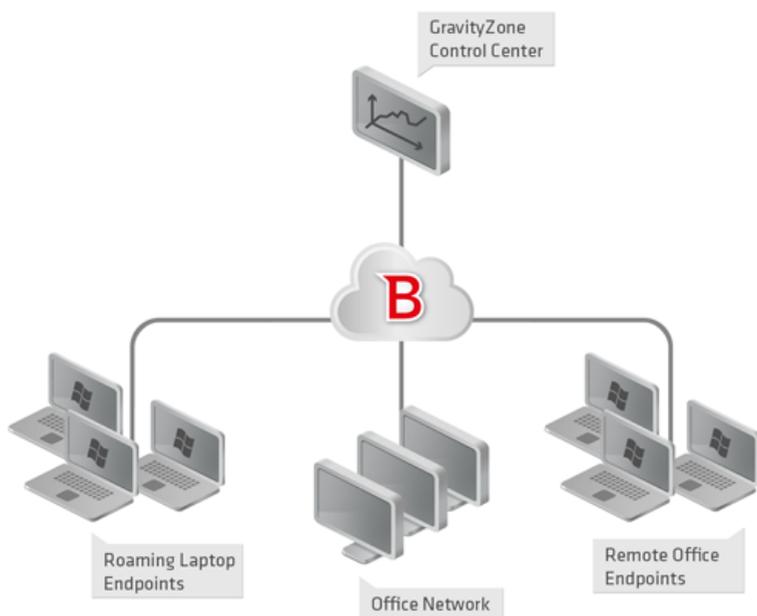


Tabla de contenidos

1. Acerca de Small Office Security	1
2. Iniciando	3
2.1. Conectar a Control Center	3
2.2. Control Center en resumen	3
2.2.1. Datos de tablas	5
2.2.2. Barras de herramientas de acción	6
2.2.3. Menú Contextual	6
2.3. Cambiar la Contraseña de Inicio de Sesión	7
2.4. Gestionar su cuenta	7
3. Panel de monitorización	9
3.1. Actualización de los datos del portlet	10
3.2. Editar los ajustes de portlets	10
3.3. Añadir un nuevo portlet	10
3.4. Eliminar un Portlet	10
3.5. Organizar portlets	11
4. Notificaciones	12
4.1. Tipo de Notificaciones	12
4.2. Ver notificaciones	13
4.3. Borrar notificaciones	15
4.4. Configurar las opciones de notificación	15
5. Usar informes	18
5.1. Tipos de informes disponibles	18
5.2. Creando Informes	21
5.3. Ver y administrar informes programados	23
5.3.1. Visualizando los Informes	25
5.3.2. Editar informes programados	25
5.3.3. Eliminar informes programados	26
5.4. Guardar Informes	26
5.4.1. Exportando los Informes	27
5.4.2. Descarga de informes	27
5.5. Enviar informes por correo	28
5.6. Imprimiendo los Informes	28
6. Registro de actividad del usuario	29
7. Obtener Ayuda	31
Glosario	32

1. Acerca de Small Office Security

Small Office Security es un servicio de protección contra malware basado en la nube desarrollado por Bitdefender para equipos que ejecutan sistemas operativos de Microsoft Windows y Macintosh. Utiliza un modelo centralizado de implementación múltiple de software como servicio adecuado para clientes corporativos, al tiempo que se apoya en tecnología de protección comprobadas en el campo del malware desarrolladas por Bitdefender para el mercado de consumo.



Architecture Small Office Security

El servicio de seguridad es hospedado en la nube pública de Bitdefender. Los suscriptores tienen acceso a una interfaz de administración basada en la web llamada **Control Center**. Desde esta interfaz, los administradores pueden remotamente instalar y administrar la protección contra malware en todos sus equipos basados en Windows y Macintosh como: servidores y estaciones de trabajo dentro de la red interna, puntos finales portátiles itinerantes o puntos finales de oficina remotos.

Una aplicación local llamada **Endpoint Security** se instala en cada equipo protegido. Los usuarios locales tienen visibilidad limitada y acceso de solo lectura a los ajustes de seguridad,

que se administran de manera central por el administrador desde la Control Center; mientras que el análisis, actualización y los cambios de configuración se realizan normalmente en segundo plano.

2. Iniciando

Las soluciones Bitdefender Small Office Security pueden configurarse y gestionarse a través de una plataforma de administración centralizada llamada Control Center. Control Center posee una interfaz Web, a la que puede acceder por medio del nombre de usuario y contraseña.

2.1. Conectar a Control Center

El acceso a Control Center se realiza a través de las cuentas de usuario. Recibirá su información de inicio de sesión por correo una vez que se haya creado su cuenta.

Requisitos:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Resolución de pantalla recomendada: 1024x768 o superior

Para conectarse a Control Center:

1. Abra su navegador Web.
2. Acceda a la siguiente dirección: <https://gravityzone.bitdefender.com>
3. Escriba la dirección de correo y contraseña de su cuenta.
4. Haga clic en **Inicio de sesión**.

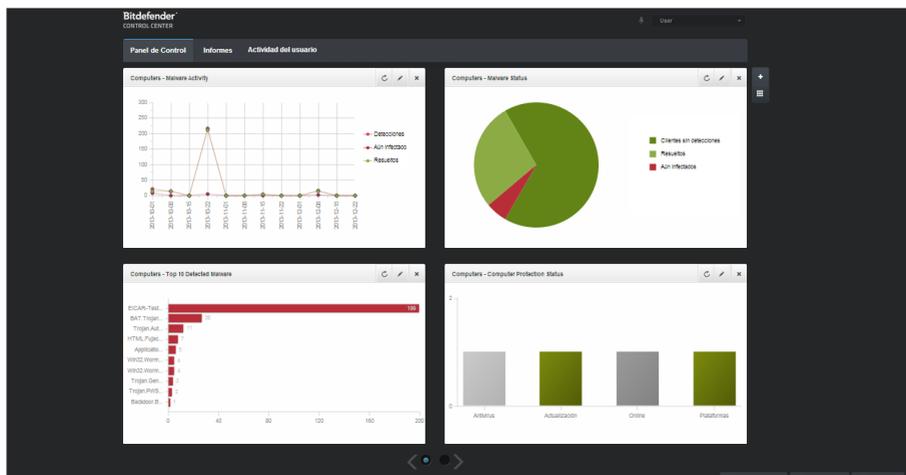


Nota

Si ha olvidado su contraseña, utilice el enlace de recuperación de contraseña para recibir una nueva. Debe proporcionar la dirección de correo de su cuenta.

2.2. Control Center en resumen

Control Center está organizada para permitir el acceso fácil a todas las funciones. Utilice la barra de menú en el área superior para navegar por la consola.



el Panel de control

Los informadores pueden acceder a las siguientes secciones desde la barra de menús:

Panel de Control

Visualice tablas de fácil lectura que proporcionan información clave sobre seguridad referente a su red.

Informes

Conseguir informes de seguridad relativos a los equipos cliente administrados.

Actividad del usuario

Compruebe el registro de actividad del usuario.

Por otra parte, en la esquina superior derecha de la consola, el icono  **Notificaciones** proporciona acceso fácil a los mensajes de notificación y también a la página **Notificaciones**.

Al apuntar sobre su nombre en la esquina superior derecha de la consola, aparecen las siguientes opciones disponibles.

- **Mi cuenta.** Haga clic en esta opción para gestionar sus detalles de la cuenta y las preferencias.
- **Finalizar Sesión.** Haga clic en esta opción para cerrar la sesión de su cuenta.

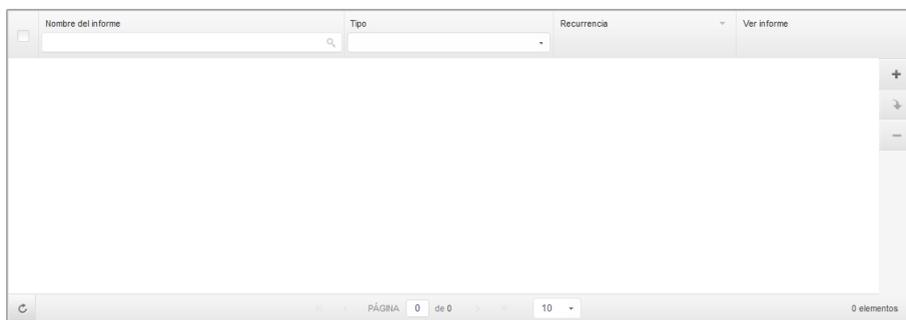
En la esquina inferior derecha de la consola están a su disposición los siguientes enlaces:

- **Ayuda y soporte.** Haga clic en este botón para obtener ayuda e información de soporte.
- **Modo Ayuda.** Haga clic en este botón para habilitar una función de ayuda que proporciona tooltips cuando sitúa el ratón sobre los elementos de Control Center. Hallará información útil referente a la funcionalidad de Control Center.

- **Feedback.** Haga clic en este botón para mostrar un formulario que le permitirá escribir y enviar sus comentarios acerca de su experiencia con Small Office Security.

2.2.1. Datos de tablas

Las tablas se usan frecuentemente en la consola para organizar los datos en un formato más fácil de usar.



La página de Informes - Tabla de informes

Navegar por las páginas

Las tablas con más de 10 entradas se distribuyen en varias páginas. Por omisión, solamente se muestran 10 entradas por página. Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Puede cambiar el número de entradas mostradas en una página seleccionando una opción diferente desde el menú junto a los botones de navegación.

Buscar entradas específicas

Para encontrar fácilmente entradas específicas, utilice los cuadros de búsqueda disponibles bajo los encabezados de las columnas.

Introduzca el término a buscar en el campo correspondiente. Los elementos coincidentes se muestran en la tabla según escribe. Para restablecer el contenido de la tabla, vacíe los campos de búsqueda.

Ordenar datos

Para ordenar datos según una columna específica, haga clic en el encabezado de la columna. Haga clic en el encabezado de la columna para invertir el orden de clasificación.

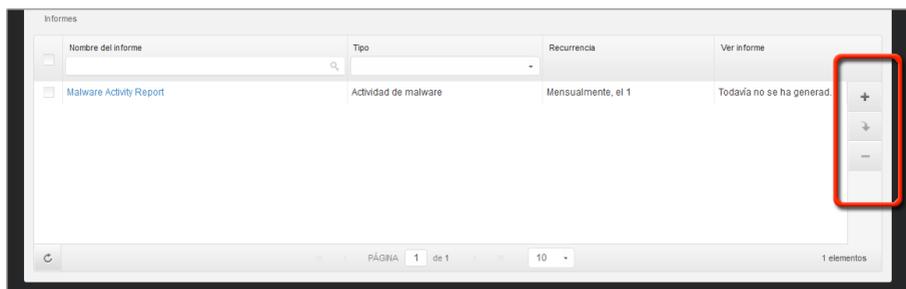
Actualizar los datos de la tabla

Para asegurarse de que la consola muestra la última información, haga clic en el botón **Actualizar** en la esquina inferior izquierda de la tabla.

2.2.2. Barras de herramientas de acción

Dentro de Control Center, las barras de herramientas de acción le permiten realizar operaciones específicas que pertenecen a la sección en la que se encuentra. Cada barra de herramientas consiste en un conjunto de iconos que normalmente se colocan en el lateral derecho de la tabla. Por ejemplo, la barra de herramientas de acción en la sección **Informes** le permite realizar las siguientes operaciones:

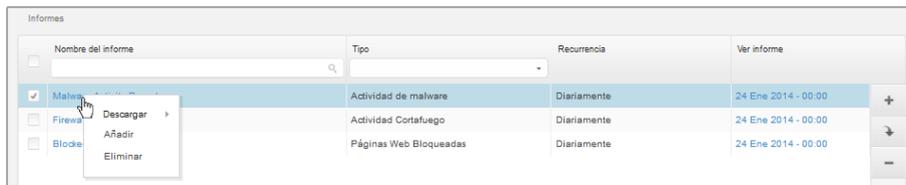
- Crear un nuevo informe.
- Descargar informes generados por un informe programado.
- Eliminar un informe programado.



La página de Informes - Barras de herramientas de acción

2.2.3. Menú Contextual

Desde el menú de contexto también se puede acceder a los comandos de la barra de herramientas. Haga clic con el botón derecho en la sección del Centro de control que esté utilizando y seleccione el comando que precise de la lista disponible.



La página de Informes - Menú contextual

2.3. Cambiar la Contraseña de Inicio de Sesión

Tras haberse creado su cuenta recibirá un correo electrónico con las credenciales de inicio de sesión.

Se recomienda hacer lo siguiente:

- Cambie la contraseña de inicio de sesión por defecto la primera vez que visite Control Center.
- Cambie periódicamente su contraseña de inicio de sesión.

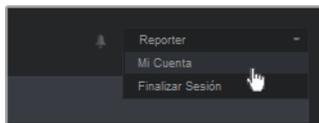
Para cambiar la contraseña de inicio de sesión:

1. Apunte a su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.
2. En **Detalles de cuenta**, haga clic en **Cambiar contraseña**.
3. Escriba su contraseña actual y la nueva contraseña en los campos correspondientes.
4. Haga clic en **Guardar** para aplicar los cambios.

2.4. Gestionar su cuenta

Para consultar o cambiar sus detalles de cuenta y configuración:

1. Apunte a su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.



El menú de Cuenta de usuario

2. Modifique o actualice sus detalles de cuenta en **Detalles de cuenta**.
 - **Nombre y apellidos.** Introduzca su nombre completo.
 - **Correo.** Esta es su dirección de correo de contacto e inicio de sesión. Los informes y notificaciones de seguridad importantes se envían a esta dirección. Las notificaciones de correo se envían automáticamente siempre que se detectan situaciones de riesgo importantes en la red.
 - **Contraseña.** Un enlace **Cambiar contraseña** le permite cambiar su contraseña de inicio de sesión.
3. Configure las opciones de cuenta según sus preferencias en **Configuración**.
 - **Zona horaria.** Elija en el menú la zona horaria de la cuenta. La consola mostrará la información de la hora de acuerdo con la zona horaria seleccionada.
 - **Idioma.** Elija en el menú el idioma de visualización de la consola.

- **Tiempo de espera de sesión.** Seleccione el intervalo de tiempo de inactividad antes de que expire su sesión de usuario.
4. Haga clic en **Guardar** para aplicar los cambios.

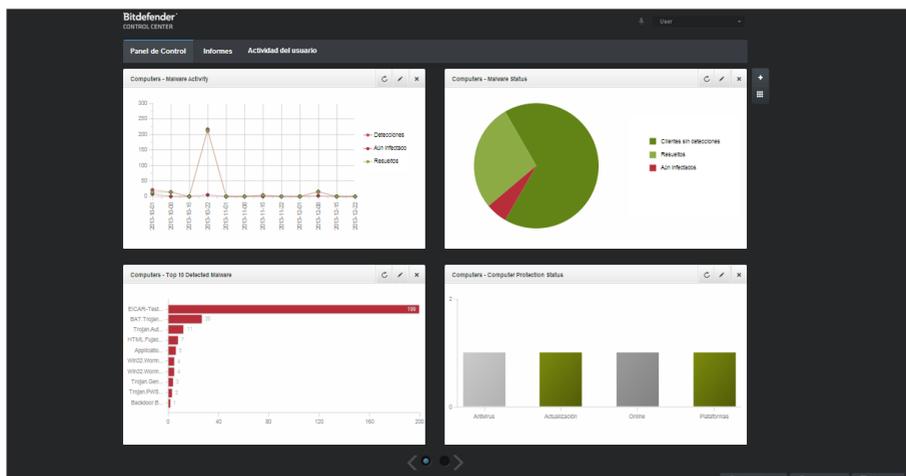
**Nota**

No puede eliminar su propia cuenta.

3. Panel de monitorización

El panel Control Center es una pantalla visual personalizable que proporciona un resumen de seguridad rápido de todos los objetos de la red protegidos.

Los portlets del panel muestran diversa información de seguridad en tiempo real utilizando tablas de fácil lectura, permitiendo así una identificación rápida de cualquier problema que pudiera requerir su atención.



el Panel de control

Esto es lo que necesita saber sobre los portlets del panel de control:

- Control Center viene con varios portlets de panel de control predefinidos.
- Cada portlet del panel incluye un informe detallado en segundo plano, accesible haciendo clic sobre el gráfico.
- Hay varios tipos de portlets que incluyen diversa información sobre la protección de sus objetos de red, como el estado de actualización, el de malware, la actividad del cortafuego, etc. Para obtener más información sobre los tipos de portlet del panel de control, consulte [“Tipos de informes disponibles” \(p. 18\)](#).
- La información mostrada por los portlets se refiere solo a los objetos de red de su cuenta. Puede personalizar el objetivo de cada portlet mediante el comando [Editar portlet](#).
- Haga clic en los elementos de la leyenda, cuando existan, para ocultar o mostrar la variable correspondiente en la gráfica.

- Los portlets se muestran en grupos de cuatro. Utilice el control deslizante situado en la parte inferior de la página para navegar por los grupos de portlets.

El panel de control es fácil de configurar basándose en las preferencias individuales. Puede [editar](#) los ajustes del portlet, [añadir](#) portlets adicionales, [eliminar](#) u [organizar](#) los portlets existentes.

3.1. Actualización de los datos del portlet

Para asegurarse de que el portlet muestra la última información, haga clic en el icono  **Actualizar** de su barra de título.

3.2. Editar los ajustes de portlets

Algunos portlets ofrecen información de estado, mientras otros informan sobre los sucesos de la seguridad en el último periodo. Puede consultar y configurar el periodo de información de un portlet haciendo clic en el icono  **Editar portlet** en su barra de título.

3.3. Añadir un nuevo portlet

Puede añadir portlets adicionales para obtener la información que necesita.

Para añadir un nuevo portlet:

1. Vaya a la página **Panel**.
2. Haga clic en el botón  **Añadir portlet** del lateral derecho del panel. Se muestra la ventana de configuración.
3. En la pestaña **Detalles**, configure los detalles del portlet:
 - Tipo de informe explicativo
 - Nombre de portlet descriptivo
 - Intervalo de actualización

Para obtener más información sobre los tipos de informe disponibles, consulte [“Tipos de informes disponibles”](#) (p. 18).

4. En la pestaña **Objetivos**, seleccione los objetos de red y grupos a incluir.
5. Haga clic en **Guardar**.

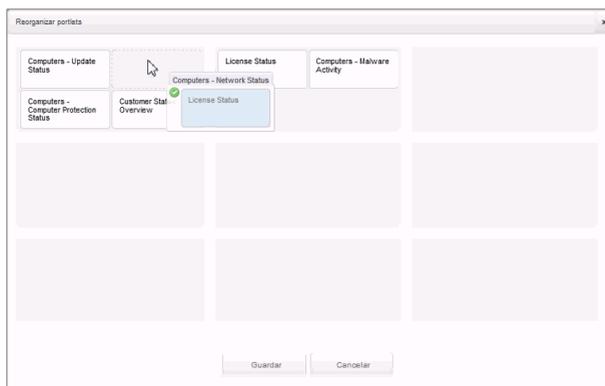
3.4. Eliminar un Portlet

Puede eliminar fácilmente cualquier portlet haciendo clic en el icono  **Eliminar** en su barra de título. Una vez eliminado el portlet, ya no puede recuperarlo. Sin embargo, puede crear otro portlet exactamente con la misma configuración.

3.5. Organizar portlets

Puede organizar los portlets del panel para que se ajusten mejor a sus necesidades. Para organizar los portlets:

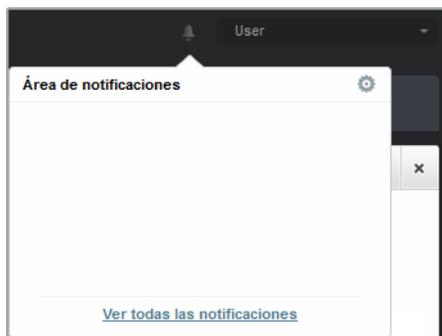
1. Vaya a la página **Panel**.
2. Haga clic en el botón  **Organizar portlets** del lateral derecho del panel. Se muestra la ventana del mapa de portlets.
3. Arrastre y suelte cada portlet en la posición deseada.
4. Haga clic en **Guardar**.



Reorganizar los portlets en el panel de control

4. Notificaciones

Dependiendo de los sucesos que puedan ocurrir en su red, Control Center mostrará diversas notificaciones para informarle del estado de seguridad de su entorno. Las notificaciones se mostrarán en el **Área de notificación**, localizada en el lado superior derecho de la interfaz de Control Center.



Área de notificación

Cuando se detecte un suceso en la red, el área de notificación mostrará  un icono rojo indicando el número de nuevos sucesos detectados. Haciendo clic en el icono se muestra la lista de sucesos detectados.

4.1. Tipo de Notificaciones

Esta es la lista de tipos de notificaciones disponibles:

Brote de malware

Esta notificación se envía a los usuarios que tienen al menos el 5% de todos sus objetos de red infectados por el mismo malware.

Puede configurar el umbral de infección malware en la ventana **Opciones de notificación**. Para más información, diríjase a [“Configurar las opciones de notificación”](#) (p. 15).

La licencia caduca

Esta notificación se envía 30 días, siete días y también un día antes de que caduque la licencia.

Se ha alcanzado el límite de utilización de licencias

Esta notificación se envía cuando se han utilizado todas las licencias disponibles.

Está a punto de alcanzarse el límite de licencia

Esta notificación se envía cuando se ha utilizado el 90% de las licencias disponibles.

Actualización disponible

Esta notificación le informa de la disponibilidad de una nueva actualización de Small Office Security.

Evento de Antiphishing

Esta notificación le informa cada vez que el agente de punto final evita el acceso a una página Web de phishing conocida. Esta notificación también proporciona información, como el punto final que intentó acceder a la página Web peligrosa (nombre e IP), el agente instalado o la URL bloqueada.

Evento de Cortafuego

Con esta notificación se le informa cada vez que el módulo de cortafuego de un agente instalado ha evitado un análisis de puertos o el acceso de una aplicación a la red, de acuerdo con la política aplicada.

Evento de AVC/IDS

Esta notificación se envía cada vez que se detecta y se bloquea una aplicación potencialmente peligrosa en un punto final de la red. También encontrará información sobre el tipo de aplicación peligrosa, su nombre y su ruta.

Evento de Control de usuarios

Esta notificación se activa cada vez que el cliente de punto final bloquea una actividad de los usuarios, como la navegación Web o una aplicación de software de acuerdo con la política aplicada.

Evento de Protección de datos

Esta notificación se envía cada vez que se bloquea el tráfico de datos en un punto final de acuerdo con las reglas de protección de datos.

Evento de Módulos del producto

Esta notificación se envía cada vez que se desactiva un módulo de seguridad de un agente instalado.

Evento de Registro del producto

Esta notificación le informa cuando ha cambiado el estado de registro de un agente instalado en su red.

4.2. Ver notificaciones

Para ver las notificaciones, haga clic en el botón  **Área de notificación** y luego haga clic en **Ver todas las notificaciones**. Se muestra una tabla que contiene todas las notificaciones.

Notificaciones	
Tipo	Creado
<input type="checkbox"/>	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Brote de malware	8 Abr 2013, 20:33:42
<input type="checkbox"/> Brote de malware	8 Abr 2013, 16:42:57
<input type="checkbox"/> Brote de malware	8 Abr 2013, 14:32:31
<input type="checkbox"/> Brote de malware	8 Abr 2013, 12:57:11
<input type="checkbox"/> Brote de malware	8 Abr 2013, 12:32:06
<input type="checkbox"/> Brote de malware	8 Abr 2013, 11:31:54

PÁGINA 1 de 25 > >> 10 243 elementos

La página Notificaciones

Dependiendo del número de notificaciones, la tabla puede distribuirse a lo largo de varias páginas (por defecto solo se muestran 10 entradas por página).

Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla.

Para cambiar el número de entradas mostradas en una página, seleccione una opción desde el menú junto a los botones de navegación.

Si hay muchas entradas, puede utilizar los cuadros de búsqueda bajo los encabezados de las columnas o el menú de filtros en la parte superior de la tabla para filtrar los datos mostrados.

- Para filtrar las notificaciones, seleccione el tipo de notificación que desea ver desde el menú **Tipo**. Opcionalmente, puede seleccionar el intervalo de tiempo durante el cual se generaron las notificaciones, para reducir el número de entradas de la tabla, especialmente si se han generado un número elevado de notificaciones.
- Para ver los detalles de las notificaciones, haga clic en el nombre de la notificación en la tabla. Se muestra una sección de **Detalles** debajo de la tabla, donde puede ver el evento que generó la notificación.

4.3. Borrar notificaciones

Para borrar notificaciones:

1. Haga clic en el botón  **Área de notificación** en el lateral derecho de la barra de menús y luego haga clic en **Ver todas las notificaciones**. Se muestra una tabla que contiene todas las notificaciones.
2. Seleccione las notificaciones que desee eliminar.
3. Haga clic en el botón  **Eliminar** del lateral derecho de la tabla.

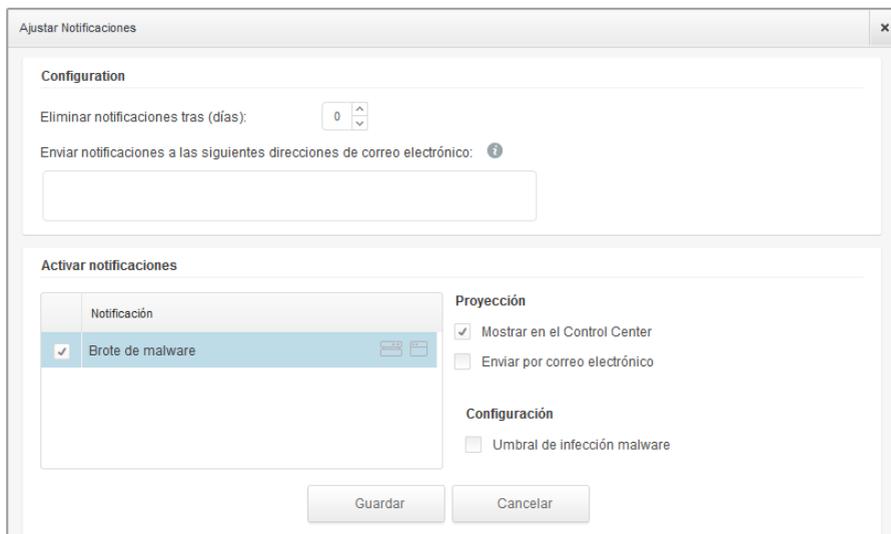
También puede configurar las notificaciones para que se borren automáticamente tras un cierto número de días. Para más información, diríjase a [“Configurar las opciones de notificación”](#) (p. 15).

4.4. Configurar las opciones de notificación

Para cada usuario, puede configurarse el tipo de notificaciones a enviar y las direcciones de correo de envío.

Para configurar las opciones de notificación:

1. Haga clic en el botón  **Área de notificación** en el lateral derecho de la barra de menús y luego haga clic en **Ver todas las notificaciones**. Se muestra una tabla que contiene todas las notificaciones.
2. Haga clic en el botón  **Configurar** del lateral derecho de la tabla. Se mostrará la ventana **Opciones de notificación**.



Ajustar Notificaciones



Nota

También puede acceder a la ventana de **Opciones de notificación** directamente mediante el icono  **Configurar** de la esquina superior derecha de la ventana **Área de notificación**.

3. En la sección **Configuración** puede definir los siguientes ajustes:

- Puede configurar las notificaciones para que se borren automáticamente tras un cierto número de días. Introduzca el número de días que desee en el campo **Eliminar notificaciones tras (días)**.
- Opcionalmente, puede elegir enviar las notificaciones por email a direcciones de correo específicas. Escriba las direcciones de correo en el campo correspondiente, pulsando la tecla **Intro** después de cada dirección.

4. En la sección **Activar notificaciones** puede elegir el tipo de notificaciones que desea recibir de Small Office Security. También puede configurar la visibilidad y las opciones de envío de forma individual para cada tipo de notificación.

Seleccione en la lista el tipo de notificación que desee. Para más información, diríjase a [“Tipo de Notificaciones”](#) (p. 12). Al seleccionar un tipo de notificación, puede configurar sus opciones concretas en la zona de la derecha:

- **Mostrar en consola** especifica que este tipo de eventos se muestra en Control Center, con la ayuda del icono  del **Área de notificación**.

- **Enviar por correo electrónico** especifica que este tipo de eventos también se envía a determinadas direcciones de correo electrónico. En este caso, se le pedirá que introduzca las direcciones de correo electrónico en el campo correspondiente, pulsando `Intro` después de cada dirección.



Nota

Por defecto, la Notificación de infección malware se envía a los usuarios que tienen al menos el 5% de todos sus objetos de red administrados infectados por el mismo malware. Para cambiar el umbral de infección malware, seleccione la opción **Usar umbral personalizado** y, a continuación, introduzca el valor que desee en el campo **Umbral de infección malware**.

5. Haga clic en **Guardar**.

5. Usar informes

Control Center le permite crear y visualizar informes centralizados sobre el estado de seguridad de los objetos de red administrados. Los informes pueden usarse para múltiples propósitos, tales como:

- Monitorizar y asegurar el cumplimiento de las políticas de seguridad de la empresa.
- Comprobar y evaluar el estado de seguridad de la red.
- Identificar los problemas de seguridad, amenazas y vulnerabilidades de la red.
- Monitorizar los incidentes de seguridad y la actividad malware.
- Proporcionar una administración superior con datos de fácil interpretación sobre la seguridad de la red.

Hay disponibles varios tipos de informes diferentes para que pueda conseguir fácilmente la información que necesita. La información se presenta como gráficos y tablas interactivas de fácil lectura, que le permiten una comprobación rápida del estado de seguridad de la red e identificar incidencias en la seguridad.

Los informes pueden consolidar información de toda la red de objetos de red administrados o únicamente de grupos concretos. De este modo, en un sólo informe puede encontrar la siguiente información:

- Datos estadísticos sobre todos o grupos de elementos de red administrados.
- Información detallada para cada objeto de red administrado.
- La lista de equipos que cumplen un criterio específico (por ejemplo, aquellos que tienen desactivada la protección antimalware).

Todos los informes programados están disponibles en Control Center pero puede guardarlos en su equipo o enviarlos por correo.

Los formatos disponibles incluyen Portable Document Format (PDF) y Comma-Separated Values (CSV).

5.1. Tipos de informes disponibles

Esta es la lista de tipos de informe disponibles para equipos:

Actualización

Le muestra el estado de actualización de la protección de Endpoint Security instalada en los equipos seleccionados. El estado de actualización se refiere a la versión del producto y versión del motor (firmas).

Mediante los filtros disponibles, puede descubrir fácilmente qué clientes se han actualizado o no en las últimas 24 horas.

Actividad de malware

Le proporciona información general sobre las amenazas de malware detectadas durante un periodo de tiempo dado en los equipos seleccionados. Puede ver:

- Número de detecciones (archivos que se han encontrado infectados con malware)
- Número de infecciones resueltas (archivos que han sido desinfectados correctamente o movidos a la cuarentena)
- Número de infecciones sin resolver (archivos que no pudieron desinfectarse, pero a los que se ha denegado el acceso; por ejemplo, un archivo infectado almacenado en algún formato de archivo propietario)

Por cada amenaza detectada, si hace clic en los enlaces disponibles en las columnas de resultados de desinfección, podrá ver la lista de los equipos afectados y las rutas de los archivos. Por ejemplo, si hace clic en el número de la columna **Resueltos**, verá los archivos y los equipos de los que se eliminó la amenaza.

Estado del Malware

Le ayuda a encontrar cuántos y cuáles de los equipos seleccionados han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas.

Los equipos se agrupan basándose en estos criterios:

- Equipos sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)
- Equipos con problemas de malware solucionados (todos los archivos detectados han sido desinfectados correctamente o movidos a la cuarentena)
- Equipos aún infectados con malware (se ha rechazado el acceso a alguno de los archivos detectados)

Por cada equipo, si hace clic en los enlaces disponibles en las columnas de resultados de desinfección, podrá ver la lista de amenazas y las rutas de los archivos afectados.

Estado de la Red

Le proporciona información detallada sobre el estado de seguridad general de los equipos seleccionados. Los equipos se agrupan basándose en estos criterios:

- Estado de incidencias
- Estado de administración
- Estado de infección
- Estado de protección antimulware
- Estado actualización de producto
- Estado de licencia
- Estado de la actividad de la red para cada equipo (conectado/desconectado). Si el equipo está desconectado cuando se genera el informe, verá la fecha y hora en la que Control Center lo vio conectado por última vez.

Los equipos más infectados

Muestra los equipos más infectados en número total de detecciones durante un periodo de tiempo específico de los equipos seleccionados.



Nota

La tabla de detalles muestra todo el malware detectado en los equipos más infectados.

Malware más detectado

Le muestra las amenazas malware más detectadas en un periodo de tiempo específico en los equipos seleccionados.



Nota

La tabla de detalles muestra todos los equipos infectados por el malware más frecuentemente detectado.

Actividad Cortafuego

Le informa sobre la actividad del módulo de Cortafuego de Endpoint Security. Puede ver el número de intentos de tráfico bloqueados y análisis de puertos bloqueados en los equipos seleccionados.

Páginas Web Bloqueadas

Le informa sobre la actividad del módulo de Control de acceso Web de Endpoint Security. Puede ver el número de sitios Web bloqueados en los equipos seleccionados.

Aplicaciones Bloqueadas

Le informa sobre la actividad del módulo de Control de aplicaciones de Endpoint Security. Puede ver el número de aplicaciones bloqueadas en los equipos seleccionados.

Actividad antiphishing

Le informa sobre la actividad del módulo de Antiphishing de Endpoint Security. Puede ver el número de sitios Web bloqueados en los equipos seleccionados.

Estado de protección del equipo

Le proporciona diversa información del estado de los equipos seleccionados de su red.

- Estado de protección antimalware
- Estado de actualización de Endpoint Security
- Estado de actividad de la red (online/offline)
- Estado de administración

Puede aplicar filtros según aspectos de la seguridad y estado para encontrar la información que está buscando.

Protección de datos

Le informa sobre la actividad del módulo de Protección de datos de Endpoint Security. Puede ver el número de mensajes de correo y sitios Web bloqueados en los equipos seleccionados.

Aplicaciones bloqueadas por el análisis de comportamiento

Le informa acerca de las aplicaciones bloqueadas por AVC (Active Virus Control) / IDS (Sistema de detección de intrusos). Puede ver el número de aplicaciones bloqueadas por AVC / IDS para cada equipo seleccionado. Haga clic en el número de aplicaciones bloqueadas del equipo del cual quiera ver la lista de aplicaciones bloqueadas y su información correspondiente (nombre de la aplicación, el motivo por el que ha sido bloqueada, el número de intentos bloqueados y la fecha y hora del último intento bloqueado).

Estado de los módulos de punto final

Proporciona una visión general del estado de los módulos de protección de Endpoint Security para los equipos seleccionados. Puede ver qué módulos están activos y cuáles deshabilitados o no instalados.

5.2. Creando Informes

Puede crear dos categorías de informes:

- **Informes instantáneos.** Los informes instantáneos se muestran automáticamente una vez generados.
- **Informes programados.** Los informes programados pueden configurarse para que se ejecuten en una hora y fecha especificada y se muestra una lista de todos los informes programados en la página **Informes**.



Importante

Los informes instantáneos se eliminan automáticamente cuando cierra la página del informe. Los informes programados se guardan y muestran en la página **Informes**.

Para crear un informe:

1. Diríjase a la página **Informes**.
2. Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.

Crear Informe

Detalles

Tipo:

Nombre: *

Configuración

Ahora

Programado

Ocurrencia:

El día:

Hora de inicio: :

Intervalo de informe:

Mostrar:

Todo el malware

Sólo malware sin resolver

Entregar: Enviar por correo a las

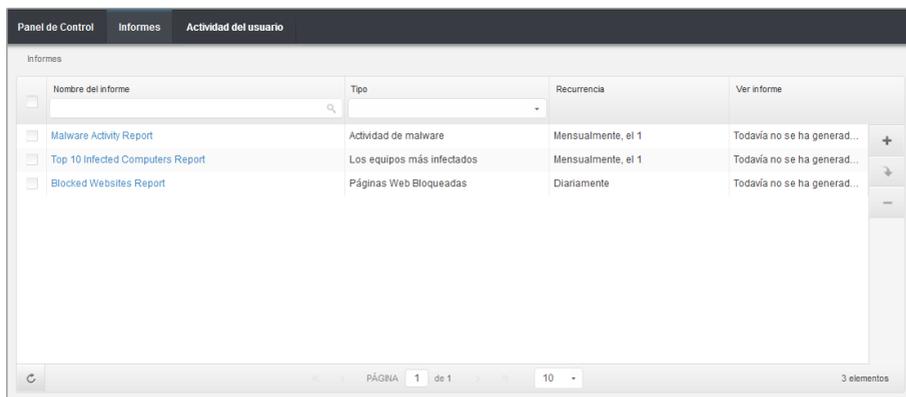
Opciones de informes de equipos

3. Seleccione el tipo de informe deseado desde el menú. Para más información, diríjase a [“Tipos de informes disponibles”](#) (p. 18).
4. Escriba un nombre descriptivo para el informe. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.
5. Configure la recurrencia del informe:
 - Seleccione **Ahora** para crear un informe instantáneo.
 - Seleccione **Programado** para establecer que el informe se genere automáticamente en el intervalo de tiempo que desee:
 - Cada hora, en el intervalo especificado entre horas.
 - Diariamente. En este caso, también puede establecer la hora de inicio (horas y minutos).

- Semanalmente, en los días especificados de la semana y a la hora de inicio seleccionada (horas y minutos).
 - Mensualmente, en los días especificados del mes y a la hora de inicio seleccionada (horas y minutos).
6. Para la mayoría de tipos de informe debe especificar el intervalo de tiempo al que se refieren los datos que contienen. El informe mostrará únicamente información sobre el periodo de tiempo seleccionado.
7. Varios tipos de informes ofrecen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Utilice las opciones de filtrado en la sección **Mostrar** para obtener únicamente la información deseada.
- Por ejemplo, para un informe de **Estado de actualización** puede seleccionar ver únicamente la lista de equipos que se han actualizado en el periodo de tiempo seleccionado, o aquellos que necesitan reiniciarse para completar la actualización.
8. **Entregar.** Para recibir un informe programado por email, seleccione la opción correspondiente. Introduzca las direcciones de correo electrónico que desee en el campo de abajo.
9. **Seleccionar objetivo.** Desplácese hacia abajo para configurar el objetivo del informe. Seleccione el grupo sobre el que quiere generar un informe.
10. Haga clic en **Generar** para crear un informe instantáneo o **Guardar** para crear un informe programado.
- Si ha elegido crear un informe instantáneo, se mostrará inmediatamente después de hacer clic en **Generar**. El tiempo requerido para crear los informes puede variar dependiendo del número de equipos administrados. Por favor, espere a que finalice la creación del informe.
 - Si ha elegido crear un informe programado, se mostrará en la lista de la página **Informes**. Una vez que se haya generado el informe, puede verlo haciendo clic en su enlace correspondiente en la columna **Ver informe** de la página **Informes**.

5.3. Ver y administrar informes programados

Para ver y administrar los informes programados, diríjase a la página **Informes**.



Nombre del informe	Tipo	Recurrencia	Ver informe
Malware Activity Report	Actividad de malware	Mensualmente, el 1	Todavía no se ha generad...
Top 10 Infected Computers Report	Los equipos más infectados	Mensualmente, el 1	Todavía no se ha generad...
Blocked Websites Report	Páginas Web Bloqueadas	Diariamente	Todavía no se ha generad...

La página Informes

Todos los informes programados se muestran en una tabla. Puede ver los informes programados generados así como información útil sobre ellos:

- Nombre del informe y tipo.
- Cuándo se generará el informe.



Nota

Los informes programados solo están disponibles para el usuario que los haya creado.

Para ordenar los informes según una columna específica, haga clic en el encabezado de esa columna. Haga clic en el encabezado de la columna nuevamente para cambiar el sentido de ordenación.

Los detalles del informe se muestran en una tabla que consiste en varias columnas que ofrecen variada información. La tabla puede distribirse en varias páginas (por omisión se muestran únicamente 10 entradas por página). Para navegar por las páginas de detalle, use los botones en la parte inferior de la tabla.

Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna.

Para ordenar los detalles del informe según una columna específica, simplemente haga clic en el encabezado de esa columna. Haga clic en el encabezado de la columna nuevamente para cambiar el sentido de ordenación.

Para vaciar un cuadro de búsqueda, sitúe el cursor sobre él y haga clic en el icono **Borrar**.

Para asegurar que se muestra la última información, haga clic en el icono **Actualizar** en la esquina inferior izquierda de la tabla.

5.3.1. Visualizando los Informes

Para ver un informe:

1. Diríjase a la página **Informes**.
2. Ordene informes por nombre, tipo o recurrencia para hallar fácilmente el informe que busque.
3. Haga clic en el enlace correspondiente de la columna **Ver informe** para mostrar el informe.

Todos los informes constan de una sección de resumen (la mitad superior de la página del informe) y una sección de detalles (la mitad inferior de la página del informe).

- La sección de resumen le proporciona datos estadísticos (gráficos circulares y diagramas) para todos los grupos u objetos de red objetivo, así como información general sobre el informe, como el periodo del informe (si procede), objetivo del informe, etc.
- La sección de detalles le proporciona información detallada para cada objeto de red administrado.



Nota

- Para configurar la información mostrada en el gráfico, haga clic en los elementos de la leyenda para mostrar u ocultar los datos seleccionados.
- Haga clic en el área del gráfico que le interese para ver los detalles correspondientes en la tabla situada debajo del mismo.

5.3.2. Editar informes programados



Nota

Al editar un informe programado, cualquier actualización se aplicará al comienzo de cada repetición de informes. Los informes generados anteriormente no se verán afectados por la edición.

Para cambiar la configuración de un informe programado:

1. Diríjase a la página **Informes**.
2. Haga clic en el nombre del informe.
3. Cambiar los ajustes del informe según sea necesario. Puede cambiar lo siguiente:
 - **Nombre del informe.** Elija un nombre descriptivo para el informe para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe. Los informes generados por un informe programado basan en él su nombre.
 - **Recurrencia del informe (programación).** Puede programar el informe para que se genere automáticamente cada hora (en un intervalo de horas determinado), todos

los días (con una hora de inicio concreta), semanalmente (en un día y hora de inicio específicos de la semana) o mensualmente (en un día y hora de inicio concretos del mes). Dependiendo del programa seleccionado, el informe incluirá sólo datos del último día, semana o mes, respectivamente.

- **Configuración.**

- Puede programar el informe para que se genere automáticamente cada hora (en un intervalo de horas determinado), todos los días (con una hora de inicio concreta), semanalmente (en un día y hora de inicio específicos de la semana) o mensualmente (en un día y hora de inicio concretos del mes). Dependiendo del programa seleccionado, el informe incluirá sólo datos del último día, semana o mes, respectivamente.
- El informe solo incluirá datos del intervalo de tiempo seleccionado. Puede cambiar el intervalo empezando con la siguiente repetición.
- La mayoría de informes poseen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Cuando visualiza el informe en la consola, toda la información está disponible, independientemente de las opciones seleccionadas. Sin embargo, si descarga o envía por correo el informe, solamente se incluirá en el archivo PDF el resumen del informe y la información seleccionada. Los detalles del informe solo estarán disponibles en formato CSV.
- Puede elegir recibir el informe por email.

- **Seleccionar objetivo.** La opción seleccionada indica el tipo de objetivo del informe actual (ya sean grupos u objetos de red individuales). Haga clic en el enlace correspondiente para ver el objetivo de informe actual. Para cambiarlo, seleccione los objetos de red o grupos a incluir en el informe.

4. Haga clic en **Guardar** para aplicar los cambios.

5.3.3. Eliminar informes programados

Cuando ya no se necesita un informe programado, lo mejor es eliminarlo. Al eliminar un informe programado se eliminarán todos los informes que se han generado automáticamente hasta ese punto.

Para eliminar un informe programado:

1. Diríjase a la página **Informes**.
2. Seleccione el informe que desea eliminar.
3. Haga clic en el botón  **Borrar** del lateral derecho de la tabla.

5.4. Guardar Informes

Por omisión, los informes programados se guardan automáticamente en Control Center.

Si necesita que los informes estén disponibles durante periodos de tiempo más largos, puede guardarlos en su equipo. El resumen del informe estará disponible en formato PDF, mientras que los detalles del informe estarán disponibles solo en formato CSV.

Dispone de dos formas de guardar informes:

- [Aceptar](#)
- [Descargar](#)

5.4.1. Exportando los Informes

Para exportar el informe a su equipo:

1. Haga clic en el botón **Exportar** en la esquina superior derecha de la página de informe.

The screenshot shows a web interface titled 'Informes'. In the top right corner, there are two buttons: 'Aceptar' (highlighted with a red box) and 'Correo'. The main content area is titled 'Informe de estado de actualización' and contains the following details:

- Generado por: reporter@bd.com
- Activado: 21 Ene 2014, 18:34:27
- Recurrencia: Ahora
- Periodo de informe: Últimas 24 horas
- Intervalo del informe: 20 Ene 2014, 18:34 - 21 Ene 2014, 18:34
- Objetivos: Documentation

To the right of the text is a pie chart with a legend:

- Reinicio pendiente (light green)
- Actualizados (dark green)
- Obsoleto (red)

Below the pie chart is a table with the following columns: nombre, ip, Actualización, Versión del producto, Última actualización, Versión de los motores, and Nombre Empresa.

nombre	ip	Actualización	Versión del producto	Última actualización	Versión de los motores	Nombre Empresa
DOC-XP	10.0.2.15	Reinicio pendiente	5.3.3.358	16 Ene 2014, 13:09:48	7.52689 (108255...)	Documentation

Informes - Opción de exportación

2. Seleccione el formato del informe deseado:
 - Portable Document Format (PDF) o
 - Comma Separated Values (CSV)
3. Dependiendo de la configuración de su navegador, puede que su archivo se descargue automáticamente a una ubicación de descarga predeterminada, o que aparezca una ventana de descarga en la que deberá indicar la carpeta de destino.

5.4.2. Descarga de informes

Un archivo de informe contiene tanto el resumen del informe como los detalles del mismo. Para descargar un archivo de informe:

1. Diríjase a la página **Informes**.
2. Seleccione el informe que desea guardar.

3. Haga clic en el botón  **Descargar** y seleccione **Instancia última** para descargar la última instancia generada del informe, o bien **Archivo completo** para descargar un archivo que contenga todas las instancias.

Dependiendo de la configuración de su navegador, puede que su archivo se descargue automáticamente a una ubicación de descarga predeterminada, o que aparezca una ventana de descarga en la que deberá indicar la carpeta de destino.

5.5. Enviar informes por correo

Puede enviar informes por e-mail con las siguientes opciones:

1. Para enviar por correo el informe que está viendo, haga clic en el botón **Email** en la esquina superior derecha de la página del informe. El informe se enviará a la dirección de correo asociada con su cuenta.
2. Para configurar el envío por e-mail de los informes planificados deseados:
 - a. Diríjase a la página **Informes**.
 - b. Haga clic en el nombre del informe deseado.
 - c. En **Opciones > Entrega**, seleccione **Enviar por correo a**.
 - d. Proporcione la dirección de e-mail deseada en el campo inferior. Puede añadir tantas direcciones de e-mail como desee.
 - e. Haga clic en **Guardar**.



Nota

El archivo PDF enviado por e-mail solo incluirá el resumen del informe y el gráfico. Los detalles del informe estarán disponibles en el archivo CSV.

5.6. Imprimiendo los Informes

Control Center no soporta actualmente la funcionalidad de un botón para imprimir. Para imprimir un informe, primero debe guardarlo en su equipo.

6. Registro de actividad del usuario

Control Center registra todas las operaciones y acciones ejecutadas por los usuarios. La lista de actividad del usuario incluye los siguientes eventos, en función de su nivel de privilegios administrativos:

- Iniciar y cerrar sesión
- Crear, editar, renombrar y eliminar informes
- Añadir y eliminar portlets del panel

Para examinar los registros de actividad del usuario, acceda a la página **Cuentas > Actividad del usuario**.

Usuario	Rol	Acción	Área	Objetivo	Creado
---------	-----	--------	------	----------	--------

La página de actividad del usuario

Para mostrar los eventos registrados que le interesen ha de definir una búsqueda. Complete los campos disponibles con el criterio de búsqueda y haga clic en el botón **Buscar**. Todos los registros que cumplan sus criterios se mostrarán en la tabla.

Las columnas de la tabla le proporcionan información sobre los eventos listados:

- El nombre de usuario de quien llevó a cabo la acción.
- Función del usuario.
- Acción que produjo el evento.
- Tipo de objeto de la consola afectado por la acción.
- Objeto de consola concreto afectado por la acción.
- Hora en la que sucedió el evento.

Para ordenar eventos por una columna específica, simplemente haga clic en el encabezado de esa columna. Haga clic en el encabezado de la columna nuevamente para invertir el sentido de ordenación.

Para ver información detallada sobre un evento, selecciónelo y compruebe la sección bajo la tabla.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

7. Obtener Ayuda

Para cualquier problema o pregunta relativa a Control Center, contacte con un administrador.

Glosario

Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender posee su propio módulo de actualización que le permite comprobar manualmente las actualizaciones, o actualizar automáticamente el producto.

Adware

El adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95, la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

Backdoor

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Explorador

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer. Ambos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Extensión de un archivo

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Firma malware

Las firmas de malware son fragmentos de código extraídos de muestras reales de malware. Los programas antivirus las utilizan para realizar el reconocimiento de patrones y la detección de malware. Las firmas también se utilizan para eliminar el código malware de los archivos infectados.

La Base de Datos de Firmas Malware de Bitdefender es una colección de firmas de malware actualizada cada hora por los investigadores de malware de Bitdefender.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.

Heurístico

Un método basado en reglas para identificar nuevos virus. Este método de análisis no se basa en firmas de virus específicas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de un virus existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Malware

Malware es el término genérico que define al software diseñado para causar daños - una contracción de 'malicious software'. Todavía no se usa de forma universal, pero su popularidad como término general para definir virus, troyanos, gusanos y código móvil malicioso está creciendo.

No Heurístico

Este método de análisis se basa en firmas de virus específicas. La ventaja del análisis no heurístico es que no se le puede engañar con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

Phishing

El acto de enviar un email a un usuario simulando pertenecer a una empresa legítima e intentar estafar al usuario solicitándole información privada que después se utilizará para realizar el robo de identidad. El email conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, de la seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y hacía referencia a herramientas recompiladas que proporcionaba a los intrusos de derechos de administrador, permitiéndoles ocultar su presencia para no ser visto por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periférica, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Spam

Correo basura o los posts basura en los grupos de noticias. Se conoce generalmente como correo no solicitado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información sobre direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término viene de la historia de la lliada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como

oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar Troya.

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Virus de boot

Es un virus que infecta el sector de arranque hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

Virus de macro

Es un tipo de virus informático que se encuentra codificado como una macro incluida en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir un macro en un documento y también que el macro se ejecute cada vez que se abra el documento.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.