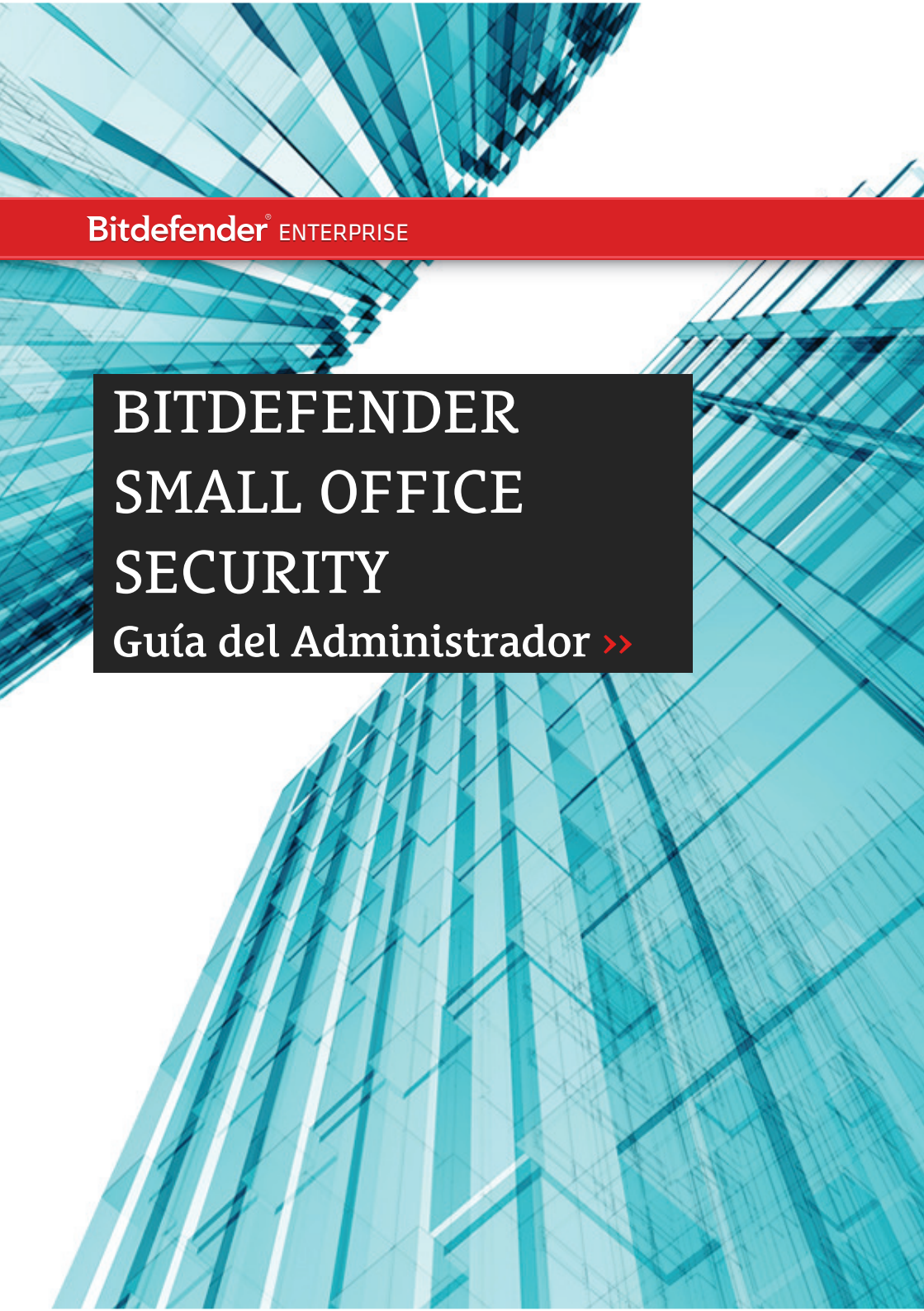

Bitdefender® ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Guía del Administrador ››

Bitdefender Small Office Security
Guía del Administrador

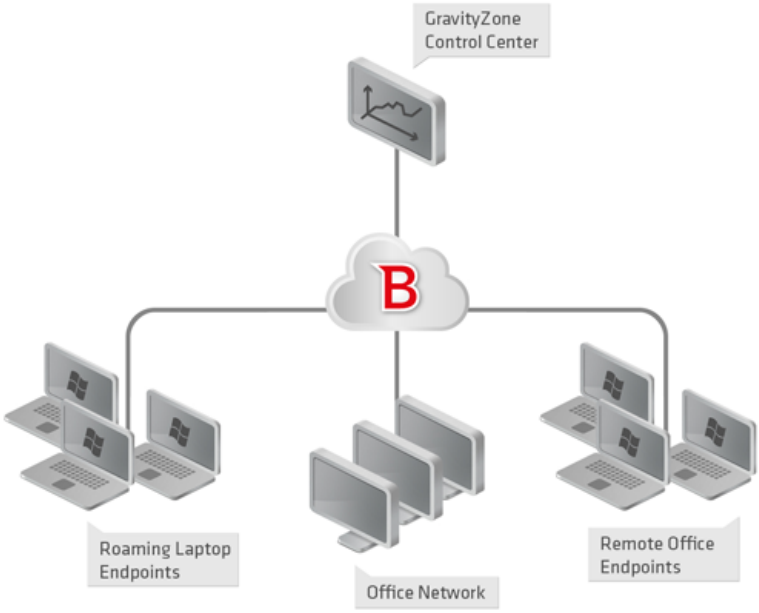
fecha de publicación 2015.01.22


Bitdefender

Tabla de contenidos

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 hosteado 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 características de 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

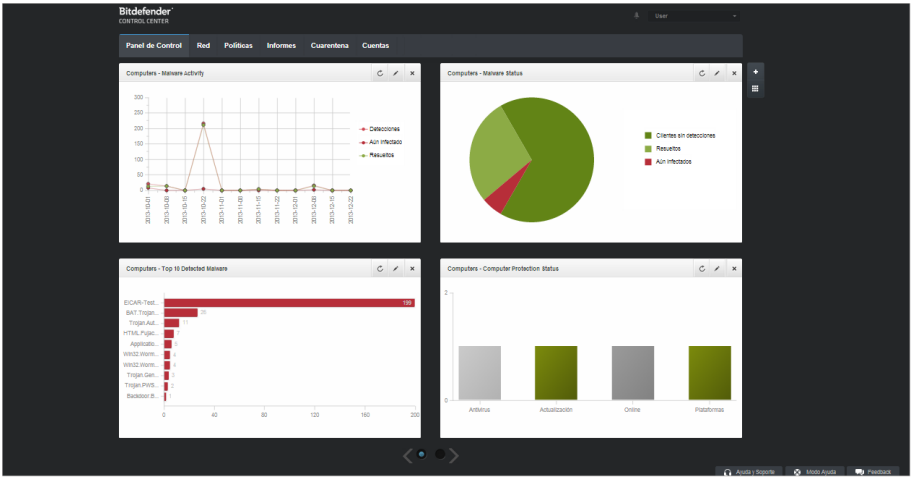
Para conectarse a Control Center:

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. Las características disponibles dependen del tipo de usuario que accede a la consola.



el Panel de control

2.2.1. Descripción general de Control Center

Los usuarios con rol de administrador de empresa tienen todos los privilegios para la configuración de Control Center y los ajustes de seguridad de red, mientras que los usuarios con rol de administrador tienen acceso a las características de seguridad de red, incluyendo la administración de usuarios.

En función de su rol, los administradores de Small Office Security 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.

Red
Instalar protección, aplicar políticas para gestionar las opciones de seguridad, ejecutar tareas de forma remota y crear informes rápidos.

Políticas
Crear y administrar las políticas de seguridad.

Informes
Conseguir informes de seguridad relativos a los equipos cliente administrados.

Cuarentena
Administrar de forma remota los archivos en cuarentena.

Cuentas
Administrar el acceso a Control Center para otros empleados de la empresa.

Nota
Este menú solo está disponible para usuarios con privilegios de Administración de usuarios.

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.

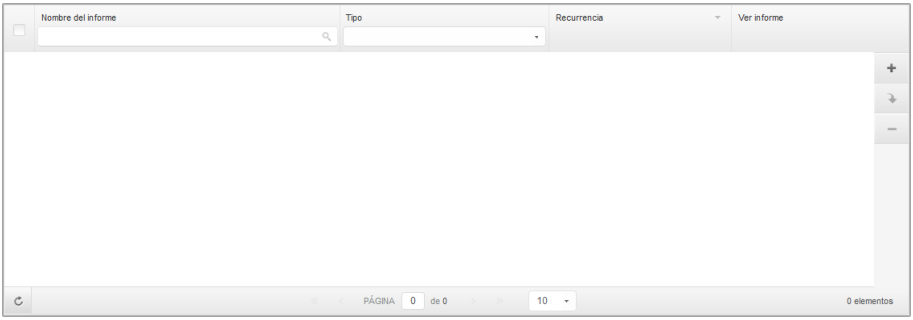
- **Mi cuenta**. Haga clic en esta opción para gestionar sus detalles de la cuenta y las preferencias.
- **Mi Empresa**. Haga clic en esta opción para gestionar la información de su cuenta de empresa y sus preferencias.
- **Administrador de Credenciales**. Haga clic en esta opción para añadir y administrar las credenciales de autenticación necesarias para tareas de instalación remotas.
- **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 las características 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.

2.2.2. 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

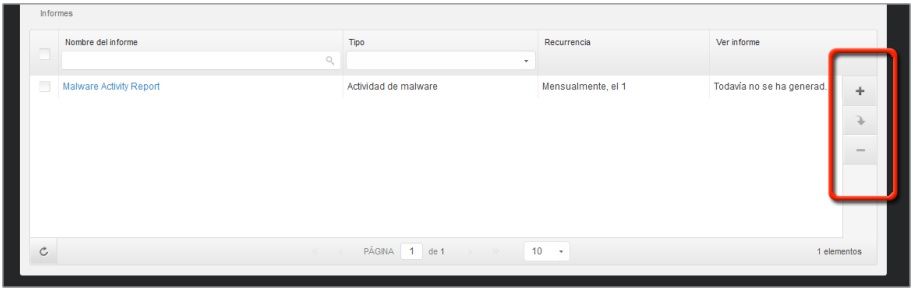
Para asegurarse de que la consola muestra la última información, haga clic en el botón **Actualizar** en la esquina inferior izquierda de la tabla.

2.2.3. 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:

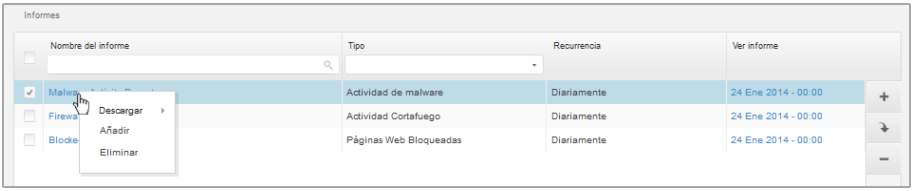
- Crear un nuevo informe.
- Descargar informes generados por un informe programado.
- Eliminar un informe programado.



La página de Informes - Barras de herramientas de acción

2.2.4. 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.

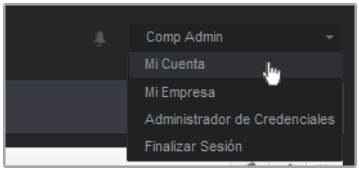


La página de Informes - Menú contextual

2.3. 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

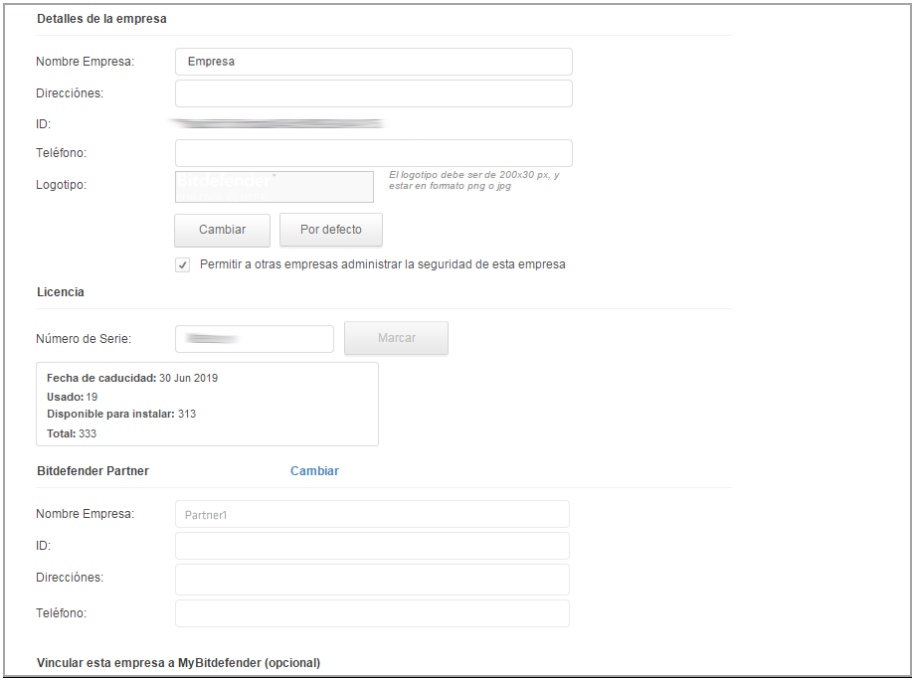
2. Modifique o actualice sus detalles de cuenta en **Detalles de cuenta**.
   - **Nombre y apellidos.** Introduzca su nombre completo.
   - **Correo.** Esta es su dirección de correo de contacto e inicio de sesión. Los informes y notificaciones de seguridad importantes se envían a esta dirección. Las 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.

2.4. Administración de su empresa

Como usuario con rol de Administrador de empresa, puede comprobar o modificar los datos de su empresa y la configuración de la licencia:

1. Señale su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.



Mi página de empresa

2. En **Detalles de la empresa**, introduzca la información de su empresa, como por ejemplo el nombre de la empresa, la dirección y el teléfono.
3. Puede cambiar el logotipo que aparece en Control Center y también en los informes de su empresa y en las notificaciones de correo electrónico como se indica a continuación:
   - Haga clic en **Cambiar** para buscar el logotipo en su equipo. El formato de archivo de imagen debe ser .png o .jpg y el tamaño de la imagen ha de ser 200x30 píxeles.
   - Haga clic en **Predeterminada** para borrar la imagen y restaurar la proporcionada por Bitdefender.
4. Por defecto, su empresa puede ser administrada por las cuentas de partner de otras empresas que puedan tener a la suya en su Bitdefender Control Center. Puede bloquear el acceso de esas empresas a su red deshabilitando la opción **Permitir a otras empresas administrar la seguridad de esta empresa**. Una vez hecho esto, su red ya no será visible en la Control Center de otras empresas y ya no podrán administrar su suscripción.
5. Puede consultar y modificar los detalles de su licencia en la sección **Licencia**.
   - Para añadir una nueva clave de licencia:
     a. En el **menú Tipo**, seleccione un tipo de suscripción de **licencia**.

b. Introduzca la licencia en el campo **Clave de licencia**.

c. Haga clic en el botón **Comprobar** y espere a que Control Center recupere la información acerca de la clave de licencia introducida.

- Para verificar los detalles de su clave de licencia, consulte la información que se muestra debajo de la clave de licencia:
  - **Fecha de caducidad**: la fecha hasta la cual se puede utilizar la clave de licencia.
  - **Utilizado**: el número de puestos utilizados de la cantidad total de puestos de la clave de licencia. Un puesto de licencia se utiliza cuando se ha instalado el cliente de Bitdefender en un punto final de la red bajo su administración.
  - **Disponible para instalar**: el número de puestos libres de la cantidad total de puestos de un grupo de licencias mensuales (excluyendo los puestos utilizados).
  - **Total**: el número total de puestos de licencia disponibles para su suscripción.

6. En **Partner de Bitdefender** puede encontrar información acerca de su empresa proveedora de servicios.

   Para cambiar su proveedor de servicios administrados:

   a. Haga clic en el botón **Cambiar**.

   b. Introduzca el ID de empresa del partner en el campo **ID del partner**.

   Nota
   Todas las empresas puede encontrar su ID en la página **Mi empresa**. Una vez que haya llegado a un acuerdo con una empresa partner, su representante debe proporcionarle su ID del Control Center.

   c. Haga clic en **Guardar**.

   Una vez hecho esto, su empresa se traslada automáticamente de la Control Center del partner anterior a la del nuevo.

7. Opcionalmente, puede vincular su empresa a su cuenta de MyBitdefender mediante los campos proporcionados.
8. Haga clic en **Guardar** para aplicar los cambios.

2.5. Cambiar la Contraseña de Inicio de Sesión

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

- 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:

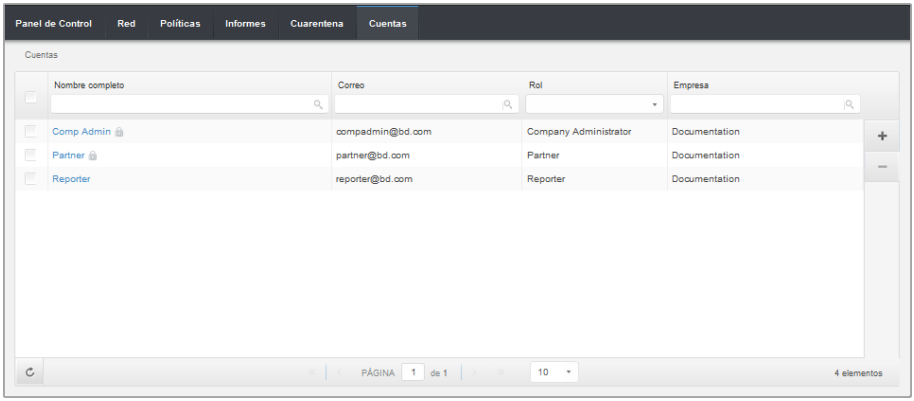
1. Apunte a su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.
2. En **Detalles de cuenta**, haga clic en **Cambiar contraseña**.
3. Escriba su contraseña actual y la nueva contraseña en los campos correspondientes.
4. Haga clic en **Guardar** para aplicar los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

3. Gestión de cuentas de usuario

El servicio Security for Endpoints puede configurarse y administrarse desde Control Center mediante la cuenta recibida tras suscribirse al servicio.

Esto es lo que necesita saber sobre las cuentas de usuario de Small Office Security:

- Para permitir a otros empleados de la empresa acceder a Control Center, puede crear cuentas de usuario internas. Puede asignar cuentas de usuario con diferentes roles, según su nivel de acceso en la empresa.
- Para cada cuenta de usuario, puede personalizar el acceso a las características de Small Office Security o a partes concretas de la red a la que pertenezca.
- Todas las cuentas con privilegios de **Administrar usuarios** pueden crear, modificar y eliminar otras cuentas de usuario.
- Solo puede administrar cuentas con los mismos privilegios que su cuenta o menos.
- Puede crear y administrar cuentas de usuario en la página **Cuentas**.



La página Cuentas

Las cuentas existentes se muestran en la tabla. Para cada cuenta de usuario, puede ver:

- El nombre de usuario de la cuenta (usado para iniciar sesión en Control Center).
- Dirección de correo de la cuenta (usada como dirección de contacto). 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.

– Rol de usuario (partner / administrador de empresa / administrador de red / informes / personalizado).

3.1. Roles de usuario

Un rol de usuario consiste en una determinada combinación de privilegios de usuario. Al crear una cuenta de usuario, puede elegir uno de los roles predefinidos o crear un rol personalizado, seleccionando solo determinados privilegios de usuario.

Nota
Puede conceder a las cuentas de usuario los mismos privilegios que tenga su cuenta o menos.

Hay disponibles los siguientes roles de usuario:

1. **Administrador de empresa** - Adecuado para administradores de empresas cliente que hayan adquirido una licencia de Small Office Security a un partner. Un administrador de empresa administra la licencia, el perfil de la empresa y toda su implementación de Small Office Security, permitiendo un control de máximo nivel sobre todos los ajustes de seguridad (a no ser que sea anulado por la cuenta partner principal en caso de un proveedor de servicios de seguridad). Los administradores de empresa pueden compartir o delegar sus responsabilidades operativas a cuentas de usuario de generadores de informes o administradores subordinados.
2. **Administrador de red** - Se pueden crear varias cuentas con rol de Administrador de red para una empresa, con privilegios administrativos sobre la totalidad de la implementación de Security for Endpoints en la empresa o sobre un grupo determinado de equipos, incluyendo la administración de usuarios. Los administradores de la red son los responsables de administrar activamente los ajustes de seguridad de la red.
3. **Informador** - Las cuentas de informador son cuentas internas de solo lectura. Únicamente permiten el acceso a informes y logs. Dichas cuentas pueden distribuirse entre el personal con responsabilidades de monitorización u otros empleados que deban estar informados sobre el estado de la seguridad.
4. **Personalizado** - Los roles de usuario predefinidos incluyen una determinada combinación de privilegios de usuario. Si un rol de usuario predefinido no encaja en sus necesidades, puede crear una cuenta personalizada seleccionando solo los privilegios que le interesen.

La siguiente tabla resume las relaciones entre los diferentes roles de cuentas y sus privilegios. Para información detallada, diríjase a “Privilegios de usuario” (p. 14).

Rol de cuenta	Cuentas hijo permitidas	Privilegios de usuario
Administrador de empresa	Administradores de empresa, Administradores de red, Informes	Administrar empresa Administrar usuarios

Rol de cuenta	Cuentas hijo permitidas	Privilegios de usuario
		Administrar redes
		Administrar informes
Administrador de red	Administradores de red, Informes	Administrar usuarios
		Administrar redes
		Administrar informes
Informador	-	Administrar informes

3.2. Privilegios de usuario

Puede asignar los siguientes privilegios de usuario a las cuentas de usuario de Small Office Security:

- **Administrar usuarios**. Cree, edite o elimine cuentas de usuario.
- **Administrar empresa**. Los usuarios pueden administrar su propia clave de licencia de Small Office Security y modificar los ajustes de su perfil de empresa. Este privilegio es privativo de las cuentas de administrador de empresa.
- **Administrar redes**. Proporciona privilegios administrativos sobre los ajustes de seguridad de la red (inventario de red, políticas, tareas, paquetes de instalación y cuarentena). Este privilegio es privativo de las cuentas de administrador de red.
- **Administrar informes**. Crear, modificar o eliminar informes y administrar el panel de control.

3.3. Crear cuentas de usuario

Antes de crear una cuenta de usuario, asegúrese de tener a mano la dirección de correo electrónico necesaria. Esta dirección es obligatoria para crear la cuenta de usuario de Small Office Security. Los usuarios recibirán su información de inicio de sesión en Small Office Security en la dirección de correo electrónico suministrada. Los usuarios utilizarán también la dirección de correo electrónico para iniciar sesión en Small Office Security.

Para crear una cuenta de usuario:

1. Diríjase a la página **Cuentas**.
2. Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
3. En la sección **Detalles**, complete la información de la cuenta.
   - **E-mail**. Escriba la dirección de correo electrónico del usuario. La información de inicio de sesión se enviará a esta dirección inmediatamente después de crear la cuenta.

Nota
La dirección de correo electrónico debe ser exclusiva. No puede crear otra cuenta de usuario con la misma dirección de correo electrónico.

- **Nombre completo**. Escriba el nombre completo del propietario de la cuenta.

4. En la sección **Ajustes y privilegios**, configure los siguientes ajustes:
   - **Zona horaria**. Elija desde 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 desde el menú el idioma de visualización de la consola.
   - **Rol**. Seleccione el rol del usuario. Para más información sobre los roles de usuarios, consulte “Roles de usuario” (p. 13).
   - **Derechos**. Cada rol de usuario predefinido tiene una determinada configuración de privilegios. No obstante, puede seleccionar únicamente los privilegios que necesite. En tal caso, el rol de usuario cambia a **Personalizado**. Para más información sobre los privilegios de los usuarios, consulte “Privilegios de usuario” (p. 14).
   - **Seleccionar objetivos**. Desplácese hacia abajo en la ventana de configuración para mostrar la sección de objetivos. Seleccione los grupos de red a los que tendrá acceso el usuario. Puede restringir el acceso del usuario a áreas concretas de la red.
5. Haga clic en **Guardar** para añadir el usuario. La nueva cuenta se mostrará en la lista de cuentas de usuario.

Nota
La contraseña de cada cuenta de usuario se genera automáticamente una vez que se crea la cuenta, y se envía a la dirección de correo electrónico del usuario junto con la restante información de la misma.
Puede cambiar la contraseña una vez creada la cuenta. Haga clic en el nombre de cuenta en la página de **Cuentas** para modificar su contraseña. Una vez modificada la contraseña, se le notificará inmediatamente al usuario por correo electrónico.
Los usuarios pueden cambiar su contraseña de inicio de sesión desde Control Center, accediendo a la página **Mi cuenta**.

3.4. Editar cuentas

Edite las cuentas para mantener al día los detalles de la cuenta o cambiar la configuración de la misma.

Para editar una cuenta de usuario:

1. Iniciar sesión en Control Center.
2. Diríjase a la página **Cuentas**.
3. Haga clic en el nombre de usuario.
4. Cambie la configuración y detalles de la cuenta según sea necesario.

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

Nota
Todas las cuentas con privilegios de **Administrar usuarios** pueden crear, modificar y eliminar otras cuentas de usuario. Solo puede administrar cuentas con los mismos privilegios que su propia cuenta o menos.

3.5. Eliminar cuentas

Elimine las cuentas cuando ya no sean necesarias. Por ejemplo, si el propietario de la cuenta ya no está en la empresa.

Para eliminar una cuenta:

1. Iniciar sesión en Control Center.
2. Diríjase a la página **Cuentas**.
3. Seleccione la cuenta desde la lista.
4. Haga clic en el botón **Borrar** del lateral derecho de la tabla.

3.6. Restablecer las contraseñas de inicio de sesión

Los propietarios de cuentas que olviden su contraseña pueden restablecerla usando el enlace de recuperación de contraseña en la página de inicio de sesión. También puede restablecer una contraseña de inicio de sesión olvidada editando la cuenta correspondiente desde la consola.

Para restablecer la contraseña de inicio de sesión para un usuario:

1. Iniciar sesión en Control Center.
2. Diríjase a la página **Cuentas**.
3. Haga clic en el nombre de usuario.
4. Escriba una nueva contraseña en los campos correspondientes (en **Detalles**).
5. Haga clic en **Guardar** para aplicar los cambios. El propietario de la cuenta recibirá un e-mail con la nueva contraseña.

4. Instalar Security for Endpoints

Security for Endpoints se destina a equipos y portátiles que ejecuten los sistemas operativos Windows y Mac OS X y a servidores Windows. Para proteger sus equipos físicos con Security for Endpoints, debe instalar Endpoint Security (el software cliente) en cada uno de ellos. Endpoint Security administra la protección en el equipo local. También se comunica con Control Center para recibir los comandos del administrador y enviar los resultados de sus acciones.

Puede instalar Endpoint Security con uno de los siguientes roles (disponibles en el asistente de instalación):

1. **Punto final**, cuando el equipo correspondiente es un punto final normal de la red.
2. **Endpoint Security Relay**, cuando otros puntos finales de la red utilizan el equipo en cuestión para comunicarse con Control Center. El rol Endpoint Security Relay instala Endpoint Security junto con un servidor de actualizaciones, que puede utilizarse para actualizar los demás clientes de la red. Los puntos finales de la misma red se pueden configurar mediante políticas para comunicarse con Control Center a través de uno o varios equipos con rol Endpoint Security Relay. Así, cuando un Endpoint Security Relay no está disponible, se pasa al siguiente para garantizar la comunicación del equipo con Control Center.

Aviso

- El primer equipo en que instale la protección ha de tener rol de Endpoint Security Relay, o no podrá implementar Endpoint Security en otros equipos de la red.
- El equipo con rol de Endpoint Security Relay debe estar encendido y conectado para que los clientes se comuniquen con Control Center.

Puede instalar Endpoint Security en los equipos ejecutando los paquetes de instalación localmente o ejecutando las tareas de instalación remotamente desde Control Center.

Es muy importante leer y seguir cuidadosamente las instrucciones para prepararse para la instalación.

Endpoint Security posee una interfaz de usuario mínima. Sólo permite a los usuarios comprobar el estado de protección y ejecutar tareas de seguridad básicas (actualizaciones y análisis), sin permitir el acceso a la configuración.

Por defecto, el idioma mostrado por la interfaz de usuario en los equipos protegidos se define en el momento de la instalación basándose en el idioma de su cuenta.

Para instalar la interfaz de usuario en otro idioma en determinados equipos, puede crear un paquete de instalación y establecer el idioma preferido en las opciones de configuración

del paquete. Para obtener más información sobre la creación de paquetes de instalación, consulte “Crear paquetes de instalación de Endpoint Security” (p. 21).

4.1. Requisitos del Sistema

4.1.1. Sistemas operativos soportados

Security for Endpoints actualmente protege los siguientes sistemas operativos:

Sistemas operativos de estaciones de trabajo:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista con Service Pack 1
- Windows XP con Service Pack 2 64 bits
- Windows XP con Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Tablets y sistemas operativos integrados:

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded con Service Pack 2*
- Windows XP Tablet PC Edition*

*Deben instalarse módulos específicos del sistema operativo para que funcione Security for Endpoints.

Sistemas operativos de servidor:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 con Service Pack 1

- Windows Home Server

4.1.2. Requisitos de Hardware

- Procesador Intel® Pentium compatible:

  Sistemas operativos de estaciones de trabajo
  - 1 GHz o más para Microsoft Windows XP SP3, Windows XP SP2 64 bit y Windows 7 Enterprise (32 y 64 bit)
  - 2 GHz o más para Microsoft Windows Vista SP1 o superior (32 y 64 bit), Microsoft Windows 7 (32 y 64 bit), Microsoft Windows 7 SP1 (32 y 64 bit), Windows 8
  - 800 MHZ o más para Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded con Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Sistemas operativos de servidor
  - Mínimo: CPU de un solo núcleo a 2,4 GHz
  - Recomendado: CPU Intel Xeon multinúcleo a 1,86 GHz o más
- **Memoria RAM libre**:
  - Para Windows 512 MB mínimos, 1 GB recomendados
  - Para Mac: 1 GB mínimo
- **Espacio en disco duro**:
  - 1.5 GB de espacio libre en disco

Nota
Se requieren al menos 6 GB de espacio libre en disco para entidades con rol de Endpoint Security Relay, dado que almacenarán todos los paquetes de instalación y actualizaciones.

4.1.3. Navegadores soportados

La seguridad del navegador del punto final se ha comprobado que funciona con los siguientes navegadores:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

4.1.4. Puertos de comunicación de Small Office Security

La siguiente tabla proporciona información de los puertos utilizados por los componentes de Small Office Security:

Puerto	Usabilidad
80 (HTTP) / 443 (HTTPS)	Puerto utilizado para acceder a la consola Web de Control Center.
80	Puerto del Servidor de Actualización.
8443 (HTTPS)	Puerto utilizado por el software cliente/agente para conectarse al Servidor de comunicación.
7074 (HTTP)	Comunicación con Endpoint Security Relay (si está disponible)

Para obtener información detallada sobre los puertos de Small Office Security, consulte este artículo de la base de conocimientos.

4.2. Preparándose para la Instalación

Antes de la instalación, siga estos pasos preparatorios para asegurarse de que todo vaya bien:

1. Asegúrese de que los equipos cumplen los requisitos de sistema mínimos. Para algunos equipos es posible que tenga que instalar el último service pack disponible o liberar espacio en disco. Configure una lista de equipos que no cumplan los requisitos necesarios para que pueda excluirlos de la administración.
2. Desinstale (no sólo desactive) cualquier antimalware, cortafuego o software de seguridad de su equipo. Ejecutar Endpoint Security simultáneamente con otro software de seguridad en un equipo puede afectar a su funcionamiento y causar serios problemas en el sistema.

   Muchos de los programas de seguridad con los que Endpoint Security no es compatible, se detectan y eliminan automáticamente durante la instalación. Para más información y para ver la lista de software de seguridad detectado, consulte este artículo de la base de conocimientos.

   Importante
   No es necesario preocuparse de las funciones de seguridad de Windows (Windows Defender, Windows Firewall), ya que se desactivan automáticamente antes de que se inicie la instalación.

3. La instalación requiere disponer de privilegios de administrador y acceso a Internet. Asegúrese de que tiene a mano las credenciales necesarias para todos los equipos.
4. Los equipos deben tener conexión con Control Center.

4.3. Instalación local

Una forma de instalar Endpoint Security en un equipo es ejecutar un paquete de instalación localmente.

Puede crear y administrar paquetes de instalación según sus necesidades en la página **Red > Paquetes**.

El menú Red > Paquetes

Aviso

- El primer equipo en que instale la protección ha de tener rol de Endpoint Security Relay, o no podrá implementar Endpoint Security en otros equipos de la red.
- El equipo con rol de Endpoint Security Relay debe estar encendido y conectado para que los clientes se comuniquen con Control Center.

Nota

Una vez instalado el primer cliente, se utilizará para detectar otros equipos de la misma red, basándose en el mecanismo de Detección de redes. Para información detallada sobre la detección de redes, consulte “Cómo funciona la detección de red” (p. 29).

Para instalar Endpoint Security localmente en un equipo, siga estos pasos:

1. Cree un paquete de instalación según sus necesidades.

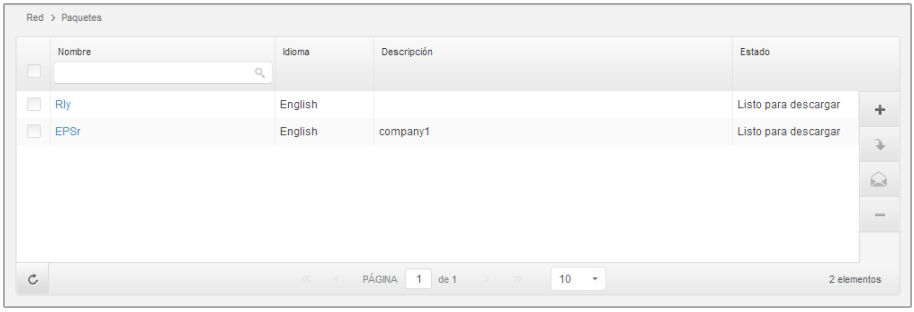
   Nota
   Este paso no es obligatorio si ya se ha creado un paquete de instalación para la red correspondiente a su cuenta.

2. Descargue el paquete de instalación en el equipo.
3. Ejecute el paquete de instalación en el equipo.

4.3.1. Crear paquetes de instalación de Endpoint Security

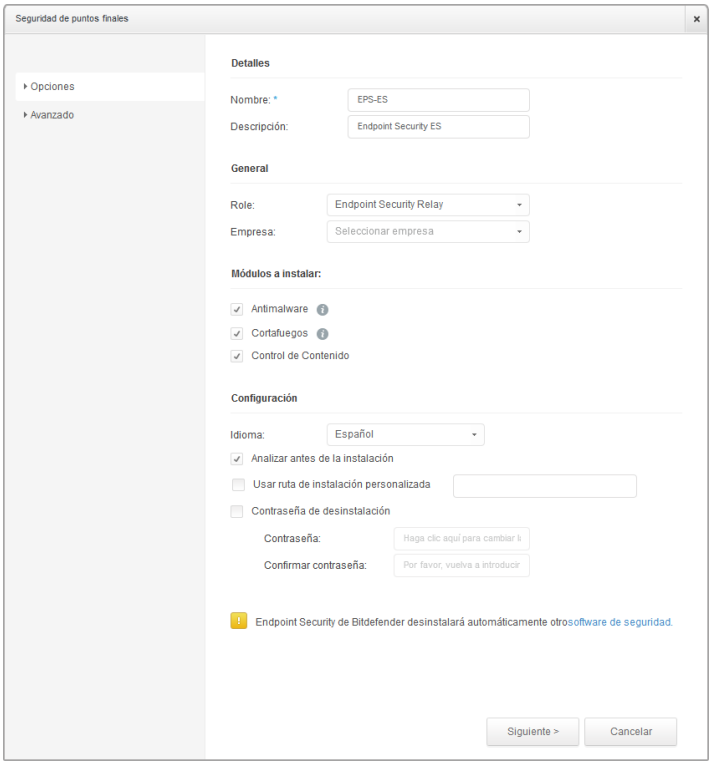
Para crear un paquete de instalación de Endpoint Security:

1. Conéctese e inicie sesión en Control Center usando su cuenta.
2. Vaya a la página **Red > Paquetes**.



La página Paquetes

3. Haga clic en el botón + **Añadir** del lateral derecho de la tabla. Aparecerá una nueva ventana de configuración.



Crear paquetes Endpoint Security - Opciones

4. Escriba un nombre adecuado y una descripción para el paquete de instalación que quiere crear.
5. Seleccione el rol del equipo objetivo:
   - **Punto final**. Seleccione esta opción para crear el paquete para un punto final normal.
   - **Endpoint Security Relay**. Seleccione esta opción para crear el paquete para un punto final con rol Endpoint Security Relay. Endpoint Security Relay es un rol especial que instala un servidor de actualizaciones en el equipo objetivo junto con Endpoint Security. Éste puede utilizarse para actualizar los demás clientes de la red, reduciendo el uso de ancho de banda entre las máquinas clientes y Control Center.
6. Seleccione la empresa donde se utilizará el paquete de instalación.
7. Seleccione los módulos de protección que desea instalar.
8. En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.
9. Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
10. Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security en una ubicación diferente. En este caso, escriba la ruta deseada en el campo correspondiente. Utilice las reglas de Windows al escribir la ruta (por ejemplo, `D:\carpeta`). Si la carpeta especificada no existe, se creará durante la instalación.
11. Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.
12. Haga clic en **Siguiente**.
13. Dependiendo del rol del paquete de instalación (punto final o Endpoint Security Relay), escoja la entidad a la que se conectarán periódicamente los equipos objetivo para actualizar el cliente:
    - **Bitdefender Cloud**, si desea actualizar los clientes directamente desde Internet.
    - **Endpoint Security Relay**, si desea conectar los puntos finales a un Endpoint Security Relay instalado en su red. Todos los equipos con rol de Endpoint Security Relay detectados en su red figurarán en la tabla que se muestra a continuación. Seleccione el Endpoint Security Relay que desee. Los puntos finales conectados se comunicarán con Control Center solo mediante el Endpoint Security Relay especificado.

Importante
El puerto 7074 debe estar abierto para que funcione la implementación mediante Endpoint Security Relay.

14. Haga clic en **Guardar**.

El nuevo paquete de instalación aparecerá en la lista de paquetes de la empresa objetivo.

4.3.2. Descargar los paquetes de instalación

Para descargar los paquetes de instalación de Endpoint Security:

1. Inicie sesión en Control Center desde el equipo en el que desee instalar la protección.
2. Vaya a la página **Red > Paquetes**.
3. Seleccione el paquete de instalación de Endpoint Security que desee descargar.
4. Haga clic en el botón **Descargar** a la derecha de la tabla y seleccione el tipo de instalador que quiera utilizar. Hay disponibles dos tipos de archivos de instalación:
   - **Downloader**. El downloader primero descarga el kit de instalación completo desde los servidores de la nube de Bitdefender y luego inicia la instalación. Es pequeño en tamaño y puede ejecutarse tanto en sistemas de 32-bit como de 64-bit (lo que lo hace más fácil de distribuir). Por otro lado, requiere una conexión a Internet activa.
   - **Kit completo**. El kit completo se utiliza para instalar la protección en los equipos sin conexión a Internet o con conexiones lentas. Descargue este archivo en un equipo conectado a Internet y distribúyalo a otros equipos usando un medio de almacenamiento externo o compartiéndolo en la red.

     Nota
     Versiones de kit completo disponibles:
     - **SO Windows:** sistemas de 32 bits y 64 bits
     - **Mac OS X:** solo sistemas de 64 bits

     Asegúrese de usar la versión correcta para el equipo donde instala.
5. Guarde el archivo en el equipo.

4.3.3. Ejecutar los paquetes de instalación

Para que funcione la instalación, el paquete de instalación debe ejecutarse utilizando privilegios de administrador o desde una cuenta de administrador.

1. Conéctese e inicie sesión en Control Center.
2. Descargue o copie el archivo de instalación al equipo objetivo o a un medio compartido de la red accesible desde ese equipo.
3. Ejecutar el paquete de instalación.
4. Siga las instrucciones que aparecen en la pantalla.

Una vez instalado Endpoint Security, el equipo se mostrará como administrado en Control Center (página **Red**) en unos minutos.

4.4. Instalación remota

Una vez que haya instalado localmente el primer cliente con rol de Endpoint Security Relay, pueden tardarse unos minutos en que el resto de equipos de la red aparezcan en la Control Center. Desde este punto, puede instalar remotamente Endpoint Security en equipos bajo su administración mediante tareas de instalación desde Control Center.

Endpoint Security incluye un mecanismo automático de detección de redes que le permite detectar otros equipos en su red. Los equipos detectados se muestran como **equipos no administrados** en la página de **Red**.

Para información detallada sobre la detección de redes, consulte "Cómo funciona la detección de red" (p. 29).

4.4.1. Requisitos de la instalación remota de Endpoint Security

Para que funcione la instalación remota:

- Debe haber instalado un Endpoint Security Relay en su red.
- Cada equipo objetivo debe tener habilitados la compartición de recursos administrativos admin$. Configure cada estación de trabajo objetivo para el uso compartido de archivos avanzado.
- Desactive temporalmente el control de cuentas de usuario para todos los equipos que ejecutan sistemas operativos Windows que incluyan esta característica de seguridad (Windows Vista, Windows 7, Windows Server 2008, etc.). Si los equipos están en un dominio, puede utilizar una política de grupo para desactivar el Control de Cuentas de Usuario de forma remota.
- Desactive o apague la protección del cortafuego en los equipos. Si los equipos están en un dominio, puede utilizar una política de grupo para desactivar el Firewall de Windows de forma remota.

4.4.2. Ejecución de tareas de instalación remota de Endpoint Security

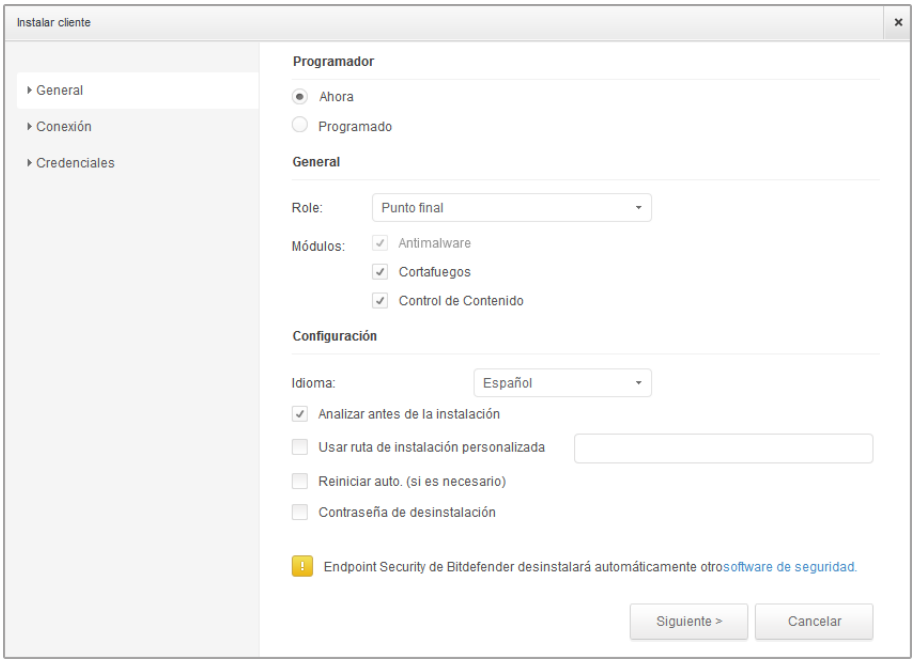
Para ejecutar una tarea de instalación remota:

1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.
3. Seleccione el grupo de red deseado en el panel de la izquierda. Las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.

Nota

Opcionalmente, puede aplicar filtros para mostrar únicamente los equipos no administrados. Haga clic en el botón **Filtros** y seleccione las siguientes opciones: **No administrados** de la categoría **Seguridad** y **Todos los elementos recursivamente** de la categoría **Profundidad**.

4. Seleccione las entidades (equipos o grupos de equipos) en las que desee instalar la protección.
5. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Instalar cliente**. El asistente de **Instalar cliente** se está mostrando.



Instalación de Endpoint Security desde el menú Tareas

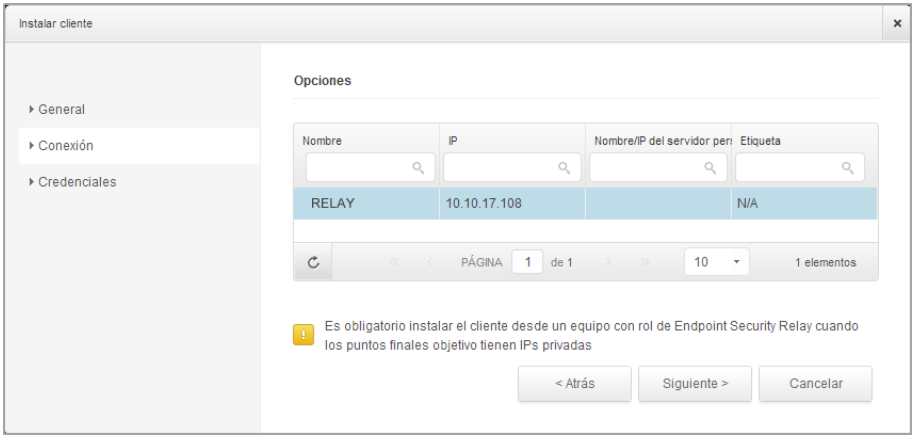
6. Configure las opciones de instalación:
   - Programe el momento de la instalación:
     - **Ahora**, para poner en marcha la implementación de inmediato.
     - **Programado**, para configurar el intervalo de recurrencia de la implementación. En este caso, seleccione el intervalo de tiempo que desee (cada hora, a diario o semanalmente) y configúrelo según sus necesidades.

Nota

Por ejemplo, cuando hay que realizar determinadas operaciones en el equipo objetivo antes de instalar el cliente (como la desinstalación de otros programas y el reinicio del sistema operativo), puede programar la tarea de implementación para que se ejecute cada 2 horas. La tarea se lanzará en los equipos objetivo cada 2 horas hasta que culmine correctamente.

- Seleccione los módulos de protección que desea instalar. Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.
- En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.
- Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
- Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security en una ubicación diferente. En este caso, escriba la ruta deseada en el campo correspondiente. Utilice las reglas de Windows al escribir la ruta (por ejemplo, `D:\carpeta`). Si la carpeta especificada no existe, se creará durante la instalación.
- Durante la instalación silenciosa, se analiza el equipo en busca de malware. A veces es necesario un reinicio del sistema para completar la eliminación del malware.

  Seleccionar **Reiniciar automáticamente (si es necesario)** para asegurarse de que el malware detectado es eliminado por completo antes de la instalación. De lo contrario la instalación puede fallar.
- Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.
- Haga clic en **Siguiente**.
- La pestaña **Conexión** muestra la lista de puntos finales con rol de Endpoint Security Relay instalados en la red. Cada nuevo cliente debe estar conectado por lo menos a un Endpoint Security Relay de la misma red, que actuará como Servidor de actualizaciones y de comunicaciones. Seleccione el Endpoint Security Relay que quiere vincular a los nuevos clientes.



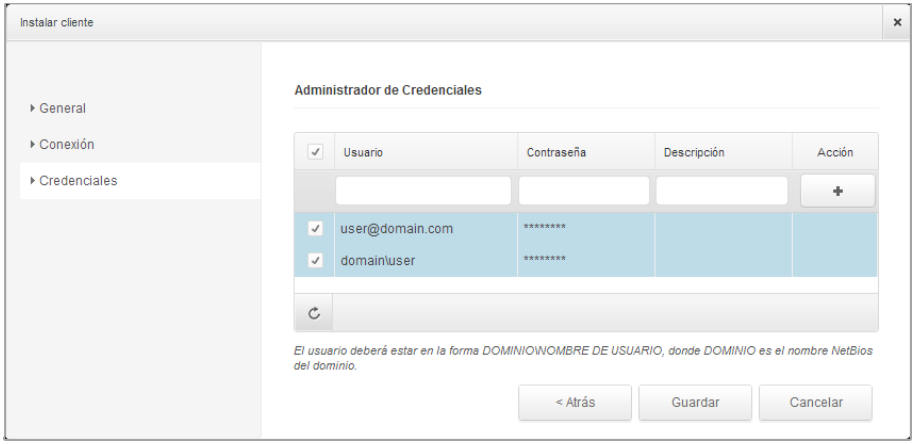
7. Haga clic en **Siguiente**.
8. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los puntos finales seleccionados Puede añadir las credenciales requeridas escribiendo el usuario y contraseña de cada sistema operativo objetivo.

Importante

Para estaciones Windows 8.1, debe proporcionar las credenciales de la cuenta de administrador integrada o de una cuenta de administrador de dominio. Para obtener más información, consulte este artículo de la base de conocimientos.

Nota

Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota Endpoint Security en los equipos.



Para añadir las credenciales del sistema operativo requeridas:

a. Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta. Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

   Utilice las convenciones de Windows cuando introduzca el nombre de una cuenta de usuario de dominio, por ejemplo, `usuario@dominio.com` o `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas en ambas formas (`usuario@dominio.com` y `dominio\usuario`).

   Nota
   Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

b. Haga clic en el botón + **Añadir**. La cuenta se añade a la lista de credenciales.

c. Marque las casillas de verificación correspondientes a la cuenta que desea usar.

9. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**.

4.5. Cómo funciona la detección de red

Security for Endpoints incluye un mecanismo automático de detección de red pensado para detectar los equipos del grupo de trabajo.

Security for Endpoints se basa en el **servicio Microsoft Computer Browser** para realizar una detección de red. El servicio Computer Browser es una tecnología de red utilizada por los equipos basados en Windows para mantener listas actualizadas de dominios, grupos de trabajo y los equipos en ellos, y para suministrar estas listas a equipos cliente que lo soliciten. Los equipos detectados en la red por el servicio Computer Browser pueden visualizarse ejecutando el comando de **net view** en una ventana de símbolo del sistema.

El comando Net view

Para activar el descubrimiento (detección) de la red, primero debe tener instalado Endpoint Security en al menos un equipo de la red. Este equipo se utilizará para analizar la red.

Importante

Control Center no utiliza la información de red del Active Directory o de la función de mapa de red disponible en Windows Vista y posterior. El mapa de red se basa en una tecnología de detección de red diferente: el protocolo Link Layer Topology Discovery (LLTD).

Control Center no forma parte activa de la operación del servicio de Computer Browser. Endpoint Security sólo consulta al servicio Computer Browser respecto a la lista de estaciones de trabajo y servidores visible actualmente en la red (conocida como lista de examen) y luego la envía a Control Center. Control Center procesa la lista de examen, añadiendo nuevos equipos detectados a su lista de **Equipos no administrados**. Los equipos anteriormente detectados no se borran después de una nueva consulta de detección de red, así que deberá excluir y borrar manualmente los equipos que ya no estén en la red.

La consulta inicial de la lista de examen la lleva a acabo el primer Endpoint Security instalado en la red.

- Si Endpoint Security está instalado en un equipo de un grupo de trabajo, sólo los equipos de ese grupo de trabajo serán visibles en Control Center.
- Si Endpoint Security está instalado en un equipo de dominio, sólo los equipos de ese dominio serán visibles en Control Center. Los equipos de otros dominios pueden detectarse si hay una relación de confianza con el dominio donde Endpoint Security está instalado.

Las consultas posteriores sobre detección de red se realizan regularmente cada hora. Para cada nueva pregunta, Control Center divide el espacio administrado de los equipos en áreas de visibilidad y entonces designa un Endpoint Security en cada área donde realizar la tarea.

Un área de visibilidad es un grupo de equipos que se detectan entre ellos. Normalmente, un área de visibilidad se define por un grupo de trabajo o dominio, pero esto depende de la topología de la red y su configuración. En algunos casos, un área de visibilidad puede consistir en múltiples dominios y grupos de trabajo.

Si un Endpoint Security seleccionado falla al realizar la consulta, Control Center espera a la siguiente consulta programada, sin escoger otro Endpoint Security para intentarlo de nuevo.

Para una visibilidad de toda la red, Endpoint Security deberá estar instalado en al menos un equipo en cada grupo de trabajo o dominio en su red. Lo ideal seria que Endpoint Security estuviera instalado en al menos un equipo en cada subred de trabajo.

4.5.1. Más sobre el servicio Microsoft Computer Browser

Datos sobre el servicio Computer Browser:

- Funciona independientemente de Active Directory.
- Funciona exclusivamente en redes IPv4 y opera independientemente dentro de los límites de un grupo LAN (grupo de trabajo o dominio). Se compila y mantiene una lista de examen para cada grupo LAN.
- Normalmente utiliza transmisiones del servidor sin conexión para comunicarse entre nodos.
- Utiliza NetBIOS en TCP/IP (NetBT).
- Requiere resolución de nombre de NetBIOS. Se recomienda tener una infraestructura de Servicio de Windows de nombre de Internet (WINS) funcionando en la red.
- No está habilitado por omisión en Windows Server 2008 y 2008 R2.

Para información detallada sobre el servicio Computer Browser, compruebe la Referencia técnica del servicio de navegador del equipo en Microsoft Technet.

4.5.2. Requisitos de descubrimiento de red

Para poder detectar satisfactoriamente todos los equipos (servidores y estaciones de trabajo) que se administrarán desde Control Center, se necesita lo siguiente:

- Los equipos deben estar unidos a un grupo de trabajo o dominio y conectados a través de una red local IPv4. El servicio Computer Browser no funciona en redes IPv6.
- Varios equipos en cada grupo LAN (grupo de trabajo o dominio) deben ejecutar el servicio Computer Browser. Los controladores de dominio primario también deben ejecutar el servicio.
- Las NetBIOS en TCP/IP (NetBT) deben estar habilitadas en los equipos. El cortafuegos local debe permitir el tráfico NetBT.

- La compartición de archivos debe estar habilitada en los equipos. El cortafuegos local debe permitir la compartición de archivos.
- Hay que establecer una infraestructura de Windows Internet Naming Service (WINS) que funcione correctamente.
- Para Windows Vista y posterior, la detección de red ha de estar activada (**Panel de control > Centro de redes y recursos compartidos > Cambiar ajustes de compartición avanzados**).

  Para poder activar esta característica, han de iniciarse los siguientes servicios:
  - Cliente DNS
  - Publicación de recurso de detección de función
  - Descubrimiento de SSDP
  - Host de dispositivo UPnP
- En entornos con múltiples dominios, se recomienda establecer relaciones de confianza entre dominios de manera que los equipos puedan acceder a las listas de examen de otros dominios.

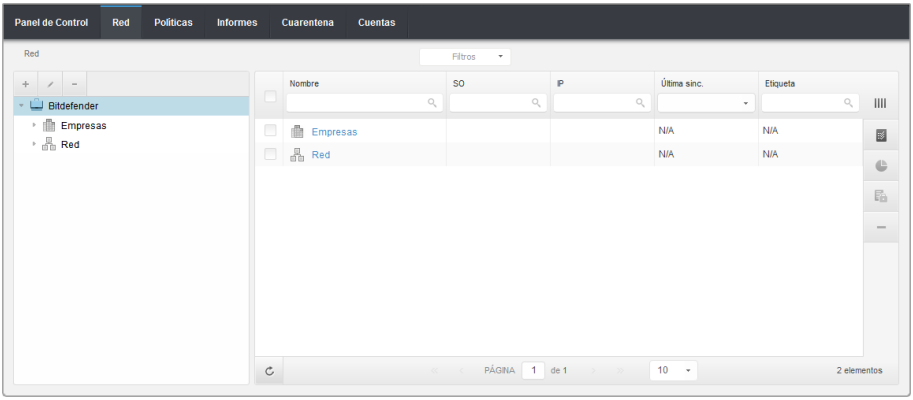
Los equipos desde los cuales Endpoint Security accede al servicio Computer Browser deben poder resolver nombres NetBIOS.

Nota

El mecanismo de detección de redes funciona en todos los sistemas operativos soportados, incluyendo las versiones de Windows Embedded, siempre que se cumplan los requisitos.

5. Administrar equipos

La página **Red** proporciona diversas características para explorar y administrar los equipos disponibles. La vista **Red** consiste en una interfaz de dos paneles que muestra el estado en tiempo real de todos los objetos de la red:



La página Red

1. El panel izquierdo muestra la estructura en árbol de la red disponible.

   Nota
   Puede consultar y administrar sólo los grupos en los que tiene derechos de administrador.

2. El panel derecho muestra el contenido del grupo que ha seleccionado en el árbol de directorios. Este panel consiste en una cuadrícula, donde las filas contienen objetos de red y las columnas muestran información específica para cada tipo de objeto.

   Desde este panel, puede hacer lo siguiente:

   - Consultar información detallada sobre cada objeto de red bajo su cuenta. Puede ver el estado de cada objeto marcando el icono junto a su nombre. Haga clic en el nombre del objeto para mostrar una ventana con más detalles específicos.
   - Utilice la Barra de herramientas de acción a la derecha de la tabla para llevar a cabo operaciones específicas para cada objeto de red (como ejecutar tareas, crear informes, asignar políticas y eliminarlas).
   - Actualizar datos de la tabla.

Desde la sección **Red** puede administrar también los paquetes de instalación y la lista de tareas para cada tipo de objeto de red.

Para consultar los equipos de su cuenta, diríjase a la página **Red** y seleccione el grupo de red deseado a la izquierda de la página.

Puede ver la red de equipos disponible en el panel izquierdo y consultar detalles sobre cada equipo en el panel derecho.

Para personalizar los detalles del equipo que se muestran en la tabla:

1. Haga clic en el botón **Columnas** del lateral derecho del encabezado de la tabla.
2. Seleccione los nombres de las columnas que desea ver.
3. Haga clic en el botón **Restablecer** para volver a la vista predeterminada de columnas.

Desde la sección **Red** puede administrar los equipos de la forma siguiente:

- Compruebe el estado del equipo.
- Organice los equipos en grupos.
- Consulte la información del equipo.
- Clasifique, filtre y busque por equipos.
- Ejecutar tareas en los equipos.
- Crear informes rápidos.
- Asignar políticas.
- Eliminar equipos del inventario de red.

5.1. Comprobar el estado del equipo

Cada equipo está representado en la página de red con un icono correspondiente al estado del equipo. Puede ver los estados de los equipos y los iconos correspondientes en la siguiente tabla:

icono	Estado
	Equipo, Administrado, Sin problemas, Online
	Equipo, Administrado, Con problemas de seguridad, Online
	Equipo, Administrado, Sin problemas, Offline
	Equipo, Administrado, Con problemas de seguridad, Offline
	No administrado
	Eliminados

Para obtener más información detallada, consulte:

- “Equipos Administrados, No administrados y Eliminados” (p. 35)
- “Equipos conectados y desconectados” (p. 35)

- “Equipos con problemas de seguridad” (p. 36)

5.1.1. Equipos Administrados, No administrados y Eliminados

Los equipos pueden tener distintos estados de administración:

- **Administrados** - Equipos en las que se ha instalado la protección Endpoint Security.
- **No administrados** - los equipos detectados en los que la protección Endpoint Security todavía no se ha instalado.
- **Eliminado** - equipos que ha eliminado de Control Center. Para más información, diríjase a “Eliminar equipos del inventario de red” (p. 60).

5.1.2. Equipos conectados y desconectados

El estado de conexión se refiere únicamente a los equipos administrados. Desde este punto de vista, los equipos administrados pueden estar:

- **Online**. Un icono azul indica que el equipo está online (conectado).
- **offline**. Un icono gris indica que el equipo está offline (desconectado).

Un equipo se considera offline si Endpoint Security está inactivo durante más de 5 minutos. Posibles razones por las cuales los equipos aparecen offline:

- El equipo está apagado, en suspensión o hibernando.

  Nota
  Los equipos normalmente aparecen online incluso cuando están bloqueados o el usuario está desconectado.

- Endpoint Security carece de conexión con Bitdefender Control Center o con el Endpoint Security Relay asignado:
  - El equipo puede estar desconectado de la red.
  - Un cortafuego de red o router puede estar bloqueando la comunicación entre Endpoint Security y Bitdefender Control Center o el Endpoint Security Relay asignado.
- Endpoint Security se ha desinstalado manualmente del equipo mientras éste carecía de conexión con Bitdefender Control Center o con el Endpoint Security Relay asignado. Normalmente, cuando se desinstala Endpoint Security manualmente de un equipo, se notifica a Control Center, y el equipo se marca como no administrado.
- Puede que Endpoint Security no esté funcionando correctamente.

Para averiguar cuánto tiempo han estado inactivos los equipos:

1. Mostrar sólo los equipos administrados. Haga clic en el menú **Filtros** situado encima de la tabla, seleccione **Administrados (puntos finales)** y **Administrados (Endpoint Security Relay)** en la categoría **Seguridad** y haga clic en **Guardar**.
2. Haga clic en el encabezado de la columna **Visto última vez** para organizar los equipos por periodo de inactividad.

Puede ignorar periodos de inactividad más cortos (minutos, horas) pues probablemente sean resultado de una situación temporal. Por ejemplo, el equipo está actualmente apagado.

Los periodos de inactividad más largos (días, semanas) normalmente indican un problema con el equipo.

5.1.3. Equipos con problemas de seguridad

El estado de seguridad se refiere únicamente a los equipos administrados. Busque el icono de estado que muestra un símbolo de advertencia para localizar los equipos con problemas de seguridad:

- Equipo administrado, con problemas, online.
- Equipo administrado, con problemas, offline.

Un equipo tiene problemas de seguridad siempre que se dé al menos una de las siguientes situaciones:

- La protección antimalware está desactivada.
- La licencia de Endpoint Security ha caducado.
- Endpoint Security está desactualizado.
- Las firmas están obsoletas.
- Se ha detectado malware.

Si observa un equipo con problemas de seguridad, haga clic en su nombre para mostrar la página **Detalles del equipo**. Puede identificar los problemas de seguridad mediante el icono. Consulte el tooltip del icono para conocer más detalles. Puede ser necesaria más investigación local.

5.2. Organice los equipos en grupos

Puede administrar grupos de equipos en el panel de la izquierda de la página **Red**, en los grupos de **Red**.

La ventaja principal es que puede usar las políticas de grupo para cumplir distintos requisitos de seguridad.

En el grupo de **Red** perteneciente a su empresa puede crear, eliminar, renombrar y mover grupos de equipos dentro de una estructura de árbol personalizada.

Importante
Por favor, tenga en cuenta lo siguiente:

- Un grupo puede contener tanto equipos como otros grupos.
- Cuando se selecciona un grupo en el panel del lado izquierdo, puede ver todos los equipos excepto aquellos ubicados en sus subgrupos. Para ver todos los equipos incluidos en el grupo y sus subgrupos, haga clic en el menú **Filtros** situado encima de la tabla y seleccione **Todos los elementos recursivamente** en la sección **Profundidad**.

Creando Grupos

Antes de empezar a crear grupos, piense en las razones por las que los necesita y elabore un esquema de agrupación. Por ejemplo, puede agrupar los equipos basándose en uno o en una combinación de los siguientes criterios:

- Estructura de la organización (Ventas, Marketing, Control de calidad, Desarrollo de software, Dirección, etc.).
- Necesidades de seguridad (equipos de escritorio, portátiles, servidores, etc.).
- Ubicación (sede central, oficinas locales, trabajadores remotos, oficinas domésticas, etc.).

Para organizar su red en grupos:

1. Seleccione el grupo de **Red** en el panel de la izquierda.
2. Haga clic en el botón **Añadir grupo** en la parte superior del panel izquierdo.
3. Escriba un nombre descriptivo para el grupo y haga clic en **Aceptar**.

Renombrando Grupos

Para renombrar un grupo:

1. Seleccione el grupo en el panel lateral izquierdo.
2. Haga clic en el botón **Editar grupo** de la parte superior del panel izquierdo.
3. Introduzca el nuevo nombre en el campo correspondiente.
4. Haga clic en **Aceptar** para confirmar.

Mover grupos y equipos

Puede mover grupos y usuarios a cualquier lugar de la jerarquía de grupos de **Red**. Para mover un grupo o usuario, arrastre y suelte desde la ubicación actual a la nueva.

Nota

La entidad movida heredará los ajustes de políticas del nuevo grupo padre, a menos que se le haya asignado una política diferente. Para obtener más información sobre la herencia de políticas, consulte “Asignar políticas a objetos de red” (p. 73).

Eliminando Grupos

No puede eliminarse un grupo si contiene al menos un equipo. Mueva a otro grupo todos los equipos del grupo que desee eliminar. Si el grupo incluye subgrupos, puede elegir mover todos los subgrupos en lugar de equipos individuales.

Para eliminar un grupo:

1. Seleccione el grupo vacío en el panel de la derecha de la **página Red**.
2. Haga clic en el botón **Eliminar grupo** en la parte superior del panel izquierdo. Tendrá que confirmar esta acción haciendo clic en **Sí**.

5.3. Consulta de la información del equipo

Puede obtener información detallada sobre cada equipo en la página **Red**, incluyendo el sistema operativo, IP, fecha y hora en la que fue visto por última vez, etc.

Para consultar información sobre un equipo:

1. Diríjase a la página **Red**.
2. Seleccione el grupo de red deseado en el panel de la izquierda.

   Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Puede identificar fácilmente el estado del equipo consultando el icono correspondiente. Para información detallada, diríjase a “Comprobar el estado del equipo” (p. 34).
4. Consulte la información mostrada en las columnas para cada equipo:
   - **Nombre**: nombre del equipo.
   - **FQDN**: Nombre de dominio completo que incluye el nombre del host y el del dominio.
   - **SO**: sistema operativo instalado en el equipo.
   - **IP**: dirección IP del equipo.
   - **Detectada por última vez**: información sobre el estado de conexión del equipo.

     Nota

     Es importante supervisar el campo **Visto por última vez** dado que largos periodos de inactividad podrían indicar que el equipo está desconectado.

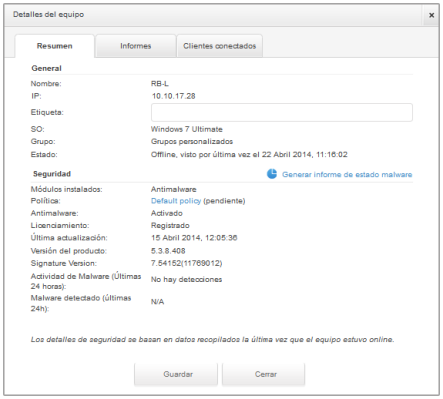
   - **Etiqueta**: la etiqueta añadida al equipo en la ventana **Detalles del equipo**.

5. Haga clic en el nombre del equipo administrado en el que está interesado. Se muestra la ventana **Detalles del equipo**.
   - Acceda a la pestaña **General** para hallar la siguiente información:
     - Información general del equipo, como nombre, dirección IP, sistema operativo, grupo padre y estado actual. También puede asignar una etiqueta al equipo. Por tanto, puede buscar y filtrar equipos por etiqueta mediante el campo de búsqueda de la columna **Etiqueta** de la tabla de la derecha de la página **Red**.
     - Detalles de seguridad relativos al Endpoint Security instalado en el equipo seleccionado, como módulos instalados, política asignada, estado antimalware, estado de la licencia, última actualización, las versiones del producto y de la firma y malware detectado en las últimas 24 horas. También puede obtener un resumen rápido acerca del número de detecciones de malware en el equipo el día de hoy.
     - Haga clic en **Generar informe de estado malware** para acceder a las opciones de informe para el equipo seleccionado.

       Para obtener más información, consulte"Creando Informes" (p. 126)

       Nota

       Cada propiedad que genera problemas de seguridad se marca con un icono. Consulte el tooltip del icono para conocer más detalles. Puede ser necesaria más investigación local.



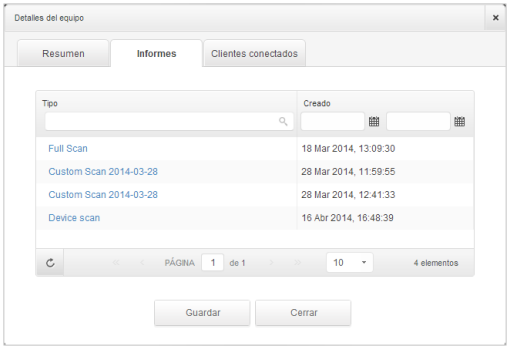
Detalles del equipo - Información general

     - La sección **Endpoint Security Relay** (disponible para clientes de punto final normales) muestra información sobre el Endpoint Security Relay al que está conectado el equipo actual.

- Haga clic en la pestaña **Registros de análisis** para ver información detallada sobre todas las tareas de análisis ejecutadas en el equipo. Haga clic en el informe de análisis que le interese para abrirlo en una página nueva del navegador.

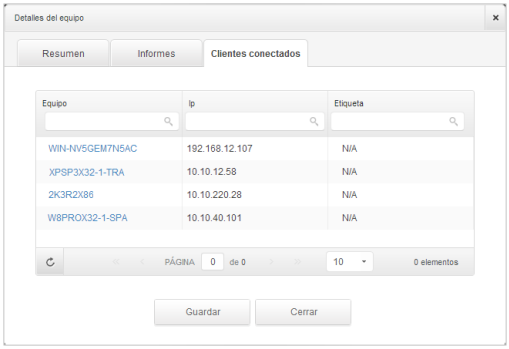
  Para moverse por las páginas, use las opciones de navegación en la parte inferior de la tabla. Si hay muchas entradas, puede usar las opciones de filtrado disponibles en la parte superior de la tabla.

  Haga clic en el botón **Actualizar** de la esquina inferior izquierda de la tabla para actualizar la lista de registros de análisis.



Detalles del equipo - Registros de análisis

- Para equipos con rol de Endpoint Security Relay, también está disponible la pestaña **Clientes conectados**, donde puede ver la lista de puntos finales conectados.



Detalles del equipo - Clientes conectados

5.4. Clasificación, filtrado y búsqueda de equipos

Dependiendo del número de equipos, la tabla de equipos puede ampliarse a varias páginas (sólo se muestran de forma predeterminada 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. Por ejemplo, puede buscar un equipo específico o elegir ver únicamente los equipos administrados.

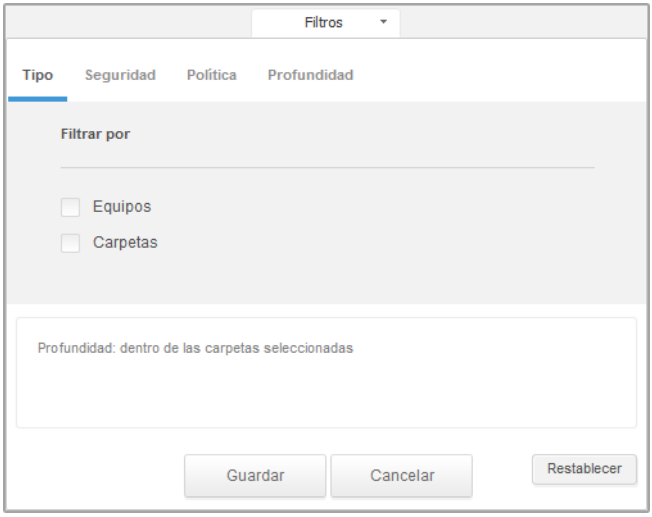
5.4.1. Ordenar equipos

Para ordenar datos según una columna específica, haga clic en los encabezados de las columnas. Por ejemplo, si desea ordenar los equipos por el nombre, haga clic en el encabezado **Nombre**. Si hace clic en el encabezado otra vez, los equipos se mostrarán en orden inverso.

Ordenar equipos

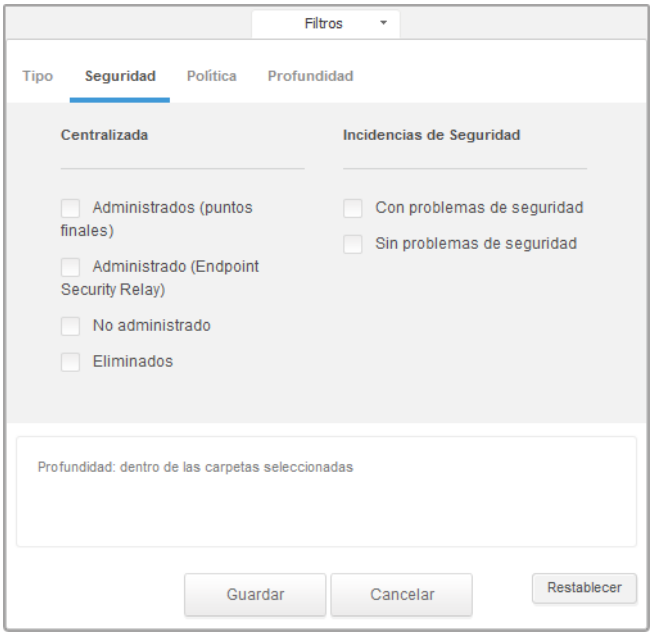
5.4.2. Filtrar equipos

1. Seleccione el grupo deseado desde el panel lateral izquierdo.
2. Haga clic en el menú **Filtros** ubicado encima de la tabla.
3. Seleccione el criterio de filtrado de la siguiente manera:
   - **Tipo**. Seleccione el tipo de entidades que desea mostrar (equipos, carpetas o ambas).



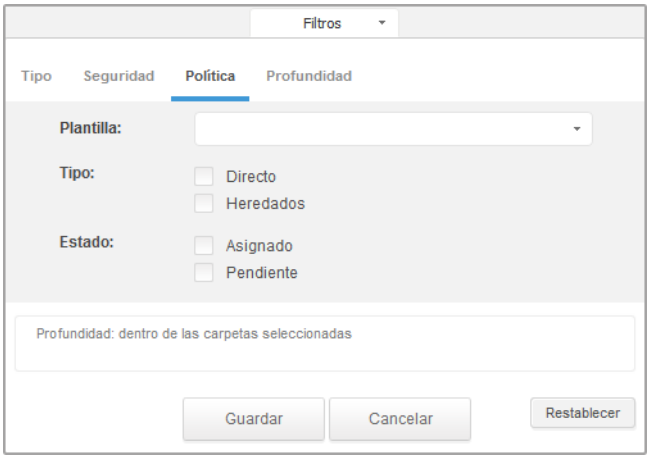
Equipos - Filtrar por tipo

- **Seguridad**. Elíjalo para mostrar equipos por estado de seguridad y administración.



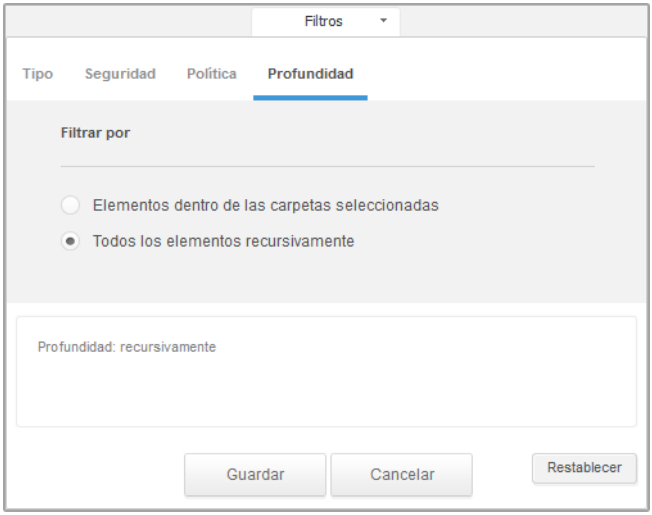
Equipos - Filtrar por seguridad

- **Política**. Seleccione la plantilla de política según la cual quiere filtrar los equipos, el tipo de asignación de política (Directa o Heredada), así como el estado de asignación de la política (Asignada o Pendiente).



Equipos - Filtrar por política

- **Profundidad**. Al administrar una red de equipos con estructura de árbol, los equipos incluidos en subgrupos no se muestran cuando se selecciona el grupo raíz. Seleccione **Todos los elementos recursivamente** para ver todos los equipos incluidos en el grupo actual y en sus subgrupos.



Equipos - Filtrar por profundidad

Nota
En la parte inferior de la ventana **Filtros**, puede ver todos los criterios de filtrado seleccionados.
Si desea eliminar todos los filtros, haga clic en el botón **Restablecer**.

4. Haga clic en **Guardar** para filtrar los equipos por el criterio seleccionado. El filtro permanece activo en la página **Red** hasta que cierra la sesión o restablece el filtro.

5.4.3. Buscando Equipos

1. Seleccione el grupo deseado desde el panel lateral izquierdo.
2. Escriba el término de búsqueda en el cuadro correspondiente bajo los encabezados de las columnas (Nombre, SO o IP) desde el panel lateral derecho. Por ejemplo, escriba la IP del equipo que está consultando en el campo **IP**. Sólo aparecerá en la tabla el equipo coincidente.

   Vacíe el cuadro de búsqueda para mostrar la lista completa de equipos.

Buscar equipos

5.5. Ejecutar tareas en los equipos

Desde la página **Red**, puede ejecutar de forma remota un determinado número de tareas administrativas en los equipos.

Esto es lo que puede hacer:

- “Analizar” (p. 45)
- “Instalar cliente” (p. 52)
- “Modificar instalador” (p. 55)
- “Desinstalar cliente” (p. 56)
- “Actualizar” (p. 57)
- “Reiniciar el Equipo” (p. 57)
- “Descubrimiento de red” (p. 58)

Puede elegir crear tareas individuales para cada equipo o para grupos de equipos. Por ejemplo, puede instalar de forma remota el Endpoint Security en un grupo de equipos no administrados. En otro momento posterior, puede crear una tarea de análisis para un determinado equipo desde el mismo grupo.

Para cada equipo, sólo puede ejecutar tareas compatibles. Por ejemplo, si selecciona un equipo no administrado, sólo puede elegir **Instalar cliente**; todas las demás tareas aparecen desactivadas.

Para un grupo, la tarea seleccionada se creará únicamente para equipos compatibles. Si ninguno de los equipos en el grupo es compatible con la tarea seleccionada, se le notificará que la tarea no pudo crearse.

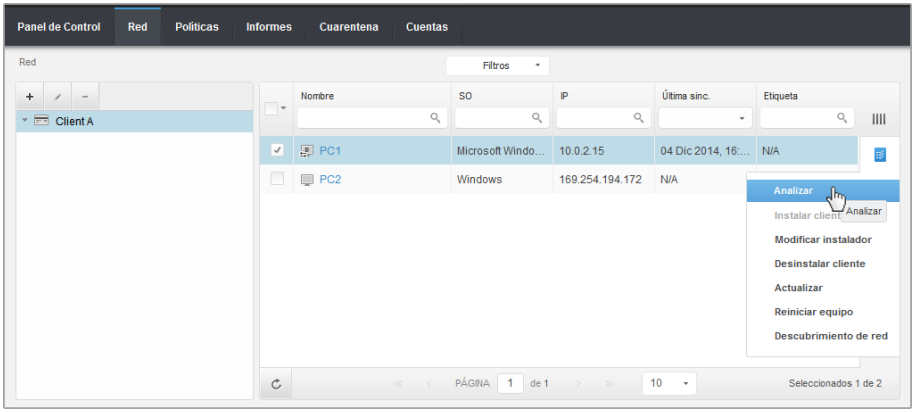
Una vez creada, la tarea se iniciará inmediatamente en los equipos conectados. Si un equipo no está conectado, la tarea se ejecutará tan pronto como vuelva a conectarse.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.1. Analizar

Para ejecutar de forma remota una tarea de análisis en uno o varios equipos:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación correspondientes a los equipos que quiere analizar.
4. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Analizar**.

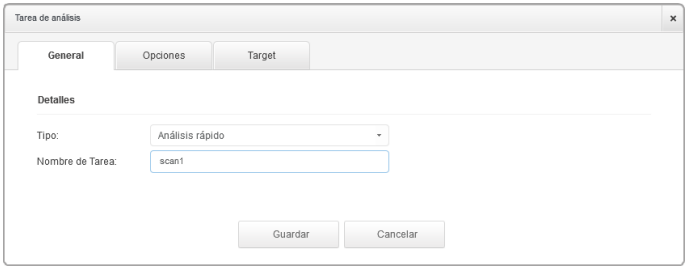


Tarea de análisis de equipos

Aparecerá una nueva ventana de configuración.

5. Configure las opciones de análisis:

   - En la pestaña **General** puede seleccionar el tipo de análisis y puede escribir un nombre para la tarea de análisis. El nombre de la tarea de análisis está para ayudarle a identificar fácilmente el análisis actual en la página **Tareas**.



Tarea de análisis de equipos - Configuración de ajustes generales

Seleccione el tipo de análisis desde el menú **Tipo**:

– **Quick Scan** utiliza el análisis en la nube para detectar malware ejecutándose en el sistema. Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.

Nota

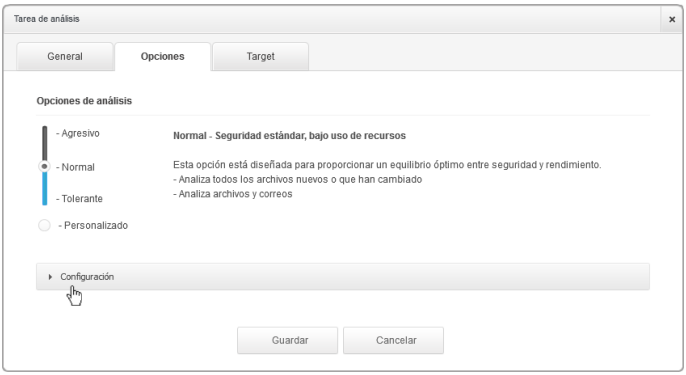
Quick Scan sólo detecta malware existente, sin emprender ninguna acción. Si se encuentra malware durante un análisis Quick Scan, debe ejecutar una tarea de análisis completo del sistema para eliminar el malware detectado.

– **Análisis completo** analiza el equipo por completo en busca de todo tipo de malware que pueda amenazar su seguridad, como virus, spyware, adware, rootkits y otros.

– **Análisis personalizado** le permite elegir las ubicaciones a analizar y configurar las opciones de análisis. Para definir un análisis personalizado:

  • Diríjase a la pestaña **Opciones** para definir las opciones de análisis. Haga clic en el nivel de seguridad que mejor se adapte a sus necesidades (Agresivo, Normal o Tolerante). Use la descripción del lateral derecho de la escala como guía para su elección.

    Las opciones de análisis de la sección **Ajustes** se configuran automáticamente, basándose en el perfil seleccionado. Sin embargo, si lo desea, puede configurarlas en detalle. Para hacer esto, marque la casilla de verificación **Personalizado** y diríjase a la sección **Opciones**.



Tarea de análisis de equipos

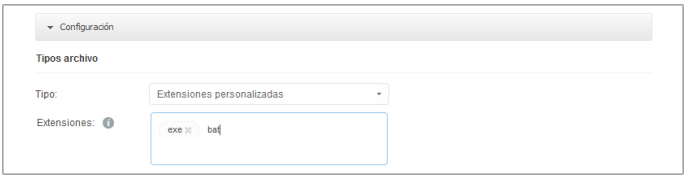
Tiene las siguientes opciones a su disposición:

– **Tipos archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede ajustar Endpoint Security para analizar todos los archivos (con independencia de su extensión), archivos de aplicación solamente o extensiones de archivo específicas que considere peligrosas. Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.

Nota

Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a “Lista de tipos de archivos de aplicación” (p. 151).

Si desea que sólo se analicen extensiones específicas, elija **Extensiones personalizadas** desde el menú y luego introduzca las extensiones en el campo de edición, pulsando `Intro` después de cada extensión.



Opciones de la tarea de análisis de equipos - Añadir extensiones personalizadas

– **Archivos.** Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. El malware puede afectar al sistema sólo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

> **Nota**
> El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar el interior de los comprimidos.** Seleccione esta opción si desea comprobar los archivos comprimidos en busca de malware. Si decide utilizar esta opción, puede configurar las siguientes opciones y optimización:
  - **Limitar tamaño de archivo a (MB).** Puede establecer un límite de tamaño aceptado máximo para los archivos a analizar. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).
  - **Máxima profundidad de archivo (niveles).** Marque la casilla de verificación correspondiente y elija la profundidad de archivo máxima desde el menú. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.
- **Analizar archivos de correo.** Seleccione esta opción si desea habilitar el análisis archivos de mensajes de correo y bases de datos de correo, incluyendo formatos de archivo tales como .eml, .msg, .pst, .dbx, .mbx, .tbb y otros.

Nota
Tenga en cuenta que el análisis de adjuntos de correo hace un uso intensivo de los recursos y puede afectar al rendimiento de su sistema.

– **Varios.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.

  • **Analizar los sectores de arranque.** Para analizar el sector de arranque del sistema. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

  • **Analizar registro.** Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.

  • **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de rootkits y objetos ocultos que utilicen este tipo de software.

  • **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger.

  • **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.

  • **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en el equipo.

  • **Analizar archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.

  • **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Una aplicación potencialmente no deseada (APND) es un programa que podría haberse instalado en el PC contra su voluntad y que a veces acompaña a software freeware. Estos programas pueden instalarse sin el consentimiento del usuario (también llamados adware) o incluirse por defecto en el kit de instalación. Los efectos potenciales de estos programas incluyen la visualización de ventanas emergentes, la instalación de barras de herramientas no deseadas en el navegador por defecto o la ejecución de diversos procesos en segundo plano y la disminución del rendimiento del PC.

– **Acciones.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:

- **Al encontrar un archivo infectado.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Endpoint Security puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Si se detecta un archivo infectado, Endpoint Security intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

  Importante
  Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **al encontrar un archivo sospechoso.** Los archivos detectados como sospechosos por el análisis heurístico. Dado que B-HAVE es una tecnología de análisis heurístico, Endpoint Security no puede asegurar que el archivo esté realmente infectado con malware. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

  Las tareas de análisis se configuran de forma predeterminada para ignorar los archivos sospechosos. Quizá desee cambiar la acción predeterminada para mover archivos sospechosos a la cuarentena. Los archivos en cuarentena se envían periódicamente para su análisis a los laboratorios de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

- **Cuando se encuentra un rootkit.** Los rootkits representan un software especializado utilizado para ocultar archivos del sistema operativo. Aunque no son dañinos por su naturaleza, los rootkits se usan normalmente para ocultar malware o para encubrir la presencia de un intruso en el sistema.

  Los rootkits detectados y archivos ocultos se ignoran de forma predeterminada.

Aunque no se recomienda, puede cambiar las acciones predeterminadas. Puede indicar la segunda acción a realizar en caso que la primera falle, y diferentes acciones para cada categoría. Seleccione, en los menús correspondientes, la primera y segunda acción a realizar para cada tipo de archivo detectado. Dispone de las siguientes opciones:

Desinfectar
Elimina el código de malware de los archivos infectados. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados.

Mover a Cuarentena
Mueva los archivos detectados desde su ubicación actual a la carpeta de cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de cuarentena desde la página Cuarentena de la consola.

Eliminar
Elimina los archivos detectados del disco, sin mostrar advertencia alguna. Se aconseja que evite utilizar esta acción.

Omitir
No se realizará ninguna acción sobre los archivos detectados. Estos archivos solo aparecerán en el log de análisis.

- Diríjase a la pestaña **Objetivo** para añadir las ubicaciones que desea que se analicen en los equipos objetivos.

  En la sección **Analizar objetivo** puede añadir un archivo nuevo o carpeta para analizar:

  a. Elija desde el menú desplegable una ubicación predefinida o introduzca las **Rutas específicas** que quiere analizar.

  b. Especifique la ruta del objeto a analizar en el campo de edición.

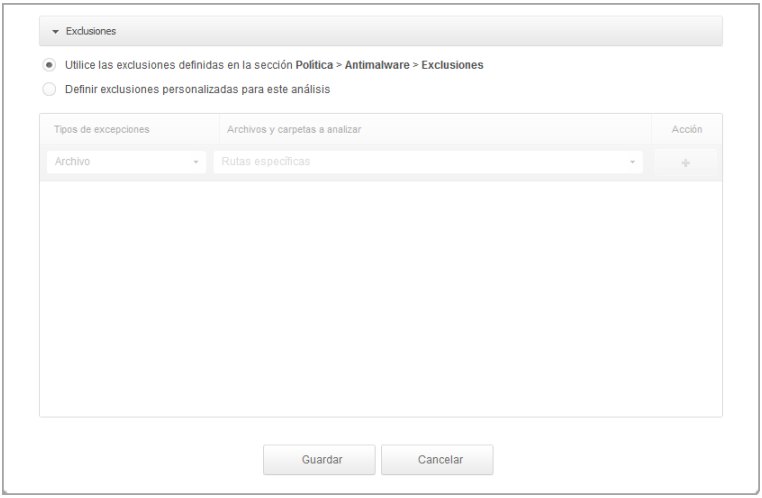
  – Si ha escogido una ubicación predefinida, complete la ruta según sea necesario. Por ejemplo, para analizar la carpeta `Archivos de programa` completa, es suficiente con seleccionar la ubicación predefinida correspondiente desde el menú desplegable. Para analizar una carpeta específica desde `Archivos de programa`, debe completar la ruta añadiendo una barra invertida (\) y el nombre de la carpeta.

  – Si ha elegido **Rutas específicas**, escriba la ruta completa del objeto a analizar. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo. Para obtener más información con respecto a las variables del sistema, consulte"Usar variables de sistema" (p. 151)

  c. Haga clic en el botón + **Añadir** correspondiente.

  Para editar una ubicación existente, haga clic en ella. Para eliminar una ubicación de la lista, mueva el cursor sobre ella y haga clic en el botón − **Borrar** correspondiente.

Haga clic en las secciones **Excepciones** si desea definir excepciones de objetivos.



Tarea de análisis de equipos - Definición de exclusiones

Puede, o bien utilizar las exclusiones definidas por la política, o bien definir exclusiones explícitas para la tarea de análisis actual. Para obtener más información sobre excepciones, consulte “Exclusiones” (p. 97).

6. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.
7. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.2. Instalar cliente

Para proteger sus equipos con Security for Endpoints, debe instalar Endpoint Security en cada uno de ellos.

Aviso

- El primer equipo en que instale la protección ha de tener rol de Endpoint Security Relay, o no podrá implementar Endpoint Security en otros equipos de la red.
- El equipo con rol de Endpoint Security Relay debe estar encendido y conectado para que los clientes se comuniquen con Control Center.

Una vez que haya instalado un cliente Endpoint Security con rol de Endpoint Security Relay en una red, éste detectará automáticamente los equipos desprotegidos de esa red.

La protección de Security for Endpoints puede instalarse en esos equipos de forma remota desde Control Center.

La instalación remota se ejecuta en segundo plano, sin que el usuario lo perciba.

Aviso

Antes de realizar la instalación, asegúrese de desinstalar software antimalware y cortafuego ya existente en los equipos. Instalar Security for Endpoints sobre software de seguridad existente puede afectar al funcionamiento y causar problemas importantes con el sistema. Windows Defender y el Cortafuego de Windows se desactivarán automáticamente cuando se inicie la instalación.

Para instalar de forma remota la protección de Security for Endpoints en uno o varios equipos:

1. Diríjase a la página **Red**.
2. Seleccione el grupo de red deseado en el panel de la izquierda. Las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.

   Nota

   Opcionalmente, puede aplicar filtros para mostrar únicamente los equipos no administrados. Haga clic en el botón **Filtros** y seleccione las siguientes opciones: **No administrados** de la categoría **Seguridad** y **Todos los elementos recursivamente** de la categoría **Profundidad**.

3. Seleccione las entidades (equipos o grupos de equipos) en las que desee instalar la protección.
4. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Instalar cliente**. El asistente de **Instalar cliente** se está mostrando.
5. Configure las opciones de instalación:
   - Programe el momento de la instalación:
     - **Ahora**, para poner en marcha la implementación de inmediato.
     - **Programado**, para configurar el intervalo de recurrencia de la implementación. En este caso, seleccione el intervalo de tiempo que desee (cada hora, a diario o semanalmente) y configúrelo según sus necesidades.

       Nota

       Por ejemplo, cuando hay que realizar determinadas operaciones en el equipo objetivo antes de instalar el cliente (como la desinstalación de otros programas y el reinicio del sistema operativo), puede programar la tarea de implementación para que se ejecute cada 2 horas. La tarea se lanzará en los equipos objetivo cada 2 horas hasta que culmine correctamente.

   - Seleccione el rol que desee que tenga el cliente:

  - **Punto final**. Seleccione esta opción si desea instalar el cliente en un punto final normal.
  - **Endpoint Security Relay**. Seleccione esta opción para instalar el cliente con rol Endpoint Security Relay en el equipo objetivo. Endpoint Security Relay es un rol especial que instala un servidor de actualizaciones en el equipo objetivo junto con Endpoint Security. Éste puede utilizarse para actualizar los demás clientes de la red, reduciendo el uso de ancho de banda entre las máquinas clientes y Control Center.
- Seleccione los módulos de protección que desea instalar. Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.
- En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.
- Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
- Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security en una ubicación diferente. En este caso, escriba la ruta deseada en el campo correspondiente. Utilice las reglas de Windows al escribir la ruta (por ejemplo, `D:\carpeta`). Si la carpeta especificada no existe, se creará durante la instalación.
- Durante la instalación silenciosa, se analiza el equipo en busca de malware. A veces es necesario un reinicio del sistema para completar la eliminación del malware.

  Seleccionar **Reiniciar automáticamente (si es necesario)** para asegurarse de que el malware detectado es eliminado por completo antes de la instalación. De lo contrario la instalación puede fallar.
- Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.
- Haga clic en **Siguiente**.
- Dependiendo del rol del cliente (punto final o Endpoint Security Relay), escoja la entidad a través de la cual se comunicarán los clientes:
  - **Bitdefender Cloud**, si desea actualizar los clientes directamente desde Internet.
  - **Endpoint Security Relay**, si desea conectar los puntos finales a un Endpoint Security Relay instalado en su red. Todos los equipos con rol de Endpoint Security Relay detectados en su red figurarán en la tabla que se muestra a continuación. Seleccione el Endpoint Security Relay que desee. Los puntos finales conectados se comunicarán con Control Center solo mediante el Endpoint Security Relay especificado.

Importante
El puerto 7074 debe estar abierto para que funcione la implementación mediante Endpoint Security Relay.

6. Haga clic en **Siguiente**.
7. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los puntos finales seleccionados

   Puede añadir las credenciales requeridas escribiendo el usuario y contraseña de cada sistema operativo objetivo.

   Nota
   Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota Endpoint Security en los equipos.

   Para añadir las credenciales del sistema operativo requeridas:

   a. Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta. Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

      Utilice las convenciones de Windows cuando introduzca el nombre de una cuenta de usuario de dominio, por ejemplo, `usuario@dominio.com` o `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas en ambas formas (`usuario@dominio.com` y `dominio\usuario`).

      Nota
      Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

   b. Haga clic en el botón **+ Añadir**. La cuenta se añade a la lista de credenciales.
   c. Marque las casillas de verificación correspondientes a la cuenta que desea usar.
8. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.3. Modificar instalador

Para cambiar los módulos de protección instalados en uno o varios equipos:

1. Diríjase a la página **Red**.

2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación correspondientes a los equipos administrados en los que quiere modificar los módulos de protección instalados.
4. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Modificar instalador**.
5. En la sección **Módulos** seleccione únicamente los módulos de protección que desea que se instalen:

   Antimalware
   El módulo Antimalware protege al sistema contra todo tipo de amenazas de malware (virus, troyanos, spyware, rootkits, adware y otros).

   Cortafuegos
   El Cortafuego protege el equipo de los intentos de conexión entrantes y salientes no autorizados.

   Control de Contenido
   El módulo Control de contenido le ayuda a controlar el acceso de usuarios a Internet y a las aplicaciones. Por favor, tenga en cuenta que la configuración del Control de contenido se aplica a todos los usuarios que inician sesión en los equipos de destino.

   Nota
   Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.

6. Marque la opción **Reiniciar si es necesario** para permitir que el equipo se reinicie automáticamente para completar la instalación.
7. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.4. Desinstalar cliente

Para desinstalar de forma remota la protección de Security for Endpoints de uno o varios equipos:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación correspondientes a los equipos en los que quiere desinstalar la protección de Security for Endpoints.

4. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Desinstalar cliente**.
5. Se muestra una ventana de configuración que le permite optar por conservar los elementos en la cuarentena de la máquina cliente.
6. Haga clic en **Guardar** para crear la tarea. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

Nota
Si quiere reinstalar la protección, asegúrese primero de reiniciar el equipo.

5.5.5. Actualizar

Consulte el estado de los equipos periódicamente. Si observa un equipo con problemas de seguridad, haga clic en su nombre para mostrar la página **Detalles del equipo**. Para más información, diríjase a "Equipos con problemas de seguridad" (p. 36).

Los clientes obsoletos o las firmas sin actualizar representan un problema de seguridad. En este caso, debería ejecutar una actualización en el equipo correspondiente. Esta tarea puede realizarse localmente desde el equipo mismo, o bien de forma remota desde Control Center.

Para actualizar el cliente y las firmas de forma remota en equipos administrados:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación de los equipos donde quiere realizar la actualización del cliente.
4. Haga clic en el botón **Tarea** del lateral derecho de la tabla y seleccione **Actualización**. Aparecerá una nueva ventana de configuración.
5. Puede optar por actualizar solo el producto, solo las firmas de virus, o ambos.
6. Haga clic en **Actualizar** para ejecutar la tarea. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.6. Reiniciar el Equipo

Puede elegir reiniciar de forma remota los equipos administrados.

Nota

Consulte la página **Red > Tareas** antes de reiniciar determinados equipos. Las tareas creadas previamente pueden estar todavía en proceso en los equipos objetivo.

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación correspondientes a los equipos que quiere reiniciar.
4. Haga clic en el botón **Tareas** del lateral derecho de la tabla y seleccione **Reiniciar equipo**.
5. Seleccione la opción reiniciar programación:
   - Seleccione **Reiniciar ahora** para reiniciar los equipos inmediatamente.
   - Seleccione **Reiniciar el** y use los campos inferiores para programar el reinicio en la fecha y hora deseadas.
6. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.5.7. Descubrimiento de red

Endpoint Security con rol de Endpoint Security Relay lleva a cabo automáticamente la detección de redes cada hora. No obstante, puede ejecutar manualmente la tarea de detección de redes desde Control Center cuando desee, partiendo de cualquier máquina protegida por Endpoint Security.

Para ejecutar una tarea de descubrimiento de red en su red:

1. Diríjase a la página **Red**.
2. Seleccione el grupo de equipos deseado en el panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque las casillas de verificación correspondientes a los equipos con los que quiere llevar a cabo el descubrimiento de red.
4. Haga clic en el botón **Tarea** a la derecha de la tabla y elija **Descubrimiento de red**.
5. Aparecerá un mensaje de confirmación. Haga clic en **Sí**.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a Viewing and Managing Tasks.

5.6. Crear informes rápidos

Puede elegir crear informes instantáneos de los equipos administrados empezando desde la página **Red**:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.

   Opcionalmente, puede filtrar los contenidos del grupo seleccionado solo por los equipos administrados.
3. Marque las casillas de verificación correspondientes a los equipos que se incluirán en el informe.
4. Haga clic en el botón **Informe** del lateral derecho de la tabla y seleccione el tipo de informe desde el menú. Los informes de actividad solamente incluirán datos de la última semana. Para más información, diríjase a “Tipos de informes disponibles” (p. 123).
5. Configure las opciones del informe. Para obtener más información, consulte“Creando Informes” (p. 126)
6. Haga clic en **Generar**. El informe se mostrará inmediatamente. El tiempo requerido para crear los informes puede variar dependiendo del número de equipos seleccionados.

5.7. Asignando Políticas

Los ajustes de seguridad en los equipos administrados se administran usando políticas.

Desde la sección **Red** puede consultar, modificar y asignar políticas para cada equipo o grupo de equipos.

Nota

Puede consultar o modificar los ajustes de seguridad para los equipos administrados o para los grupos. Para facilitar esta tarea, puede filtrar los contenidos de la tabla por equipos administrados.

Para ver la política asignada a un equipo concreto:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Haga clic en el nombre del equipo administrado en el que está interesado. Aparecerá una ventana de detalles.
4. En la sección **Seguridad**, haga clic en el nombre de la política actual para consultar sus ajustes.

5. Puede cambiar los ajustes de seguridad según sus necesidades, siempre y cuando el propietario de la política haya permitido que otros usuarios realicen cambios en dicha política. Tenga en cuenta que cualquier cambio que realice afectará a todos los demás equipos que tengan la misma política asignada.

   Para obtener más información sobre la modificación de políticas de equipos consulte “Políticas de equipos” (p. 75).

Para asignar una política a un equipo o grupo:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque la casilla de verificación del equipo o grupo deseado. Puede seleccionar uno o varios objetos del mismo tipo solamente desde el mismo nivel.
4. Haga clic en el botón **Política** del lateral derecho de la tabla.
5. Haga los ajustes necesarios en la ventana **Asignación de política**. Para más información, diríjase a “Asignar políticas a objetos de red” (p. 73).

5.8. Eliminar equipos del inventario de red

Si no tiene previsto administrar algunos de los equipos detectados, puede elegir excluirlos del inventario de red. Además puede eliminar permanentemente los equipos excluidos del inventario de la red.

5.8.1. Exclusión de equipos del inventario de red

Para excluir equipos del inventario de red:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Marque la casilla de verificación correspondiente al equipo que quiere excluir.
4. Haga clic en el botón **Eliminar** del lateral derecho de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

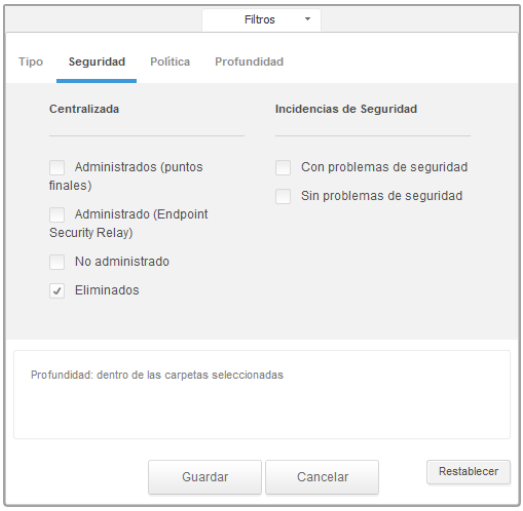
   

   Nota

   Si elimina un equipo administrado, Endpoint Security se desinstalará automáticamente de este equipo.

   Una vez que haya eliminado un equipo ya no podrá verlo en la tabla. Los equipos eliminados todavía existen en la base de datos de Small Office Security, pero ya no son visibles.

Es posible que quiera volver a administrar algunos de los equipos anteriormente eliminados En este caso, tiene que mostrar los equipos eliminados e instalar Endpoint Security en los que le interese. Para mostrar los equipos eliminados, haga clic en el menú **Filtros** situado encima de la tabla, acceda a la pestaña **Seguridad**, marque la opción **Eliminados** y haga clic en **Guardar**.



Equipos - Filtrar por puntos finales eliminados

Nota
Si reinstala la protección en un equipo excluido, se detectará como administrado y restaurado en la tabla.

5.8.2. Eliminar equipos de forma permanente

Para eliminar equipos permanentemente del inventario de red:

1. Diríjase a la página **Red**.
2. Seleccione el grupo deseado desde el panel lateral izquierdo. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Filtre el contenido de la tabla por equipos **Eliminados**.
4. Marque las casillas de verificación correspondientes a los equipos que quiere eliminar.
5. Haga clic en el botón **Eliminar** del lateral derecho de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

Los equipos correspondientes se eliminan permanentemente de la base de datos de Small Office Security.

Aviso
No puede restaurar un equipo eliminado permanentemente en la base de datos de Small Office Security.

5.9. Paquetes de instalación

Los componentes de protección de Small Office Security pueden instalarse en los objetos de red objetivo ya sea implementándolos desde Control Center o descargando el paquete de instalación necesario y ejecutándolo manualmente en los objetos de red objetivo.

Puede administrar paquetes de instalación desde la página **Red > Paquetes**.

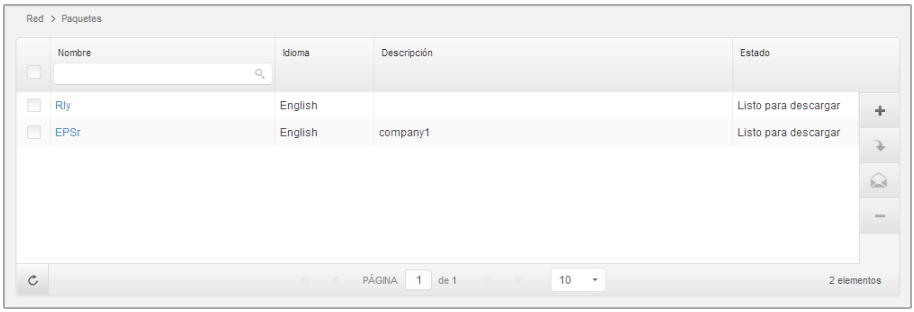
5.9.1. Crear paquetes de instalación

Puede que necesite hacer determinadas personalizaciones en los paquetes de instalación, para que se ajusten mejor a sus necesidades de seguridad.

Crear paquetes de instalación de Endpoint Security

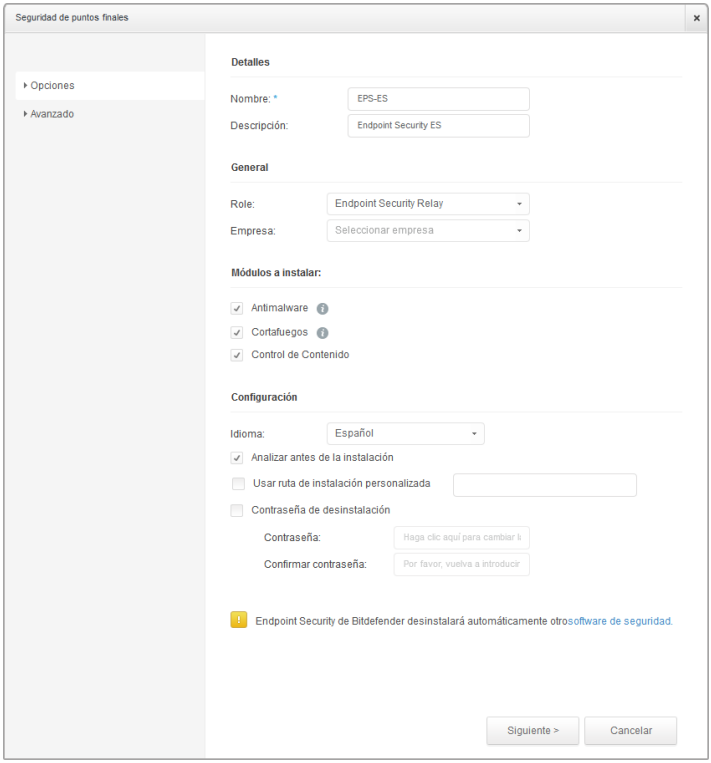
Para crear un paquete de instalación de Endpoint Security:

1. Conéctese e inicie sesión en Control Center usando su cuenta.
2. Vaya a la página **Red > Paquetes**.



La página Paquetes

3. Haga clic en el botón + **Añadir** del lateral derecho de la tabla. Aparecerá una nueva ventana de configuración.



Crear paquetes Endpoint Security - Opciones

4. Escriba un nombre adecuado y una descripción para el paquete de instalación que quiere crear.
5. Seleccione el rol del equipo objetivo:
   - **Punto final**. Seleccione esta opción para crear el paquete para un punto final normal.
   - **Endpoint Security Relay**. Seleccione esta opción para crear el paquete para un punto final con rol Endpoint Security Relay. Endpoint Security Relay es un rol especial que instala un servidor de actualizaciones en el equipo objetivo junto con Endpoint Security. Éste puede utilizarse para actualizar los demás clientes de la red, reduciendo el uso de ancho de banda entre las máquinas clientes y Control Center.
6. Seleccione la empresa donde se utilizará el paquete de instalación.
7. Seleccione los módulos de protección que desea instalar.
8. En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.

9. Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
10. Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security en una ubicación diferente. En este caso, escriba la ruta deseada en el campo correspondiente. Utilice las reglas de Windows al escribir la ruta (por ejemplo, `D:\carpeta`). Si la carpeta especificada no existe, se creará durante la instalación.
11. Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.
12. Haga clic en **Siguiente**.
13. Dependiendo del rol del paquete de instalación (punto final o Endpoint Security Relay), escoja la entidad a la que se conectarán periódicamente los equipos objetivo para actualizar el cliente:
    - **Bitdefender Cloud**, si desea actualizar los clientes directamente desde Internet.
    - **Endpoint Security Relay**, si desea conectar los puntos finales a un Endpoint Security Relay instalado en su red. Todos los equipos con rol de Endpoint Security Relay detectados en su red figurarán en la tabla que se muestra a continuación. Seleccione el Endpoint Security Relay que desee. Los puntos finales conectados se comunicarán con Control Center solo mediante el Endpoint Security Relay especificado.

      Importante
      El puerto 7074 debe estar abierto para que funcione la implementación mediante Endpoint Security Relay.
14. Haga clic en **Guardar**.

El nuevo paquete de instalación aparecerá en la lista de paquetes de la empresa objetivo.

5.9.2. Descargar los paquetes de instalación

Para descargar los paquetes de instalación de Endpoint Security:

1. Inicie sesión en Control Center desde el equipo en el que desee instalar la protección.
2. Vaya a la página **Red > Paquetes**.
3. Seleccione el paquete de instalación de Endpoint Security que desee descargar.
4. Haga clic en el botón **Descargar** a la derecha de la tabla y seleccione el tipo de instalador que quiera utilizar. Hay disponibles dos tipos de archivos de instalación:
    - **Downloader**. El downloader primero descarga el kit de instalación completo desde los servidores de la nube de Bitdefender y luego inicia la instalación. Es pequeño en

tamaño y puede ejecutarse tanto en sistemas de 32-bit como de 64-bit (lo que lo hace más fácil de distribuir). Por otro lado, requiere una conexión a Internet activa.

- **Kit completo**. El kit completo se utiliza para instalar la protección en los equipos sin conexión a Internet o con conexiones lentas. Descargue este archivo en un equipo conectado a Internet y distribúyalo a otros equipos usando un medio de almacenamiento externo o compartiéndolo en la red.

Nota
Versiones de kit completo disponibles:

– **SO Windows:** sistemas de 32 bits y 64 bits

– **Mac OS X:** solo sistemas de 64 bits

Asegúrese de usar la versión correcta para el equipo donde instala.

5. Guarde el archivo en el equipo.

5.9.3. Enviar enlaces de descarga de paquetes de instalación por correo electrónico

Es posible que tenga que informar rápidamente a otros usuarios de que hay un paquete de instalación listo para descargar. En tal caso, siga los pasos descritos a continuación:

1. Vaya a la página **Red > Paquetes**.
2. Seleccione el paquete de instalación que desee.
3. Haga clic en el botón **Enviar enlaces de descarga** del lateral derecho de la tabla. Aparecerá una nueva ventana de configuración.
4. Introduzca la dirección de correo electrónico de cada usuario que desea que reciba el enlace de descarga del paquete de instalación. Pulse `Intro` tras cada dirección.

   Asegúrese de la validez de todas las direcciones de correo electrónico que introduzca.
5. Si desea ver los enlaces de descarga antes de enviarlos por correo electrónico, haga clic en el botón **Ver enlaces de instalación**.
6. Haga clic en **Enviar**. Se envía un correo electrónico que contiene el enlace de instalación a cada dirección de correo electrónico especificada.

5.10. Ver y administrar tareas

La página **Red > Tareas** le permite ver y administrar todas las tareas que haya creado.

Una vez creada la tarea para uno de los diversos objetos de la red, puede ver la tarea en la tabla.

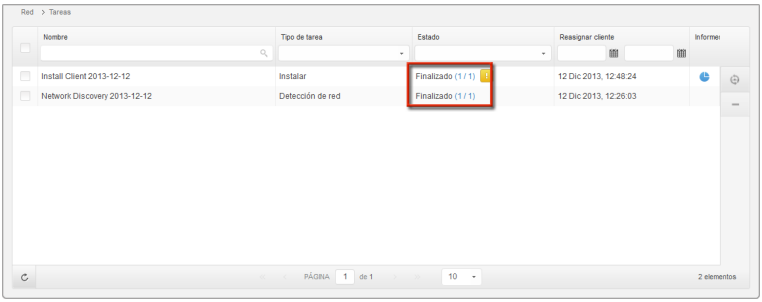
Desde la página **Red > Tareas** puede hacer lo siguiente:

- Comprobar el estado de la tarea
- Ver informes de tareas
- Volver a ejecutar tareas
- Eliminar Tareas

5.10.1. Comprobar el estado de la tarea

Cada vez que cree una tarea para uno o varios objetos de red, querrá consultar su progreso y recibir notificaciones cuando se produzca un error.

Diríjase a la página **Red > Tareas** y compruebe la columna **Estado** para cada tarea en la que esté interesado. Puede comprobar el estado de la tarea principal y también puede obtener información detallada sobre cada subtarea.



La página Tareas

- **Comprobación del estado de la tarea principal**.

  La tarea principal se refiere a la acción ejecutada sobre los objetos de la red (como instalar un cliente o hacer un análisis) y contiene un número determinado de subtareas, una para cada objeto de red seleccionado. Por ejemplo, una tarea de instalación principal creada para ocho equipos contiene ocho subtareas. Los números entre corchetes representan el grado de finalización de las subtareas. Por ejemplo, (2/8) significa que se han finalizado dos de las ocho tareas.

  El estado de la tarea principal puede ser:
  - **Pendiente**, cuando no ha comenzado todavía ninguna de las subtareas.
  - **En curso**, cuando todas las subtareas están en ejecución. El estado de la tarea principal se mantiene En curso hasta que finaliza la última subtarea.
  - **Terminado**, cuando todas las subtareas se han finalizado (correctamente o incorrectamente). En caso de realizarse incorrectamente una subtarea, se muestra un símbolo de advertencia.

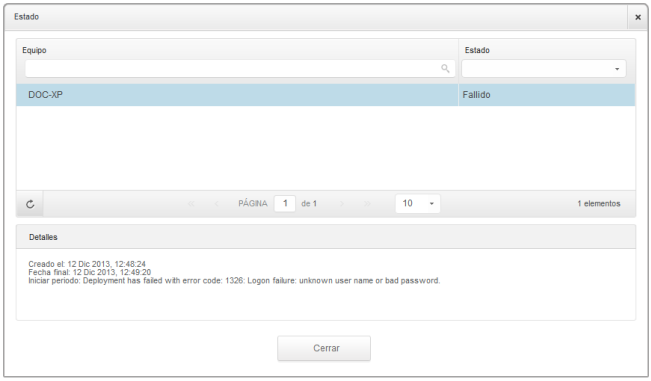
- **Comprobar el estado de las subtareas**.

  Diríjase a la subtarea que le interese y haga clic en el enlace disponible en la columna **Estado** para abrir la ventana **Estado**. Puede ver la lista de objetos de red asignada con

la tarea principal y el estado correspondiente a la subtarea. El estado de las subtareas puede ser:

- **En curso**, cuando la subtarea todavía está en ejecución.
- **Finalizado**, cuando la subtarea ha finalizado correctamente.
- **Pendiente**, cuando la subtarea todavía no se ha iniciado. Esto puede ocurrir en las siguientes situaciones:
  - La subtarea está esperando en la cola.
  - Hay problemas de conexión entre Control Center y el objeto de red objetivo.
- **Fallido**, cuando la subtarea no puede iniciarse o se ha detenido a consecuencia de un error, como la autenticación incorrecta o la falta de espacio en memoria.

Para ver los detalles de cada subtarea, selecciónela y consulte la sección **Detalles** en la parte inferior de la tabla.



Detalles de estado de la tarea

Obtendrá información sobre:

- Fecha y hora en la que se inició la tarea.
- Fecha y hora en la que se terminó la tarea.
- Descripción de los errores encontrados.

5.10.2. Ver los informes de tareas

Desde la página **Red > Tareas** tiene la opción de ver rápidamente informes de tareas de análisis.

1. Diríjase a la página **Red > Tareas**.
2. Marque la casilla de verificación correspondiente a la tarea de análisis que le interese.

3. Haga clic en el botón correspondiente de la columna **Informes**. Espere hasta que se muestre el informe. Para más información, diríjase a “Usar informes” (p. 123).

5.10.3. Volver a ejecutar tareas

Por diversas razones, las tareas de instalación, desinstalación o actualización del cliente quizá no lleguen a completarse. Puede escoger volver a ejecutar esas tareas fallidas en lugar de crear otras nuevas, siguiendo estos pasos:

1. Diríjase a la página **Red > Tareas**.
2. Marque las casillas de verificación correspondientes a las tareas fallidas.
3. Haga clic en el botón **Ejecutar de nuevo** a la derecha de la tabla. Se reiniciarán las tareas fallidas y su estado cambiará a **Intentando de nuevo**.

Nota
Para tareas con múltiples subtareas, la opción **Ejecutar de nuevo** está disponible solo cuando todas las subtareas han terminado y únicamente ejecutará las subtareas fallidas.

5.10.4. Eliminar Tareas

Para evitar que la lista de tareas se desorganice, se recomienda eliminar las tareas que ya no necesite.

1. Diríjase a la página **Red > Tareas**.
2. Marque la casilla de verificación correspondiente a la tarea que desee eliminar.
3. Haga clic en el botón **Borrar** del lateral derecho de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

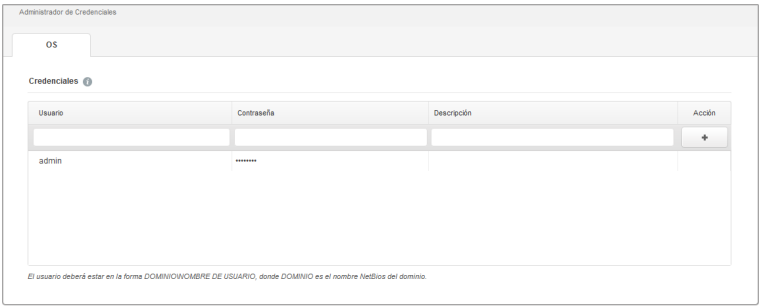
Aviso
Suprimir una tarea pendiente también cancelará la tarea.
Si se elimina una tarea en curso, se cancelarán cualesquiera subtareas pendientes. En tal caso, no podrá deshacerse ninguna subtarea finalizada.

5.11. Administrador de Credenciales

El Gestor de credenciales le ayuda a administrar las credenciales necesarias para la autenticación remota en los distintos sistemas operativos en su red.

Para abrir el Gestor de credenciales, vaya a su nombre de usuario en la esquina superior derecha de la página y seleccione **Gestor de credenciales**.

5.11.1. Añadir credenciales al Gestor de credenciales



Administrador de Credenciales

1. Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta. Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

   Utilice las convenciones de Windows cuando introduzca el nombre de una cuenta de usuario de dominio, por ejemplo, `usuario@dominio.com` o `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas en ambas formas (`usuario@dominio.com` y `dominio\usuario`).

2. Haga clic en el botón + **Añadir**. El nuevo conjunto de credenciales se añade a la tabla.

Nota
Si no ha especificado las credenciales de autenticación, necesitará introducirlas cuando ejecute tareas de instalación. Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

5.11.2. Eliminación de credenciales del Gestor de credenciales

Para eliminar credenciales obsoletas del Gestor de credenciales:

1. Vaya a la fila de la tabla que contiene las credenciales que desea eliminar.
2. Haga clic en el botón − **Eliminar** a la derecha de la fila de la tabla correspondiente. La cuenta seleccionada se eliminará.

6. Políticas de Seguridad

Una vez instalada, la protección de Bitdefender puede configurarse y administrarse desde Control Center usando políticas de seguridad. Una política especifica la configuración de seguridad a aplicar en los equipos.

Inmediatamente después de la instalación, se asigna a los elementos de inventario de la red la política predeterminada, que está definida con las opciones de protección recomendadas. No puede editar o borrar la política predeterminada. Sólo puede utilizarla como una plantilla para crear nuevas políticas.

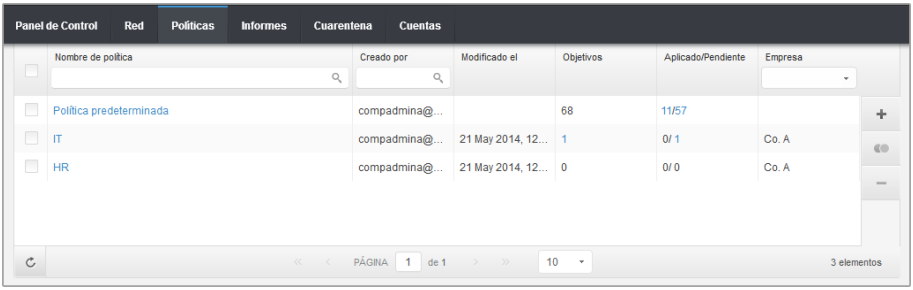
Puede crear tantas políticas como precise en función de los requisitos de seguridad.

Esto es lo que necesita saber sobre políticas:

- Las políticas se crean en la página **Políticas** y se asignan a elementos de red en la página **Red**.
- Los elementos de red solo pueden tener una política activa en cada momento.
- Las políticas se transfieren a los elementos de red objetivos inmediatamente tras su creación o modificación. La configuración debería aplicarse a los elementos de red en menos de un minuto (siempre que estén conectados). Si un equipo o elemento de red no está conectado, la configuración se aplicará tan pronto como vuelva a conectarse.
- La política se aplica únicamente a los módulos de protección instalados. Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.
- No puede editar políticas creadas por otros usuarios (a menos que los propietarios de la política lo permitan en los ajustes de la política), pero puede sobrescribirlas asignando a los elementos objetivos una política diferente.

6.1. Administrando las Políticas

Puede ver y administrar las políticas en la página **Políticas**.



La página Políticas

Las políticas existentes se muestran en la tabla. Para cada política, puede ver:

- Nombre de política.
- El usuario que creó la política.
- Fecha y hora en la que se editó por última vez la política.
- El número de objetivos a los que se envió la política. Haga clic en el número para mostrar los objetivos correspondientes en el inventario de red.
- El número de objetivos a los que se aplicó la política o para los que está pendiente de aplicar. Haga clic en el número que desee para mostrar los objetivos correspondientes en el inventario de red.

Puede ordenar las políticas disponibles y buscar también determinadas políticas usando los criterios disponibles.

6.1.1. Crear políticas

Puede crear políticas según dos métodos: añadir una nueva, o duplicar (clonar) una política existente.

Para crear una nueva política:

1. Diríjase a la página **Políticas**.
2. Seleccione el método de creación de políticas:
   - **Añadir nueva política**.
     - Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. Este comando crea una nueva política empezando desde la plantilla de política predeterminada.

- **Clonar una política existente**.
  a. Marque la casilla de verificación de la política que desea duplicar.
  b. Haga clic en el botón **Clonar** del lateral derecho de la tabla.

3. Configure los ajustes de la política. Para información detallada, diríjase a “Políticas de equipos” (p. 75).
4. Haga clic en **Guardar** para crear la política y volver a la lista de políticas.

6.1.2. Modificar los ajustes de políticas

Las opciones de la política pueden configurarse en el momento de crear la política. Puede modificarlas más adelante según sea necesario.

Nota
De forma predeterminada, solo el usuario que creó la política puede modificarla. Para cambiar esto, el propietario de la política debe marcar la opción **Permitir a otros usuarios cambiar esta política** en la página de **Detalles** de la política.

Para cambiar los ajustes de una política existente:

1. Diríjase a la página **Políticas**.
2. Encuentre la política que está buscando en la lista y haga clic en su nombre para editarla.
3. Configure las opciones de la política según sea necesario. Para información detallada, diríjase a “Políticas de equipos” (p. 75).
4. Haga clic en **Guardar**.

   Las políticas se aplican a los elementos de red objetivos inmediatamente tras la edición de las asignaciones de la política o tras modificar sus ajustes. La configuración debería aplicarse a los elementos de red en menos de un minuto (siempre que estén conectados). Si un equipo o elemento de red no está conectado, la configuración se aplicará tan pronto como vuelva a conectarse.

6.1.3. Renombrando Políticas

Las políticas deberían tener nombres descriptivos de forma que usted u otro administrador pueda identificarlas rápidamente.

Para renombrar una política:

1. Diríjase a la página **Políticas**.
2. Haga clic en el nombre de la política. Esto abrirá la página de políticas.
3. Escriba un nombre nuevo para la política.
4. Haga clic en **Guardar**.

Nota
El nombre de la política es único. Debe introducir un nombre diferente para cada nueva política.

6.1.4. Eliminando Políticas

Si ya no necesita una política, elimínela. Una vez eliminada la política, se asignará la política del grupo padre a los objetos de red a los que se aplicaba la política anterior. Si no se aplica otra política, finalmente se aplicará la política predeterminada.

Nota
De forma predeterminada, solo el usuario que creó la política puede eliminarla. Para cambiar esto, el propietario de la política debe marcar la opción **Permitir a otros usuarios cambiar esta política** en la página de **Detalles** de la política.

Para eliminar una política:

1. Diríjase a la página **Políticas**.
2. Seleccione la casilla correspondiente.
3. Haga clic en el botón **Borrar** del lateral derecho de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

6.1.5. Asignar políticas a objetos de red

Una vez definidas las políticas necesarias en la sección **Políticas**, puede asignarlas a los elementos de red en la sección **Red**.

A todos los objetos de red se les asigna inicialmente la política predeterminada.

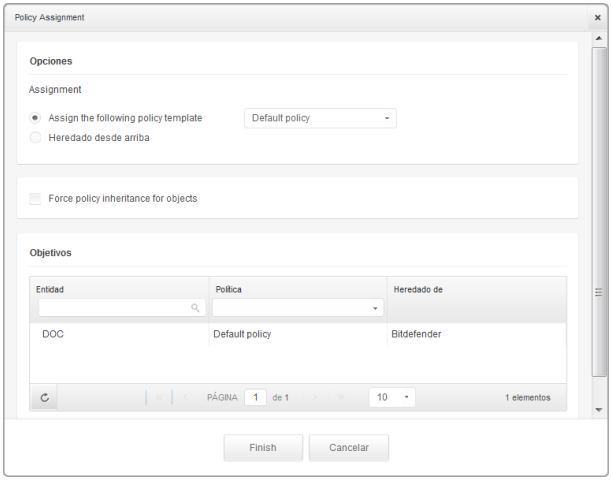
Nota
Solo puede asignar políticas que haya creado usted mismo. Para asignar una política creada por otro usuario, primero debe duplicarla en la página de **Políticas**.

Para asignar una política:

1. Diríjase a la página **Red**.
2. Marque la casilla de verificación del elemento de red deseado. Puede seleccionar uno o varios objetos solo del mismo nivel.
3. Haga clic en el botón **Asignar política** a la derecha de la tabla.

   Nota
   También puede hacer clic con el botón derecho en un grupo del árbol de red y elegir **Asignar política** en el menú contextual.

   Se muestra la ventana **Asignación de política** :



Ajustes de asignación de políticas

4. Configure los ajustes de asignación de políticas para los objetos seleccionados:
   - Consulte las asignaciones de políticas actuales para los objetos seleccionados en la tabla bajo la sección **Objetivos**.
   - **Asignar la siguiente plantilla de política**. Seleccione esta opción para asignar a los objetos objetivo una política del menú mostrado a la derecha. Solo están disponibles en el menú las políticas creadas desde su cuenta de usuario.
   - **Heredado desde arriba**. Seleccione la opción **Heredar desde arriba** para asignar la política del grupo padre a los objetos de red seleccionados.
   - **Forzar herencia de políticas para objetos**. De forma predeterminada cada objeto de red hereda la política del grupo padre. Si cambia la política del grupo, se verán afectados todos los hijos del mismo, excepto los miembros del grupo a los que haya asignado específicamente otra política.

     Seleccione la opción **Forzar herencia de políticas para objetos** para aplicar la política escogida a un grupo, incluyendo a los hijos del mismo que tuvieran asignada una política diferente. Es este caso, la tabla situada a continuación mostrará los hijos del grupo seleccionado que no heredan la política del grupo.
5. Haga clic en **Finalizar** para guardar y aplicar los cambios.

Las políticas se aplican a los elementos de red objetivos inmediatamente tras la edición de las asignaciones de la política o tras modificar sus ajustes. La configuración debería aplicarse a los elementos de red en menos de un minuto (siempre que estén conectados). Si un equipo o elemento de red no está conectado, la configuración se aplicará tan pronto como vuelva a conectarse.

Para comprobar si se ha asignado la política correctamente, acceda a la página de **Red** y haga clic en el nombre del objeto que le interese para mostrar la ventana de **Detalles**. Consulte la sección de **Política** para ver el estado de la política actual. Si está en estado pendiente, la política no se ha aplicado todavía al objeto objetivo.

6.2. Políticas de equipos

Las opciones de la política pueden configurarse en el momento de crear la política. Puede modificarlas más adelante según sea necesario.

Para cambiar la configuración de una política:

1. Diríjase a la página **Políticas**.
2. Haga clic en el nombre de la política. Esto abrirá la página de configuración de políticas.
3. Configure las opciones de la política según sea necesario. Los ajustes se organizan en las siguientes categorías:
   - General
   - Antimalware
   - Cortafuegos
   - Control de Contenido

   Puede seleccionar la categoría de configuración usando el menú del lateral izquierdo de la página.
4. Haga clic en **Guardar** para guardar los cambios y aplicarlos a los equipos objetivo. Para abandonar la página de política sin guardar los cambios, haga clic en **Cancelar**.

Nota
Para saber cómo utilizar las políticas, diríjase a “Administrando las Políticas” (p. 71).

6.2.1. General

Los ajustes generales le ayudan a administrar las opciones de visualización de la interfaz de usuario, opciones de comunicación, preferencias de actualización, protección por contraseña y otros ajustes de Endpoint Security.

Los ajustes se organizan en las siguientes categorías:

- Detalles
- Visualizar
- Comunicación
- Avanzado
- Actualizar

Detalles

La página Detalles muestra los detalles de políticas generales:

- Nombre de política
- El usuario que creó la política
- Fecha y hora en la que se creó la política.
- Fecha y hora en la que se editó por última vez la política.

Políticas de equipos

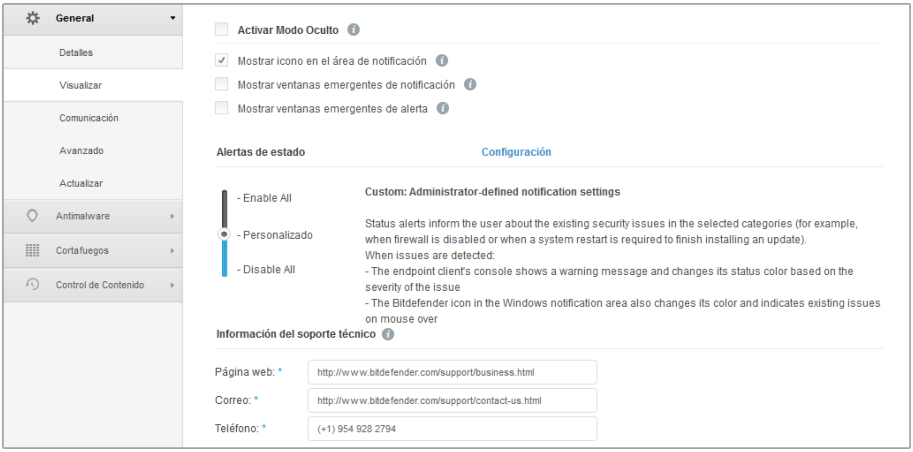
Puede renombrar la política escribiendo el nombre nuevo en el campo correspondiente y haciendo clic en **guardar**. Las políticas deberían tener nombres descriptivos de forma que usted u otro administrador pueda identificarlas rápidamente.

Nota

De forma predeterminada, solo el usuario que creó la política puede modificarla. Para cambiar esto, el propietario de la política debe marcar la opción **Permitir a otros usuarios cambiar esta política** en la página de **Detalles** de la política.

Visualizar

En esta sección puede configurar las opciones de visualización de la interfaz de usuario.

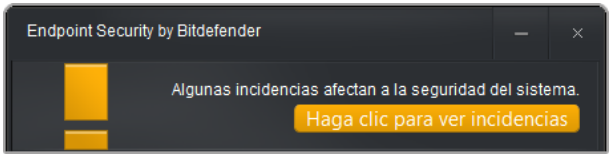


Políticas de equipos - Ajustes de visualización

- **Activar Modo Oculto.** Utilice el conmutador para activar o desactivar el modo Silencioso. El modo silencioso está diseñado para ayudarle a desactivar fácilmente la interacción del usuario en Endpoint Security. Cuando se activa el modo Silencioso, se aplican los siguientes cambios en la configuración de la política:
  - Se desactivarán las opciones **Mostrar icono en el área de notificación**, **Mostrar ventanas emergentes de notificación** y **Mostrar ventanas emergentes de alertas** de esta sección.
  - Si se estableció el nivel de protección del cortafuego en **Juego de reglas y preguntar** o **Juego de reglas, archivos conocidos y preguntar** se cambiará a **Juego de reglas, archivos conocidos y permitir**. De lo contrario, la configuración del nivel de protección permanecerá sin cambios.
- **Mostrar icono en el área de notificación.** Seleccione esta opción para mostrar el icono de Bitdefender en el área de notificación (también conocida como bandeja del sistema). El icono informa a los usuarios sobre su estado de protección al cambiar su apariencia y mostrar una ventana emergente de notificación. Por otra parte, los usuarios pueden hacer clic con botón derecho para abrir rápidamente la ventana principal de Endpoint Security o la ventana **Acerca de**. Abrir la ventana **Acerca de** inicia automáticamente una actualización bajo demanda.
- **Mostrar ventanas emergentes de notificación.** Seleccione esta opción para informar a los usuarios sobre eventos de seguridad importantes como la detección de malware y las acciones llevadas a cabo a través de pequeñas ventanas emergentes de notificación. Las ventanas emergentes desaparecen automáticamente en unos pocos segundos sin la intervención del usuario.

- **Mostrar ventanas emergentes de alerta.** A diferencia de las ventanas emergentes de notificación, las ventanas emergentes de alerta solicitan la acción del usuario. Si elige no mostrar alertas emergentes, Endpoint Security llevará a cabo automáticamente la acción recomendada. Las ventanas emergentes de alerta se generan en las siguientes situaciones:
  - Si el cortafuego está configurado para solicitar al usuario una acción cuando aplicaciones desconocidas soliciten acceso a Internet o a la red.
  - Si está habilitado Active Virus Control / Sistema de detección de intrusiones, siempre que se detecta una aplicación potencialmente peligrosa.
  - Si está habilitado el análisis de dispositivo, siempre que se conecte un dispositivo de almacenamiento externo al equipo. Puede configurar este ajuste en la sección de **Antimalware > Bajo demanda**.
- **Alertas de estado.** Los usuarios saben si su punto final tiene problemas de configuración de seguridad u otros riesgos de seguridad en función de las alertas de estado. Así, los usuarios pueden saber si existe algún problema relacionado con su protección antimalware, como por ejemplo: el módulo de análisis on-access está deshabilitado o no se ha realizado un análisis completo del sistema.

  Se informa a los usuarios sobre el estado de su protección de dos formas:
  - El área de notificación de la ventana principal muestra un mensaje de estado adecuado y cambia de color dependiendo de los problemas de seguridad. Los usuarios tienen la posibilidad de ver la información sobre las incidencias haciendo clic en el botón correspondiente.



Área de notificación de Endpoint Security

  - Por el icono de Bitdefender en la bandeja del sistema, que cambia de aspecto cuando se detectan problemas.

  Endpoint Security utiliza el siguiente esquema de colores para el área de notificación:
  - Verde: no se han detectado problemas.
  - Naranja: el punto final sufre problemas que afectan a su seguridad, aunque no son críticos. Los usuarios no tienen por qué interrumpir su trabajo actual para resolver estas incidencias.

– Rojo: el punto final tiene problemas críticos que requieren una acción inmediata del usuario.

Para configurar las alertas de estado, seleccione el nivel de alerta que mejor se adapte a sus necesidades (**Activar todo**, **Personalizado** y **Desactivar todo**). Use la descripción del lateral derecho de la escala como guía para su elección.

Si desea personalizar las alertas:

1. Seleccione el nivel **Personalizado** de la escala.
2. Haga clic en el enlace **Ajustes** para abrir la ventana de configuración.
3. Seleccione los aspectos de la seguridad que quiere monitorizar. Las opciones se describen aquí:
   – **General**. La alerta de estado se genera cada vez que se requiere reiniciar el sistema tras una operación de mantenimiento del producto o a lo largo de la misma. Puede optar por mostrar la alerta como una advertencia o como una incidencia crítica.
   – **Antimalware**. Las alertas de estado se generan en las siguientes situaciones:
     • El análisis on-access está habilitado pero se omiten muchos archivos locales.
     • Ha pasado un determinado número de días desde que se realizó el último análisis completo del sistema de la máquina.

     Puede escoger cómo mostrar las alertas y definir el número de días desde el último análisis completo del sistema.
   – **Cortafuegos**. Esta alerta de estado se genera cuando se desactiva el módulo de Cortafuego.
   – **Control de Contenido**. Esta alerta de estado se genera cuando se desactiva el módulo de Control de contenidos.
   – **Actualizar**. La alerta de estado se genera cada vez que se requiere reiniciar el sistema para completar una actualización. Puede optar por mostrar la alerta como una advertencia o como una incidencia crítica.

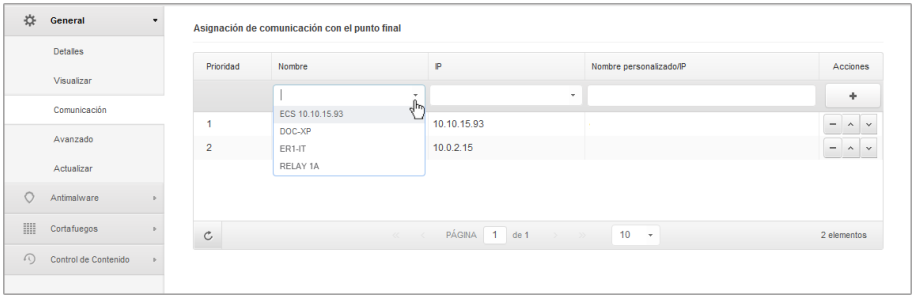
- **Información del soporte técnico.** Puede personalizar la información de contacto y soporte técnico disponibles en Endpoint Security completando los campos correspondientes. Los usuarios pueden acceder a esta información desde la ventana Endpoint Security haciendo clic en el icono en la esquina inferior derecha, o bien haciendo clic con el botón derecho en el icono de Bitdefender del área de notificación del sistema y seleccionando **Acerca de**.

Comunicación

Cuando hay varios Endpoint Security Relays disponibles en la red objetivo, puede asignar a los equipos seleccionados uno o varios Endpoint Security Relays mediante políticas.

Para asignar un Endpoint Security Relay a equipos objetivo:

1. En la tabla de **Asignación de comunicación de punto final**, haga clic en el campo **Nombre**. Se muestra la lista de Endpoint Security Relays detectados en su red.
2. Seleccione una entidad.



Políticas de equipos - Ajustes de comunicación

3. Haga clic en el botón **Añadir** del lateral derecho de la tabla.

   El Endpoint Security Relay se añade a la lista. Todos los equipos objetivo se comunicarán con Control Center mediante el Endpoint Security Relay especificado.
4. Siga los mismos pasos para añadir varios Endpoint Security Relay, si existen.
5. Puede configurar las prioridades del Endpoint Security Relay mediante las flechas arriba y abajo disponibles a la derecha de cada entidad. La comunicación con equipos objetivo se llevará a cabo a través de la entidad situada en la parte superior de la lista. Cuando no se pueda establecer la comunicación con esta entidad, se pasará a considerar la siguiente.
6. Para eliminar una entidad de la lista, haga clic en el botón **Borrar** correspondiente del lateral derecho de la tabla.

Avanzado

En esta sección puede configurar los ajustes generales y la contraseña de desinstalación.

Políticas de equipos - Ajustes avanzados

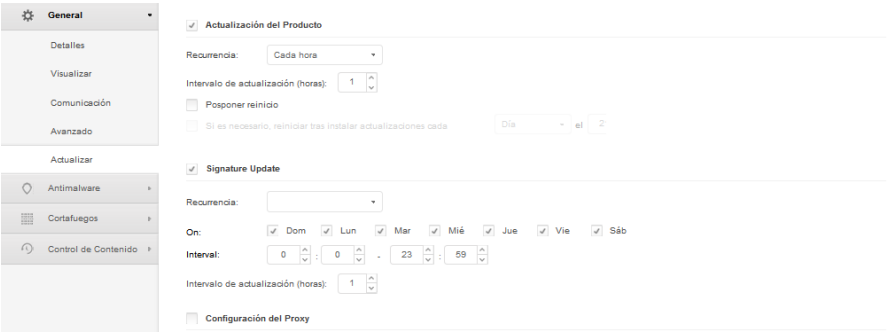
- **Eliminar eventos con una antigüedad superior a (días).** Endpoint Security mantiene un registro detallado de los eventos relacionados con la actividad en el equipo (incluyendo también las actividades del equipo supervisadas por el Control de contenido). Por omisión, los eventos se eliminan del registro pasados 30 días. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.
- **Enviar informes de bloqueos a Bitdefender.** Seleccione esta opción de forma que los informes se envíen a los laboratorios de Bitdefender para su análisis si Endpoint Security se bloquea. Los informes ayudarán a nuestros ingenieros a descubrir qué causó el problema y evitar que éste vuelva a ocurrir. No sé enviará información personal.
- **Configuración de contraseña.** Para evitar que usuarios con derechos administrativos desinstalen la protección, debe configurar una contraseña.

  La contraseña de desinstalación puede configurarse antes de la instalación personalizando el paquete de instalación. Si lo ha hecho así, seleccione **Mantener configuración actual** para conservar la contraseña actual.

  Para establecer la contraseña, o cambiar la contraseña actual, seleccione **Activar contraseña** e introduzca la contraseña deseada. Para eliminar la protección por contraseña, seleccione **Desactivar contraseña**.

Actualizar

En esta sección puede configurar las opciones de actualización de Endpoint Security y los ajustes de actualización de firmas de virus. Las actualizaciones son muy importantes ya que permiten luchar contra las últimas amenazas.



Políticas de equipos - Opciones de actualización

- **Actualización del Producto.** Endpoint Security comprueba automáticamente si existen descargas e instala actualizaciones cada hora (configuración predeterminada). Las actualizaciones automáticas se ejecutan de forma silenciosa en segundo plano.
  - **Recurrencia**. Para cambiar la recurrencia de la actualización automática, elija una opción diferente en el menú y configúrela según sus necesidades en los campos siguientes.
  - **Posponer reinicio**. Algunas actualizaciones necesitan reiniciar el sistema para instalarse y funcionar adecuadamente. Al seleccionar esta opción, el programa seguirá trabajando con los archivos antiguos hasta que se reinicie el equipo, sin informar al usuario. Por el contrario, una notificación de la interfaz de usuario solicitará a éste el reinicio del sistema siempre que lo requiera una actualización.
  - Si elige posponer el reinicio, puede establecer la hora adecuada a la que los equipos se iniciarán de forma automática si (todavía) es necesario. Esto puede ser muy útil para los servidores. Si es necesario, seleccione **Reiniciar tras instalar las actualizaciones** y especifique cuándo es conveniente reiniciar (diaria o semanalmente en un día determinado, a una hora determinada del día).
- **Actualización de Firmas.** Endpoint Security comprueba automáticamente si existen actualizaciones de firmas cada hora (configuración predeterminada). Las actualizaciones automáticas se ejecutan de forma silenciosa en segundo plano. Para cambiar la recurrencia de la actualización automática, elija una opción diferente en el menú y configúrela según sus necesidades en los campos siguientes.
- **Configuración del Proxy.** Seleccione esta opción si los equipos se conectan a Internet (o al servidor de actualización local) a través de un servidor proxy. Hay tres opciones para establecer la configuración del proxy:
  - **Importar conf. proxy navegador predet.** Endpoint Security puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Internet Explorer, Mozilla Firefox y Opera.

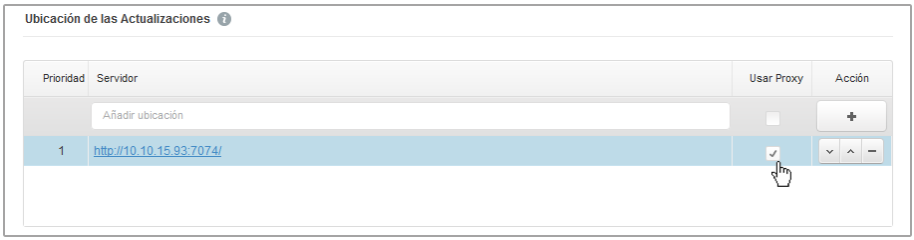
- **Autodetectar proxy de red.** Endpoint Security utiliza el protocolo Web Proxy Auto-Discovery (WPAD) incluido en Windows para recuperar automáticamente la configuración del proxy desde un archivo Proxy Auto-Configuration (PAC) publicado en la red local. Si no está disponible el archivo PAC, las actualizaciones fallarán.
- **Usar configuración del proxy personalizada.** Si conoce los ajustes del proxy, seleccione esta opción y luego especifíquelos:
  - **Servidor** - escriba la IP del servidor proxy.
  - **Puerto** - introduzca el puerto utilizado para conectar con el servidor proxy.
  - **Nombre** - escriba un nombre de usuario que el proxy reconozca.
  - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

Nota

Cambiar la opción de configuración del proxy sobrescribe los ajustes existentes del proxy en Endpoint Security.

Además, debe seleccionar la casilla de verificación **Usar proxy** correspondiente a la dirección de actualización a la que corresponden los ajustes (la dirección del servidor de actualización local o de Internet).

- **Ubicación de las Actualizaciones**. Para evitar la sobrecarga del tráfico exterior de la red, Endpoint Security está configurado para actualizarse desde http://upgrade.bitdefender.com. También puede añadir a la lista otras direcciones de servidor de actualizaciones local y configurar sus prioridades mediante los botones de subir y bajar que se muestran al pasar el ratón por encima. Si la primera ubicación de actualización no está disponible, se comprueba la siguiente y así sucesivamente.



Políticas de equipos - Ubicaciones de actualización

Para establecer la dirección de actualización local:

1. Introduzca la dirección del servidor de actualización local en el campo **Añadir dirección**. Use una de estas sintaxis:
   - `update_ server_ip:port`
   - `update_ server_name:port`

   El puerto predeterminado es 7074.

2. Si los equipos cliente se conectan al servidor de actualización local a través de un servidor proxy, seleccione **Usar proxy**.
3. Haga clic en el botón **Añadir** del lateral derecho de la tabla.
4. Utilice las flechas de Arriba / Abajo de la columna **Acción** para poner la dirección de actualización local al comienzo de la lista. Coloque el cursor sobre la fila correspondiente para hacer que se muestren las flechas.

Para eliminar una ubicación de la lista, mueva el cursor sobre ella y haga clic en el botón **Borrar** correspondiente. Aunque puede eliminar la dirección de actualización predeterminada, no es recomendable que lo haga.

6.2.2. Antimalware

El módulo Antimalware protege al sistema contra todo tipo de amenazas de malware (virus, troyanos, spyware, rootkits, adware y otros). La protección se divide en dos categorías:

- Análisis On-access: evita que nuevas amenazas de malware se introduzcan en el sistema.
- Análisis bajo demanda: permite detectar y eliminar malware que ya reside en su sistema.

Cuando detecte un virus u otro malware, Endpoint Security intentará eliminar automáticamente el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden desinfectarse se trasladan a la cuarentena para aislar la infección. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

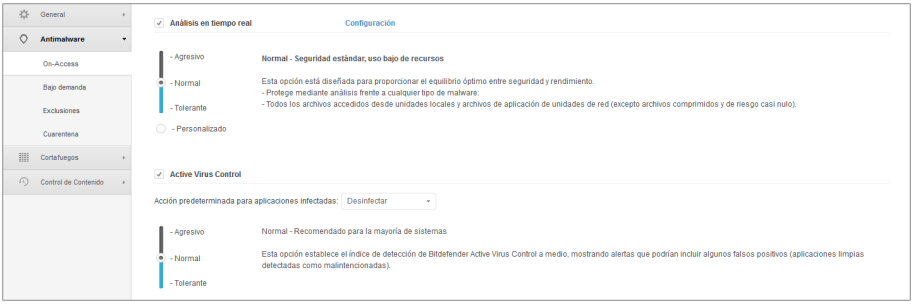
Los usuarios avanzados pueden configurar exclusiones de análisis si no desean que se analicen ciertos archivos o tipos de archivo.

Los ajustes se organizan en las siguientes categorías:

- On-Access
- Bajo demanda
- Exclusiones
- Cuarentena

On-Access

En esta sección puede configurar los dos componentes de la protección antimalware en tiempo real:



Políticas de equipos - Ajustes on-access

- Análisis en tiempo real
- Active Virus Control

Configuración de análisis On-access

El análisis on-access evita que entren en el sistema nuevas amenazas de malware gracias al análisis de los archivos locales y de red cuando se accede a ellos (al abrirlos, moverlos, copiarlos o ejecutarlos), al análisis de los sectores de arranque y al de las aplicaciones potencialmente no deseadas (APND).

Para configurar el análisis on-access:

1. Utilice el conmutador para activar o desactivar el análisis on-access Si desactiva el análisis on-access, los equipos serán vulnerables al malware.
2. Para una configuración rápida, haga clic en el nivel de seguridad que mejor se ajuste a sus necesidades (Agresivo, Normal o Tolerante). Use la descripción del lateral derecho de la escala como guía para su elección.
3. Puede configurar en detalle las opciones de análisis mediante la selección del nivel de protección **Personalizado** y haciendo clic en el enlace **Opciones**. Aparecerá la ventana **Ajustes de análisis on-access** con diversas opciones organizadas en dos pestañas, **General** y **Avanzado**. Se describen a continuación las opciones desde la primera pestaña a la última:
   - **Analizar archivos locales**. Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Las preferencias de análisis pueden configurarse de forma independiente para los archivos locales (almacenados en el equipo local) o archivos de red (almacenados en los recursos compartidos de la red). Si se instala la protección antimalware en todos los equipos de la red, puede desactivar el análisis de archivos de red para permitir un acceso a la red más rápido.

     Puede ajustar Endpoint Security para analizar todos los archivos a los que se ha accedido (con independencia de su extensión), archivos de aplicación solamente o extensiones de archivo específicas que considere peligrosas. Analizando todos los

archivos proporciona una mejor protección, mientras analizando solo aplicaciones puede ser utilizado para mejorar el rendimiento del sistema.

Nota
Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a "Lista de tipos de archivos de aplicación" (p. 151).

Si desea que sólo se analicen extensiones específicas, elija **Extensiones definidas por el usuario** desde el menú y luego introduzca las extensiones en el campo de edición, pulsando `Intro` después de cada extensión.

De cara a un mejor rendimiento del sistema, puede también excluir del análisis a los archivos grandes. Marque la casilla de verificación **Tamaño máximo (MB)** e indique el límite de tamaño para los archivos que se analizarán. Utilice esta opción con prudencia, dado que el malware también puede afectar a los archivos grandes.

- **Archivos comprimidos** Seleccione **Analizar dentro de los archivos** si desea activar el análisis on-access de los archivos comprimidos. Analizar dentro de archivos es una proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para la protección en tiempo real. Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. El malware puede afectar al sistema sólo si el archivo infectado se extrae del archivo comprimido y se ejecuta sin tener activada la protección de análisis on-access.

  Si decide utilizar esta opción, puede configurar las siguientes opciones y optimización:

  – **Tamaño de archivo máximo (MB).** Puede establecer un límite máximo de tamaño aceptado para los archivos analizados en tiempo real. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).

  – **Profundidad de archivo máxima (niveles).** Marque la casilla de verificación correspondiente y elija la profundidad de archivo máxima desde el menú. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.

- **Varios.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.

  – **Analizar los sectores de arranque.** Para analizar el sector de arranque del sistema. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

  – **Analizar sólo nuevos&modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.

- **Analizar en busca de keyloggers.** Los Keyloggers registran lo que escribe en el teclado y envían informes por Internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.
- **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Una aplicación potencialmente no deseada (APND) es un programa que podría haberse instalado en el PC contra su voluntad y que a veces acompaña a software freeware. Estos programas pueden instalarse sin el consentimiento del usuario (también llamados adware) o incluirse por defecto en el kit de instalación. Los efectos potenciales de estos programas incluyen la visualización de ventanas emergentes, la instalación de barras de herramientas no deseadas en el navegador por defecto o la ejecución de diversos procesos en segundo plano y la disminución del rendimiento del PC.

- **Acciones del Análisis.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
  - **Acción predeterminada para archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Endpoint Security puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

    Si se detecta un archivo infectado, Endpoint Security intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

    Importante
    Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

  - **Acción predeterminada para archivos infectados.** Los archivos detectados como sospechosos por el análisis heurístico. Dado que B-HAVE es una tecnología de análisis heurístico, Endpoint Security no puede asegurar que el archivo esté realmente infectado con malware. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

    Cuando se detecte un archivo sospechoso, los usuarios no podrán acceder a ese archivo para evitar una posible infección.

  Aunque no se recomienda, puede cambiar las acciones predeterminadas. Puede definir dos acciones por cada tipo de archivo. Dispone de las siguientes opciones:

  Bloquear acceso
  Bloquear el acceso a los archivos detectados.

Desinfectar

Elimina el código de malware de los archivos infectados. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados.

Eliminar

Elimina los archivos detectados del disco, sin mostrar advertencia alguna. Se aconseja que evite utilizar esta acción.

Mover a Cuarentena

Mueva los archivos detectados desde su ubicación actual a la carpeta de cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de cuarentena desde la página Cuarentena de la consola.

Opciones Active Virus Control

Bitdefender Active Virus Control es una tecnología de detección proactiva innovadora que utiliza avanzados métodos heurísticos para detectar nuevas amenazas potenciales en tiempo real.

Active Virus Control continuamente monitoriza las aplicaciones que se están ejecutando en su equipo, buscando acciones de malware. Cada una de estas acciones se puntúa y se calcula una puntuación global para cada proceso. Cuando la puntuación general de un proceso alcanza un valor dado, el proceso se considera peligroso. Active Virus Control tratará automáticamente de desinfectar el archivo detectado. Si la rutina de desinfección fracasa, Active Virus Control eliminará el archivo.

Nota

Antes de aplicar la acción de desinfección, se envía una copia del archivo a la cuarentena con el fin de que pueda restaurarlo posteriormente, en caso de tratarse de un falso positivo. Esta acción se puede configurar mediante la opción **Copiar archivos a la cuarentena antes de aplicar la acción de desinfección** disponible en la pestaña **Cuarentena** de los ajustes de política. Esta opción está activada por defecto en las plantillas de política.

Nota

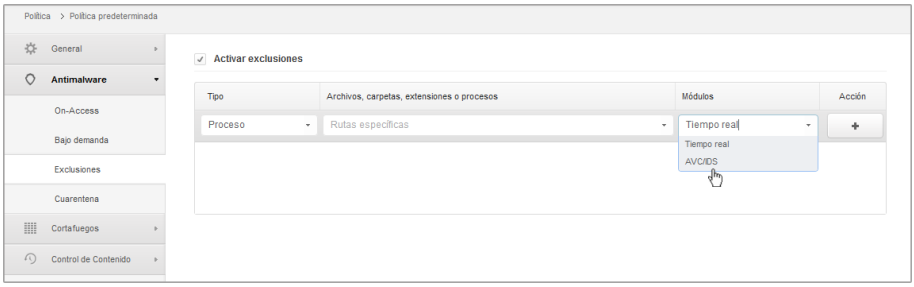
Para más información, vaya a nuestro sitio Web y lea el documento técnico sobre Active Virus Control.

Para configurar Active Virus Control:

1. Utilice el conmutador para activar o desactivar Active Virus Control. Si desactiva Active Virus Control, los equipos serán vulnerables al malware desconocido.
2. La acción por defecto para las aplicaciones infectadas detectadas por Active Virus Control es desinfectar. Para establecer otra acción por defecto, use el menú disponible.
3. Haga clic en el nivel de seguridad que mejor se adapte a sus necesidades (Agresivo, Normal o Tolerante). Use la descripción del lateral derecho de la escala como guía para su elección.

Nota
A medida que aumente el nivel de protección, Active Virus Control necesitará menos signos de comportamiento de estilo malware para informar de un proceso. Esto conducirá a un número mayor de aplicaciones objeto de informe, y al mismo tiempo, un aumento de falsos positivos (aplicaciones limpias detectadas como maliciosas).

4. Debería crear reglas de exclusión para las aplicaciones más conocidas o usadas para evitar falsos positivos (detección incorrecta de aplicaciones legítimas). Vaya a la pestaña Exclusiones y configure las **reglas de exclusión de procesos AVC/IDS** para las aplicaciones de confianza.



Política de equipos - Exclusión de procesos AVC/IDS

Bajo demanda

En esta sección puede configurar las tareas de análisis antimalware que se ejecutarán frecuentemente en los equipos objetivo, según el calendario que especifique.

Políticas de equipos - Tareas de análisis bajo demanda

El análisis se realiza de forma silenciosa en segundo plano. El usuario tendrá constancia de que se está realizando un proceso de análisis mediante un icono que aparecerá en la bandeja del sistema.

Aunque no es obligatorio, se recomienda programar un análisis completo del sistema que se ejecute semanalmente en todos los equipos. Analizar los equipos frecuentemente es una medida de seguridad proactiva que puede ayudar a detectar y bloquear malware que pudiera superar las funciones de protección en tiempo real.

Aparte de los análisis normales, también puede configurar la detección automática y el análisis de unidades de almacenamiento externas.

Administración de tareas de análisis

La tabla de Tareas de análisis le informa de las tareas de análisis existentes, ofreciéndole importante información de cada una de ellas:

- Nombre de tarea y tipo.
- Programa basado en que la tarea se ejecute regularmente (recurrencia).
- Hora en la que se ejecutó la tarea por primera vez.

Hay dos tareas de análisis de sistema predeterminadas que puede configurar para ejecutarlas según sea necesario:

- **Quick Scan** utiliza el análisis en la nube para detectar malware ejecutándose en el sistema. Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.
- **Análisis completo** analiza el equipo por completo en busca de todo tipo de malware que pueda amenazar su seguridad, como virus, spyware, adware, rootkits y otros.

Las opciones de análisis de las tareas de análisis predeterminadas están preconfiguradas y no se pueden cambiar.

Además de las tareas de análisis predeterminadas (que no puede eliminar duplicar), puede crear todas las tareas de análisis personalizadas que desee. Una tarea de análisis personalizada le permite elegir las ubicaciones específicas a analizar y configurar las opciones de análisis.

Para crear y configurar una nueva tarea de análisis personalizado, haga clic en el botón + **Añadir** del lateral derecho de la tabla. Para modificar la configuración de una tarea de análisis existente, haga clic en el nombre de esa tarea. Consulte el siguiente tema para saber cómo configurar las opciones de tareas.

Para eliminar una tarea de la lista, seleccione la tarea y haga clic en el botón − **Borrar** del lateral derecho de la tabla.

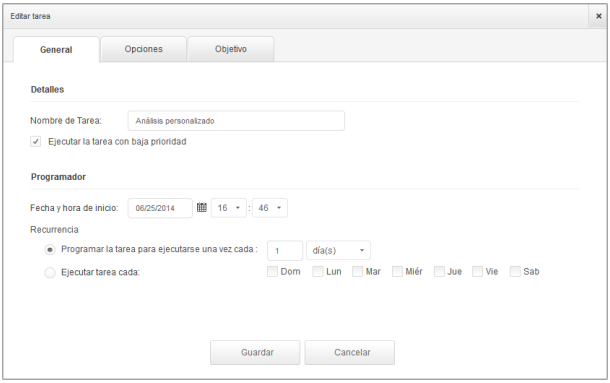
Configurando una Tarea de Análisis

Las opciones para las tareas de análisis se organizan en tres pestañas:

- **General**: establezca el nombre de la tarea y el programa para ejecutarla.

- **Opciones**: escoja un perfil de análisis para una configuración rápida de sus ajustes y defina los ajustes para un análisis personalizado.
- **Objetivo**: seleccione los archivos y carpetas a analizar.

Se describen a continuación las opciones desde la primera pestaña a la última:



Políticas de equipos - Configuración de los ajustes generales de las tareas de análisis bajo demanda

- **Detalles.** Elija un nombre descriptivo para la tarea para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el objetivo de la tarea de análisis y posiblemente la configuración de análisis.
- **Programador.** Utilice las opciones de programación para configurar el programa de análisis. Puede configurar el análisis para que se ejecute cada pocas horas, días o semanas, empezando a una hora y fecha específica.

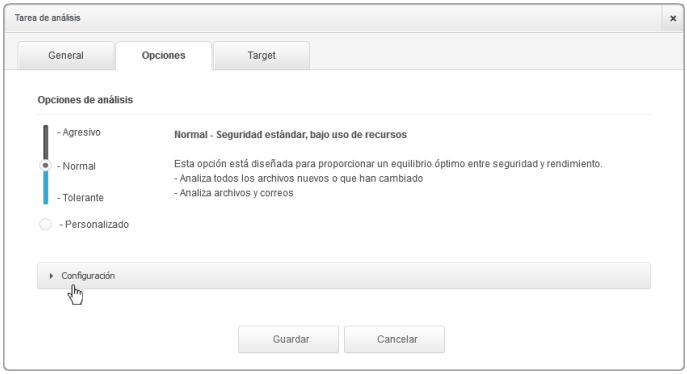
  Tenga en cuenta que los equipos deben estar encendidos a la hora programada. Un análisis programado no se ejecutará en su momento adecuado si el equipo está apagado, hibernado o en modo suspensión, o si ningún usuario ha iniciado sesión. En tales situaciones, el análisis se aplazará hasta la próxima vez.

  Nota
  El análisis programado se ejecutará a la hora local del punto final objetivo. Por ejemplo, si el inicio del análisis está programado para las 6:00 PM y el punto final se halla en una franja horaria distinta que Control Center, el análisis empezará a las 6:00 PM (hora del punto final).

- **Opciones de análisis.** Haga clic en el nivel de seguridad que mejor se adapte a sus necesidades (Agresivo, Normal o Tolerante). Use la descripción del lateral derecho de la escala como guía para su elección.

  Las opciones de análisis de la sección **Ajustes** se configuran automáticamente, basándose en el perfil seleccionado. Sin embargo, si lo desea, puede configurarlas en

detalle. Para hacer esto, marque la casilla de verificación **Personalizado** y diríjase a la sección **Opciones**.



Tarea de análisis de equipos

- **Tipos archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede ajustar Endpoint Security para analizar todos los archivos (con independencia de su extensión), archivos de aplicación solamente o extensiones de archivo específicas que considere peligrosas. Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.

  Nota

  Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a “Lista de tipos de archivos de aplicación” (p. 151).

  Si desea que sólo se analicen extensiones específicas, elija **Extensiones definidas por el usuario** desde el menú y luego introduzca las extensiones en el campo de edición, pulsando `Intro` después de cada extensión.

- **Archivos.** Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. El malware puede afectar al sistema sólo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

  Nota

  El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar el interior de los comprimidos.** Seleccione esta opción si desea comprobar los archivos comprimidos en busca de malware. Si decide utilizar esta opción, puede configurar las siguientes opciones y optimización:
  - **Limitar tamaño de archivo a (MB).** Puede establecer un límite de tamaño aceptado máximo para los archivos a analizar. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).
  - **Máxima profundidad de archivo (niveles).** Marque la casilla de verificación correspondiente y elija la profundidad de archivo máxima desde el menú. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.
- **Analizar archivos de correo.** Seleccione esta opción si desea habilitar el análisis archivos de mensajes de correo y bases de datos de correo, incluyendo formatos de archivo tales como .eml, .msg, .pst, .dbx, .mbx, .tbb y otros.

Nota
Tenga en cuenta que el análisis de adjuntos de correo hace un uso intensivo de los recursos y puede afectar al rendimiento de su sistema.

- **Varios.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.
  - **Analizar los sectores de arranque.** Para analizar el sector de arranque del sistema. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.
  - **Analizar registro.** Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.
  - **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de rootkits y objetos ocultos que utilicen este tipo de software.
  - **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger.
  - **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
  - **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en el equipo.
  - **Analizar archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.

- **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Una aplicación potencialmente no deseada (APND) es un programa que podría haberse instalado en el PC contra su voluntad y que a veces acompaña a software freeware. Estos programas pueden instalarse sin el consentimiento del usuario (también llamados adware) o incluirse por defecto en el kit de instalación. Los efectos potenciales de estos programas incluyen la visualización de ventanas emergentes, la instalación de barras de herramientas no deseadas en el navegador por defecto o la ejecución de diversos procesos en segundo plano y la disminución del rendimiento del PC.

- **Acciones.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:

  - **Acción predeterminada para archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Endpoint Security puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

    Si se detecta un archivo infectado, Endpoint Security intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

    Importante
    Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

  - **Acción predeterminada para archivos infectados.** Los archivos detectados como sospechosos por el análisis heurístico. Dado que B-HAVE es una tecnología de análisis heurístico, Endpoint Security no puede asegurar que el archivo esté realmente infectado con malware. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

    Las tareas de análisis se configuran de forma predeterminada para ignorar los archivos sospechosos. Quizá desee cambiar la acción predeterminada para mover archivos sospechosos a la cuarentena. Los archivos en cuarentena se envían periódicamente para su análisis a los laboratorios de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

  - **Acción predeterminada para rootkits.** Los rootkits representan un software especializado utilizado para ocultar archivos del sistema operativo. Aunque no son dañinos por su naturaleza, los rootkits se usan normalmente para ocultar malware o para encubrir la presencia de un intruso en el sistema.

    Los rootkits detectados y archivos ocultos se ignoran de forma predeterminada.

  Aunque no se recomienda, puede cambiar las acciones predeterminadas. Puede indicar la segunda acción a realizar en caso que la primera falle, y diferentes acciones para cada

categoría. Seleccione, en los menús correspondientes, la primera y segunda acción a realizar para cada tipo de archivo detectado. Dispone de las siguientes opciones:

Ninguna acción
No se realizará ninguna acción sobre los archivos detectados. Estos archivos solo aparecerán en el log de análisis.

Desinfectar
Elimina el código de malware de los archivos infectados. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados.

Eliminar
Elimina los archivos detectados del disco, sin mostrar advertencia alguna. Se aconseja que evite utilizar esta acción.

Mover a Cuarentena
Mueva los archivos detectados desde su ubicación actual a la carpeta de cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de cuarentena desde la página Cuarentena de la consola.

- **Objetivo del Análisis.** Añada a la lista todas las ubicaciones que desee analizar en los equipos objetivo.

  Para añadir un nuevo archivo o carpeta a analizar:

  1. Elija desde el menú desplegable una ubicación predefinida o introduzca las **Rutas específicas** que quiere analizar.
  2. Especifique la ruta del objeto a analizar en el campo de edición.
     - Si ha escogido una ubicación predefinida, complete la ruta según sea necesario. Por ejemplo, para analizar la carpeta `Archivos de programa` completa, es suficiente con seleccionar la ubicación predefinida correspondiente desde el menú desplegable. Para analizar una carpeta específica desde `Archivos de programa`, debe completar la ruta añadiendo una barra invertida (\) y el nombre de la carpeta.
     - Si ha elegido **Rutas específicas**, escriba la ruta completa del objeto a analizar. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo.
  3. Haga clic en el botón + **Añadir** correspondiente.

  Para editar una ubicación existente, haga clic en ella. Para eliminar una ubicación de la lista, mueva el cursor sobre ella y haga clic en el botón − **Borrar** correspondiente.

- **Exclusiones.** Puede, o bien utilizar las exclusiones definidas en la sección **Antimalware > Exclusiones** de la política actual, o bien definir exclusiones personalizadas para la tarea de análisis actual. Para obtener más información sobre excepciones, consulte “Exclusiones” (p. 97).

Análisis de dispositivos

Puede configurar Endpoint Security para detectar y analizar automáticamente dispositivos de almacenamiento externo cuando se conectan al equipo. La detección de dispositivos se dividen en una de estas categorías:

- Cds/DVDs
- Dispositivos de almacenamiento USB, como lápices flash y discos duros externos.
- Unidades de red mapeadas
- Dispositivos con más datos almacenados de una cierta cantidad.

Los análisis de dispositivo intentan automáticamente desinfectar los archivos detectados como infectados o moverlos a la cuarentena si no es posible la desinfección. Tenga en cuenta que no puede llevarse a cabo ninguna acción en archivos infectados detectados en CDs/DVDs o en unidades de red mapeadas con acceso de sólo lectura.

Nota
Durante el análisis de un dispositivo, el usuario puede acceder a cualquier información de éste.

Si las ventanas emergentes de alerta están habilitadas en la sección **General > Ver**, se le pregunta al usuario si analizar o no el dispositivo detectado en vez de comenzar automáticamente el análisis.

Cuando ha comenzado el análisis de un dispositivo:

- Una ventana emergente de notificación informa al usuario sobre el análisis del dispositivo, siempre y cuando las ventanas emergentes de notificación estén habilitadas en la sección **General > Ver**.
- Un icono de análisis aparece en el área de notificación. El usuario puede hacer doble clic en este icono para abrir la ventana de análisis y comprobar el avance del mismo.

Una vez que el análisis ha finalizado, el usuario debe comprobar las amenazas detectadas, de haberlas.

Seleccione la opción **Análisis de dispositivo** para habilitar la detección y análisis automáticos de dispositivos de almacenamiento. Para configurar el análisis de dispositivo individualmente para cada tipo de dispositivo, utilice las siguientes opciones:

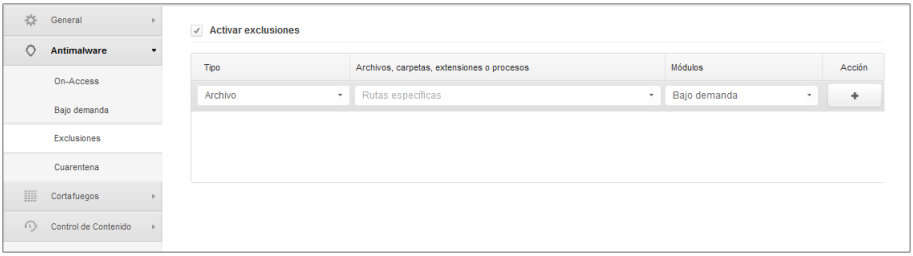
- **Medio CD/DVD**
- **Dispositivos de almacenamiento USB**
- **Unidades de red mapeadas**
- **No analizar dispositivos cuyos datos superen los (MB)**. Utilice esta opción para saltarse automáticamente el análisis de un dispositivo detectado si la cantidad de información almacenada excede el tamaño especificado. Introduzca el tamaño limite (en

megabytes) en el campo correspondiente. Cero significa que no hay restricción de tamaño.

Nota
Está opción se aplica sólo para CDs/DVDs y dispositivos de almacenamiento USB.

Exclusiones

En esta sección puede configurar las reglas de exclusión del análisis. Las exclusiones se pueden aplicar al análisis on-access, bajo demanda o a ambos. Existen cuatro tipos de exclusiones basadas en el objeto de la exclusión:



Políticas de equipos - Exclusiones antimalware

- **Exclusiones de archivo:** el archivo especificado solamente se excluye del análisis.
- **Exclusiones de carpeta:** todos los archivos dentro de una carpeta específica y todas sus subcarpetas se excluyen del análisis.
- **Exclusiones de extensiones:** todo los archivos que tengan la extensión especificada se excluirán del análisis.
- **Exclusiones de procesos:** cualquier objeto al que acceda el proceso excluido será también excluido del análisis. También puede configurar exclusiones del proceso para las tecnologías de Active Virus Control y del Sistema de detección de intrusos.

Importante
Las exclusiones de análisis son para utilizarlas en circunstancias especiales o seguir las recomendaciones de Microsoft o de Bitdefender. Lea este artículo para consultar una lista actualizada de exclusiones recomendadas por Microsoft. Si dispone de un archivo de prueba de EICAR que use para probar la protección antimalware periódicamente, debería excluirlo del análisis on-access.

Marque la casilla de verificación **Activar excepciones** para activar o desactivar las excepciones.

Para configurar una regla de exclusión:

1. Seleccione el tipo de exclusión desde el menú.
2. Dependiendo del tipo de exclusión, especifique el objeto a excluir de la forma siguiente:
   - **Exclusiones de extensiones.** Especifique una o más extensiones de archivo a excluir del análisis, separándolas con un punto y coma (;). Puede introducir las extensiones con o sin el punto precedente. Por ejemplo, introduzca `txt` para excluir archivos de texto.

     Nota
     Antes de excluir las extensiones, infórmese para ver cuáles son objetivos normales del malware y cuáles no.

   - **Exclusiones de archivos, carpeta y proceso.** Debe especificar la ruta al objeto excluido en los equipos objetivo.
     a. Elija desde el menú, bien una ubicación predefinida o bien la opción **Rutas específicas**.
     b. Si ha escogido una ubicación predefinida, complete la ruta según sea necesario. Por ejemplo, para excluir la carpeta `Archivos de programa` completa, es suficiente con seleccionar la ubicación predefinida correspondiente desde el menú. Para excluir una carpeta específica de `Archivos de programa`, debe completar la ruta añadiendo una barra invertida (\) y el nombre de la carpeta. Para procesar exclusiones debe añadir también el nombre del archivo ejecutable de la aplicación.
     c. Si ha elegido **Rutas específicas**, escriba la ruta completa del objeto a excluir. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo.
3. Seleccione los tipos de análisis a los que se aplicará la regla. Algunas exclusiones pueden ser relevantes sólo para el análisis on-access y algunas sólo para el análisis bajo demanda, mientras que otras pueden ser recomendables para ambos. Pueden configurarse exclusiones de proceso para el análisis on-access y las tecnologías de Active Virus Control y Sistema de detección de intrusos.

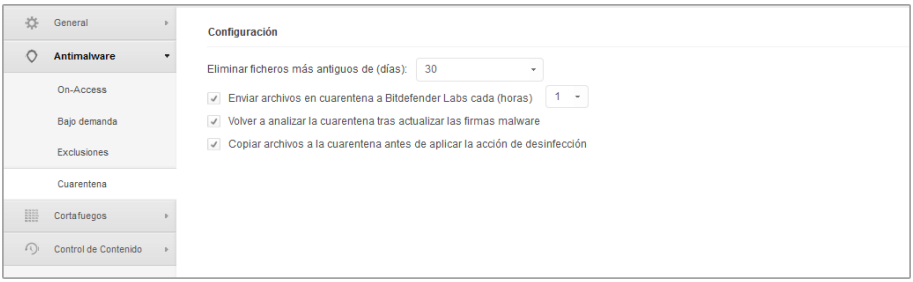
   Nota
   Por favor, tenga en cuenta que las exclusiones del análisis bajo demanda no se aplicarán al análisis contextual. El análisis contextual se inicia haciendo clic con el botón derecho sobre un archivo o carpeta y seleccionando **Analizar con Endpoint Security de Bitdefender**.

4. Haga clic en el botón + **Añadir**. La nueva regla se añadirá a la lista.

Para eliminar una regla de la lista, haga clic en el botón - **Borrar** correspondiente.

Cuarentena

En este apartado puede modificar la configuración de la cuarentena.



Políticas de equipos - Cuarentena

Puede configurar Endpoint Security para que realice automáticamente las siguientes acciones:

- **Eliminar ficheros más antiguos de (días).** Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.
- **Enviar archivos en cuarentena a Bitdefender Labs cada (horas).** Mantenga esta opción seleccionada para enviar automáticamente los archivos en cuarentena a los Laboratorios de Bitdefender. Puede modificar el intervalo de tiempo en el que se envían los archivos en cuarentena (por defecto, una hora). Los investigadores de malware de Bitdefender analizarán los archivos de muestra. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

  Por omisión, los archivos de cuarentena se envían automáticamente al laboratorio de Bitdefender cada hora. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.
- **Volver a analizar la cuarentena tras actualizar las firmas malware.** Mantenga seleccionada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de firmas malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.
- **Copiar los archivos a la cuarentena antes de aplicar la acción de desinfección.** Seleccione esta opción para evitar la pérdida de datos en caso de falsos positivos, copiando todos los archivos identificados como infectados a la cuarentena antes de aplicar la acción de desinfección. Posteriormente podrá restaurar los archivos no infectados desde la página **Cuarentena**.

6.2.3. Cortafuegos

El Cortafuego protege el equipo de los intentos de conexión entrantes y salientes no autorizados.

La funcionalidad del cortafuego se basa en los perfiles de red. Los perfiles se basan en niveles de confianza, que han de definirse para cada red.

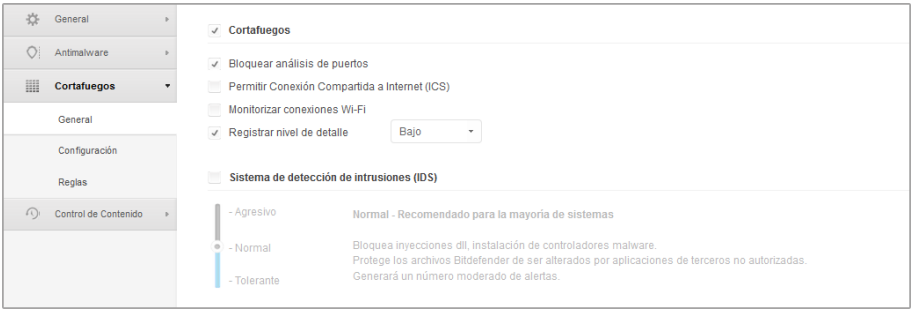
Cada vez que se crea una nueva conexión, el cortafuego detecta y compara la información del adaptador de la conexión con la información de los perfiles existentes, aplicando el perfil correcto. Para obtener más información sobre cómo se aplican los detalles, vea Ajustes de red.

Los ajustes se organizan en las siguientes categorías:

- General
- Configuración
- Reglas

General

En este apartado puede activar o desactivar el cortafuego de Bitdefender y modificar la configuración general.



Políticas de equipos - Ajustes generales del cortafuego

- **Cortafuegos.** Utilice el conmutador para activar o desactivar el cortafuego. Si desactiva la protección del cortafuego, los equipos serán vulnerables a los ataques de la red y de Internet.
- **Bloquear análisis de puertos.** Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers para averiguar los puertos abiertos en su equipo. Si encuentran un puerto vulnerable o inseguro, pueden intentar entrar en su equipo sin su autorización.
- **Permitir Conexión Compartida a Internet (ICS).** Seleccione esta opción para configurar el cortafuego para que permita el tráfico de conexión compartida a Internet.

Nota
Esta opción no activa automáticamente ICS en el sistema del usuario.

- **Monitorizar conexiones Wi-Fi.** Endpoint Security puede informar a los usuarios conectados a una red Wi-Fi cuando un nuevo equipo se une a la red. Para mostrar dichas notificaciones en la pantalla del usuario, seleccione esta opción.
- **Registrar nivel de detalle.** Endpoint Security mantiene un registro de eventos relacionados con el uso del módulo Cortafuego (activar/desactivar cortafuego, bloqueo del tráfico, modificación de la configuración) o generados por las actividades detectadas por este módulo (análisis de puertos, bloqueo de intentos de conexión o de tráfico según las reglas). Elija una opción desde el **nivel de detalle del registro** para especificar cuánta información debería incluir el registro.
- **Sistema de detección de intrusos.** El Sistema de detección de intrusiones monitoriza el sistema en busca de actividades sospechosas (por ejemplo, intentos no autorizados de modificación de archivos de Bitdefender, inyecciones DLL, intentos de keyloggers, etc.).

  Para configurar el sistema de detección de intrusos:

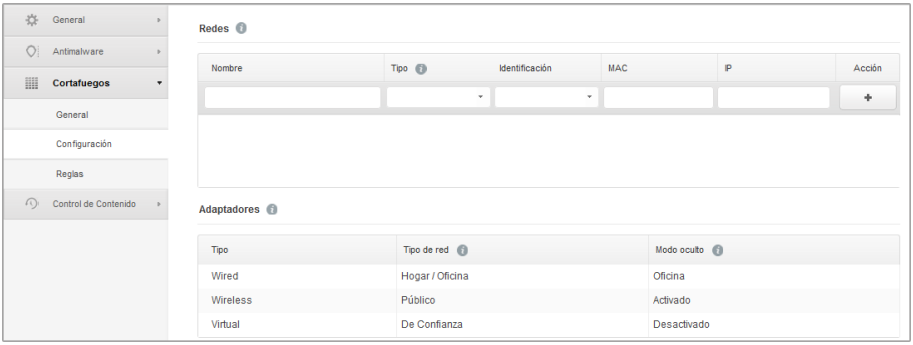
  1. Marque la casilla de verificación para activar o desactivar el Sistema de detección.
  2. Haga clic en el nivel de seguridad que mejor se adapte a sus necesidades (Agresivo, Normal o Tolerante). Use la descripción del lateral derecho de la escala como guía para su elección.

  Para evitar que una aplicación legitima sea detectada por el Sistema de detección de intrusión, añada una**regla de exclusión de proceso AVC/IDS** para esa aplicación en la sección **Antimalware > Exclusiones**.

Configuración

El cortafuego aplica automáticamente un perfil basado en el tipo de red. Puede especificar los perfiles genéricos a aplicar dependiendo del tipo de adaptador y también especificar perfiles individuales para las redes de su empresa. Los ajustes aparecen detallados en las siguientes tablas:

- Redes
- Adaptadores



Políticas de equipos - Ajustes del cortafuego

Configuración de la red

Para que el cortafuego funcione adecuadamente, el administrador tiene que definir las redes que se administrarán en la tabla **Redes**. Los campos de la tabla **Redes** se describen a continuación:

- **Nombre.** Un nombre bajo el cual el administrador reconoce la red en la
- **Tipo.** Seleccione desde el menú el tipo de perfil asignado a la red.

  Endpoint Security aplica automáticamente uno de entre cuatro perfiles de cortafuego para cada conexión de red detectada para definir las opciones de filtrado del tráfico básicas. Los perfiles de cortafuego son:

  - Red de **confianza**. Desactiva el Cortafuego en el respectivo adaptador.
  - Redes **domésticas/oficina**. Permitir todo el tráfico entrante y saliente de los equipos de la red local.
  - Red **pública**. Se filtrará todo el tráfico.
  - Red **insegura**. Bloquea por completo el tráfico de la red e Internet del adaptador de red correspondiente.
- **Identificación.** Seleccione en el menú el método a través del cual Endpoint Security identificará la red. La red puede identificarse mediante tres métodos: **DNS**, **Puerta de enlace** y **Red**.
- **MAC.** Utilice este campo para especificar la dirección MAC de un servidor DNS específico.

  Nota
  Este campo es obligatorio si se selecciona el método de identificación DNS.

- **IP.** Utilice este campo para definir la dirección IP específica en una red. También puedes usar una máscara para definir una subred completa.

Tras definir una red, haga clic en el botón **Añadir** en el lateral derecho de la tabla para añadirlo a la lista.

Ajustes de adaptadores

Si se detecta una red que no está definida en la tabla **Redes**, Endpoint Security detecta el tipo de adaptador de red y aplica un perfil correspondiente a la conexión. Los campos de la tabla **Adaptadores** se describen a continuación:

- **Tipo.** Muestra el tipo de adaptadores de red. Endpoint Security puede detectar tres tipos de adaptadores predefinidos: **Cableado**, **Inalámbrico** y **Virtual** (Virtual Private Network).
- **Tipo de red.** Describe el perfil de red asignado a un tipo de adaptador específico. Los tipos de red se describen en la sección Ajustes de red. Hacer clic en el campo tipo de red le permite cambiar la configuración. Si selecciona la opción **Dejar que decida Windows**, para cualquier nueva conexión de red detectada una vez aplicada la política, Endpoint Security aplica un perfil de cortafuego basado en la clasificación de la red en Windows, ignorando los ajustes de la tabla **Adaptadores**.

  Si la detección basada en Windows Network Manager falla, se intenta una detección básica. Se utiliza un perfil genérico en el cual el tipo de red se considera **Público** y los ajustes de ocultación se configuran como **Activos**. Si la dirección IP del dominio en el que se encuentra el equipo está en una de las redes asociadas al adaptador, entonces el nivel de confianza se considera **Hogar/Oficina** y los ajustes de ocultación se establecen como **Remoto activo**. Si los equipos no están en un dominio, esta condición no es aplicable.
- **Modo oculto.** Oculta el equipo ante software malintencionado y hackers en la red o en Internet. Configure el Modo oculto según sea necesario para cada tipo de adaptador seleccionando una de las siguientes opciones:
  - **Activado.** El equipo es invisible para la red local e Internet.
  - **Desactivado.** Cualquier usuario de la red local o Internet puede hacer ping y detectar el equipo.
  - **Oficina.** El equipo no puede ser detectado desde Internet. Cualquiera desde la red local puede hacer ping y detectar el equipo.

Reglas

En esta sección puede configurar el acceso de la aplicación a la red y las normas de tráfico de datos establecidas por el cortafuegos. Tenga en cuenta que los ajustes disponibles se aplican sólo a los perfiles de cortafuego **Home/Office** y **Público**.

Políticas de equipos - Ajustes de reglas del cortafuego

Configuración

Puede configurar los siguientes ajustes:

- **Nivel de protección.** El nivel de protección seleccionado define la lógica para la toma de decisiones utilizada cuando las aplicaciones solicitan acceso a los servicios de red o Internet. Tiene las siguientes opciones a su disposición:

  Juego de reglas y permitir
  Aplique las reglas de Cortafuego existentes y permita automáticamente todos los intentos de conexión. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

  Juego de reglas y preguntar
  Aplique las reglas de cortafuego existentes y consulte al usuario por la acción a aplicar para los restantes intentos de conexión. Se muestra en la pantalla del usuario una ventana de alerta con información detallada sobre los intentos de conexión desconocidos. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

  Juego de reglas y rechazar
  Aplique las reglas de cortafuego existentes y rechace automáticamente los restantes intentos de conexión. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

  Juego de reglas, archivos conocidos y permitir
  Aplicar las reglas de cortafuego existentes, permite automáticamente los intentos de conexión llevados a cabo por aplicaciones conocidas y permite el resto de intentos de conexión desconocidos. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

Juego de reglas, archivos conocidos y preguntar

Aplicar las reglas de cortafuego existentes, permite automáticamente los intentos de conexión llevados a cabo por aplicaciones conocidas y consulta al usuario la acción a realizar para el resto de intentos de conexión desconocidos. Se muestra en la pantalla del usuario una ventana de alerta con información detallada sobre los intentos de conexión desconocidos. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

Juego de reglas, archivos conocidos y rechazar

Aplicar las reglas de cortafuego existentes, permite automáticamente los intentos de conexión llevados a cabo por aplicaciones conocidas y rechaza los intentos de las desconocidas. Para cada nuevo intento de conexión, se crea una regla y se añade al conjunto de reglas.

Nota

Los archivos conocidos representan una gran colección de aplicaciones fiables y seguras, que es compilada y mantenida constantemente por Bitdefender.

- **Crear reglas agresivas.** Con esta opción seleccionada, el cortafuego creará reglas para cada uno de los procesos que abran la aplicación que solicita el acceso a la red o Internet.
- **Crear reglas para aplicaciones bloqueadas por IDS.** Al seleccionar esta opción, el cortafuego creará automáticamente una regla **Denegar** siempre que el Sistema de detección de intrusiones bloquee una aplicación.
- **Monitorizar cambios de procesos.** Seleccione esta opción si desea que se compruebe cada aplicación que intente conectarse a Internet, siempre que haya cambiado desde la adición de la regla que controla su acceso a Internet. Si se ha modificado la aplicación, se creará una nueva regla según el nivel de protección existente.

Nota

Normalmente, las aplicaciones cambian después de actualizarse. Sin embargo, también existe el riesgo que las aplicaciones sufran cambios a causa del malware, con el objetivo de infectar el equipo local y los otros equipos de la red.

Las aplicaciones firmadas suelen ser aplicaciones de confianza con un alto grado de seguridad. Puede marcar la casilla **Ignorar los procesos firmados** para permitir automáticamente el acceso a Internet a aquellas aplicaciones firmadas que hayan sufrido algún cambio.

Reglas

La tabla Reglas enumera las reglas de cortafuego, proporcionando información importante sobre cada una de ellas:

- Nombre de la regla o aplicación a la que se refiere.

- Protocolo sobre el que se aplica la regla.
- Acción de la regla (permitir o rechazar paquetes).
- Acciones que puede llevar a cabo en la regla.
- Prioridad de reglas.

Nota

Estas son las reglas de cortafuego impuestas explícitamente por la política. Pueden configurarse reglas adicionales en los equipos como resultado de aplicar la configuración del cortafuegos.

Varias reglas de cortafuego predefinidas le ayudan a permitir o rechazar fácilmente los tipos de tráfico más habituales. Elija la opción deseada desde el menú **Permiso**.

ICMP / ICMPv6 entrante
Permitir o rechazar mensajes ICMP / ICMPv6. Los mensajes ICMP son frecuentemente usados por los hackers para llevar a cabo ataques contra las redes de equipos. Por defecto, este tipo de tráfico es rechazada.

Conexiones de escritorio remoto entrantes
Permitir o denegar el acceso de otros equipos a través de conexiones de Escritorio Remoto. Por defecto, este tipo de tráfico está permitido.

Enviar emails
Permitir o denegar el envío de correos electrónicos a través de SMTP. Por defecto, este tipo de tráfico está permitido.

Navegación Web HTTP
Permitir o denegar la navegación Web HTTP. Por defecto, este tipo de tráfico está permitido.

Impresión en otra red
Permita o deniegue el acceso a impresoras en otra red local. Por defecto, este tipo de tráfico es rechazada.

Tráfico HTTP / FTP del Explorador de Windows
Permitir o denegar el tráfico HTTP y FTP desde el Explorador de Windows. Por defecto, este tipo de tráfico es rechazada.

Además de las reglas predeterminadas, puede crear reglas de cortafuego adicionales para otras aplicaciones instaladas en los equipos. Esta configuración, sin embargo, está reservada para administradores con sólidos conocimientos de redes

Para crear y configurar una nueva regla, haga clic en el botón + **Añadir** del lateral derecho de la tabla. Consulte el siguiente tema para obtener más información.

Para eliminar una regla de la lista, haga clic en el botón − **Borrar** correspondiente del lateral derecho de la tabla.

Nota
No puede editar ni modificar las reglas de cortafuego predeterminadas.

Configuración de reglas personalizadas

Puede configurar dos tipos de reglas para el cortafuego:

- **Reglas basadas en aplicaciones.** Ese tipo de reglas se aplican a software específico que puede encontrar en los equipos cliente.
- **Reglas basadas en conexiones.** Este tipo de reglas se aplican a cualquier aplicación o servicio que utiliza una conexión específica.

Para crear y configurar una nueva regla, haga clic en el botón + **Añadir** del lateral derecho de la tabla, y seleccione el tipo de regla deseado desde el menú. Para editar una regla existente, haga clic en el nombre de la regla.

Puede configurar las siguientes opciones:

- **Nombre de la regla.** Escriba el nombre con el que mostrará la regla en la tabla de reglas (por ejemplo, el nombre de la aplicación a la que se aplica la regla).
- **Ruta de aplicación** (sólo para reglas basadas en aplicaciones). Debe especificar la ruta al archivo ejecutable de la aplicación en los equipos objetivos.
  - Elija desde el menú una ubicación predefinida y complete la ruta según sea necesario. Por ejemplo, para una aplicación instalada en la carpeta `Archivos de programa%`, seleccione `%ProgramFiles` y complete la ruta añadiendo una barra invertida (\) y el nombre de la carpeta de la aplicación.
  - Escriba la ruta completa en el campo de edición. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo.
- **Línea de comando** (sólo para reglas basadas en aplicaciones). Si sólo desea aplicar la regla cuando la aplicación especificada se abra con un comando concreto de la interfaz de línea de comandos de Windows, escriba el comando correspondiente en el campo de texto editable. De lo contrario, déjelo vacío.
- **Application MD5** (sólo para reglas basadas en aplicaciones). Si desea que la regla analice la integridad de la información del archivo de la aplicación basándose en el código hash MD5 de la misma, introdúzcalo en el campo de edición. De lo contrario, deje el campo vacío.
- **Dirección local.** Indique la dirección IP local y el puerto a los que se aplicará la regla. Si dispone de más de un adaptador de red, puede desactivar la casilla **Cualquiera** e introducir una dirección IP específica. De igual forma, para filtrar las conexiones de un puerto o rango de puertos específico, desmarque la casilla de verificación **Cualquiera** e introduzca el puerto o rango de puertos deseado en el campo correspondiente.

- **Dirección remota.** Indique la dirección IP remota y el puerto a los que aplicará la regla. Para filtrar el tráfico entrante y saliente de un equipo específico, desmarque la casilla **Cualquiera** e introduzca su dirección IP.
- **Aplicar regla sólo a los equipos conectados directamente.** Puede filtrar el acceso basándose en la dirección Mac.
- **Protocolo.** Seleccione el protocolo IP al que se aplica la regla.
  - Si desea aplicar la regla a todos los protocolos, seleccione la casilla **Cualquiera**.
  - Si desea aplicar la regla para TCP, seleccione **TCP**.
  - Se desea aplicar la regla para UDP, seleccione **UDP**.
  - Si sólo desea aplicar la regla a un protocolo concreto, seleccione ese protocolo desde el menú **Otro**.

Nota

Los números de los protocolos IP están asignados por la Internet Assigned Numbers Authority (IANA). Puede encontrar una lista completa de los números asignados a los protocolos IP en http://www.iana.org/assignments/protocol-numbers.

- **Dirección.** Seleccione la dirección del tráfico a la que se aplica la regla.

Dirección	Descripción
Saliente	La regla se aplicará sólo para el tráfico saliente.
Entrante	La regla se aplicará sólo para el tráfico entrante.
Ambos	La regla se aplicará en ambas direcciones.

- **Versión de IP.** Seleccione la versión de IP (IPv4, IPv6 o cualquiera) a la que se aplica la regla.
- **Red.** Seleccione el tipo de red al que se aplica la regla.
- **Permisos.** Seleccione uno de los permisos disponibles:

Permisos	Descripción
Permitir	Se permitirá el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.
Bloquear	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

Haga clic en **Guardar** para añadir la regla.

Utilice las flechas situadas a la derecha de la tabla para establecer la prioridad de cada una de las reglas que creó. La regla con mayor prioridad es la más próxima al principio de la lista.

6.2.4. Control de Contenido

Utilice el módulo Control de contenido para configurar sus preferencias en lo referente al filtrado de contenidos y la protección de datos para la actividad del usuario incluyendo la navegación Web, el correo electrónico y las aplicaciones de software. Puede restringir o permitir el acceso Web y el uso de aplicaciones, configurar el análisis del tráfico, el antiphishing y las reglas de protección de datos. Por favor, tenga en cuenta que la configuración del Control de contenido se aplica a todos los usuarios que inician sesión en los equipos de destino.

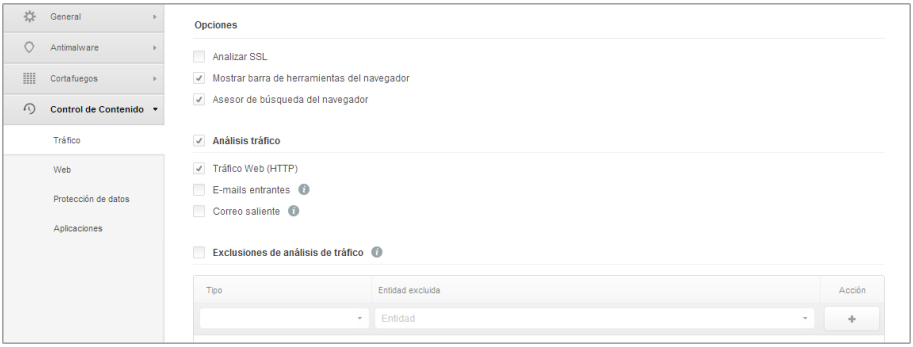
Los ajustes se organizan en las siguientes categorías:

- Tráfico
- Web
- Protección de datos
- Aplicaciones

Tráfico

Configure las preferencias de seguridad del tráfico mediante los ajustes de los siguientes apartados:

- Opciones
- Análisis tráfico
- Exclusiones de análisis de tráfico



Políticas de equipos - Control de contenidos - Tráfico

Opciones

- **Analizar SSL**. Seleccione esta opción si desea que el tráfico Web Secure Sockets Layer (SSL) sea inspeccionado por los módulos de protección Endpoint Security.
- **Mostrar barra de herramientas del navegador**. La barra de herramientas de Bitdefender informa a los usuarios sobre la clasificación de las páginas Web que están visitando. La barra de herramientas de Bitdefender no es la barra de herramientas típica de su navegador. La única cosa que agrega al navegador es un pequeño control de arrastre  en la parte superior de cada página Web. Haciendo clic en el control de arrastre se abre la barra de herramientas.

  Dependiendo de cómo clasifique Bitdefender la página Web, se muestra una de siguientes valoraciones en el lado izquierdo de la barra de herramientas:

  – Aparece el mensaje "Esta página no es segura" sobre un fondo rojo.

  – El mensaje "se aconseja precaución" aparece sobre un fondo naranja.

  – Aparece el mensaje "Esta página es segura" sobre un fondo verde.
- **Asesor de búsqueda del navegador.** El Asesor de búsqueda, valora los resultados de las búsquedas de Google, Bing y Yahoo!, así como enlaces a Facebook y Twitter, colocando un icono delante de cada resultado: Iconos utilizados y su significado:

  No debería visitar esta página web.

  Esta página Web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.

  Esta página es segura.

Análisis tráfico

Los mensajes de correo y el tráfico Web entrantes se analizan en tiempo real para evitar que se descargue malware en el equipo. Los mensajes de correo salientes se analizan para evitar que el malware infecte otros equipos. Analizando el tráfico web debe ralentizar el navegador web un poco, pero bloqueará el malware que viene de Internet, incluyendo descargas nos autorizadas.

Cuando se encuentra un email infectado, se reemplaza automáticamente con un email estándar que informa al destinatario del mensaje infectado original. Si una página Web contiene o distribuye malware se bloquea automáticamente. En su lugar se muestra una página de advertencia especial para informar al usuario de que la página Web solicitada es peligrosa.

Aunque no se recomienda, puede desactivar el análisis del tráfico Web y del correo para incrementar el rendimiento del sistema. Esto no supone una amenaza importante mientras el análisis on-access de los archivos locales permanezca activado.

Exclusiones de análisis de tráfico

Puede escoger evitar el análisis en busca de malware para determinado tráfico mientras las opciones de análisis de tráfico permanecen habilitadas.

Para definir una exclusión de análisis de tráfico:

1. Seleccione el tipo de exclusión desde el menú.
2. Dependiendo del tipo de exclusión, defina la entidad de tráfico a excluir del análisis de la siguiente manera:
   - **IP**. Introduzca la dirección IP para la que no desea analizar ni el tráfico entrante ni el saliente.
   - **URL**. Excluye del análisis la dirección Web especificada. Para definir la exclusión de análisis de una URL:
     – Introduzca una URL determinada, como por ejemplo `www.ejemplo.com/ejemplo.html`
     – Haga uso de caracteres comodín para definir patrones de direcciones Web:
       - Asterisco (*) sustituye a cero o más caracteres.
       - Signo de interrogación (?) se sustituye por exactamente un carácter. Puede usar varios signos de interrogación para definir cualquier combinación de un número específico de caracteres. Por ejemplo, ??? sustituye cualquier combinación de exactamente tres caracteres.

     En la siguiente tabla, puede encontrar distintos ejemplos de sintaxis para especificar direcciones Web.

Sintaxis:	Aplicación de excepciones
`www.ejemplo*`	Cualquier sitio Web o página Web que comience por `www.ejemplo` (sin importar la extensión del dominio). La exclusión no se aplicará a los subdominios del sitio Web especificado, como por ejemplo `subdominio.ejemplo.com`.
`*ejemplo.com`	Cualquier sitio Web que acabe en `ejemplo.com`, incluyendo páginas y subdominios del mismo.
`*cadena*`	Cualquier sitio Web o página Web que cuya dirección contenga la cadena especificada.
`*.com`	Cualquier sito Web que tenga una extensión de dominio `.com`, incluyendo páginas y subdominios del mismo. Utilice esta sintaxis para excluir del análisis dominios enteros de nivel superior.

Sintaxis:	Aplicación de excepciones
`www.ejemplo?.com`	Cualquier dirección Web que comience con `www.ejemplo?.com`, donde ? puede reemplazarse por cualquier carácter. Estos sitios Web podrían incluir: `www.ejemplo1.com` o `www.ejemploA.com`.

- **Aplicación**. Excluye del análisis la aplicación o proceso especificado. Para definir una exclusión de análisis de una aplicación:
  - Introduzca la ruta completa de la aplicación. Por ejemplo, `C:\Archivos de programa\Internet Explorer\iexplore.exe`
  - Utilice variables de entorno para especificar la ruta de la aplicación. Por ejemplo: `%programfiles%\Internet Explorer\iexplore.exe`
  - Utilice caracteres comodín para especificar cualesquiera aplicaciones cuyo nombre coincida con determinado patrón. Por ejemplo:
    - `c*.exe` corresponde a todas las aplicaciones que empiecen por "c" (chrome.exe).
    - `??????.exe` corresponde a todas las aplicaciones cuyo nombre tenga seis caracteres (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` corresponde a cualquier aplicación excepto las que empiecen por "c".
    - `[^ci]*.exe` corresponde a cualquier aplicación excepto las que empiecen por "c" o por "i".

3. Haga clic en el botón **Añadir** del lateral derecho de la tabla.

Para eliminar una entidad de la lista, pulse el botón **Eliminar** correspondiente.

Web

En este apartado puede configurar las preferencias de seguridad para la navegación Web.

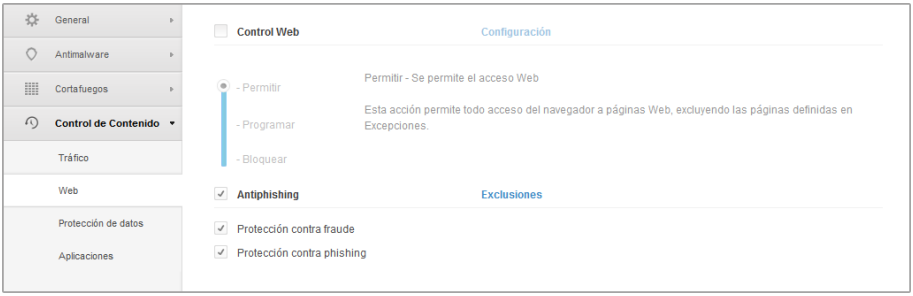
Los ajustes se organizan en los siguientes apartados:

- Control Web
- Antiphishing

Control Web

El Control Web de Navegación le ayuda a bloquear o permitir el acceso web a usuarios y aplicaciones durante el periodo de tiempo indicado.

Estas webs bloqueadas por el Control Web no se mostrarán en el navegador. En su lugar aparecerá una página predeterminada informando al usuario que la página solicitada ha sido bloqueada por el Control Web.



Políticas de equipos - Control de contenidos - Web

Utilice el conmutador para activar o desactivar el **Control Web**.

Tiene tres opciones de configuración:

- Seleccione **Permitir** para conceder siempre el acceso Web.
- Seleccione **Bloquear** para denegar siempre el acceso Web.
- Seleccione **Planificar** para habilitar restricciones de tiempo en cuanto al acceso Web según una planificación detallada.

Ya elija permitir o bloquear el acceso Web, puede definir excepciones a estas acciones para categorías Web completas o solo para direcciones Web concretas. Haga clic en **Ajustes** para configurar su planificación y excepciones al acceso Web como se indica a continuación:

Programador

Para restringir el acceso a Internet semanalmente en ciertos periodos del día:

1. Seleccione de la cuadrícula los intervalos temporales durante los cuales quiere bloquear el acceso a Internet.

   Puede hacer clic en celdas individuales, o puede hacer clic y arrastrar para cubrir mayores periodos. Haga clic de nuevo en la celda para invertir la selección.

   Para empezar una selección nueva, haga clic en **Permitir todo** o **Bloquear todo** en función del tipo de restricción que desee establecer.

2. Haga clic en **Guardar**.

Nota
Endpoint Security realizará actualizaciones cada hora sin importar si el acceso web está bloqueado.

Categorías

El Filtro de categorías Web filtra dinámicamente el acceso a sitios Web basándose en su contenido. Puede utiliza el filtro de categorías Web para definir excepciones a la acción de control Web seleccionada (permitir o bloquear) para categorías Web completas (como juegos, contenido para adultos o redes online).

Para configurar el Filtro de categorías Web:

1. Seleccione **Filtro de categorías Web**.
2. Para una configuración rápida, haga clic en uno de los perfiles predefinidos (**Agresivo**, **Normal** o **Tolerante**). Use la descripción del lateral derecho de la escala como guía para su elección. Puede ver las acciones predefinidas para las categorías Web disponibles haciendo clic en el botón **Categorías** situado debajo.
3. Si no le satisfacen los ajustes predeterminados, puede definir un filtro personalizado:
   a. Seleccione **Personalizado**.
   b. Haga clic en el botón **Categorías** para desplegar la sección correspondiente.
   c. Busque en la lista la categoría que quiera y escoja la acción deseada en el menú.
4. También puede escoger **Tratar las Categorías Web como excepciones para el Acceso Web** si desea ignorar los ajustes de Acceso Web existentes y aplicar solo el Filtro de categorías Web.
5. Haga clic en **Guardar**.

Nota

- **Permitir** categorías Web específicas también se tiene en cuenta durante los intervalos de tiempo en los que el acceso Web está bloqueado por el Control Web.
- **Permitir** los permisos funciona sólo cuando el acceso Web está bloqueado por el Control Web, mientras que **Bloquear** permisos funciona sólo cuando el acceso Web está permitido por el Control Web.
- Puede anular el permiso de la categoría para direcciones Web individuales añadiéndolas con el permiso contrario en **Control de acceso Web > Ajustes > Exclusiones**. Por ejemplo, si el Filtro de categorías bloquea una dirección Web, añada una regla Web para esa dirección con el premiso establecido como **Permitir**.

Exclusiones

También puede definir reglas Web para bloquear o permitir explícitamente ciertas direcciones Web, anulando los ajustes del Control Web. Así, por ejemplo, los usuarios podrán acceder a páginas Web específicas incluso cuando la navegación Web esté bloqueada por el Control Web.

Para crear una regla Web:

1. Seleccione **Usar excepciones** para habilitar las excepciones Web.
2. Introduzca la dirección que quiera permitir o bloquear en el campo **Direcciones Web**.
3. Seleccione **Permitir** o **Bloquear** del menú **Permiso**.
4. Haga clic en el botón **Añadir** del lateral derecho de la tabla para añadir la dirección a la lista de excepciones.

5. Haga clic en **Guardar**.

Para modificar una regla Web:

1. Haga clic en la dirección Web que desee modificar.
2. Modifique la URL existente.
3. Haga clic en **Guardar**.

Para eliminar una regla Web:

1. Sitúe el cursor sobre la dirección Web que quiera eliminar.
2. Haga clic en el botón − **Borrar**.
3. Haga clic en **Guardar**.

Antiphishing

La protección Antiphishing bloquea automáticamente las páginas Web de phishing conocidas para evitar que los usuarios puedan revelar sin darse cuenta información confidencial a impostores online. En lugar de la página Web de phishing, se muestra en el navegador una página de advertencia especial para informar al usuario de que la página Web solicitada es peligrosa.

Seleccione **Antiphishing** para activar la protección antiphishing. Puede afinar más todavía Antiphishing configurando los siguientes ajustes:

- **Protección contra fraude**. Seleccione esta opción si desea ampliar la protección a otros tipos de estafas además del phishing. Por ejemplo, los sitios Web que representan empresas falsas, que no solicitan directamente información privada, pero en cambio intentan suplantar a empresas legítimas y lograr un beneficio engañando a la gente para que hagan negocios con ellos.
- **Protección contra phishing**. Mantenga esta opción seleccionada para proteger a los usuarios frente a los intentos de phishing.

Si una página Web legítima se detecta incorrectamente como de phishing y es bloqueada, puede añadirla a la lista blanca para permitir que los usuarios puedan acceder a ella. La lista debería contener únicamente sitios Web en los que confíe plenamente.

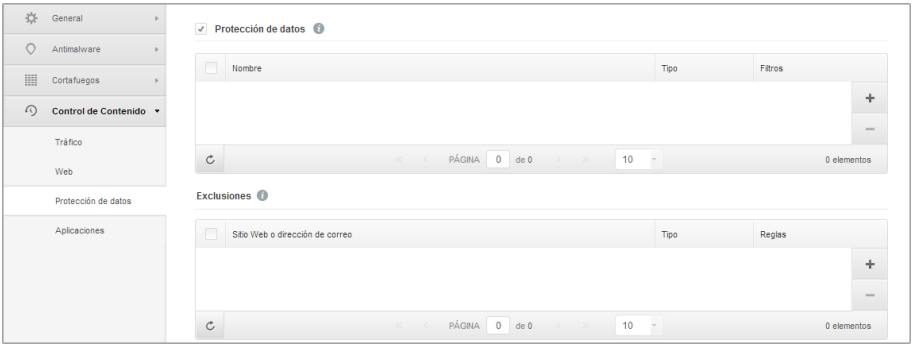
Para gestionar las excepciones antiphishing:

1. Haga clic en **Exclusiones**.
2. Introduzca la dirección Web y pulse el botón + **Añadir**.

   Para eliminar una exception de la lista, mueva el cursor sobre ella y haga clic en el botón − **Borrar** correspondiente.
3. Haga clic en **Guardar**.

Protección de datos

La Protección de datos evita la divulgación no autorizada de información sensible basándose en las reglas definidas por el administrador.



Políticas de equipos - Control de contenidos - Protección de datos

Puede crear reglas para proteger cualquier información personal o confidencial, como:

- Información personal del cliente
- Nombres y detalles clave de los productos y tecnologías en desarrollo
- Información de contacto de los ejecutivos de la empresa

La información protegida puede incluir nombres, números de teléfono, información de tarjetas de crédito o cuentas bancarias, direcciones de e-mail y otros.

Endpoint Security analiza la Web y el tráfico de correo que abandona el equipo en busca de determinadas cadenas de caracteres (por ejemplo, un número de tarjeta de crédito) basándose en las reglas de protección que haya definido. Si se produce una coincidencia, el sitio Web correspondiente o el mensaje de correo se bloquea para evitar que se envíe información protegida. El usuario es informado inmediatamente sobre la acción tomada por el Endpoint Security a través de una página web de alerta o un email.

Para configurar la Protección de datos:

1. Use la casilla de verificación para activar la Protección de datos.
2. Cree reglas de protección de datos para toda la información sensible que quiera proteger. Para crear una regla:
   a. Haga clic en el botón + **Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
   b. Escriba el nombre con el que mostrará la regla en la tabla de reglas. Elija un nombre descriptivo de forma que usted o el administrador puedan fácilmente identificar para qué se utiliza la regla.

c. Introduzca los datos que desee proteger (por ejemplo, el número de teléfono de un ejecutivo de la empresa o el nombre interno de un nuevo producto en el que trabaja la empresa). Se acepta cualquier combinación de palabras, números o cadenas compuestas de caracteres alfanuméricos y especiales (como @, # o $).

Asegúrese de introducir por lo menos cinco caracteres para evitar errores en los bloqueos de e-mails y páginas Web.

Importante

Los datos suministrados se almacenan de forma cifrada en los equipos protegidos pero pueden verse en su cuenta de Control Center. Para mayor seguridad, no introduzca toda la información que desea proteger. En este caso debe desmarcar la opción **Coincidir sólo palabras completas**.

d. Configure las opciones de análisis del tráfico como sea necesario.

- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coincidan con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (mail) y bloquea los mensajes salientes que coincidan con los datos de la regla.

Puede elegir entre aplicar las reglas sólo si los datos de la regla coinciden completamente con las palabras, o si los datos de la regla y la cadena de texto detectada coinciden en mayúsculas y minúsculas.

e. Haga clic en **Guardar**. La nueva regla se añadirá a la lista.

3. Configure las exclusiones en las reglas de protección de datos para que los usuarios puedan enviar todavía datos confidenciales a los sitios Web y destinatarios autorizados. Las exclusiones pueden aplicarse globalmente (a todas las reglas) o solo a reglas específicas. Para añadir una exclusión:
   a. Haga clic en el botón + **Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
   b. Escriba la dirección de email o Web a la que los usuarios pueden enviar datos protegidos.
   c. Seleccione el tipo de exclusión (dirección Web o de e-mail).
   d. En la tabla de **Reglas**, seleccione la regla o reglas de protección de datos a las que aplicar esta exclusión.
   e. Haga clic en **Guardar**. La nueva regla de exclusión se añadirá a la lista.

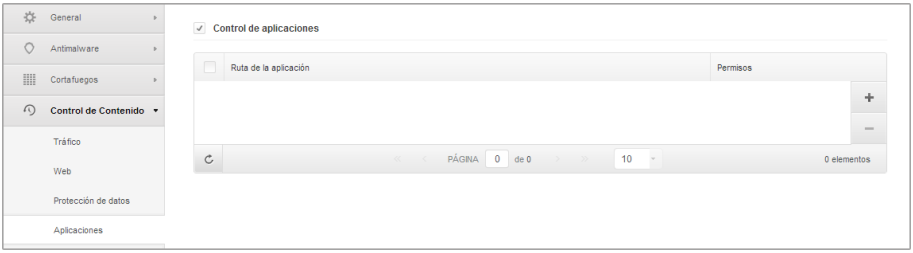
Nota

Si se envía un email que contenga información bloqueada a múltiples receptores, lo recibirán aquellos para los cuales se hayan definido exclusiones.

Para eliminar una regla o una excepción de la lista, haga clic en el botón − **Borrar** correspondiente del lateral derecho de la tabla.

Aplicaciones

En este apartado puede configurar el Control de aplicación. El Control de aplicación le ayuda a bloquear por completo o restringir el acceso de los usuarios a las aplicaciones de sus equipos. Los juegos, el software multimedia o las aplicaciones de mensajería, así como otros tipos de software, pueden bloquearse a través de este componente.



Políticas de equipos - Control de contenidos - Aplicaciones

Para configurar el Control de aplicación:

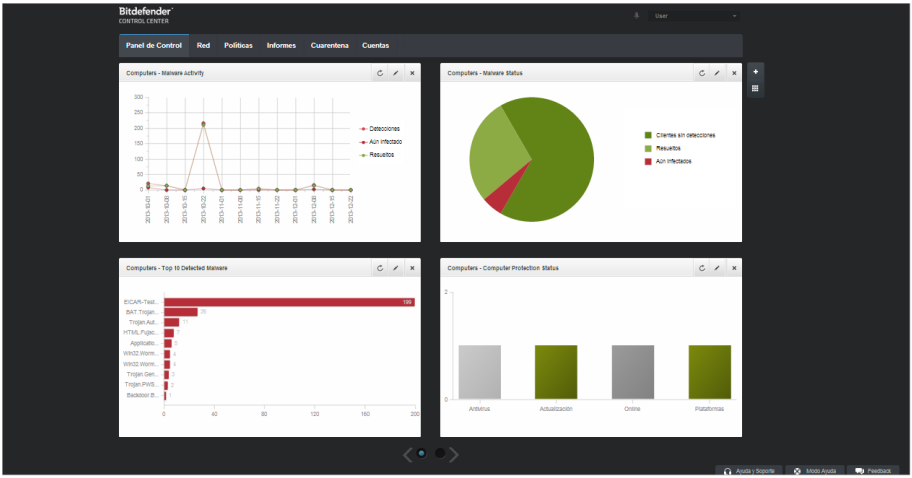
1. Utilice el conmutador para activar el Control de Aplicación.
2. Especifique las aplicaciones a las que desea restringir el acceso. Para restringir el acceso a una aplicación:
   a. Haga clic en el botón + **Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
   b. Debe especificar la ruta al archivo ejecutable de la aplicación en los equipos objetivos. Existen dos formas de hacer esto:
      - Elija desde el menú una ubicación predefinida y complete la ruta según sea necesario en el campo de edición. Por ejemplo, para una aplicación instalada en la carpeta `Archivos de programa`, seleccione `%ProgramFiles` y complete la ruta añadiendo una barra invertida (\) y el nombre de la carpeta de la aplicación.
      - Escriba la ruta completa en el campo de edición. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo.
   c. **Programador de acceso**. Programar el acceso a aplicaciones semanalmente en ciertos periodos del día:
      - Seleccione en la cuadrícula los intervalos temporales durante los cuales desee bloquear el acceso a la aplicación. Puede hacer clic en celdas individuales, o puede hacer clic y arrastrar para cubrir mayores periodos. Haga clic de nuevo en la celda para invertir la selección.
      - Para empezar una selección nueva, haga clic en **Permitir todo** o **Bloquear todo** en función del tipo de restricción que desee establecer.
      - Haga clic en **Guardar**. La nueva regla se añadirá a la lista.

Para eliminar una regla de la lista, haga clic en el botón – **Borrar** correspondiente del lateral derecho de la tabla. Para editar una regla existente, haga clic en el nombre de la aplicación.

7. 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. 123).
- 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.

7.1. 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.

7.2. 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.

7.3. 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. 123).
4. En la pestaña **Objetivos**, seleccione los objetos de red y grupos a incluir.
5. Haga clic en **Guardar**.

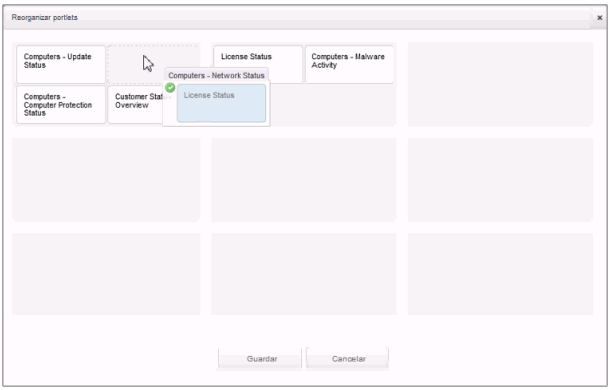
7.4. Eliminar un Portlet

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.

7.5. 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

8. 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).

8.1. 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 antimalware
- 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.

8.2. Creando Informes

Puede crear dos categorías de informes:

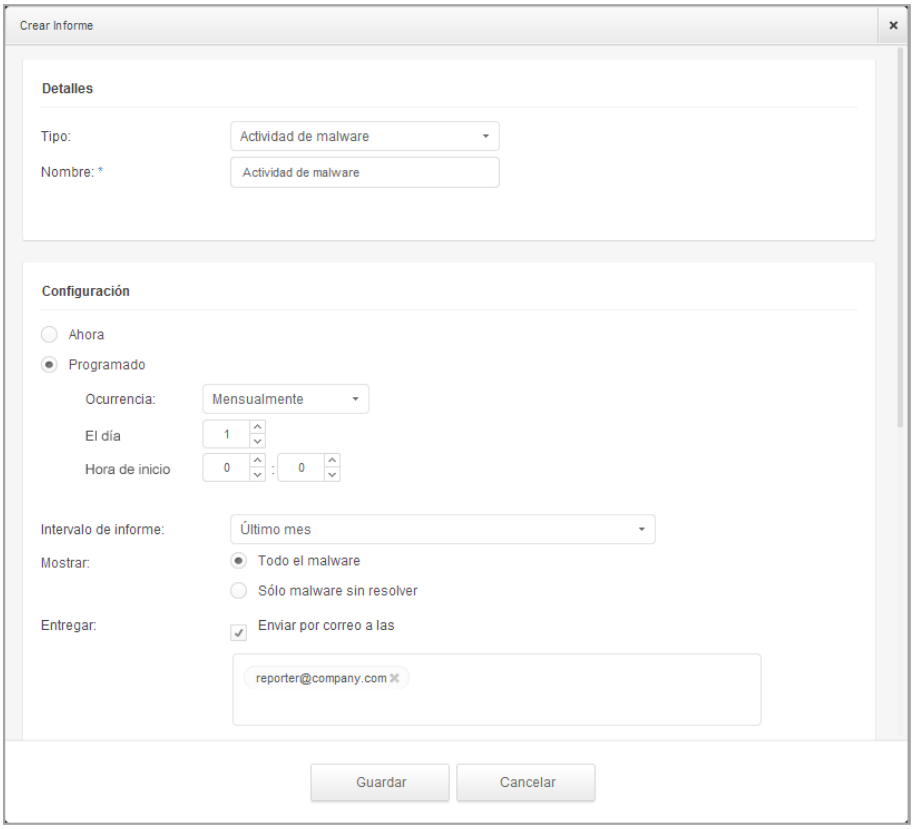
- **Informes instantáneos.** Los informes instantáneos se muestran automáticamente una vez generados.
- **Informes programados.** Los informes programados pueden configurarse para que se ejecuten en una hora y fecha especificada y se muestra una lista de todos los informes programados en la página **Informes**.

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.



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. 123).
4. Escriba un hombre 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).

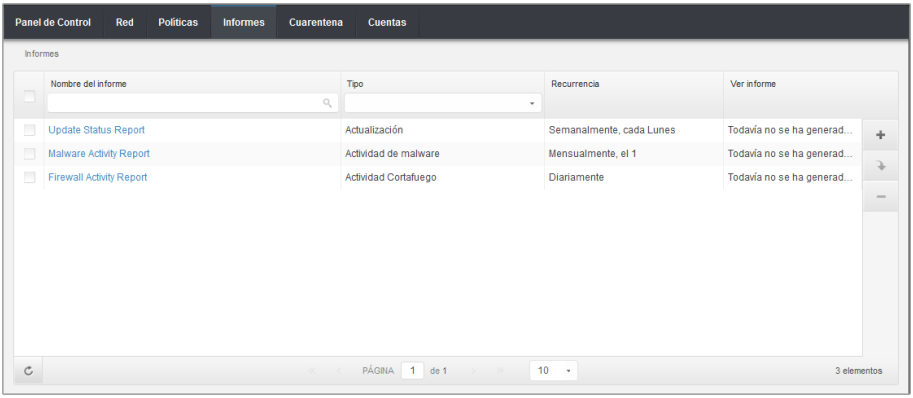
- Semanalmente, en los días especificados de la semana y a la hora de inicio seleccionada (horas y minutos).
- Mensualmente, en los días especificados del mes y a la hora de inicio seleccionada (horas y minutos).

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**.

8.3. Ver y administrar informes programados

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



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 distribuirse 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.

8.3.1. 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.

8.3.2. 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.

8.3.3. 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.

8.4. 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.

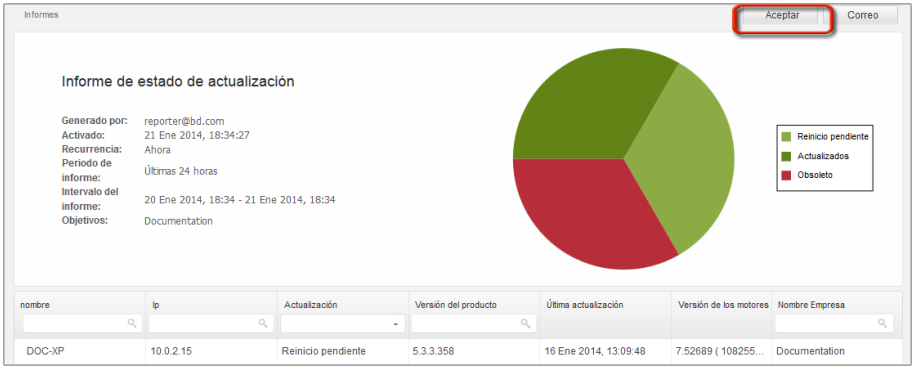
Dispone de dos formas de guardar informes:

- Aceptar
- Descargar

8.4.1. 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.



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.

8.4.2. 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.

8.5. 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.

8.6. 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.

9. Cuarentena

De forma predeterminada, Endpoint Security aísla los archivos sospechosos y los archivos infectados con malware que no pueden desinfectarse en un área segura denominada cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Security for Endpoints almacena los archivos de cuarentena en cada equipo administrado. Usando Control Center tiene la opción de eliminar o restaurar archivos específicos de la cuarentena.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Además, los archivos en cuarentena se analizan tras cada actualización de firmas malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Control Center proporciona información detallada sobre todos los archivos movidos a la cuarentena en los objetos de red administrados de su cuenta.

Para comprobar y gestionar los archivos en cuarentena, diríjase a la página **Cuarentena**.

La página Cuarentena

La información sobre los archivos en cuarentena se muestra en una tabla. Se le proporciona la siguiente información:

- El nombre del objeto de red en el que se detectó la amenaza.
- La IP del objeto de red en el que se detectó la amenaza.
- Ruta al archivo infectado o sospechoso en el objeto de red en el que se detectó.
- Nombre dado a la amenaza malware por los investigadores de seguridad de Bitdefender.

- Hora en la que el archivo fue puesto en cuarentena.
- Acción pendiente solicitada por el administrador para llevarse a cabo sobre el archivo de la cuarentena.

Para asegurarse de que se está mostrando la última información, haga clic en el botón **Refrescar** en la esquina inferior izquierda de la tabla. Esto puede ser necesario cuando dedique más tiempo a la página.

9.1. Navegación y búsqueda

Dependiendo del número de objetos de red administrados y la naturaleza de la infección, el número de archivos en la cuarentena puede a veces ser grande. La tabla puede distribuirse en varias páginas (por omisión se muestran únicamente 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 columna para filtrar la información mostrada. Por ejemplo, puede buscar una amenaza específica detectada en la red o para un objeto de red específico. También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica.

9.2. Restaurar archivos de la cuarentena

En ocasiones particulares, puede que necesite restaurar archivos en cuarentena, bien sea a sus ubicaciones originales o a una ubicación alternativa. Una situación de ese tipo es cuando quiere recuperar archivos importantes almacenados en un fichero comprimido infectado que ha sido movido la cuarentena.

Para restaurar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Marque las casillas de verificación correspondientes a los archivos en cuarentena que desee restaurar.
3. Haga clic en el botón **Restaurar** del lateral derecho de la tabla.
4. Elija la ubicación donde desea que sean restaurados los archivos seleccionados (bien sea la ubicación original o una personalizada del equipo objetivo).

   Si elige restaurar en una ubicación personalizada, debe introducir la ruta en el campo correspondiente. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo. Para más información, diríjase a “Usar variables de sistema” (p. 151).

5. Seleccione **Añadir exclusión en política automáticamente** para excluir los archivos a restaurar de análisis futuros. La exclusión se aplica a todas las políticas que afecten a los archivos seleccionados, a excepción de la política por defecto, que no se puede modificar.
6. Haga clic en **Guardar** para solicitar la acción de restauración del archivo. Puede observar la acción pendiente en la columna **Acción**.
7. La acción solicitada se envía a los equipos objetivo inmediatamente o tan pronto como vuelvan a estar online. Una vez restaurado un archivo, la entrada correspondiente desaparece de la tabla de cuarentena.

9.3. Eliminación automática de archivos de la cuarentena

Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Estos ajustes pueden cambiarse editando la política asignada a los objetos de red administrados.

Para modificar el intervalo de eliminación automático para los archivos en cuarentena:

1. Diríjase a la página **Políticas**.
2. Encuentre la política asignada a los objetos de red en los que quiera modificar los ajustes y haga clic en su nombre.
3. Vaya a la sección **Antimalware > Cuarentena**.
4. Seleccione el periodo de eliminación automática deseado desde el menú.
5. Haga clic en **Guardar** para aplicar los cambios.

9.4. Eliminar archivos de la cuarentena

Si quiere eliminar archivos de la cuarentena manualmente, debería primero asegurar que los archivos que ha elegido para borrar no son necesarios. Use estos consejos cuando elimine archivos de la cuarentena:

- Un archivo puede ser el propio malware en sí. Si su investigación le lleva a esta situación, puede buscar en la cuarentena la amenaza específica y eliminarla de la cuarentena.
- Puede eliminar con seguridad:
  - Elementos del archivo no importantes.
  - Archivos de instalación infectados.

Para eliminar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.

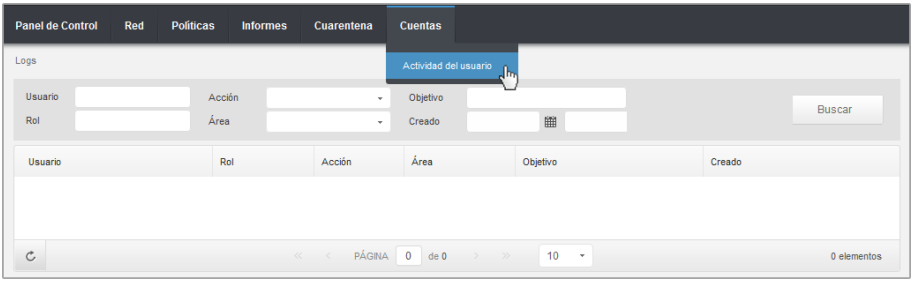
2. Compruebe la lista de archivos en la cuarentena y marque las casillas de verificación correspondientes de aquellos que desee eliminar.
3. Haga clic en el botón − **Borrar** del lateral derecho de la tabla. Puede observar el estado pendiente en la columna **Acción**.
4. La acción solicitada se envía a los equipos de red objetivo inmediatamente o tan pronto como vuelvan a estar online. Una vez que se ha eliminado un archivo, la entrada correspondiente desaparecerá de la tabla Cuarentena.

10. 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
- Crear, editar y borrar credenciales
- Crear, modificar, descargar y eliminar paquetes de red
- Crear tareas de red
- Crear, editar, renombrar y eliminar cuentas de usuario
- Eliminar o mover equipos entre grupos
- Crear, mover, renombrar y eliminar grupos
- Eliminar y restaurar archivos de la cuarentena
- Crear, editar y eliminar cuentas de usuario
- Crear, editar, renombrar, asignar y eliminar políticas

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



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.

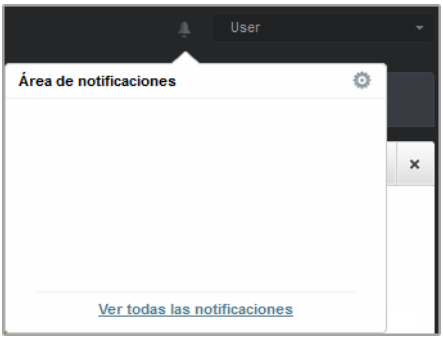
Para ordenar eventos por una columna específica, simplemente haga clic en el encabezado de esa columna. Haga clic en el encabezado de la columna nuevamente para invertir el sentido de ordenación.

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.

11. 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.

11.1. 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. 143).

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.

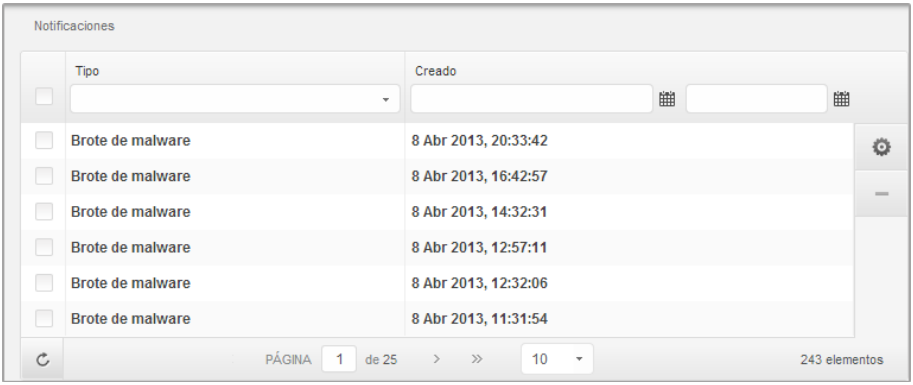
Evento de Protección de datos
Esta notificación se envía cada vez que se bloquea el tráfico de datos en un punto final de acuerdo con las reglas de protección de datos.

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.

11.2. 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.



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.

11.3. 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.

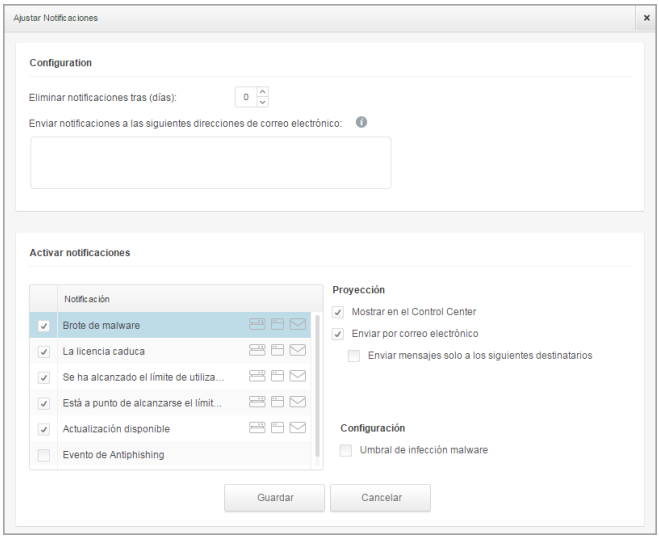
También puede configurar las notificaciones para que se borren automáticamente tras un cierto número de días. Para más información, diríjase a “Configurar las opciones de notificación” (p. 143).

11.4. 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. 140). 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**.

12. Obtener Ayuda

Bitdefender se esfuerza en proporcionar a sus clientes un incomparable soporte rápido y eficiente. Si experimenta algún problema o si tiene cualquier duda sobre su producto Bitdefender, diríjase a nuestro Centro de soporte online. Dispone de muchos recursos que puede utilizar para encontrar rápidamente una solución o respuesta a su problema. O, si lo prefiere, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

12.1. Centro de soporte de Bitdefender

El Centro de soporte de Bitdefender, disponible en http://www.bitdefender.com/support/business.html, es el lugar al que acudir para encontrar toda la asistencia técnica que necesite para su producto Bitdefender.

Podrá encontrar rápidamente una solución o una respuesta a su consulta:

- Artículos de la base de conocimiento
- Foro de soporte de Bitdefender
- Documentación del Producto

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad informática, los productos Bitdefender y la empresa.

Artículos de la base de conocimiento

La Base de conocimientos de Bitdefender es un repositorio de información online sobre los productos Bitdefender. Almacena, en un formato de fácil acceso, los informes sobre los resultados del soporte técnico en curso y las actividades de solución de errores por los equipos de soporte y desarrollo de Bitdefender, junto con artículos más generales sobre prevención de virus, la administración de las soluciones Bitdefender con explicaciones detalladas, y muchos otros artículos.

La Base de conocimiento de Bitdefender es de acceso público y puede consultarse gratuitamente. La amplia información que contiene es otro medio de proporcionar a los clientes de Bitdefender el soporte técnico y el conocimiento que necesitan. Las solicitudes de información general o informes de errores de los clientes de Bitdefender se incluyen en la Base de conocimientos de Bitdefender en forma de soluciones a los bugs, instrucciones de depuración de errores o artículos informativos como apoyo a los archivos de ayuda de los productos.

La base de conocimientos de Bitdefender para productos corporativos está permanentemente disponible en http://www.bitdefender.com/support/business.html.

Foro de soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una forma fácil de obtener ayuda y ayudar a otros. Puede publicar cualquier problema o consulta relacionada con su producto Bitdefender.

El soporte técnico de Bitdefender monitoriza el foro en busca de nuevas publicaciones con el fin de ayudarle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de postear su problema o pregunta, por favor, busque en el foro un tema similar o relacionado.

El Foro de Soporte de Bitdefender está disponible en http://forum.bitdefender.com, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano. Haga clic en el enlace **Protección empresarial** para acceder a la sección dedicada a los productos corporativos.

Documentación del Producto

La documentación del producto es la fuente más completa de información sobre su producto.

Puede consultar y descargar la última versión de la documentación para los productos corporativos de Bitdefender en Centro de soporte > Documentación.

12.2. Solicitar ayuda

Puede contactar con nosotros para solicitar ayuda a través de nuestro Centro de Soporte en línea:

1. Visite http://www.bitdefender.es/support/contact-us.html.
2. Utilice el formulario de contacto para abrir un ticket de soporte por correo electrónico o acceda a otras opciones de contacto disponibles.

12.3. Usar la herramienta de soporte

La herramienta de soporte Small Office Security está diseñada para ayudar a los usuarios y a los técnicos de soporte a obtener fácilmente la información que necesitan para la resolución de problemas. Ejecute la herramienta de soporte en los equipos afectados, y envíe el archivo resultante con la información de la resolución del problema al representante de soporte de Bitdefender.

Para usar la herramienta de soporte:

1. Descargue la herramienta de soporte y distribúyala a los equipos afectados. Para descargar la herramienta de soporte:
   a. Conéctese a Control Center usando su cuenta.
   b. Haga clic en el enlace **Ayuda y soporte** en la esquina inferior derecha de la consola.
   c. Los enlaces de descarga están disponibles en la sección **Soporte**. Hay disponibles dos versiones: una para sistemas de 32 bits y la otra para sistemas de 64 bits. Asegúrese de utilizar la versión correcta cuando ejecute la herramienta de soporte en un equipo.
2. Ejecute la herramienta de soporte localmente en cada uno de los equipos afectados.
   a. Seleccione la casilla de verificación de consentimiento y haga clic en **Siguiente**.
   b. Rellene el formulario de envío con los datos necesarios:
      i. Introduzca su dirección de correo.
      ii. Escriba su nombre.
      iii. Seleccione su país desde el menú correspondiente.
      iv. Escriba una descripción del problema que se ha encontrado.
      v. Opcionalmente, puede intentar reproducir el problema antes de empezar a recolectar datos. En tal caso, proceda de la siguiente manera:
         A. Active la opción **Intentar reproducir el problema antes de enviarlo**.
         B. Haga clic en **Siguiente**.
         C. Seleccione el tipo de incidencia que ha experimentado.
         D. Haga clic en **Siguiente**.
         E. Reproduzca el problema en su equipo. Cuando acabe, vuelva a la Herramienta de soporte y seleccione la opción **He reproducido el problema**.
   c. Haga clic en **Siguiente**. La Support Tool recoge la información de producto, información relacionada con otras aplicaciones instaladas en la máquina y la configuración del software y del hardware.
   d. Espere a que se complete el proceso.
   e. Haga clic en **Finalizar** para cerrar la ventana. Se ha creado un archivo zip en su escritorio.

      Envíe el archivo zip junto con su solicitud al representante de soporte de Bitdefender mediante el formulario de ticket de soporte por correo electrónico disponible en la página de **Ayuda y soporte** de la consola.

12.4. Información de contacto

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 10 años, Bitdefender se ha forjado una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectativas de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

12.4.1. Direcciónes

Departamento de ventas: enterprisesales@bitdefender.com
Centro de soporte:http://www.bitdefender.com/support/business.html
Documentación: documentation@bitdefender.com
Distribuidores locales:http://www.bitdefender.es/partners
Programa de Partners: partners@bitdefender.com
Relaciones con la Prensa: prensa@bitdefender.es
Envío de virus: virus_submission@bitdefender.com
Envío de Spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Sitio Web:http://www.bitdefender.es

12.4.2. Oficinas de Bitdefender

Las oficinas de Bitdefender están listas para responder a cualquier pregunta relativa a sus áreas de acción, tanto a nivel comercial como en otros asuntos. Sus direcciones y contactos están listados a continuación.

Estados Unidos

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Teléfono (comercial&soporte técnico): 1-954-776-6262
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com
Centro de soporte: http://www.bitdefender.com/support/business.html

Francia

PROFIL TECHNOLOGY
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09

Teléfono: +33 (0)1 47 35 72 73
Correo: supportpro@profiltechnology.com
Página Web: http://www.bitdefender.fr
Centro de soporte: http://www.bitdefender.fr/support/professionnel.html

España

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Tel (oficina&comercial): (+34) 93 218 96 15
Teléfono (soporte técnico): (+34) 93 502 69 10
Comercial: comercial@bitdefender.es
Página Web: http://www.bitdefender.es
Centro de soporte: http://www.bitdefender.es/support/business.html

Alemania

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Tel (oficina&comercial): +49 (0)2301 91 84 222
Teléfono (soporte técnico): +49 (0)2301 91 84 444
Comercial: vertrieb@bitdefender.de
Página Web: http://www.bitdefender.de
Centro de soporte: http://www.bitdefender.de/support/business.html

Reino Unido e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Teléfono (comercial&soporte técnico): +44 (0) 8451-305096
Correo: info@bitdefender.co.uk
Comercial: sales@bitdefender.co.uk
Página Web: http://www.bitdefender.co.uk
Centro de soporte: http://www.bitdefender.co.uk/support/business.html

Rumania

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Teléfono (comercial&soporte técnico): +40 21 2063470
Comercial: sales@bitdefender.ro
Página Web: http://www.bitdefender.ro
Centro de soporte: http://www.bitdefender.ro/support/business.html

Emiratos Árabes Unidos

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Teléfono (comercial&soporte técnico): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Centro de soporte: http://www.bitdefender.com/support/business.html

A. Apéndices

A.1. Lista de tipos de archivos de aplicación

Los motores de análisis antimalware incluidos en las soluciones Bitdefender pueden configurarse para limitar el análisis únicamente a los archivos de aplicaciones (o programas). Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos.

Esta categoría incluye los archivos con las siguientes extensiones:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu;
acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat;
bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;
dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe;
ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd;
ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam;
maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt;
mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub;
puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr;
script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx;
tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm;
wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls;
xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.2. Usar variables de sistema

Alguna de las opciones disponibles en la consola requieren especificar la ruta en los equipos objetivo. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todos los equipos objetivo.

Aquí está la lista de variables de sistema predefinidas:

`%ALLUSERSPROFILE%`
: La carpeta del perfil Todos los usuarios. Ruta típica:

  `C:\Documents and Settings\All users`

`%APPDATA%`
: La carpeta Application Data del usuario que ha iniciado sesión. Ruta típica:

- Windows XP:

  `C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7:

  `C:\Usuarios\{username}\AppData\Roaming`

`%HOMEPATH%`

Las carpetas de usuario. Ruta típica:

- Windows XP:

  `\Documents and Settings\{username}`

- Windows Vista/7:

  `\Usuarios\{username}`

`%LOCALAPPDATA%`

Los archivos temporales de las aplicaciones. Ruta típica:

`C:\Usuarios\{username}\AppData\Local`

`%PROGRAMFILES%`

La carpeta Archivos de programa. Una ruta típica es `C:\Archivos de programa`.

`%PROGRAMFILES(X86)%`

La carpeta Archivos de programa para aplicaciones de 32 bits (en sistemas de 64 bits). Ruta típica:

`C:\Archivos de programa (x86)`

`%COMMONPROGRAMFILES%`

La carpeta Common Files. Ruta típica:

`C:\Archivos de Programa\Archivos Comunes`

`%COMMONPROGRAMFILES(X86)%`

La carpeta Common files para aplicaciones de 32 bits (en sistemas de 64 bits). Ruta típica:

`C:\Archivos de Programa (x86)\Archivos Comunes`

`%WINDIR%`

El directorio Windows o SYSROOT. Una ruta típica sería `C:\Windows`.

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 especificas. 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 periféricoa, 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 Ilíada 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.