Bitdefender

GravityZone

GUÍA DEL ADMINISTRADOR

Bitdefender GravityZone
Guía del Administrador

fecha de publicación 2021.04.20

Advertencia legal

Bitdefender

Tabla de contenidos

Prólogo

Esta guía está dirigida a los administradores de red encargados de gestionar la protección de GravityZone en las instalaciones de su organización.

Este documento tiene como objetivo explicar cómo aplicar y consultar los ajustes de seguridad en los endpoints correspondientes a su cuenta mediante GravityZone Control Center. Aprenderá cómo consultar su inventario de red en Control Center, cómo crear y aplicar políticas en los endpoints administrados, cómo crear informes, cómo administrar los elementos en la cuarentena y cómo utilizar el panel de control.

1. Convenciones utilizadas en esta guía

Convenciones Tipográficas

Esta guía recurre a varios estilos de texto para mejorar su lectura. La siguiente tabla le informa sobre dichos estilos y su significado.

Apariencia	Descripción
`ejemplo`	Los nombres de comandos en línea y sintaxis, rutas y nombres de archivos, configuración, salidas de archivos y texto de entrada se muestran en caracteres de `espacio fijo`.
http://www.bitdefender.com	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
gravityzone-docs@bitdefender.com	Las direcciones de e-mail se incluyen en el texto como información de contacto.
“Prólogo” (p. viii)	Este es un enlace interno, hacia alguna localización dentro del documento.
opción	Todas las opciones del producto se muestran utilizando caracteres en **negrita**.
palabra clave	Las opciones de interfaz, palabras clave o accesos directos se destacan mediante caracteres en **negrita**.

Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.

Nota
La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante
Esta requiere su atención y no es recommendable saltársela. Normalmente proporciona información importante aunque no extremadamente crítica.

Aviso
Se trata de información crítica que debería tartar con extremada cautela. Nada malo ocurrirá si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente peligroso.

1. ACERCA DE GRAVITYZONE

GravityZone es una solución de seguridad empresarial diseñada desde cero para la virtualización y la nube, con el fin de ofrecer servicios de seguridad a endpoints físicos, dispositivos móviles, máquinas virtuales en la nube privada y pública, y servidores de correo de Exchange.

GravityZone es un producto con una consola de administración unificada disponible en la nube, alojada por Bitdefender, o como appliance virtual que se aloja en las instalaciones de la organización, y proporciona un único punto para la implementación, aplicación y administración de las políticas de seguridad para cualquier número de endpoints de cualquier tipo y en cualquier ubicación.

GravityZone aporta múltiples capas de seguridad para endpoints y para los servidores de correo de Microsoft Exchange: antimalware con monitorización del comportamiento, protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas, cortafuego, control de dispositivos, control de contenidos, antiphishing y antispam.

2. CAPAS DE PROTECCIÓN DE GRAVITYZONE

GravityZone proporciona las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- HyperDetect
- Antiexploit avanzado
- Cortafuego
- Control de Contenido
- Administración de parches
- Control de dispositivos
- Cifrado completo del disco duro
- Security for Exchange
- Control de aplicaciones
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

La capa de protección antimalware se basa en el análisis de firmas y en el análisis heurístico (B-HAVE, ATC) contra virus, gusanos, troyanos, spyware, adware, keyloggers, rootkits y otros tipos de software malicioso.

La tecnología de análisis antimalware de Bitdefender se basa en las siguientes tecnologías:

- Primero, se utiliza un método de análisis tradicional donde el contenido analizado se compara con la base de datos de firmas. La base de datos de firmas contiene patrones de bytes específicos para conocer los peligros y se actualiza regularmente por Bitdefender. Este método de análisis es efectivo contra amenazas confirmadas que han sido descubiertas y documentadas. Sin embargo, no importa lo rápidamente que se actualice la base de datos de firmas, siempre hay una ventana de tiempo vulnerable entre que la amenaza es descubierta y una solución es lanzada.
- Contra las amenazas de nueva generación indocumentadas, una segunda capa de protección facilitada por **B-HAVE**, un motor heurístico de Bitdefender. Los

algoritmos heurísticos detectan el malware en función de las características de su comportamiento. B-HAVE ejecuta los archivos sospechosos en un entorno virtual para analizar su impacto en el sistema y asegurarse de que no supongan una amenaza. Si se detecta una amenaza, el programa está prevenido de ejecutarlo.

Motores de análisis

Bitdefender GravityZone puede configurar automáticamente los motores de análisis al crear los paquetes de agentes de seguridad según la configuración del endpoint.

El administrador también puede personalizar los motores de análisis, pudiendo elegir entre varias tecnologías de análisis:

1. **Análisis local**, cuando el análisis se realiza localmente en el endpoint. El modo de análisis local es adecuado para máquinas potentes, con los contenidos de seguridad almacenados localmente.
2. **Análisis híbrido con motores ligeros (nube pública)**, con una huella media, que utiliza el análisis en la nube y, parcialmente, los contenidos de seguridad locales. Este modo de análisis conlleva el beneficio de un menor consumo de recursos, aunque implica el análisis fuera de las instalaciones.
3. **Análisis centralizado en la nube pública o privada**, con una huella reducida que requiere un Security Server para el análisis. En este caso, el conjunto de contenidos de seguridad no se almacena localmente y el análisis se descarga en el Security Server.

   Nota
   Existe un reducido conjunto de motores almacenados localmente, necesarios para descomprimir los archivos comprimidos.

4. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva* en análisis local (motores completos)**
5. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva* en análisis híbrido (nube pública con motores ligeros)**

* Al utilizar análisis con motores duales, cuando el primer motor no esté disponible, se utilizará el motor de reserva. El consumo de recursos y la utilización de la red dependerán de los motores empleados.

2.2. Control avanzado de amenazas

Para las amenazas que logran eludir incluso el motor heurístico, existe otra capa de seguridad denominada Advanced Threat Control (ATC).

Advanced Threat Control monitoriza continuamente los procesos en ejecución y detecta las conductas sospechosas, como por ejemplo los intentos de ocultar el tipo de proceso, ejecutar código en el espacio de otro proceso (secuestro de memoria del proceso para escalado de privilegios), replicar, descartar archivos, ocultarse a las aplicaciones de listado de procesos, etc. Cada comportamiento sospechoso aumenta la calificación del proceso. Cuando se alcanza un límite, salta la alarma.

2.3. HyperDetect

Bitdefender HyperDetect es una capa adicional de seguridad específicamente diseñada para detectar ataques avanzados y actividades sospechosas en la fase previa a la ejecución. HyperDetect incorpora modelos de aprendizaje automático y una tecnología de detección de ataques sigilosos contra amenazas como las de día cero, amenazas persistentes avanzadas (APT), malware ofuscado, ataques sin archivos (uso ilegítimo de PowerShell, Windows Management Instrumentation, etc.), robo de credenciales, ataques selectivos, malware personalizado, ataques basados en scripts, exploits, herramientas de pirateo informático, tráfico de red sospechoso, aplicaciones potencialmente no deseadas (APND) y ransomware.

Nota
Este módulo es un complemento disponible con una clave de licencia independiente.

2.4. Antiexploit avanzado

El Antiexploit avanzado, basado en el aprendizaje automático, es una nueva tecnología proactiva que detiene los ataques de día cero canalizados a través de exploits evasivos. El Antiexploit avanzado ataja los últimos exploits en tiempo real y mitiga las vulnerabilidades de corrupción de memoria que pueden eludir otras soluciones de seguridad. Protege las aplicaciones más habituales, como por ejemplo navegadores, Microsoft Office o Adobe Reader, así como otras que pueda imaginar. Vigila los procesos del sistema y protege contra las violaciones de la seguridad y el secuestro de procesos existentes.

2.5. Cortafuego

El Cortafuego controla el acceso de las aplicaciones a la red y a Internet. Se permite automáticamente el acceso a una amplia base de datos de aplicaciones legítimas y conocidas. Más aun, el cortafuegos puede proteger el sistema contra escaneo de puertos, restringir ICS y avisar cuando se conecten a la red Wi-Fi nuevos nodos.

2.6. Control de Contenido

El módulo de Control de contenidos ayuda a hacer cumplir las políticas de la empresa para el tráfico permitido, el acceso Web, la protección de datos y el control de aplicaciones. Los administradores pueden definir las opciones de análisis de tráfico y las exclusiones, programar el acceso Web bloqueando o permitiendo ciertas categorías Web o URLs, configurar las reglas de protección de datos y definir permisos para el uso de aplicaciones concretas.

2.7. Network Attack Defense

El módulo Network Attack Defense se basa en una tecnología de Bitdefender que se centra en detectar ataques de red diseñados para obtener acceso a endpoints a través de técnicas específicas como ataques de fuerza bruta, exploits de red, ladrones de contraseñas, vectores de infección por descargas ocultas, bots y troyanos.

2.8. Administración de parches

La Administración de parches, que está completamente integrada en GravityZone, mantiene actualizados los sistemas operativos y las aplicaciones de software al tiempo que proporciona visibilidad completa del estado de los parches en los endpoints administrados de Windows.

El módulo de Administración de parches de GravityZone incluye varias características, como análisis de parches bajo demanda o programados, aplicación manual o automática de parches o informes de los parches que faltan.

Puede obtener más información sobre los proveedores y productos compatibles con la Administración de parches de GravityZone en este artículo de la base de conocimientos.

Nota
La Administración de parches es un complemento disponible con una clave de licencia independiente para todos los paquetes de GravityZone existentes.

2.9. Control de dispositivos

El módulo de control de dispositivos permite evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo y excepciones a una amplia gama de tipos de dispositivos (como por ejemplo unidades flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.).

2.10. Cifrado completo del disco duro

Esta capa de protección le permite proporcionar un cifrado de disco completo en los endpoints, mediante la administración de BitLocker en Windows y FileVault y diskutil en macOS. Puede cifrar y descifrar los volúmenes, ya sean de arranque o no, con unos pocos clics, mientras que GravityZone gestiona todo el proceso con una mínima intervención de los usuarios. Además, GravityZone almacena las claves de recuperación necesarias para desbloquear los volúmenes cuando los usuarios olvidan sus contraseñas.

Nota
El Cifrado de disco completo es un complemento disponible con una clave de licencia independiente para todos los paquetes de GravityZone existentes.

2.11. Security for Exchange

Bitdefender Security for Exchange ofrece antimalware, antispam, antiphishing y filtrado de contenidos y adjuntos con una magnífica integración en Microsoft Exchange Server, para garantizar un entorno seguro de mensajería y colaboración y aumentar la productividad. Mediante tecnologías antispam y antimalware galardonadas, protege a los usuarios de Exchange contra el malware más reciente y sofisticado y contra los intentos de robo de datos confidenciales y demás información valiosa de los usuarios.

Importante
Security for Exchange está diseñado para proteger toda la organización de Exchange a la que pertenece el Exchange Server protegido. Esto significa que protege todos los buzones activos, incluidos los de usuario/sala/equipo/compartidos.
Además de la protección de Microsoft Exchange, la licencia también cubre los módulos de protección de endpoints instalados en el servidor.

2.12. Control de aplicaciones

El módulo de Control de aplicaciones evita el malware y los ataques de día cero, y aumenta la seguridad sin afectar a la productividad. El Control de aplicaciones pone en práctica políticas flexibles de lista blanca de aplicaciones, lo que sirve para identificar y evitar la instalación y ejecución de aplicaciones no deseadas, poco fiables o maliciosas.

2.13. Sandbox Analyzer

Sandbox Analyzer de Bitdefender proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender. En el espacio aislado de Sandbox Analyzer se emplea un amplio conjunto de tecnologías de Bitdefender para ejecutar las posibles acciones destructivas en un entorno virtual contenido alojado por Bitdefender o implementado localmente, analizar su comportamiento e informar de cualquier cambio sutil en el sistema que pueda indicar malas intenciones.

Sandbox Analyzer utiliza una serie de sensores para detonar contenidos de los endpoints administrados, la cuarentena centralizada y los servidores ICAP.

Además, Sandbox Analyzer permite el envío de muestras manual y a través de API.

2.14. Hypervisor Memory Introspection (HVI)

Es de sobra conocido que los atacantes con ánimo de lucro altamente organizados buscan vulnerabilidades desconocidas (vulnerabilidades de día cero) o utilizan exploits únicos diseñados específicamente (exploits de día cero) y otras herramientas. Los atacantes también utilizan técnicas avanzadas para retrasar y fragmentar las acciones destructivas de los ataques y así enmascarar sus actividades maliciosas. Los nuevos ataques con ánimo de lucro se diseñan para que sean sigilosos y burlen a las herramientas de seguridad tradicionales.

Para los entornos virtualizados, el problema ya está resuelto: HVI protege centros de datos con una alta densidad de máquinas virtuales contra amenazas avanzadas y sofisticadas que los motores basados en firmas no pueden afrontar. Se impone un fuerte aislamiento, y se garantiza la detección en tiempo real de los ataques, su bloqueo en cuanto se producen y la eliminación inmediata de las amenazas.

Tanto si la máquina protegida es Windows o Linux, como si se trata de un servidor o de un equipo de escritorio, HVI proporciona una visión a un nivel que es imposible alcanzar desde dentro del sistema operativo del guest. Al igual que el hipervisor controla el acceso al hardware en nombre de cada máquina virtual guest, HVI tiene un profundo conocimiento tanto en modo usuario como en modo kernel de la memoria del guest. El resultado es que HVI tiene una visión total de la memoria del guest y, por tanto, un contexto completo. Al mismo tiempo, HVI se aísla de los guests protegidos, dado que el hipervisor en sí está aislado. Al operar a nivel de hipervisor y aprovechar las funcionalidades de este, HVI supera los desafíos técnicos de la seguridad tradicional para revelar la actividad maliciosa en los centros de datos.

HVI identifica las técnicas de ataque en lugar de los patrones de ataque. Así, esta tecnología es capaz de identificar, informar y prevenir técnicas de exploit comunes. El kernel está protegido contra las técnicas de ocultación de rootkits que se utilizan durante la cadena de terminaciones de ataques para que estos pasen desapercibidos. Los procesos en modo usuario también están protegidos contra la inyección de código, el desvío de funciones y la ejecución de código desde la pila o heap.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) es una solución de seguridad de red que analiza los flujos de tráfico de IPFIX para detectar la presencia de malware y comportamientos maliciosos.

Bitdefender NTSA está pensado para actuar conjuntamente con sus medidas de seguridad existentes, como una protección complementaria capaz de cubrir los puntos ciegos que las herramientas tradicionales no monitorizan.

Las herramientas de seguridad de red tradicionales generalmente intentan evitar infecciones de malware inspeccionando el tráfico entrante (mediante espacios aislados, cortafuegos, antivirus, etc.). Bitdefender NTSA se centra únicamente en monitorizar el tráfico de red saliente en busca de comportamientos maliciosos.

2.16. Security for Storage

GravityZone Security for Storage proporciona protección en tiempo real para los principales sistemas de almacenamiento de red y de uso compartido de archivos. Las actualizaciones del algoritmo de detección de amenazas y del sistema se realizan automáticamente, sin ningún esfuerzo por su parte y sin interrumpir a los usuarios finales.

Dos o más GravityZone Security Server multiplataforma desempeñan el rol de servidor ICAP y proporcionan servicios antimalware para dispositivos de almacenamiento conectados a la red (NAS) y sistemas de uso compartido de archivos que cumplan con el protocolo de adaptación de contenidos de Internet (ICAP, según se define en RFC 3507).

Cuando un usuario solicita abrir, leer, escribir o cerrar un archivo desde un portátil, estación de trabajo, un móvil u otro dispositivo, el cliente ICAP (un NAS o un sistema de uso compartido de archivos) envía una solicitud de análisis al Security Server y recibe un veredicto respecto al archivo. En función del resultado, Security Server permite el acceso, lo deniega o borra el archivo.

Nota
Este módulo es un complemento disponible con una clave de licencia independiente.

2.17. Security for Mobile

Unifica la seguridad en toda la empresa con la administración y control de cumplimiento de dispositivos iPhone, iPad y Android, proporcionando un software de confianza y distribución de actualizaciones a través de las tiendas online de Apple y Android. La solución se ha diseñado para permitir la adopción controlada de iniciativas bring-your-own-device (BYOD) haciendo cumplir las políticas de uso en todos los dispositivos portátiles. Las características de seguridad incluyen el bloqueo de pantalla, control de autenticación, localización del dispositivo, detección de dispositivos rooteados o con jailbreak y perfiles de seguridad. En dispositivos Android el nivel de seguridad se mejora con el análisis en tiempo real y el cifrado de medios extraíbles. Así, los dispositivos móviles se encuentran bajo control y se protege la información sensible que reside en ellos.

2.18. Disponibilidad de capas de protección de GravityZone

La disponibilidad de las capas de protección de GravityZone difiere según el sistema operativo del endpoint. Para obtener más información, consulte el artículo de la base de conocimientos Disponibilidad de capas de protección de GravityZone.

3. ARCHITECTURE GRAVITYZONE

La arquitectura única de GravityZone permite escalar la solución con facilidad y proteger cualquier número de sistemas. GravityZone se puede configurar para utilizar varios appliances virtuales y varias instancias de roles específicos (base de datos, servidor de comunicaciones, servidor de actualizaciones y consola Web) para garantizar la fiabilidad y la escalabilidad.

Cada instancia de rol se puede instalar en un appliance diferente. Los balanceadores de roles integrados aseguran que la implementación de GravityZone protege incluso las redes corporativas más grandes sin ocasionar demoras ni cuellos de botella. También se puede utilizar el hardware o software de equilibrio de carga existente en lugar de los balanceadores incorporados, si la red cuenta con él.

GravityZone, suministrado en un contenedor virtual, se puede importar para ejecutarse en cualquier plataforma de virtualización, incluyendo VMware, Citrix, Microsoft Hyper-V, Nutanix Prism y Microsoft Azure.

La integración con VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element y Microsoft Azure reduce el trabajo de implementación de la protección en los endpoints físicos y virtuales.

La solución de GravityZone incluye los siguientes componentes:

- Appliance virtual GravityZone
- Security Server
- Paquete suplementario de HVI
- Agentes de seguridad

3.1. Appliance virtual de GravityZone

La solución GravityZone on-premise se proporciona como appliance virtual reforzado autoconfigurable para Linux Ubuntu, incorporado en una imagen de máquina virtual, fácil de instalar y configurar mediante una CLI (interfaz de línea de comandos). El dispositivo virtual está disponible en varios formatos y es compatible con las principales plataformas de virtualización (OVA, XVA, VHD, OVF, RAW).

3.1.1. Base de datos de GravityZone

La lógica central de la arquitectura de GravityZone. Bitdefender utiliza la base de datos no relacional MongoDB, fácil de escalar y replicar.

3.1.2. Servidor de actualizaciones de GravityZone

El Servidor de actualizaciones tiene la importante misión de actualizar la solución GravityZone y los agentes de endpoint mediante la replicación y la publicación de los paquetes o archivos de instalación necesarios.

3.1.3. Servidor de comunicaciones de GravityZone

El Servidor de comunicaciones es el vínculo entre los agentes de seguridad y la base de datos, y se ocupa de transmitir las políticas y las tareas a los endpoints protegidos, así como los eventos de los que informan los agentes de seguridad.

3.1.4. Consola web (GravityZone Control Center)

Las soluciones de seguridad de Bitdefender se gestionan desde un único punto de administración: la consola web Control Center. Esto proporciona una administración más fácil y acceso a la estrategia de seguridad general y a las amenazas globales contra la seguridad, así como control sobre todos los módulos de seguridad que protegen equipos de escritorio virtuales o físicos, servidores y dispositivos móviles. Equipado con la Arquitectura Gravity, Control Center es capaz de abordar las necesidades de incluso las organizaciones más grandes.

Control Center se integra con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a las estaciones de trabajo, servidores o dispositivos móviles no administrados que aparecen en Microsoft Active Directory, VMware vCenter, Nutanix Prism Element o Citrix XenServer, o que simplemente se detectan en la red.

3.1.5. Base de datos del generador de informes

El rol de Base de datos del Generador de informes proporciona los datos necesarios para crear informes basados en consultas.

3.1.6. Procesadores del generador de informes

El rol de Procesadores del Generador de informes es esencial para crear, administrar y almacenar los informes basados en consultas que utilizan la información de la Base de datos del Generador de informes.

3.2. Security Server

El Security Server es una máquina virtual dedicada que deduplica y centraliza la mayoría de las funciones antimalware de los agentes antimalware, actuando como servidor de análisis.

Hay tres versiones de Security Server, para cada tipo de entorno de virtualización:

- **Security Server for VMware NSX.** Esta versión se instala automáticamente en todos los hosts del cluster en los que se haya implementado Bitdefender.
- **Security Server for VMware vShield Endpoint.** Hay que instalar esta versión en cada host que vaya a protegerse.
- **Security Server Multi-Platform.** Esta versión es para otros entornos de virtualización diferentes y se debe instalar en uno o varios hosts con el fin de adaptarse al número de máquinas virtuales protegidas. Cuando utiliza HVI, debe haber instalado un Security Server en cada host que contenga las máquinas virtuales que se deseen proteger.

3.3. Paquete suplementario de HVI

El paquete HVI asegura el enlace entre el hipervisor y el Security Server en ese host. De esta manera, el Security Server es capaz de monitorizar la memoria en uso en el host en el que está instalado en función de las políticas de seguridad de GravityZone.

3.4. Agentes de seguridad

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone apropiados en los endpoints de la red.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone garantiza la protección de máquinas físicas y virtuales en Windows y Linux con Bitdefender Endpoint Security Tools, un agente de seguridad inteligente sensible al entorno que se adapta al tipo de endpoint. Bitdefender Endpoint Security Tools se puede implementar en cualquier máquina, ya sea virtual o física, y

proporciona un sistema de análisis flexible que constituye una solución ideal para entornos mixtos (físicos, virtuales y en la nube).

Además de la protección del sistema de archivos, Bitdefender Endpoint Security Tools también proporciona protección al servidor de correo para servidores de Microsoft Exchange.

Bitdefender Endpoint Security Tools utiliza una sola plantilla de política para las máquinas físicas y virtuales y una fuente de kit de instalación para cualquier entorno (físico o virtual) que ejecute Windows.

Capas de protección

Con Bitdefender Endpoint Security Tools hay disponibles las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- HyperDetect
- Cortafuego
- Control de Contenido
- Network Attack Defense
- Administración de parches
- Control de dispositivos
- Cifrado completo del disco duro
- Security for Exchange
- Sandbox Analyzer
- Control de aplicaciones

Roles de endpoint

- Usuario con Permisos
- Relay
- Servidor de almacenamiento en caché de parches
- Protección de Exchange

Usuario con Permisos

Los administradores del Control Center pueden conceder privilegios de Usuario avanzado a los usuarios de endpoints mediante los ajustes de políticas. El módulo de Usuario avanzado otorga privilegios de administración a nivel de usuario, lo que permite al usuario del endpoint acceder a los ajustes de seguridad y modificarlos

a través de una consola local. Control Center recibe una notificación cuando un endpoint está en modo de Usuario avanzado y el administrador de Control Center siempre puede sobrescribir los ajustes de seguridad locales.

Importante
Este módulo solo está disponible para sistemas operativos soportados de servidor y equipos de escritorio Windows. Para más información, consulte la Guía de instalación de GravityZone.

Relay

Los agentes de endpoint con rol de Bitdefender Endpoint Security Tools Relay actúan como servidores de comunicaciones, de actualizaciones y proxy para otros endpoints de la red. Los agentes de endpoint con rol de relay son especialmente necesarios en organizaciones con redes aisladas, donde todo el tráfico se canaliza a través de un único punto de acceso.

En las empresas con grandes redes distribuidas, los agentes de relay ayudan a reducir el uso de ancho de banda, al evitar que los endpoints protegidos y los servidores de seguridad se conecten directamente al appliance de GravityZone.

Una vez que se instala un agente Bitdefender Endpoint Security Tools Relay en la red, se pueden configurar otros endpoints mediante política para comunicarse con Control Center a través del agente de relay.

Los agentes Bitdefender Endpoint Security Tools Relay sirven para lo siguiente:

- Detección de todos los endpoints desprotegidos de la red.
- Implementación del agente de endpoint dentro de la red local.
- Actualización de los endpoints protegidos de la red.
- Garantía de la comunicación entre Control Center y los endpoints conectados.
- Funcionamiento como servidor proxy para endpoints protegidos.
- Optimización del tráfico de red durante las actualizaciones, implementaciones, análisis y otras tareas que consumen recursos.

Servidor de almacenamiento en caché de parches

Los endpoints con rol de relay también pueden actuar como servidor de almacenamiento en caché de parches. Con este rol habilitado, los relays sirven para almacenar parches de software descargados de los sitios web del proveedor y distribuirlos a los endpoints objetivo de su red. Cuando un endpoint conectado tiene software al que le falten parches, los obtiene del servidor y no del sitio web

del proveedor, lo que optimiza el tráfico generado y la carga del ancho de banda de la red.

Importante
Este rol adicional está disponible registrando un complemento de Administración de parches.

Protección de Exchange

Bitdefender Endpoint Security Tools con rol de Exchange se puede instalar en servidores Microsoft Exchange con el fin de proteger a los usuarios de Exchange contra las amenazas de correo.

Bitdefender Endpoint Security Tools con rol de Exchange protege tanto la máquina del servidor como la solución Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac es un agente de seguridad diseñado para proteger estaciones de trabajo y portátiles Macintosh basados en Intel. La tecnología de análisis disponible es la de **Análisis local**, con contenidos de seguridad almacenados localmente.

Capas de protección

Con Endpoint Security for Mac hay disponibles las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- Control de Contenido
- Control de dispositivos
- Cifrado completo del disco duro

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client extiende fácilmente las políticas de seguridad a cualquier número de dispositivos iOS y Android, protegiéndolos frente a usos no autorizados, riskware y pérdidas de datos confidenciales. Las características de seguridad incluyen el bloqueo de pantalla, control de autenticación, localización del dispositivo, detección de dispositivos rooteados o con jailbreak y perfiles de seguridad. En dispositivos Android el nivel de seguridad se mejora con el análisis en tiempo real y el cifrado de medios extraíbles.

GravityZone Mobile Client se distribuye exclusivamente en la App Store de Apple y en Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools es un agente ligero para entornos virtualizados VMware integrados con vShield Endpoint. El agente de seguridad se instala en máquinas virtuales protegidas por Security Server, lo que le permite aprovechar la funcionalidad adicional que proporciona:

- Le permite ejecutar tareas de análisis de procesos y memoria en la máquina.
- Informa al usuario sobre las infecciones detectadas y las acciones aplicadas sobre ellas.
- Añade más opciones para las exclusiones de análisis antimalware.

3.5. Arquitectura de Sandbox Analyzer

Bitdefender Sandbox Analyzer proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender.

Sandbox Analyzer está disponible en dos variantes:

- Sandbox Analyzer en la nube, alojado por Bitdefender.
- Sandbox Analyzer On-Premises, disponible como appliance virtual que se puede implementar localmente.

Sandbox Analyzer en la nube

Sandbox Analyzer en la nube contiene los siguientes componentes:

- **Portal de Sandbox Analyzer**: Un servidor de comunicaciones alojado que se utiliza para gestionar las solicitudes entre los endpoints y el cluster de Sandbox Analyzer de Bitdefender.
- **Cluster de Sandbox Analyzer**: La infraestructura alojada del espacio aislado donde se realiza el análisis de comportamiento de la muestra. En este nivel, los archivos enviados se detonan en máquinas virtuales con Windows 7.

GravityZone Control Center actúa como consola de administración y generación de informes, donde se configuran las políticas de seguridad y se visualizan los informes de análisis y las notificaciones.

Bitdefender Endpoint Security Tools, el agente de seguridad instalado en los endpoints, actúa como sensor de alimentación de Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises se proporciona como appliance virtual Linux Ubuntu, incrustado en una imagen de máquina virtual, fácil de instalar y configurar mediante una interfaz de línea de comandos (CLI). Sandbox Analyzer On-Premises está disponible en formato OVA, implementable en VMware ESXi.

Una instancia de Sandbox Analyzer On-Premises contiene los siguientes componentes:

- **Administrador de espacio aislado**. Este componente es el orquestador del espacio aislado. Sandbox Manager se conecta al hipervisor ESXi mediante API y utiliza sus recursos de hardware para crear y hacer funcionar el entorno de análisis de malware.
- **Máquinas virtuales de detonación**. Este componente consta de máquinas virtuales que Sandbox Analyzer utiliza para ejecutar archivos y analizar su comportamiento. Las máquinas virtuales de detonación pueden ejecutar sistemas operativos Windows 7 y Windows 10 de 64 bits.

GravityZone Control Center actúa como consola de administración y generación de informes, donde se configuran las políticas de seguridad y se visualizan los informes de análisis y las notificaciones.

Sandbox Analyzer On-Premises controla los siguientes sensores de alimentación:

- **Sensor de endpoints**. Bitdefender Endpoint Security Tools para Windows actúa como sensor de alimentación instalado en los endpoints. El agente de Bitdefender utiliza algoritmos avanzados de aprendizaje automático y de redes neuronales para determinar los contenidos sospechosos y enviarlos a Sandbox Analyzer, incluyendo los objetos de la cuarentena centralizada.
- **Sensor de red**. Network Security Virtual Appliance (NSVA) es un appliance virtual implementable en el mismo entorno ESXi virtualizado que la instancia de Sandbox Analyzer. El sensor de red extrae contenidos de los flujos de red y lo envían a Sandbox Analyzer.
- **Sensor ICAP**. Bitdefender Security Server, implementado en dispositivos de almacenamiento conectado a la red (NAS) con el protocolo ICAP, admite el envío de contenidos a Sandbox Analyzer.

Además de estos sensores, Sandbox Analyzer On-Premises admite el envío manual y a través de API. Para más información, consulte el capítulo **Uso de Sandbox Analyzer** de la Guía del administrador de GravityZone.

4. INICIANDO

Las soluciones GravityZone 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.

4.1. 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 o superior, Mozilla Firefox 14 o superior, Google Chrome 15 o superior, Safari 5 o superior, Microsoft Edge 20 o superior, Opera 16 o superior
- Resolución de pantalla recomendada: 1280 x 800 o superior

Aviso
Control Center no funcionará o se mostrará correctamente en Internet Explorer 9+ con la Vista de compatibilidad habilitada, que equivaldría a utilizar una versión de navegador no soportada.

Para conectarse a Control Center:

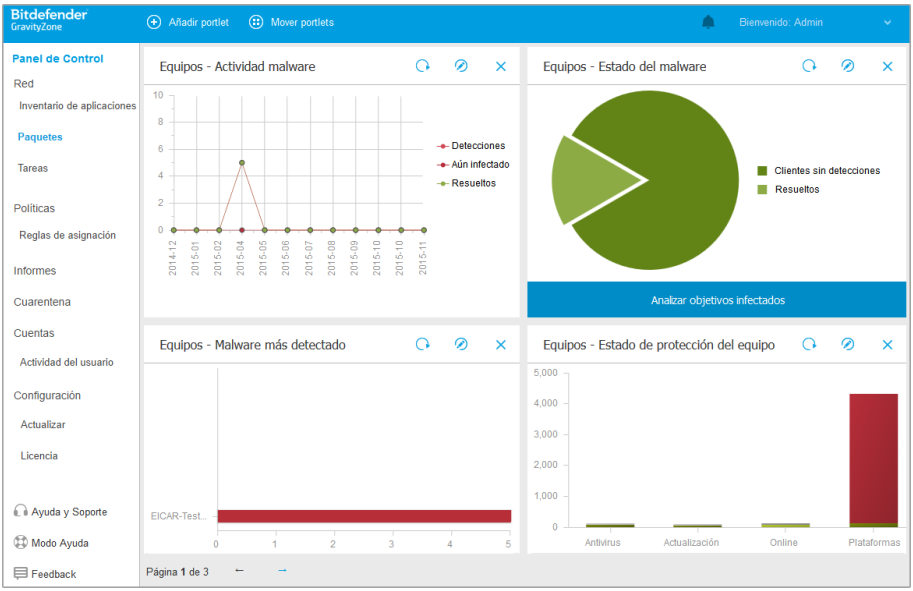
1. En la barra de dirección de su navegador Web, escriba la dirección IP o el nombre del host DNS del appliance Control Center (usando el prefijo `https://`).
2. Escriba su nombre de usuario y contraseña.
3. Introduzca el código de seis dígitos de Google Authenticator, Microsoft Authenticator o cualquier otro autenticador TOTP (Time-Based One-Time Password Algorithm) en dos fases compatible con el estándar RFC6238. Para obtener más información, consulte “Gestionar su cuenta” (p. 26).
4. Haga clic en **Inicio de sesión**.

En el primer inicio de sesión, debe aceptar las condiciones del servicio de Bitdefender. Haga clic en **Continuar** para empezar a usar GravityZone.

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.

4.2. Control Center en resumen

Control Center está organizada para permitir el acceso fácil a todas las funciones. Utilice la barra de menús de la derecha para navegar por la consola. Las características disponibles dependen del tipo de usuario que accede a la consola.



el Panel de control

4.2.1. 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.

Utilice el botón **Ver Menú** de la esquina superior izquierda para contraer a la vista de iconos, ocultar o expandir las opciones del menú. Haga clic en el botón para pasar secuencialmente por las opciones o haga doble clic para omitir.

Dependiendo de sus circunstancias, podrá acceder a las siguientes opciones de menú:

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.

En este menú también puede encontrar la página **Actividad del usuario**, que permite acceder al registro de actividad del usuario.

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

Configuración
Configure los ajustes de Control Center, como por ejemplo el servidor de correo, la integración con Active Directory o los entornos de virtualización, los certificados de seguridad y los ajustes del inventario de red, incluyendo las reglas programadas para la eliminación automática de máquinas virtuales sin uso.

Nota
Este menú solo está disponible para usuarios con privilegios de **Administrar solución**.

Al hacer clic en su nombre en la esquina superior derecha de la consola, dispone de las siguientes opciones:

- **Mi cuenta**. Haga clic en esta opción para gestionar sus detalles de la cuenta y las preferencias.

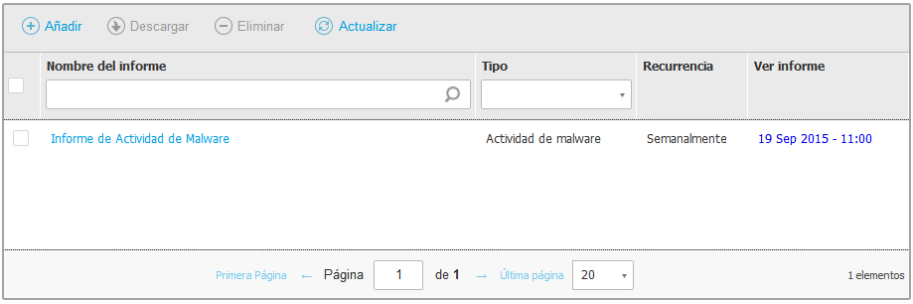
- **Administrador de Credenciales**. Haga clic en esta opción para añadir y administrar las credenciales de autenticación necesarias para tareas de instalación remotas.
- **Ayuda y soporte**. Haga clic en esta opción para obtener ayuda e información de soporte.
- **Feedback**. Haga clic en esta opción para mostrar un formulario que le permitirá escribir y enviar sus comentarios acerca de su experiencia con GravityZone.
- **Finalizar Sesión**. Haga clic en esta opción para cerrar la sesión de su cuenta.

Además, en la esquina superior derecha de la consola puede encontrar lo siguiente:

- El icono **Modo de ayuda**, que proporciona textos explicativos cuando sitúa el ratón sobre los elementos de Control Center. Puede hallar información útil referente a las características de Control Center.
- El icono **Notificaciones**, que brinda fácil acceso a los mensajes de notificación y también a la página **Notificaciones**.

4.2.2. Datos de tablas

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



La página Informes

Navegar por las páginas

Las tablas con más de 20 entradas se distribuyen en varias páginas. Por defecto, solo se muestran 20 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

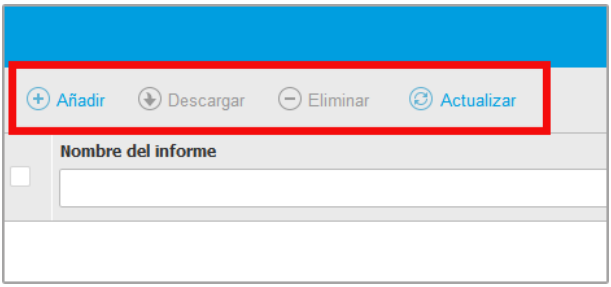
Para asegurarse de que la consola muestra la información más reciente, haga clic en el botón **Actualizar** de la parte superior de la tabla.

Esto puede ser necesario cuando dedique más tiempo a la página.

4.2.3. 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. Las barras de herramientas consisten en un conjunto de iconos que normalmente se colocan en la parte superior de la tabla. Por ejemplo, la barra de herramientas de acción en la sección **Informes** le permite realizar las siguientes operaciones:

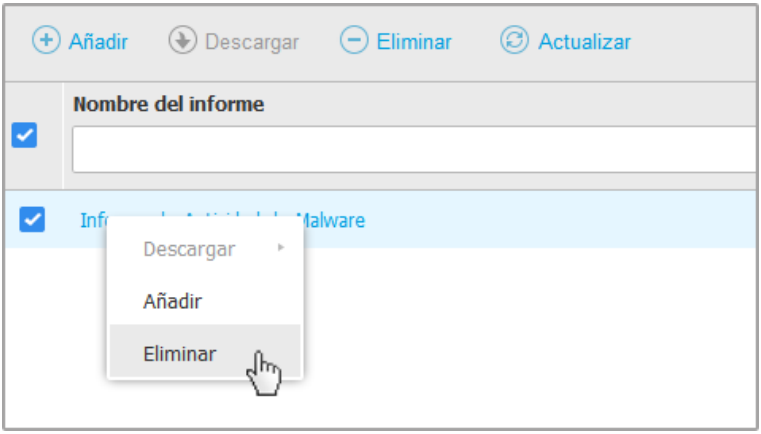
- Crear un nuevo informe.
- Descargar un informe programado.
- Eliminar un informe programado.



La página de Informes - Barra de herramientas de acción

4.2.4. 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 de Control Center que esté utilizando y seleccione el comando que precise de la lista disponible.



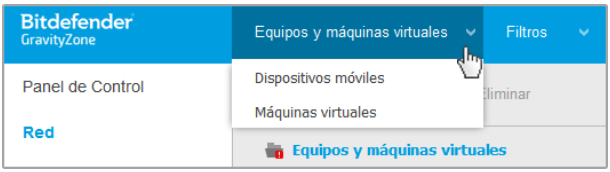
La página de Informes - Menú contextual

4.2.5. Selector de vistas

Si trabaja con diferentes tipos de endpoints, puede tenerlos organizados por tipo en la página **Red** en diversas vistas de red:

- **Equipos y máquinas virtuales**: muestra los grupos de Active Directory y equipos, y también estaciones de trabajo físicas y virtuales fuera de Active Directory detectadas en la red.
- **Máquinas virtuales**: muestra la infraestructura del entorno virtual integrado con Control Center y todas las máquinas virtuales que contiene.
- **Dispositivos móviles**: muestra los usuarios y los dispositivos móviles que se les asignen.

Para seleccionar la vista de red que desee, haga clic en el menú de vistas en la esquina superior derecha de la página.



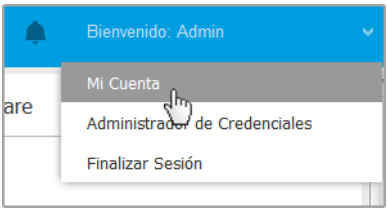
El selector de vistas

Nota
Solamente verá los endpoints para los que tiene permisos de visualización, los cuales le son otorgados por el administrador que añadió su usuario a Control Center.

4.3. Gestionar su cuenta

Para consultar o cambiar sus detalles de cuenta y configuración:

1. Haga clic en 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**. Si usa una cuenta de usuario de Active Directory, no puede cambiar los detalles de la cuenta.
   - **Usuario.** El nombre de usuario es el identificador único de una cuenta de usuario y no puede modificarse.
   - **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.
   - 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 la zona horaria de su cuenta en el menú. 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. En **Seguridad de inicio de sesión**, configure la autenticación en dos fases y compruebe el estado de las políticas disponibles para proteger su cuenta de GravityZone. Las políticas establecidas para toda la empresa son de solo lectura.

   Para activar la autenticación en dos fases:

   a. **Autenticación en dos fases.** La autenticación en dos fases aporta una capa adicional de seguridad a su cuenta de GravityZone, ya que requiere un código de autenticación además de sus credenciales de Control Center.

      Al iniciar sesión por primera vez en su cuenta de GravityZone, se le anunciará que debe descargar e instalar la app Google Authenticator, Microsoft Authenticator o cualquier otro autenticador TOTP (Time-Based One-Time Password Algorithm) en dos fases compatible con el estándar RFC 6238 en un dispositivo móvil, vincularlo a su cuenta de GravityZone y, luego, usarlo para cada inicio de sesión en Control Center. Google Authenticator genera un código de seis dígitos cada treinta segundos. Para finalizar el inicio de sesión en Control Center, después de introducir la contraseña deberá proporcionar el código de seis dígitos de Google Authenticator.

Nota
Puede omitir este proceso hasta tres veces, después de lo cual no podrá iniciar sesión sin la autenticación en dos fases.

Para activar la autenticación en dos fases:

i. Haga clic en el botón **Habilitar** bajo el mensaje de la **autenticación en dos fases**.

ii. En el cuadro de diálogo, haga clic en el enlace apropiado para descargar e instalar Google Authenticator en su dispositivo móvil.

iii. En su dispositivo móvil, abra Google Authenticator.

iv. En la pantalla **Añadir una cuenta**, escanee el código QR para vincular la app con su cuenta de GravityZone.

También puede introducir la clave secreta manualmente.

Esta acción solo se requiere una vez para activar esta característica en GravityZone.

Importante
Asegúrese de copiar y guardar la clave secreta en un lugar seguro. Haga clic en **Imprimir una copia de seguridad** para crear un archivo PDF con el código QR y la clave secreta. Si pierde o sustituye el dispositivo móvil utilizado para activar la autenticación en dos fases, deberá instalar Google Authenticator en el nuevo dispositivo y proporcionar la clave secreta para vincularlo con su cuenta de GravityZone.

v. Introduzca el código de seis dígitos en el campo **Código de Google Authenticator**.

vi. Haga clic en **Activar** para finalizar la activación de la característica.

Nota
El administrador de su empresa puede hacer que la autenticación en dos fases sea obligatoria para todas las cuentas de GravityZone. En tal caso, se le solicitará que configure su autenticación en dos fases al iniciar sesión. Al mismo tiempo, no podrá desactivar la autenticación en dos fases para su cuenta mientras el administrador de su empresa imponga esta medida.
Tenga en cuenta que, si la autenticación en dos fases actualmente configurada se desactiva para su cuenta, esta clave secreta ya no será válida.

b. **Política de caducidad de contraseñas.** Los cambios periódicos de su contraseña brindan una capa adicional de protección contra el uso no autorizado de contraseñas o limitan la duración de dicho uso no autorizado. Cuando se habilita, GravityZone le requiere que cambie su contraseña cada noventa días como muy tarde.

c. **Política de bloqueo de cuentas.** Esta política impide el acceso a su cuenta después de cinco intentos fallidos de inicio de sesión consecutivos. Esta medida se adopta para protegerse contra ataques de fuerza bruta.

   Para desbloquear su cuenta, debe restablecer la contraseña desde la página de inicio de sesión o ponerse en contacto con otro administrador de GravityZone.

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

Nota
No puede eliminar su propia cuenta.

4.4. Cambiar la Contraseña de Inicio de Sesión

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

A menos que utilice credenciales de Active Directory para acceder a Control Center, se recomienda hacer lo siguiente:

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

Para cambiar la contraseña de inicio de sesión:

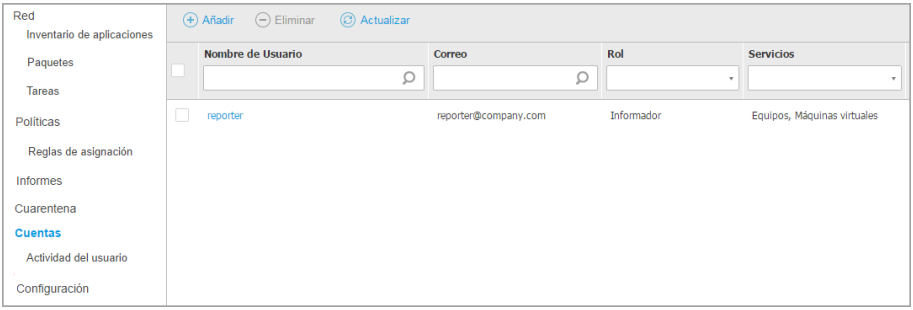
1. Haga clic en su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.
2. En **Detalles de cuenta**, haga clic en **Cambiar contraseña**.
3. Escriba su contraseña actual y la nueva contraseña en los campos correspondientes.
4. Haga clic en **Guardar** para aplicar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

5. CUENTAS DE USUARIO

Puede crear la primera cuenta de usuario de GravityZone durante la configuración inicial de Control Center, tras implementar el appliance GravityZone. La cuenta de usuario de Control Center inicial tiene rol de administrador de empresa, con privilegios totales sobre la configuración de Control Center y la administración de red. Desde esta cuenta puede crear todas las demás cuentas de usuario necesarias para la administración de la red de su empresa.

Esto es lo que necesita saber sobre las cuentas de usuario de GravityZone:

- Para permitir que otros empleados de la empresa accedan a Control Center, puede crear cuentas de usuario individualmente o habilitar el acceso dinámico para múltiples cuentas mediante integraciones de Active Directory o reglas de acceso. 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 GravityZone o a partes concretas de la red a la que pertenezca.
- Solo puede administrar cuentas con privilegios iguales o menores que los de su propia cuenta.



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 (administrador de empresa/administrador de red/analista de seguridad/personalizado).
- Los servicios de seguridad GravityZone que el usuario puede administrar (equipos, máquinas virtuales, dispositivos móviles).
- El estado de la autenticación en dos fases, que permite comprobar rápidamente si el usuario la ha activado.
- El estado de la regla de acceso indica una cuenta de usuario creada a través de una regla de permisos de acceso. Las cuentas de usuario creadas manualmente mostrarán **N/A**.

5.1. 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** - Normalmente, se crea una cuenta de usuario exclusiva con rol de Administrador de empresa para cada empresa, con acceso completo a todas las funciones de administración de las soluciones GravityZone. Un administrador de empresa configura los ajustes de Control Center, administra las claves de licencia de los servicios de seguridad y administra cuentas de usuario al tiempo que tiene privilegios administrativos sobre los ajustes de seguridad de la red de la empresa. Los administradores de empresa pueden compartir o delegar sus responsabilidades operativas en cuentas de usuario de analistas de seguridad 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 agentes de seguridad en la empresa o sobre un grupo determinado de endpoints, incluyendo la administración de usuarios. Los

administradores de la red son los responsables de administrar activamente los ajustes de seguridad de la red.

3. **Analista de seguridad**: Las cuentas de analistas de seguridad son cuentas de solo lectura. Únicamente permiten el acceso a informes, registros y datos relacionados con la seguridad. Dichas cuentas pueden distribuirse entre el personal con responsabilidades de monitorización de la seguridad u otros empleados que deban estar informados sobre el estado de esta.
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. 32).

Rol de cuenta	Cuentas hijo permitidas	Privilegios de usuario
Administrador de empresa	Administradores de empresa, Administradores de red, Informes	Administrar solución Administrar empresa Administrar usuarios Administrar redes Ver y analizar datos
Administrador de red	Administradores de red, analistas de seguridad	Administrar usuarios Administrar redes Ver y analizar datos
Analista de seguridad	-	Ver y analizar datos

5.2. Privilegios de usuario

Puede asignar los siguientes privilegios de usuario a las cuentas de usuario de GravityZone:

- **Administrar solución**. Permite configurar los ajustes de Control Center (ajustes de proxy y servidor de correo, integración con Active Directory y plataformas de virtualización, certificados de seguridad y actualizaciones de GravityZone). Este privilegio es privativo de las cuentas de administrador de empresa.

- **Administrar usuarios**. Cree, edite o elimine cuentas de usuario.
- **Administrar empresa**. Los usuarios pueden administrar su propia clave de licencia de GravityZone 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.
- **Ver y analizar datos**. Consulte registros y eventos relacionados con la seguridad, además de administrar informes y el panel de control.

5.3. Gestión de cuentas de usuario

Para crear, editar, eliminar y configurar cuentas de usuario, emplee los siguientes métodos:

- Administrar cuentas de usuario individualmente. Utilice este método para añadir cuentas de usuario locales o cuentas de Active Directory. Para establecer una integración de Active Directory, consulte la Guía de instalación de GravityZone.

  Antes de crear una cuenta de usuario, asegúrese de tener a mano la dirección de correo electrónico necesaria. El usuario recibe la información de inicio de sesión de GravityZone en la dirección de correo electrónico suministrada.
- Administrar múltiples cuentas de usuario. Utilice este método para habilitar el acceso dinámico mediante reglas de permisos de acceso. Este método requiere una integración de dominio de Active Directory. Para más información sobre la integración de Active Directory, consulte la Guía de instalación de GravityZone.

5.3.1. Administrar cuentas de usuario individualmente

En Control Center puede crear, editar y eliminar cuentas de usuario individualmente.

Dependencias

- Las cuentas creadas localmente pueden eliminar cuentas creadas a través de la integración de Active Directory, independientemente de su rol.
- Las cuentas creadas localmente no pueden eliminar una cuenta similar, independientemente de su rol.

Crear cuentas de usuario individualmente

Para añadir una cuenta de usuario en Control Center:

1. Diríjase a la página **Cuentas**.
2. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Aparece una ventana de configuración.
3. En la sección **Detalles**, configure lo siguiente:
   - Para las cuentas de usuario de Active Directory configure la siguiente información:

     Nombre de usuario para las cuentas de usuario de Active Directory (AD). Elija una cuenta de usuario de la lista desplegable y vaya al paso 4.

     Solo puede añadir cuentas de usuario de AD si la integración está configurada. Al añadir una cuenta de usuario de AD, los datos del usuario se importan desde su dominio asociado. El usuario inicia sesión en Control Center usando el nombre de usuario y contraseña de AD.

     Nota

     – Para asegurarse de que los últimos cambios de Active Directory se hayan importado a Control Center, haga clic en el botón **Sincronizar**.

     – Los usuarios con privilegios de **Administración de la solución** pueden configurar el intervalo de sincronización de Active Directory mediante las opciones disponibles en la pestaña **Configuración > Active Directory**. Para obtener más información, consulte los capítulos **Instalación de la protección > Instalación** y **Configuración de GravityZone > Configuración de los ajustes de Control Center Center** de la Guía de instalación de GravityZone.

   - Para las cuentas locales, configure la siguiente información:
     – **Nombre de usuario** de la cuenta local. Inhabilite **Importar de Active Directory** e introduzca un nombre de usuario.

     – **E-mail**. Escriba la dirección de correo electrónico del usuario.

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

       GravityZone utiliza esta dirección de correo electrónico para enviar notificaciones.

- **Nombre completo**. Introduzca el nombre completo del usuario.
- **Contraseña**. Introduzca una contraseña que el usuario pueda emplear para iniciar sesión.

  La contraseña debe contener al menos un carácter en mayúsculas, uno en minúsculas, y un número o un carácter especial.
- **Confirme la contraseña**. Confirme la contraseña para validar.

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. 31).
   - **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. 32).
   - **Seleccionar objetivos**. Seleccione los grupos de red a los que tendrá acceso el usuario para todos los servicios de seguridad disponibles. Puede restringir el acceso del usuario a determinado servicio de seguridad de GravityZone o a áreas específicas de la red.

     Nota
     Las opciones de selección de objetivos no se mostrarán para los usuarios con privilegios de Administración de la solución, que, por defecto, tienen privilegios sobre la totalidad de la red y los servicios de seguridad.

     Importante
     Siempre que efectúe cambios a su estructura de red o cuando establezca una nueva integración con otro vCenter Server o sistema XenServer, recuerde revisar y actualizar los privilegios de acceso para los usuarios existentes.

5. Haga clic en **Guardar** para añadir el usuario. La nueva cuenta se mostrará en la lista de cuentas de usuario.

Control Center envía automáticamente un e-mail al usuario con los detalles de inicio de sesión, siempre y cuando se hayan configurado correctamente los ajustes del servidor de correo. Para obtener más información sobre la configuración del servidor de correo electrónico, consulte el capítulo **Instalación de la protección > Instalación y configuración de GravityZone > Configuración de los ajustes de Control Center Center** de la Guía de instalación de GravityZone.

Editar cuentas de usuario individualmente

Para añadir una cuenta de usuario en Control Center

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 de usuario 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 privilegios iguales o menores que los de su propia cuenta.

Eliminar cuentas de usuario individualmente

Para eliminar una cuenta de usuario en Control Center

1. Iniciar sesión en Control Center.
2. Diríjase a la página **Cuentas**.
3. Seleccione la cuenta de usuario en la lista.
4. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla.
   Haga clic en **Sí** para confirmar.

5.3.2. Administrar múltiples cuentas de usuario

Cree reglas de acceso para otorgar acceso a GravityZone Control Center a los usuarios de Active Directory en función de los grupos de seguridad.

Requisitos

Para administrar varias cuentas de usuario, necesita una integración de dominio de Active Directory con GravityZone. Para integrar y sincronizar un dominio de Active Directory, consulte el capítulo de **Active Directory** de la Guía de instalación de GravityZone.

Dependencias

Las reglas de permisos de acceso van vinculadas a los grupos de seguridad de Active Directory (AD) y a las cuentas de usuario asociadas. Cualquier cambio realizado en los dominios de Active Directory puede afectar a las reglas de permisos de acceso asociadas. Esto es lo que necesita saber sobre la relación entre reglas, usuarios y dominios de Active Directory:

- Una regla de permiso de acceso añade una cuenta de usuario solo si el correo electrónico no está asociado aún con una cuenta existente.
- Para direcciones de correo electrónico duplicadas dentro de un grupo de seguridad, la regla de permiso de acceso crea una cuenta de usuario de GravityZone solo para la primera cuenta de usuario de Active Directory que inicie sesión en Control Center.

  Por ejemplo, un grupo de seguridad contiene una dirección de correo electrónico duplicada para diferentes usuarios y todos intentan iniciar sesión en Control Center con sus credenciales de Active Directory. Si se asocia una regla de permiso de acceso a este dominio concreto de Active Directory, creará una sola cuenta de usuario para el primer usuario que inició sesión en Control Center utilizando la dirección de correo electrónico duplicada.
- Las cuentas de usuario creadas mediante las reglas de permisos de acceso pasan a estar inactivas si se eliminan de su grupo de seguridad de AD asociado. Los mismos usuarios pueden activarse si están asociados a una nueva regla de acceso.
- Las reglas de acceso pasan a ser de solo lectura una vez que un dominio de Active Directory asociado deja de estar integrado con GravityZone. Los usuarios asociados con estas reglas pasan a estar inactivos.
- Las cuentas de usuario creadas mediante reglas de acceso no pueden eliminar usuarios creados localmente.
- Las cuentas de usuario creadas mediante reglas de acceso no pueden eliminar cuentas similares que tengan rol de administrador de empresa.

Crear múltiples cuentas de usuario

Para añadir múltiples cuentas de usuario, cree reglas de permisos de acceso. Las reglas de permisos de acceso van asociadas a los grupos de seguridad de Active Directory.

Para añadir una regla de permisos de acceso:

1. Acceda a **Configuración > Active Directory > Permisos de acceso**.
2. Si tiene varias integraciones, seleccione un dominio en el lado superior izquierdo de la tabla.
3. Haga clic en ⊕ **Añadir** a la izquierda de la tabla.
4. Configure los siguientes ajustes de permisos de acceso:
   - **Prioridad**. Las reglas se procesan por orden de prioridad. Cuanto menor sea el número, mayor será la prioridad.
   - **Nombre**. El nombre de la regla de acceso.
   - **Dominio**. El dominio desde el que se añaden grupos de seguridad.
   - **Grupos de seguridad**. Los grupos de seguridad que contienen sus futuros usuarios de GravityZone. Puede usar el cuadro de autocompletar. Los grupos de seguridad añadidos en esta lista no pueden sufrir cambios, adiciones o eliminaciones tras guardar la regla de acceso.
   - **Zona horaria**. La zona horaria del usuario.
   - **Idioma**. El idioma de visualización de la consola.
   - **Rol**. Roles de usuario predefinidos. Para más información, consulte el capítulo **Cuentas de usuario** de la Guía del administrador de GravityZone.

     Nota
     Puede otorgar y revocar privilegios a otros usuarios con los mismos o menos privilegios que su cuenta.

   - **Derechos**. Cada rol de usuario predefinido tiene una determinada configuración de privilegios. Para más información, consulte el capítulo **Cuentas de usuario** de la Guía del administrador de GravityZone.
   - **Seleccionar objetivos** Seleccione los grupos de red a los que tendrá acceso el usuario para todos los servicios de seguridad disponibles. Puede restringir el acceso del usuario a determinado servicio de seguridad de GravityZone o a áreas específicas de la red.

Nota
Las opciones de selección de objetivos no se mostrarán para los usuarios con privilegios de Administración de la solución, que, por defecto, tienen privilegios sobre la totalidad de la red y los servicios de seguridad.

5. Haga clic en **Guardar**.

   La regla de acceso se guarda si los usuarios no se ven afectados. De lo contrario, se le pedirá que especifique exclusiones de usuarios. Por ejemplo, cuando añada una regla con una prioridad más alta, los usuarios afectados asociados a otra regla permanecerán vinculados a la regla anterior.
6. En caso necesario, seleccione los usuarios que desea excluir. Para más información, consulte Exclusiones de cuentas de usuario.
7. Haga clic en **Confirmar**. La regla se muestra en la página **Permisos de acceso**.

Los usuarios dentro de los grupos de seguridad especificados por las reglas de acceso pueden acceder ahora a GravityZone Control Center con sus credenciales de dominio. Control Center crea automáticamente nuevas cuentas de usuario cuando inicien sesión por primera vez, utilizando su dirección de correo electrónico y contraseña de Active Directory.

Las cuentas de usuario creadas a través de una regla de acceso muestran el nombre de la regla de acceso en la página **Cuentas**, en la columna **Regla de acceso**.

Editar múltiples cuentas de usuario

Para editar una regla de permisos de acceso:

1. Acceda a **Configuración > Active Directory > Permisos de acceso**.
2. Seleccione el nombre de su regla de acceso para abrir la ventana de configuración.
3. Edite los ajustes del permiso de acceso. Para más información, consulte Añadir permisos de acceso.
4. Haga clic en **Guardar**. La regla se guarda si los usuarios no se ven afectados. De lo contrario, se le pedirá que especifique exclusiones de cuentas de usuario. Por ejemplo, si actualiza la prioridad de una regla, los usuarios afectados pueden cambiar a otra regla diferente.
5. En caso necesario, seleccione los usuarios que desea excluir. Para más información, consulte Exclusiones de cuentas de usuario.
6. Haga clic en **Confirmar**.

Nota
Puede desvincular las cuentas de usuario creadas mediante una regla de acceso modificando sus privilegios en Control Center. La cuenta de usuario no se puede volver a vincular a la regla de acceso.

Eliminar múltiples cuentas de usuario

Para eliminar una regla de acceso:

1. Acceda a **Configuración > Active Directory > Permisos de acceso**.
2. Seleccione la regla de acceso que desea eliminar y haga clic en el botón ⊖ **Eliminar**. Una ventana le solicita que confirme su acción. Si afecta a algún usuario, se le pedirá que especifique exclusiones de cuentas de usuario. Por ejemplo, es posible que desee especificar exclusiones para los usuarios afectados por la eliminación de la regla.
3. En caso necesario, seleccione los usuarios que desea excluir. Para más información, consulte Exclusiones de usuarios.
4. Haga clic en **Confirmar**.

Al eliminar una regla, se revocará el acceso a las cuentas de usuario asociadas. Se eliminarán todos los usuarios creados a través de ella, a menos que haya otras reglas que les otorguen acceso.

Exclusiones de cuentas de usuario

Al añadir, editar o eliminar reglas de permisos de acceso que afectan a usuarios, es posible que desee especificar exclusiones de cuentas de usuario. También puede ver las razones y efectos sobre los usuarios afectados.

Especifique las exclusiones de usuarios de la siguiente manera:

1. Seleccione los usuarios que desea excluir. O marque la casilla de verificación en la parte superior de la tabla para añadir a todos los usuarios a la lista.
2. Haga clic en **X** dentro de un cuadro de nombre de usuario para eliminarlo de la lista.

5.4. 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.

5.5. Administración de la autenticación en dos fases

Al hacer clic en una cuenta de usuario, podrá ver su estado de autenticación en dos fases (activado o desactivado) en la sección **Autenticación en dos fases**. Puede llevar a cabo las siguientes acciones:

- **Restablecer o desactivar la autenticación en dos fases del usuario**. Si un usuario con la autenticación en dos fases activada ha cambiado o borrado el dispositivo móvil y perdido la clave secreta:
  1. Introduzca su contraseña de GravityZone en el campo correspondiente.
  2. Haga clic en **Restablecer** (cuando se aplica la autenticación en dos fases) o en **Desactivar** (cuando no se aplica).
  3. Un mensaje de confirmación le informará de que se ha restablecido o desactivado la autenticación en dos fases para el usuario actual.

     Tras restablecer la autenticación en dos fases cuando se impone esta característica, al iniciar sesión, una ventana de configuración solicitará al usuario que vuelva a configurar la autenticación en dos fases con una nueva clave secreta.
- Si el usuario tiene desactivada la autenticación en dos fases y desea activarla, deberá solicitar al usuario que active esta característica desde los ajustes de su cuenta.

> **Nota**
> Si tiene una cuenta de administrador de empresa, puede obligar a la activación de la autenticación en dos fases en todas las cuentas de GravityZone. Para

obtener más información, consulte el capítulo **Instalación de la protección > Instalación y configuración de GravityZone > Configuración de los ajustes de Control Center** de la Guía de instalación.

Importante
La aplicación de autenticación escogida (Google Authenticator, Microsoft Authenticator o cualquier otro autenticador TOTP (Time-Based One-Time Password Algorithm) en dos fases compatible con el estándar RFC 6238) combina la clave secreta con la fecha y hora actuales del dispositivo móvil para generar el código de seis dígitos. Tenga en cuenta que los datos de fecha y hora en el dispositivo móvil y en el appliance GravityZone tienen que coincidir para que el código de seis dígitos sea válido. Para evitar cualquier problema de sincronización de fecha y hora, recomendamos activar la configuración automática de fecha y hora en el dispositivo móvil.

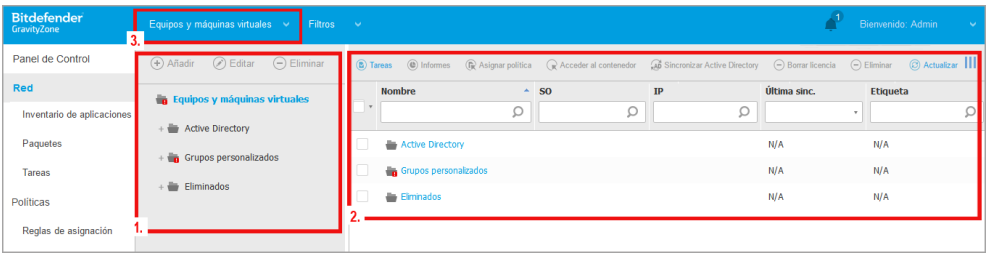
Otra forma para comprobar los cambios de la autenticación en dos fases de las cuentas de usuario es acceder a la página **Cuentas > Actividad del usuario** y filtrar los registros de actividades mediante los siguientes filtros:

- Área > Cuentas / Empresa
- Acción > Editado

Para obtener más información sobre la activación de la autenticación en dos fases, consulte"Gestionar su cuenta" (p. 26)

6. GESTIÓN DE ELEMENTOS DE RED

La página **Red** proporciona diversas opciones para explorar y administrar todos los tipos de objetos de red disponibles en Control Center (equipos, máquinas virtuales y dispositivos móviles). La sección **Red** consiste en una interfaz de dos paneles que muestra el estado en tiempo real de los objetos de red:



La página Red

1. El panel izquierdo muestra el árbol de red disponible. En función de la vista de red seleccionada, este panel muestra la infraestructura de red integrada con Control Center como Active Directory, vCenter Server o Xen Server.

   Al mismo tiempo, todos los equipos y máquinas virtuales detectadas en la red que no pertenezcan a ninguna infraestructura integrada se mostrarán en **Grupos personalizados**.

   Todos los endpoints eliminados se almacenan en la carpeta **Eliminados**. Para obtener más información, consulte "Eliminación de endpoints del inventario de red" (p. 214).

   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 panel izquierdo. 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.

Mueva el cursor del ratón sobre el icono para ver la información sobre herramientas. Haga clic en el nombre del objeto para mostrar una ventana con más detalles específicos.

Todos los tipos de objetos, como un equipo, una máquina virtual o una carpeta, están representados por un icono determinado. Al mismo tiempo, cada objeto de red puede tener un determinado estado en lo que respecta a su estado de administración, problemas de seguridad, conexión, etc. Para obtener más información sobre la descripción de cada icono de los objetos de red y sus estados disponibles, consulte "Tipos y estados de los objetos de red" (p. 525).

- Utilice la Barra de herramientas de acción de la parte superior de la tabla para llevar a cabo operaciones específicas para cada objeto de red (como ejecutar tareas, crear informes, asignar políticas y eliminarlas) y actualizar los datos de la tabla.

3. El selector de vistas de la parte superior de los paneles de red permite pasar entre los contenidos de los diversos inventario de red, según el tipo de endpoint con el que desee trabajar.
4. El menú **Filtros**, disponible en la parte superior de los paneles de red, le ayuda a mostrar fácilmente solo determinados objetos de red gracias a diversos criterios de filtrado. Las opciones del menú **Filtros** están relacionadas con la vista de red seleccionada actualmente.

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

Nota
Para más información sobre los paquetes de instalación, consulte la Guía de instalación de GravityZone.

Para obtener información detallada sobre los objetos de red, consulte:

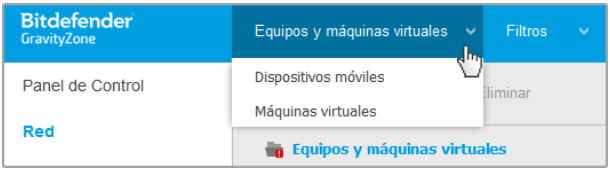
- "Trabajar con vistas de red" (p. 45)
- "Equipos" (p. 48)
- "Máquinas virtuales" (p. 107)
- "Dispositivos móviles" (p. 168)
- "Inventario de parches" (p. 201)
- "Ver y administrar tareas" (p. 210)
- "Eliminación de endpoints del inventario de red" (p. 214)
- "Configuración de los ajustes de red" (p. 215)
- "Configuración de los ajustes de Security Server" (p. 218)

- “Administrador de Credenciales” (p. 219)

6.1. Trabajar con vistas de red

Los distintos tipos de endpoints disponibles en Control Center se agrupan en la página **Red** por diferentes vistas de red. Cada vista de red muestra un tipo determinado de infraestructura de red, según el tipo de endpoint que desee administrar.

Para cambiar la vista de red, vaya a la zona superior izquierda de la página **Red** y haga clic en el selector de vistas:



El selector de vistas

Dispone de las siguientes vistas de red:

- Equipos y máquinas virtuales
- Máquinas virtuales
- Dispositivos móviles

6.1.1. Equipos y máquinas virtuales

Esta vista está pensada para equipos y máquinas virtuales integradas en Active Directory, y proporciona acciones específicas y opciones de filtrado para administrar los equipos de la red. Si se dispone de una integración de Active Directory, se carga el árbol de Active Directory junto con los endpoints correspondientes.

Mientras trabaja en la vista **Equipos y máquinas virtuales** puede sincronizar los contenidos de Control Center con su Active Directory en cualquier momento gracias al botón **Sincronizar con Active Directory** de la barra de herramientas de acción.

Al mismo tiempo, todos los equipos y máquinas virtuales que no están integradas en Active Directory se agrupan en grupos personalizados. Esta carpeta puede contener los siguientes tipos de endpoints:

- Equipos y máquinas virtuales disponibles en su red fuera de Active Directory.

- Máquinas virtuales de una infraestructura virtualizada disponible en su red.
- Servidores de seguridad ya instalados y configurados en un host de su red.

Nota
Cuando dispone de una infraestructura virtualizada, puede implementar y administrar servidores de seguridad desde la vista **Máquinas virtuales**. En caso contrario, los servidores de seguridad solo pueden instalarse y configurarse localmente en el host.

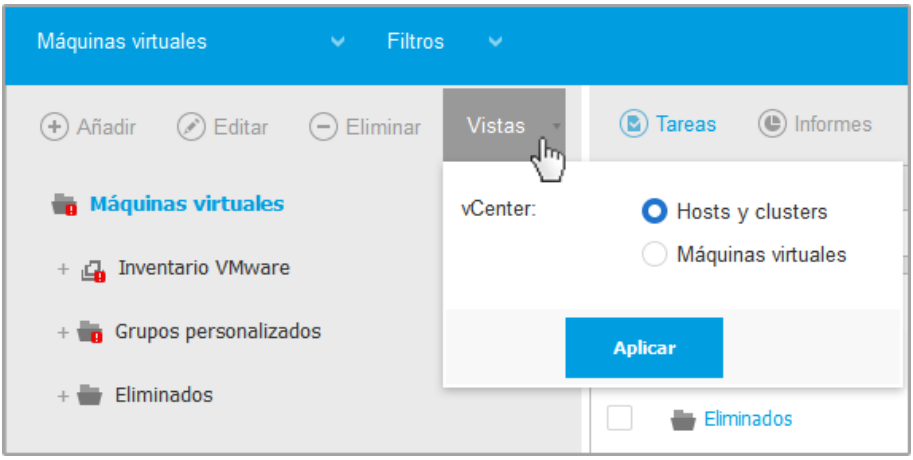
Importante
La asignación de políticas a máquinas virtuales desde la vista **Equipos y máquinas virtuales** puede restringirla el administrador de la solución GravityZone al configurar vCenter Server o un Xen Server en la página **Configuración > Proveedores de virtualización**. Para obtener más información, consulte el capítulo **Instalación de la protección > Instalación y configuración de GravityZone** de la Guía de instalación de GravityZone.

6.1.2. Máquinas virtuales

Esta vista ha sido diseñada específicamente para mostrar las integraciones de su infraestructura virtualizada. Las opciones de filtro disponibles en esta vista le permiten elegir criterios especiales para la visualización de las entidades del entorno virtual.

Puede ver sus inventarios virtuales de Citrix, VMware o Nutanix en el panel izquierdo.

En la parte superior del panel de la izquierda también puede hallar el menú **Vistas**, que le permite elegir el modo de visualización de los inventarios virtuales.



La página Red - Vistas de máquinas virtuales

Todas las máquinas virtuales en la red que no están integradas en una infraestructura virtual se muestran en **grupos personalizados**.

Para acceder a la infraestructura virtualizada integrada con Control Center, debe proporcionar sus credenciales de usuario para cada sistema vCenter Server disponible. Control Center usa sus credenciales para conectar con la infraestructura virtualizada, mostrando solamente los recursos a los que tiene acceso (según se define en el vCenter Server). Si no ha especificado sus credenciales de autenticación, necesitará introducirlas cuando intente examinar el inventario de cualquier vCenter Server. Una vez introducidas las credenciales, se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

6.1.3. Dispositivos móviles

Esta vista ha sido diseñada exclusivamente para ver y administrar los dispositivos móviles disponibles en su red, y proporciona acciones y opciones de filtrado específicas.

En esta vista concreta, puede mostrar las entidades de red por usuarios o por dispositivos.

El panel de red muestra la estructura de árbol de Active Directory, de estar disponible. En este caso, todos los usuarios de Active Directory aparecerán en su inventario de red, así como los dispositivos móviles que tengan asignados.

Nota
La información de los usuarios de Active Directory se carga automáticamente y no se puede cambiar.

Los grupos personalizados contienen todos los usuarios de dispositivos móviles que ha añadido manualmente a Control Center.

6.2. Equipos

Para consultar los equipos de su cuenta, diríjase a la página **Red** y seleccione **Equipos y máquinas virtuales** desde el selector de vistas.

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

Al principio, todos los equipos y máquinas virtuales que se detectan en su red se muestran como no administrados de manera que puede instalar la protección en ellos de forma remota.

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

1. Haga clic en el botón **Columnas** de la derecha de la barra de herramientas de acción.
2. Seleccione las columnas que desea ver.
3. Haga clic en el botón **Restablecer** para volver a la vista predeterminada de columnas.

Desde la página **Red** puede administrar los equipos de la siguiente manera:

- Comprobar el estado del equipo
- Consultar la información del equipo.
- Organizar equipos en grupos.
- Ordenar, filtrar y buscar.
- Administrar parches
- Ejecutar tareas.
- Crear informes rápidos
- Asignar políticas
- Sincronizar con Active Directory

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

6.2.1. Comprobación del estado del equipo

Los equipos están representados en la página de red mediante el icono correspondiente a su tipo y estado.

Consulte "Tipos y estados de los objetos de red" (p. 525) para ver una lista con todos los tipos de iconos y estados disponibles.

Para obtener información detallada sobre el estado, consulte:

- Estado de administración
- Estado de conexión
- Estado de seguridad

Estado de administración

Los equipos pueden tener los siguientes estados de administración:

- **Administrados** - equipos en los que se ha instalado el agente de seguridad.
- **Reinicio pendiente**: Endpoints que requieren un reinicio del sistema después de instalar o actualizar la protección de Bitdefender.
- **No administrados** - equipos detectados en los que no se ha instalado aún el agente de seguridad.
- **Eliminado** - equipos que ha eliminado de Control Center. Para más información, diríjase a "Eliminación de endpoints del inventario de red" (p. 214).

Estado de conexión

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 el agente de seguridad permanece 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 aparecen online incluso cuando están bloqueados o cuando el usuario ha finalizado la sesión.

- El agente de seguridad no tiene conexión con el Servidor de comunicaciones de GravityZone:
  - El equipo puede estar desconectado de la red.
  - Un router o un cortafuego de red pueden estar bloqueando la comunicación entre el agente de seguridad y el Servidor de comunicaciones de GravityZone.
  - El equipo se encuentra detrás de un servidor proxy y los ajustes del proxy no se han configurado correctamente en la política aplicada.

    Aviso
    En el caso de equipos detrás de un servidor proxy, los ajustes del proxy deben estar configurados correctamente en el paquete de instalación del agente de seguridad, pues de lo contrario el equipo no se comunicará con la consola de GravityZone y siempre aparecerá offline, aunque se aplique una política con los ajustes de proxy adecuados después de la instalación.

- Puede que el agente de seguridad no esté funcionando adecuadamente.

Para averiguar cuánto tiempo han estado inactivos los equipos:

1. Mostrar sólo los equipos administrados. Haga clic en el menú **Filtros** situado en la zona superior de la tabla, seleccione en la pestaña **Seguridad** todas las opciones "Administrados" que precise, elija **Todos los elementos recursivamente** en la pestaña **Profundidad** 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.

Nota
Se recomienda actualizar la tabla de red de vez en cuando para actualizar la información de los endpoints con los últimos cambios.

Estado de seguridad

El estado de seguridad se refiere únicamente a los equipos administrados. Los iconos de estado muestran un símbolo de advertencia que le permite identificar 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.
- Si la licencia ha caducado.
- El agente de seguridad está obsoleto.
- Los contenidos de seguridad no están actualizados.
- Se ha detectado malware.
- No se pudo establecer la conexión con Bitdefender Cloud Services debido a una de las siguientes razones:
  - El equipo tiene problemas de conexión a Internet.
  - Un cortafuego de red bloquea la conexión con Bitdefender Cloud Services.
  - El puerto 443, necesario para la comunicación con Bitdefender Cloud Services, está cerrado.

  En este caso, la protección antimalware se basa únicamente en los motores locales, mientras que el análisis en la nube está desconectado, lo que significa que el agente de seguridad no puede proporcionar protección completa en tiempo real.

Si observa un equipo con problemas de seguridad, haga clic en su nombre para mostrar la ventana **Información**. Puede identificar los problemas de seguridad mediante el icono **!** . Asegúrese de revisar la información de seguridad de todas las pestañas de la página de información. Muestre la información sobre herramientas del icono para conocer más detalles. Puede ser necesaria más investigación local.

Nota
Se recomienda actualizar la tabla de red de vez en cuando para actualizar la información de los endpoints con los últimos cambios.

6.2.2. Consulta de la información del equipo

Puede obtener información detallada sobre cada equipo en la página **Red** de la siguiente manera:

- Comprobación de la página **Red**
- Comprobación de la ventana **Información**

Comprobación de la página Red

Para conocer más detalles sobre un equipo, consulte la información disponible en la tabla del panel derecho de la página **Red**.

Puede añadir o eliminar columnas con información de endpoints haciendo clic en el botón **Columnas** de la esquina superior derecha del panel.

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.

   Todos los endpoints del grupo seleccionado se muestran en la tabla del panel derecho.
4. Puede identificar fácilmente el estado del equipo consultando el icono correspondiente. Para información detallada, diríjase a "Comprobación del estado del equipo" (p. 49).
5. Consulte la información mostrada en las columnas para cada equipo.

   Utilice la fila de encabezado para ir buscando endpoints concretos mientras escribe en función de los criterios disponibles:

   - **Nombre**: nombre del endpoint.
   - **FQDN**: Nombre de dominio completo que incluye el nombre del host y el del dominio.
   - **SO**: sistema operativo instalado en el endpoint.
   - **IP**: dirección IP del endpoint.
   - **Detectado por última vez**: fecha y hora en la que el endpoint fue visto conectado por última vez.

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

- **Etiqueta**: una cadena personalizada con información adicional sobre el endpoint. Puede añadir una etiqueta en la ventana **Información** del endpoint y luego usarla en las búsquedas.
- **Política**: la política aplicada al endpoint, con un enlace para ver o cambiar los ajustes de esta.

Comprobación de la ventana Información

En el panel derecho de la página **Red**, haga clic en el nombre del endpoint que le interese para mostrar la ventana **Información**. Esta ventana muestra solo los datos disponibles para el endpoint seleccionado, agrupados en varias pestañas.

A continuación encontrará la lista exhaustiva de información que puede hallar en la ventana **Información**, de acuerdo con el tipo de endpoint y su información de seguridad concreta.

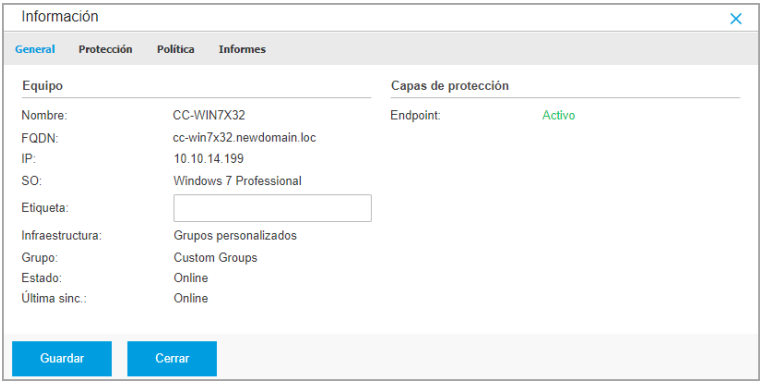
Pestaña General

- Información general del equipo, como nombre, información FQDN (nombre completo), dirección IP, sistema operativo, infraestructura, grupo padre y estado actual de la conexión.

  En esta sección puede asignar una etiqueta al endpoint. Podrá encontrar rápidamente endpoints con la misma etiqueta y adoptar acciones sobre ellos, independientemente de dónde se encuentren en la red. Para obtener más información sobre el filtrado de endpoints, consulte "Clasificación, filtrado y búsqueda de equipos" (p. 67).
- Información sobre las capas de protección, incluida la lista de tecnologías de seguridad adquiridas con su solución GravityZone y su estado de licencia, que puede ser:
  - **Disponible/Activo**: la clave de licencia de esta capa de protección está activa en el endpoint.
  - **Caducado**: la clave de licencia de esta capa de traducción ha caducado.
  - **Pendiente**: La clave de licencia no está confirmada aún.

Nota
Hay disponible información adicional sobre las capas de protección en la pestaña **Protección**.

- **Conexión del relay**: el nombre, IP y etiqueta del relay al que está conectado el endpoint, si es el caso.



Ventana de Información - pestaña General

Pestaña Protección

Esta pestaña contiene información sobre la protección aplicada en el endpoint referida a lo siguiente:

- Información del agente de seguridad como el nombre del producto, la versión, el estado de actualización y las ubicaciones de actualización, así como la configuración de los motores de análisis y las versiones de los contenidos de seguridad. Para la protección de Exchange, también está disponible la versión del motor antispam.
- Estado de seguridad para cada capa de protección. Este estado aparece a la derecha del nombre de la capa de protección:
  - **Seguro**, cuando no se ha informado de ningún problema de seguridad en los endpoints a los que se ha aplicado la capa de protección.
  - **Vulnerable**, cuando se ha informado de algún problema de seguridad en los endpoints a los que se ha aplicado la capa de protección. Para obtener más información, consulte “Estado de seguridad” (p. 51).

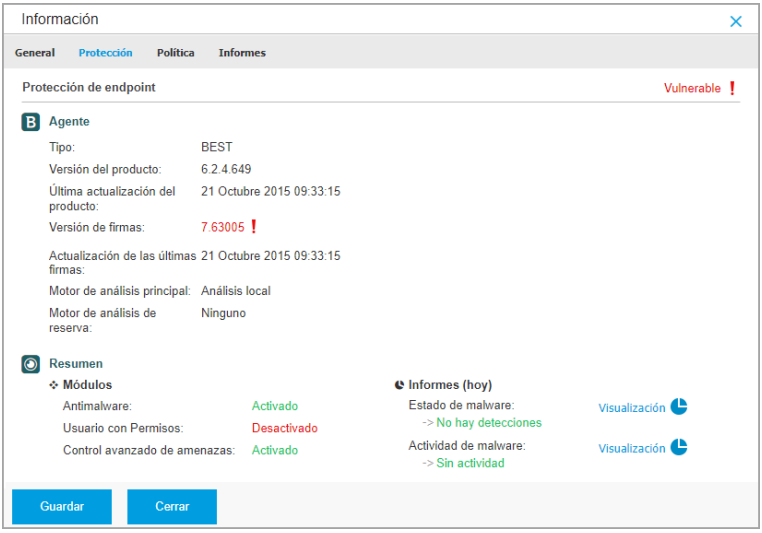
- Security Server asociado. Cada Security Server asignado se muestra en caso de implementaciones sin agente o cuando los motores de análisis de los agentes de seguridad se configuran para utilizar el análisis remoto. La información del Security Server ayuda a identificar el dispositivo virtual y conocer su estado de actualización.
- El estado de los módulos de protección. Puede ver fácilmente qué módulos de protección se han instalado en el endpoint, así como el estado de los módulos disponibles (**Activado/Desactivado**) que se ha establecido mediante la política aplicada.
- Una rápida visión de conjunto sobre la actividad de los módulos y los informes de malware de ese día.

  Haga clic en el enlace **Ver** para acceder a las opciones de informes y, a continuación, generar el informe. Para obtener más información, consulte "Creando Informes" (p. 444).
- Información sobre la capa de protección Sandbox Analyzer:
  - El estado de uso de Sandbox Analyzer en el endpoint, que se muestra a la derecha de la ventana:
    - **Activo**: Sandbox Analyzer cuenta con licencia (disponible) y se ha activado mediante la política en el endpoint.
    - **Inactivo**: Sandbox Analyzer cuenta con licencia (disponible) pero no se ha activado mediante la política en el endpoint.
  - Nombre del agente que actúa como sensor de alimentación.
  - Estado del módulo en el endpoint:
    - **Activado**: Sandbox Analyzer está activado mediante la política en el endpoint.
    - **Desactivado**: Sandbox Analyzer no está activado mediante la política en el endpoint.
  - Detecciones de amenazas durante la última semana, haciendo clic en el enlace **Ver** para acceder al informe.
- Información adicional sobre el módulo de Cifrado, como por ejemplo:
  - Volúmenes detectados (mencionando la unidad de arranque).

– Estado de cifrado de cada volumen (que puede ser **Cifrado**, **Cifrado en curso**, **Descifrado en curso**, **Sin cifrar**, **Bloqueado** o **En pausa**).

  Haga clic en el enlace **Recuperar** para obtener la clave de recuperación correspondiente al volumen cifrado. Para obtener más información sobre cómo conseguir las claves de recuperación, consulte "" (p. 106).

- Estado de la telemetría de seguridad, que le dice si la conexión entre el endpoint y el servidor SIEM se ha establecido y funciona, está inhabilitada o presenta algún problema.



Ventana Información - pestaña Protección

Pestaña Protección

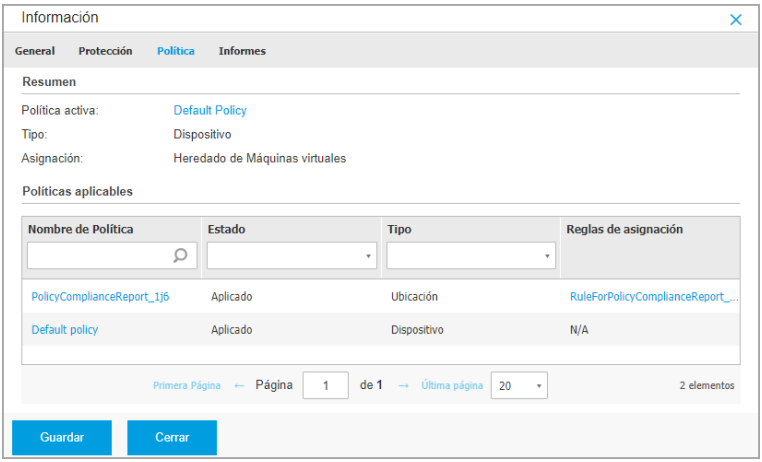
A un endpoint se le pueden aplicar una o varias políticas, pero solo puede haber una activa a la vez. La pestaña **Política** muestra información sobre todas las políticas que se aplican al endpoint.

- El nombre de la política activa. Haga clic en el nombre de la política para abrir la plantilla de política y ver sus ajustes.
- El tipo de política activa, que puede ser:

- **Dispositivo**: cuando el administrador de la red asigna manualmente la política al endpoint.
- **Ubicación**: una política basada en reglas asignada automáticamente al endpoint si los ajustes de red de este cumplen las condiciones dadas de una regla de asignación existente.

  Por ejemplo, un portátil tiene asignadas dos políticas basadas en la ubicación: una denominada `Oficina`, que se activa cuando se conecta a la red local de la empresa, y otra llamadas `Itinerancia`, que se activa cuando el usuario trabaja de forma remota y se conecta a otras redes.
- **Usuario**: una política basada en reglas asignada automáticamente al endpoint si cumple con el objetivo de Active Directory especificado en una regla de asignación existente.
- **Externo (NSX)**: cuando la política se define en el entorno VMware NSX.

- El tipo de asignación de política activa, que puede ser:
  - **Directo**: cuando la política se aplica directamente al endpoint.
  - **Heredado**: cuando el endpoint hereda la política de un grupo padre.
- **Políticas aplicables**: muestra la lista de políticas vinculadas a las reglas de asignación existentes. Estas políticas pueden aplicarse al endpoint cuando cumple las condiciones dadas de las reglas de asignación vinculadas.

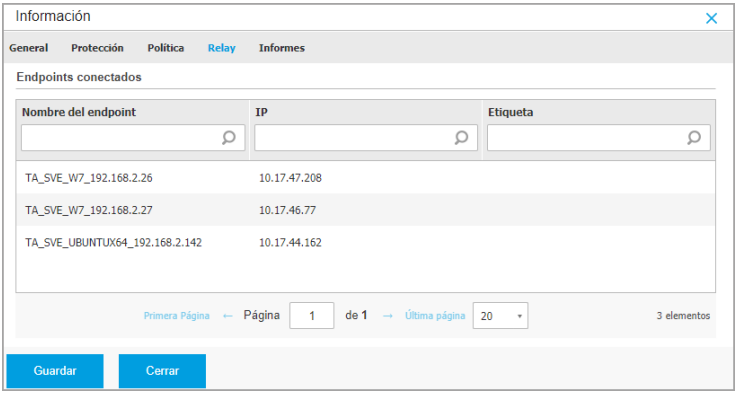


Ventana Información - pestaña Política

Para obtener más información con respecto a las políticas, consulte"Modificar los ajustes de políticas" (p. 236)

Pestaña Endpoints conectados

La pestaña **Endpoints conectados** solo está disponible para los endpoints con rol de relay. Esta pestaña muestra información sobre los endpoints conectados al relay actual, como son el nombre, la IP y la etiqueta.

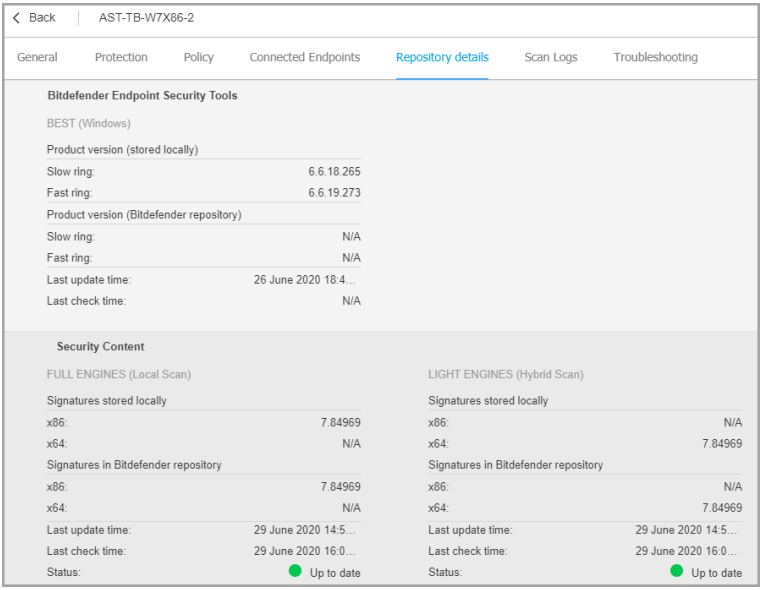


Ventana Información - pestaña Endpoints conectados

Pestaña Detalles del repositorio

La pestaña **Detalles del repositorio** está disponible solo para endpoints con rol de relay y muestra información sobre las actualizaciones del agente de seguridad y de los contenidos de seguridad.

La pestaña incluye detalles acerca de las versiones de producto y firmas almacenadas en el relay, así como las disponibles en el repositorio oficial, anillos de actualización, la fecha y hora de la actualización y la última búsqueda de nuevas versiones.



Ventana Información - pestaña Detalles del repositorio

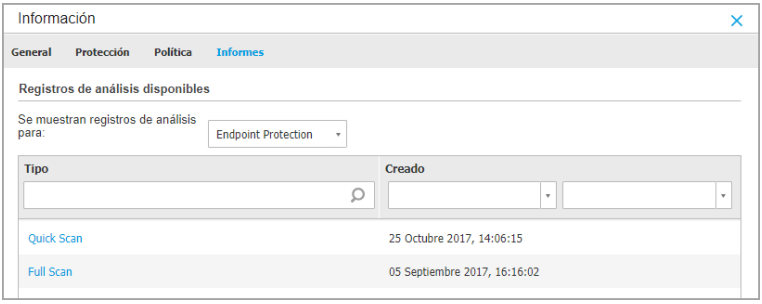
Pestaña Registros de análisis

La pestaña **Registros de análisis** muestra información detallada sobre todas las tareas de análisis ejecutadas en el endpoint.

Los registros se agrupan por capa de protección y se puede elegir, en el menú desplegable, de qué capa mostrar los registros.

Haga clic en la tarea de análisis que le interese y se abrirá el registro en una página nueva del navegador.

Cuando hay muchos registros de análisis disponibles, puede que tengan varias páginas. 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.

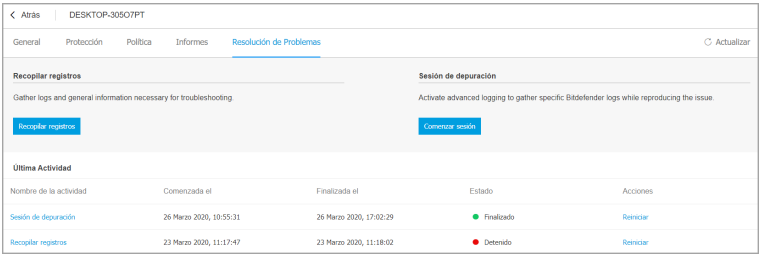


Ventana Información - pestaña Registros de análisis

Pestaña de Solución de problemas

Esta sección se dedica a la solución de problemas del agente. Puede recopilar registros generales o específicos de la verificación del endpoint o adoptar medidas sobre los eventos de solución de problemas actuales y ver la actividad anterior.

Importante
La solución de problemas está disponible para Windows, Linux, macOS y todos los tipos de Servidor de seguridad.



Ventana Información - Pestaña Solución de problemas

- **Recopilar registros**

Esta opción le ayuda a recopilar un conjunto de registros e información general necesaria para la solución de problemas, como los ajustes, los módulos activos o la política aplicada específicamente a la máquina objetivo. Todos los datos generados se guardan en un archivo comprimido.

Se recomienda utilizar la opción cuando no esté clara la causa del problema.

Para iniciar el proceso de solución de problemas:

1. Haga clic en el botón **Recopilar registros**. Se muestra una ventana de configuración.
2. En la sección **Almacenamiento de registros**, elija una ubicación de almacenamiento:
   - **Máquina objetivo**: el archivo de registros se guarda en la ruta local proporcionada. La ruta no es configurable para los Servidores de seguridad.
   - **Recurso compartido de red**: el archivo de registros se guarda en la ruta proporcionada de la ubicación compartida.

   Puede usar la opción **Guardar registros también en la máquina objetivo** para guardar una copia de seguridad del archivo de registros en la máquina afectada.
3. Rellene la información necesaria (ruta local, credenciales para el recurso compartido de red y ruta a la ubicación compartida) según la ubicación seleccionada.
4. Haga clic en el botón **Recopilar registros**.

- **Sesión de depuración**

  Con la sesión de depuración, puede activar el registro avanzado en la máquina objetivo para recopilar registros específicos mientras reproduce el problema.

  Debe utilizar esta opción cuando haya descubierto qué módulo está causando problemas o por recomendación del servicio de soporte técnico empresarial de Bitdefender. Todos los datos generados se guardan en un archivo comprimido.

  Para iniciar el proceso de solución de problemas:

  1. Haga clic en el botón **Comenzar sesión**. Se muestra una ventana de configuración.

2. En la sección **Tipo de problema**, seleccione el problema que considera que afecta a la máquina.

   Tipos de problemas para máquinas con Windows y macOS:

Tipo de incidencia	Caso de uso
Antimalware (análisis on-access y bajo demanda)	– Lentitud general del endpoint – Un programa o recurso del sistema tarda demasiado en responder – Un proceso de análisis tarda más de lo habitual – Error de conexión al servicio de seguridad del host
Errores de actualización	– Mensajes de error aparecidos durante las actualizaciones de contenidos de seguridad o del producto
Control de contenido (análisis de tráfico y control de usuarios)	– No se carga el sitio web – Los elementos de la página web no se muestran correctamente
Conectividad de Cloud Services	– El endpoint carece de conectividad con los servicios de Bitdefender Cloud
Problemas generales del producto (registro con mucho texto)	– Reproduzca un problema del que se informa genéricamente con el registro detallado

   Tipos de problemas para máquinas con Linux:

Tipo de incidencia	Caso de uso
Antimalware y actualización	– Un proceso de análisis tarda más tiempo de lo habitual y consume más recursos – Mensajes de error aparecidos durante las actualizaciones de contenidos de seguridad o del producto

Tipo de incidencia	Caso de uso
	– El endpoint no se puede conectar a la consola GravityZone.
Problemas generales del producto (registro con mucho texto)	– Reproduzca un problema del que se informa genéricamente con el registro detallado

Tipos de problemas para Servidores de seguridad:

Tipo de incidencia	Caso de uso
Antimalware (análisis on-access y bajo demanda)	Cualquier comportamiento inesperado del Servidor de seguridad, que incluye: – Las máquinas virtuales no están protegidas adecuadamente – Las tareas de análisis antimalware no se ejecutan o tardan más de lo esperado – Las actualizaciones del producto no están instaladas debidamente – El Servidor de seguridad genérico no funciona correctamente (los daemons de bd no se ejecutan)
Comunicación con GravityZone Control Center	Cualquier comportamiento inesperado observado de la consola de GravityZone: – No se informa correctamente de las máquinas virtuales en la consola de GravityZone – Problemas de política (no se aplica la política) – El Servidor de seguridad no puede establecer conexión con la consola de GravityZone **Nota** Utilice este método por recomendación del servicio de soporte técnico empresarial de Bitdefender.

3. En la **Duración de la sesión de depuración**, elija el intervalo de tiempo tras el cual finalizará automáticamente la sesión de depuración.

   Nota
   Se recomienda detener manualmente la sesión mediante la opción **Finalizar sesión** nada más reproducir el problema.

4. En la sección **Almacenamiento de registros**, elija una ubicación de almacenamiento:
   - **Máquina objetivo**: el archivo de registros se guarda en la ruta local proporcionada. La ruta no es configurable para los Servidores de seguridad.
   - **Recurso compartido de red**: el archivo de registros se guarda en la ruta proporcionada de la ubicación compartida.

   Puede usar la opción **Guardar registros también en la máquina objetivo** para guardar una copia de seguridad del archivo de registros en la máquina afectada.
5. Rellene la información necesaria (ruta local, credenciales para el recurso compartido de red y ruta a la ubicación compartida) según la ubicación seleccionada.
6. Haga clic en el botón **Comenzar sesión**.

   Importante
   Solo puede ejecutar un proceso de solución de problemas a la vez (**Recopilar registros** / **Sesión de depuración**) en la máquina afectada.

- **Historial de solución de problemas**

  La sección **Última actividad** presenta la actividad de solución de problemas en el equipo afectado. La cuadrícula muestra solo los últimos diez eventos de solución de problemas por orden cronológico inverso y elimina automáticamente la actividad anterior a treinta días.

  La cuadrícula muestra los detalles de cada proceso de solución de problemas.

  El proceso tiene estados principales e intermedios. Dependiendo de los ajustes personalizados, puede tener los siguientes estados, donde debe adoptar medidas:

- **En curso (listo para reproducir el problema)**: Acceda a la máquina afectada de forma manual o remota y reproduzca el problema.

A continuación se exponen las diversas opciones que tiene para detener un proceso de solución de problemas:

- **Finalizar sesión**: Finaliza la sesión de depuración y el proceso de recopilación en la máquina objetivo al tiempo que guarda todos los datos recopilados en la ubicación de almacenamiento especificada.

  Se recomienda usar esta opción nada más reproducir el problema.

- **Cancelar**: Esta opción cancela el proceso y no se recopilan registros.

  Use esta opción cuando no desee recopilar ningún registro de la máquina objetivo.

- **Forzar detención**: Detiene forzosamente el proceso de solución de problemas.

  Use esta opción si la cancelación de la sesión tarda demasiado o si la máquina objetivo no responde, con lo que podrá comenzar una nueva sesión transcurridos unos minutos.

Para reiniciar un proceso de solución de problemas:

- **Reiniciar**: Este botón, asociado a cada evento y ubicado en **Acciones**, reinicia la actividad de solución de problemas seleccionada manteniendo los ajustes previos.

Importante

- Para asegurarse de que la consola muestra la información más reciente, use el botón **Actualizar** de la parte superior derecha de la página **Solución de problemas**.
- Para obtener más información sobre un evento concreto, haga clic en el nombre del evento en la cuadrícula.

6.2.3. Organice los equipos en grupos

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

La ventaja principal de esta característica es que puede utilizar políticas de grupo para satisfacer diferentes requisitos de seguridad.

Los equipos importados desde Active Directory se agrupan en la carpeta **Active Directory**. No puede editar los grupos Active Directory. Sólo puede consultar y administrar los equipos correspondientes.

Todos los equipos ajenos a Active Directory detectados en su red se sitúan en **Grupos personalizados**, donde puede organizarlos en grupos como desee. Bajo **Grupos personalizados** puede crear, eliminar, renombrar y mover grupos de equipos dentro de una estructura de árbol personalizada.

Nota

- Un grupo puede contener tanto equipos como otros grupos.
- Cuando se selecciona un grupo en el panel izquierdo, puede ver todos los equipos excepto los ubicados en sus subgrupos. Para ver todos los equipos incluidos en el grupo y sus subgrupos, haga clic en el menú **Filtros** situado en la zona superior 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 endpoints basándose en uno de los siguientes criterios o en una combinación de los mismos:

- 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 **Grupos personalizados** en el panel lateral izquierdo.
2. Haga clic en el botón ⊕ **Añadir grupo** en la zona superior del panel de la izquierda.
3. Escriba un nombre descriptivo para el grupo y haga clic en **Aceptar**. El nuevo grupo aparecerá en la carpeta **Grupos personalizados**.

Renombrando Grupos

Para renombrar un grupo:

1. Seleccione el grupo en el panel lateral izquierdo.

2. Haga clic en el botón **Editar grupo** en la zona superior del panel de la izquierda.
3. Introduzca el nuevo nombre en el campo correspondiente.
4. Haga clic en **Aceptar** para confirmar.

Mover grupos y equipos

Puede mover entidades a **Grupos personalizados** en cualquier lugar dentro de la jerarquía del grupo. Para mover una entidad, arrástrela desde el panel de la derecha y suéltela en el grupo que desee en el de la izquierda.

Nota

La entidad movida heredará los ajustes de políticas del nuevo grupo padre, a menos que se le haya asignado directamente una política diferente. Para obtener más información sobre la herencia de políticas, consulte "Políticas de Seguridad" (p. 222).

Eliminando Grupos

La eliminación de un grupo es una acción definitiva. Como resultado de ello, se eliminará el agente de seguridad instalado en el endpoint seleccionado.

Para eliminar un grupo:

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

6.2.4. Clasificación, filtrado y búsqueda de equipos

Dependiendo del número de endpoints, la tabla del panel de la derecha puede tener varias páginas (por defecto solo se muestran 20 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 zona superior de la página para mostrar solo las entidades que le interesen. Por ejemplo, puede buscar un equipo específico o elegir ver únicamente los equipos administrados.

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

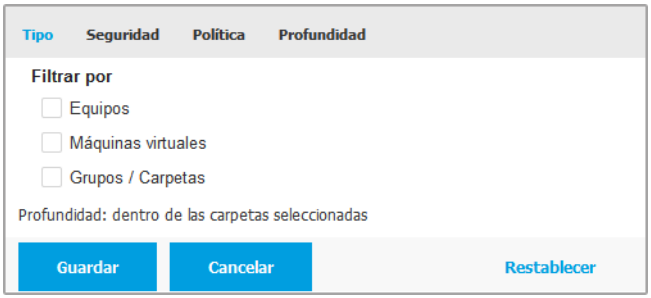
clic en el encabezado **Nombre**. Si hace clic en el encabezado otra vez, los equipos se mostrarán en orden inverso.

Ordenar equipos

Filtrar equipos

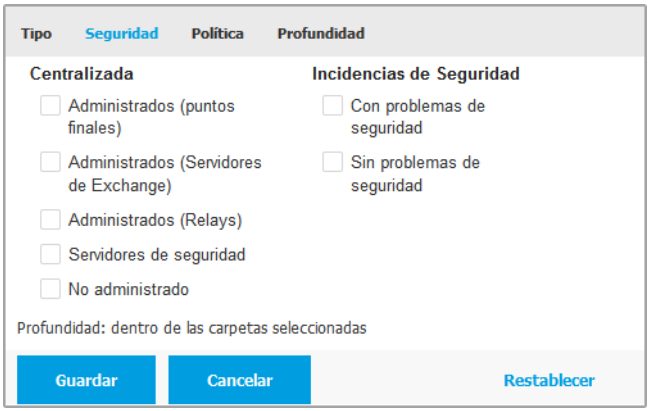
Para filtrar sus entidades de red, utilice el menú **Filtros** de la zona superior del área de paneles de red.

1. Seleccione el grupo que desee en el panel de la izquierda.
2. Haga clic en el menú **Filtros** de la zona superior del área de paneles de red.
3. Use el criterio de filtrado de la siguiente manera:
   - **Tipo**. Seleccione el tipo de entidades que desea mostrar (equipos, máquinas virtuales o carpetas).



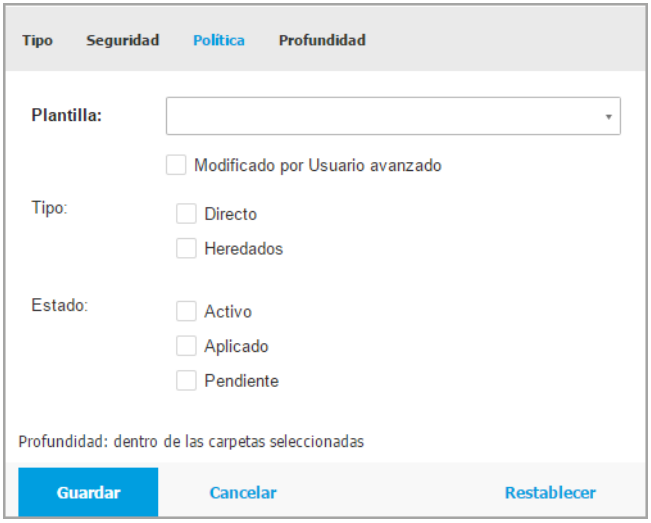
Equipos - Filtrar por tipo

   - **Seguridad**. Elija mostrar los equipos por administración de la protección, estado de seguridad o actividad pendiente.



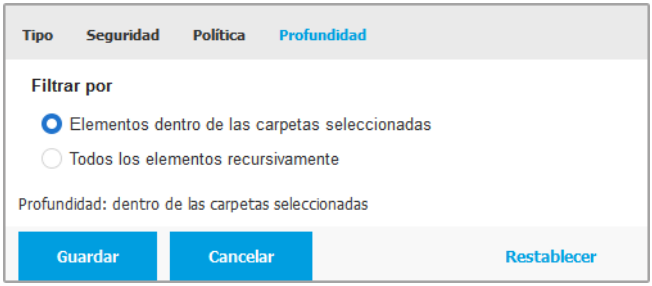
Equipos - Filtrar por seguridad

- **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 (activo, aplicado o pendiente). También puede optar por mostrar solo las entidades con políticas editadas en el modo de usuario avanzado.



Equipos - Filtrar por política

- **Profundidad**. Al administrar una red 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 todos sus subgrupos.



Equipos - Filtrar por profundidad

Si elige ver todos los elementos de forma recursiva, Control Center los muestra en una simple lista. Para averiguar dónde está un elemento, selecciónelo y, a continuación, haga clic en el botón **Acceder al contenedor** de la zona superior de la tabla. Se le redirigirá al contenedor padre del elemento seleccionado.

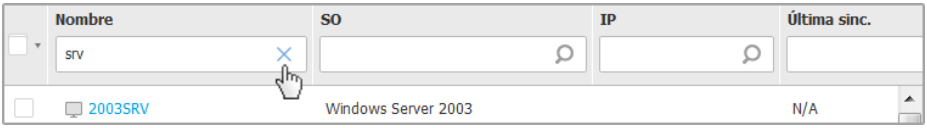
Nota
En la parte inferior de la ventana **Filtros**, puede ver todos los criterios de filtrado seleccionados.
Si desea eliminar todos los filtros, haga clic en el botón **Restablecer**.

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.

Buscando Equipos

1. Seleccione el grupo deseado desde el panel lateral izquierdo.
2. Escriba el término de búsqueda en el cuadro correspondiente de los encabezados de columnas del panel de la derecha. 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

6.2.5. Ejecución de tareas

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. 72)
- "Tareas de parches" (p. 82)
- "Análisis de Exchange" (p. 84)
- "Instalar" (p. 89)
- "Desinstalar cliente" (p. 95)
- "Actualizar cliente" (p. 96)
- "Reconfigurar cliente" (p. 97)
- "Reparar cliente" (p. 99)
- "Reiniciar máquina" (p. 100)
- "Descubrimiento de red" (p. 100)
- "Detección de aplicaciones" (p. 101)
- "Actualizar Security Server" (p. 102)
- "Herramienta personalizada de inyección" (p. 102)

Puede elegir crear tareas individuales para cada equipo o para grupos de equipos. Por ejemplo, puede instalar de forma remota el agente de seguridad 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, solo puede elegir instalar el agente de seguridad; todas las demás tareas aparecen deshabilitadas.

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.

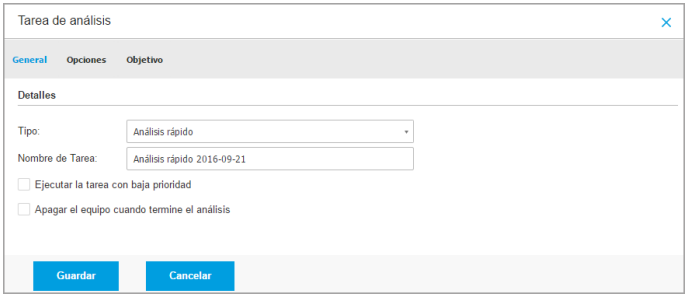
Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Analizar

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

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación correspondientes a los equipos que quiera analizar.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Analizar**.

   Aparecerá una nueva ventana de configuración.
6. 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. Este tipo de análisis está configurado de forma predeterminada para analizar únicamente ubicaciones del sistema críticas de Windows y Linux. 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.

  Cuando se encuentran rootkits o malware, Bitdefender procede automáticamente a la desinfección. Si por alguna razón no se pudiese desinfectar el archivo, este se trasladará a la cuarentena. Este tipo de análisis ignora los archivos sospechosos.

- **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.

  Bitdefender trata automáticamente de desinfectar los archivos en los que se ha detectado malware. En caso de que no se pueda eliminar el malware, se recluye en la cuarentena, donde no puede causar ningún daño. Los archivos sospechosos se ignoran. Si quiere actuar también sobre los archivos sospechosos, o si desea escoger otras acciones por defecto para los archivos infectados, efectúe un Análisis personalizado.

- **Análisis de memoria** comprueba los programas que se ejecutan en la memoria del equipo.

- El **Análisis de red** es un tipo de análisis personalizado que permite analizar unidades de red utilizando el agente de seguridad de Bitdefender instalado en el endpoint objetivo.

  Para que funcione la tarea de análisis de red:

  - Tiene que asignar la tarea a un solo endpoint de su red.
  - Ha de introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red objetivo para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red. Las credenciales requeridas se pueden configurar en la pestaña **Objetivo** de la ventana de tareas.

- **Análisis personalizado** le permite elegir las ubicaciones a analizar y configurar las opciones de análisis.

Para los análisis de memoria, red y personalizados, dispone también de estas opciones:

– **Ejecutar la tarea con baja prioridad**. Marque esta casilla de verificación para disminuir la prioridad del proceso de análisis y permitir que otros programas se ejecuten más rápido. Esto aumentará el tiempo necesario para que finalice el proceso de análisis.

  Nota
  Esta opción se aplica solo a Bitdefender Endpoint Security Tools y Endpoint Security (agente antiguo).

– **Apagar el equipo cuando termine el análisis**. Marque esta casilla de verificación para apagar su máquina si no va a utilizarla durante un tiempo.

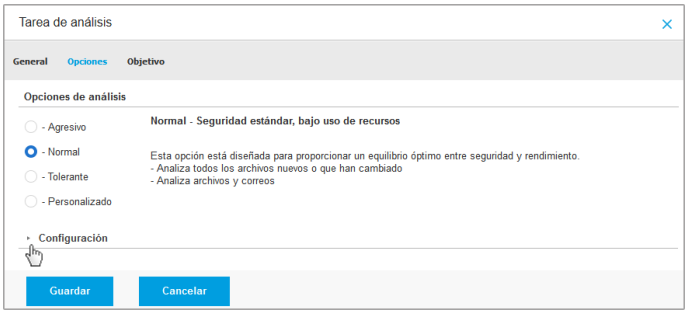
  Nota
  Esta opción se aplica a Bitdefender Endpoint Security Tools, Endpoint Security (agente antiguo) y Endpoint Security for Mac.

Nota
Estas dos opciones se aplican solo a Bitdefender Endpoint Security Tools y Endpoint Security (agente antiguo).

Para análisis personalizados, configure los siguientes ajustes:

– Acceda 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 expanda la sección **Ajustes**.



Tarea de análisis de equipos - Configuración de un análisis personalizado

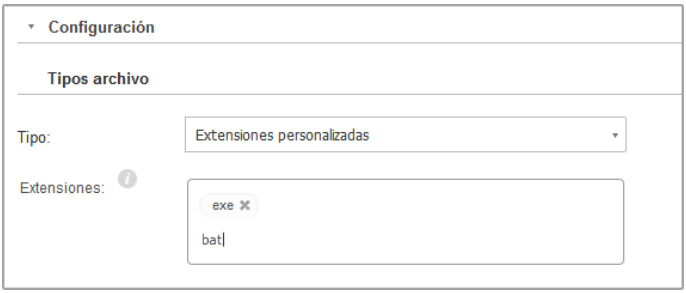
Tiene las siguientes opciones a su disposición:

- **Tipos archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede ajustar el agente de seguridad para analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación 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 "Tipos de archivos de aplicación" (p. 527).

  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.

  Importante
  Los agentes de seguridad de Bitdefender instalados en los sistemas operativos Windows y Linux analizan la mayoría de los formatos .ISO, pero no llevan a cabo ninguna acción sobre ellos.



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. No obstante, se recomienda analizar los archivos empaquetados con el fin de detectar y eliminar cualquier amenaza potencial, incluso aunque no se trate de una amenaza inmediata.

  Importante
  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.

  Importante
  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 recursos compartidos.** Esta opción analiza las unidades de red montadas.

    Esta opción está desactivada por defecto para los Quick Scans. Está activada por defecto para los análisis completos. Para los análisis personalizados, si establece el nivel de seguridad en **Agresivo/Normal**, la opción **Analizar recursos compartidos** se activa automáticamente. Si establece el nivel de seguridad en

Tolerante, la opción **Analizar recursos compartidos** se desactiva automáticamente.

- **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.
- **Análisis de dispositivos extraíbles.** Seleccione esta opción para analizar cualquier unidad de almacenamiento extraíble conectada al equipo.

- **Acciones.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
  - **Al encontrar un archivo infectado.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA). El agente de seguridad de Bitdefender 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, el agente de seguridad de Bitdefender 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 se detectan como sospechosos mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos). 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 configurar las ubicaciones que desea que se analicen en los equipos objetivo.

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 respecto a las variables del sistema, consulte "Variables del sistema" (p. 529).

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

Para editar una ubicación existente, haga clic en ella. Para eliminar una ubicación de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente.

Para las tareas de análisis de red, tiene que introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red objetivo, para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red.

Haga clic en la sección **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. 293).

7. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Nota
Para programar una tarea de análisis, acceda a la página **Políticas**, seleccione la política asignada a los equipos en los que está interesado, y añada una tarea de

análisis en la sección **Antimalware > Bajo demanda**. Para más información, diríjase a "Bajo demanda" (p. 272).

Tareas de parches

Se recomienda comprobar regularmente las actualizaciones de software y aplicarlas lo antes posible. GravityZone automatiza este proceso a través de políticas de seguridad, pero si necesita actualizar el software inmediatamente en ciertos endpoints, ejecute las siguientes tareas por este orden:

1. Análisis de parches
2. Instalación de parches

Requisitos

- El agente de seguridad con el módulo de Administración de parches está instalado en los endpoints objetivo.
- Para que las tareas de análisis e instalación tengan éxito, los endpoints de Windows deben cumplir estas condiciones:
  - Las **entidades de certificación raíz de confianza** almacenan el certificado **DigiCert Assured ID Root CA**.
  - Las **entidades de certificación intermedias** incluyen **DigiCert SHA2 Assured ID Code Signing CA**.
  - Los endpoints han instalado los parches para Windows 7 y Windows Server 2008 R2 mencionados en este artículo de Microsoft: Aviso de seguridad de Microsoft 3033929

Análisis de parches

Los endpoints con software obsoleto son vulnerables a los ataques. Se recomienda comprobar regularmente el software instalado en sus endpoints y actualizarlo lo antes posible. Para analizar sus endpoints en busca de parches que falten:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione los endpoints objetivo.

5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Análisis de parches**. Aparecerá una ventana de configuración.
6. Haga clic en **Sí** para crear la tarea de análisis.

   Cuando la tarea finaliza, GravityZone añade al Inventario de parches todos los que su software necesita. Para obtener más información, consulte "Inventario de parches" (p. 201).

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Nota
Para programar el análisis de parches, edite las políticas asignadas a los endpoints objetivo y configure los ajustes en la sección **Administración de parches**. Para más información, diríjase a "Administración de parches" (p. 341).

Instalación de parches

Para instalar uno o más parches en los endpoints objetivo:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Instalación de parches**.

   Aparecerá una nueva ventana de configuración. Aquí puede ver todos los parches que faltan en los endpoints objetivo.
5. Si es necesario, use las opciones de clasificación y filtrado de la parte superior de la tabla para encontrar parches concretos.
6. Haga clic en el botón **Columnas** de la esquina superior derecha del panel para ver solo la información relevante.
7. Seleccione los parches que desea instalar.

   Ciertos parches dependen de otros. En tal caso, se seleccionan automáticamente con el parche.

Al hacer clic en los números de **CVE** o de **Productos,** se mostrará un panel en el lado izquierdo. Dicho panel contiene información adicional, como por ejemplo las CVE que resuelve el parche o los productos a los que se aplica. Cuando termine de leer, haga clic en **Cerrar** para ocultar el panel.

8. Seleccione **En caso necesario, reiniciar los endpoints después de instalar el parche** para reiniciar los endpoints inmediatamente después de la instalación del parche, en caso de que sea necesario reiniciar el sistema. Tenga en cuenta que esta acción puede interrumpir la actividad del usuario.
9. Haga clic en **Instalar**.

   Se crea la tarea de instalación junto con las subtareas para cada endpoint objetivo.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Nota

- Para programar la implementación de parches, edite las políticas asignadas a los endpoints objetivo y configure los ajustes en la sección **Administración de parches**. Para más información, diríjase a "Administración de parches" (p. 341).
- Asimismo, puede instalar un parche desde la página **Inventario de parches**, a partir de un cierto parche que le interese. En tal caso, seleccione el parche de la lista, haga clic en el botón **Instalar** en la parte superior de la tabla y configure los detalles de instalación del parche. Para obtener más información, consulte "Instalación de parches" (p. 205).
- Tras instalar un parche, recomendamos enviar una tarea de Análisis de parches a los endpoints objetivo. Dicha acción actualizará la información del parche almacenada en GravityZone para sus redes administradas.

Puede desinstalar parches:

- De forma remota, enviando una tarea de Desinstalación de parche desde GravityZone.
- Localmente en el endpoint. En tal caso, debe iniciar sesión como administrador en el endpoint y ejecutar el desinstalador manualmente.

Análisis de Exchange

Puede analizar de forma remota la base de datos de un servidor de Exchange mediante la ejecución de una tarea **Análisis de Exchange**.

Para poder analizar la base de datos de Exchange, debe habilitar el análisis bajo demanda proporcionando las credenciales de un administrador de Exchange. Para más información, diríjase a "Análisis del almacén de Exchange" (p. 366).

Para analizar una base de datos de servidor de Exchange:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. En el panel de la izquierda, seleccione el grupo que contiene el servidor de Exchange objetivo. Puede encontrar el servidor en el panel de la derecha.

   Nota
   Opcionalmente, puede aplicar filtros para encontrar rápidamente el servidor objetivo:
   - Haga clic en el menú **Filtros** y seleccione las siguientes opciones: **Administrados (Servidores de Exchange)** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.
   - Introduzca el nombre de host del servidor o su IP en los campos de los encabezados de las columnas correspondientes.

4. Marque la casilla de verificación del servidor de Exchange cuya base de datos quiera analizar.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y elija **Análisis de Exchange**. Aparecerá una nueva ventana de configuración.
6. Configure las opciones de análisis:
   - **General.** Escriba un nombre descriptivo para la tarea.

     Con bases de datos grandes, la tarea de análisis puede tardar mucho tiempo y es posible que afecte al rendimiento del servidor. En tales casos, marque la casilla de verificación **Detener el análisis si tarda más de** y seleccione un intervalo de tiempo oportuno en los menús correspondientes.
   - **Objetivo.** Seleccione los contenedores y objetos que desea analizar. Puede optar por analizar los buzones, las carpetas públicas o ambos. Además de los correos electrónicos, puede optar por analizar otros objetos como **Contactos**, **Tareas**, **Citas** y **Elementos para exponer**. Además, puede establecer las siguientes restricciones a los contenidos que se analizarán:
     - Solo los mensajes no leídos.
     - Solo los elementos con adjuntos.
     - Solo los elementos nuevos recibidos en un intervalo de tiempo determinado.

Por ejemplo, puede elegir analizar solo los mensajes de correo electrónico de los buzones de los usuarios recibidos en los últimos siete días.

Marque la casilla de verificación **Exclusiones** si desea definir excepciones de análisis. Para crear una excepción, utilice los campos del encabezado de la tabla de la siguiente manera:

a. Seleccione el tipo de repositorio en el menú.
b. Dependiendo del tipo de repositorio, indique el objeto que haya que excluir:

Tipo de repositorio	Formato de objeto
Buzón de Correo	Dirección de correo:
Carpeta pública	Ruta de la carpeta, a partir de la raíz
Base de Datos	La identidad de la base de datos

Nota
Para obtener la identidad de la base de datos, utilice el comando shell de Exchange:
`Get-MailboxDatabase | fl name,identity`

Solo puede indicar los elementos uno a uno. Si tiene varios elementos del mismo tipo, debe definir tantas reglas como elementos tenga.

c. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para guardar la excepción y añadirla a la lista.

Para eliminar una regla de excepción de la lista, haga clic en el botón ⊖ **Eliminar** correspondiente.

- **Opciones.** Configure las opciones de análisis para mensajes de correo electrónico que cumplan la regla:
  - **Tipos de archivos analizados.** Utilice esta opción para especificar los tipos de archivo que desee analizar. Puede optar por analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación o extensiones de archivo concretas que considere peligrosas. Analizar todos los archivos aporta la mayor protección, mientras que se recomienda analizar solo las aplicaciones para 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 "Tipos de archivos de aplicación" (p. 527).

Si desea analizar solo los archivos con determinadas extensiones, tiene dos alternativas:

- **Extensiones definidas por el usuario**, donde debe proporcionar solo las extensiones que se analizarán.
- **Todos los archivos, excepto extensiones concretas**, donde debe introducir solo las extensiones que no se analizarán.

– **Tamaño máximo del adjunto/cuerpo del mensaje (MB).** Marque esta casilla de verificación e introduzca un valor en el campo correspondiente para establecer el tamaño máximo aceptado de un archivo adjunto o del cuerpo del mensaje de correo electrónico que se va a analizar.

– **Profundidad de archivo máxima (niveles).** Marque la casilla de verificación y elija la profundidad máxima del archivo comprimido en el campo correspondiente. Cuanto menor sea el nivel de profundidad, mayor será el rendimiento, pero menor el grado de protección.

– **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Marque esta casilla de verificación para buscar aplicaciones maliciosas o potencialmente no deseadas, como por ejemplo adware, que pueden instalarse en los sistemas sin el consentimiento del usuario, cambiar el comportamiento de diversos productos de software y reducir el rendimiento del sistema.

- **Acciones.** Puede especificar diferentes acciones para que el agente de seguridad las aplique automáticamente a los archivos, en función del tipo de detección.

  El tipo de detección divide los archivos en tres categorías:

  – **Archivos infectados.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA).

  – **Archivos sospechosos.** Estos archivos se detectan mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos).

– **Archivos no analizables.** Estos archivos no se pueden analizar. Los archivos que no se pueden analizar incluyen, pero no se limitan, a los archivos protegidos con contraseña, cifrados o sobrecomprimidos.

Para cada tipo de detección, dispone de una acción por defecto o principal y de una acción alternativa por si falla la principal. Aunque no es recomendable, puede cambiar estas acciones mediante los menús correspondientes. Elija la acción a adoptar:

– **Desinfectar.** Elimina el código de malware de los archivos infectados y reconstruye el archivo original. Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.
– **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
– **Eliminar archivo.** Elimina los archivos adjuntos problemáticos sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
– **Reemplazar archivo.** Elimina los archivos problemáticos e inserta un archivo de texto que comunica al usuario las acciones adoptadas.
– **Mover archivo a la cuarentena.** Mueve los archivos detectados a la carpeta de cuarentena e inserta un archivo de texto que comunica al usuario las acciones adoptadas. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de la cuarentena desde la página **Cuarentena**.

> **Nota**
> Tenga en cuenta que la cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad. El tamaño de la cuarentena depende del número de elementos almacenados y de su tamaño.

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

- Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

7. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Instalar

Para proteger sus equipos con el agente de seguridad de Bitdefender, debe instalarlo en cada uno de ellos.

Importante
En redes aisladas que carecen de conexión directa con el appliance GravityZone, puede instalar el agente de seguridad con rol de relay. En tal caso, la comunicación entre el appliance GravityZone y los demás agentes de seguridad se efectuará a través del agente de relay, que actuará también como servidor de actualizaciones local para los agentes de seguridad que protegen la red aislada.
Una vez que haya instalado un agente de relay, éste detectará automáticamente los equipos no protegidos de la misma red.

Nota

- Se recomienda que el equipo en que instale el agente de relay esté siempre encendido.
- Si no se instala un agente de relay en la red, la detección de equipos desprotegidos se puede hacer manualmente enviando una tarea de **Detección de redes** a un endpoint protegido.

La protección de Bitdefender puede instalarse en 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 la protección de Bitdefender sobre software de seguridad existente puede afectar al funcionamiento y causar problemas importantes en el sistema. Windows Defender y el Cortafuego de Windows se desactivarán automáticamente cuando se inicie la instalación.

Si desea implementar el agente de seguridad en un equipo con Bitdefender Antivirus for Mac 5.x, primero debe quitar manualmente este último. Para obtener una guía de los pasos a dar, consulte este artículo de la base de conocimientos.

Para implementar el agente a través de un relay de Linux, deben cumplirse las siguientes condiciones:

- El endpoint de relay debe tener instalado el paquete Samba (`smbclient`) versión 4.1.0 o superior y el comando/binario `net` para poder implementar agentes de Windows.

  Nota

  El comando/binario `net` viene generalmente con los paquetes samba-client o samba-common. En algunas distribuciones de Linux (como CentOS 7.4), el comando `net` solo se instala cuando se instala la suite completa de Samba (Common + Client + Server). Asegúrese de que su endpoint de relay disponga del comando `net`.

- Los endpoints de Windows objetivo deben tener habilitados el Recurso compartido de red y el Recurso compartido administrativo.
- Los endpoints objetivo de Linux y Mac deben tener habilitado SSH y el cortafuego desactivado.

Para ejecutar una tarea de instalación remota:

1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.
3. Elija **Equipos y máquinas virtuales** en el selector de vistas.
4. Seleccione el grupo deseado desde el panel lateral izquierdo. 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 endpoints no administrados. Haga clic en el menú **Filtros** y seleccione las siguientes opciones: **No administrados** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.

5. Seleccione las entidades (endpoints o grupos de endpoints) en las que desee instalar la protección.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Instalar**.

   El asistente de **Instalar cliente** se está mostrando.

Instalación de Bitdefender Endpoint Security Tools desde el menú Tareas

7. En la sección **Opciones**, configure 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.

8. Si quiere que los endpoints objetivo se reinicien automáticamente para completar la instalación, seleccione **Reiniciar automáticamente (si es necesario)**.
9. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los endpoints objetivo. Puede añadir las credenciales escribiendo el usuario y contraseña para 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.

   Para añadir las credenciales del sistema operativo requeridas:

   a. Introduzca el nombre de usuario y contraseña de una cuenta de administrador en los campos correspondientes del encabezado de la tabla.

      Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

      Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

      - Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
      - Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

      Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta.

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

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

Para acceder al Gestor de credenciales, señale su nombre de usuario en la esquina superior derecha de la consola.

Importante
Si las credenciales proporcionadas no son válidas, la implementación del cliente fallará en los endpoints correspondientes. Asegúrese de actualizar las credenciales del SO introducidas en el Gestor de credenciales cuando éstas cambien en los endpoints objetivo.

10. Marque las casillas de verificación correspondientes a las cuentas que desee usar.

Nota
Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota el agente de seguridad en los endpoints.

11. En la sección **Implementador**, seleccione la entidad a la que se conectarán los endpoints objetivo para instalar y actualizar el cliente:
    - **Appliance GravityZone**, cuando los endpoints se conectan directamente al appliance GravityZone.

      En este caso, también puede definir:

      – Un Servidor de comunicaciones personalizado introduciendo su IP o nombre de host, de ser necesario.

      – Ajustes de proxy, si los endpoints objetivo se comunican con el appliance GravityZone mediante un proxy. En este caso, seleccione **Utilizar un proxy para la comunicación** e introduzca los ajustes necesarios del proxy en los campos que figuran a continuación.
    - **Endpoint Security Relay**, si desea conectar los endpoints a un cliente de relay instalado en su red. Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla que se muestra a continuación. Seleccione la máquina de relay que desee. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.

Importante
El puerto 7074 debe estar abierto para que funcione la implementación mediante el agente de relay.

12. Utilice la sección **Objetivos adicionales** si quiere implementar el cliente en equipos concretos de su red que no se muestren en el inventario de red. Despliegue la sección e introduzca las direcciones IP o los nombres de host de esas máquinas en el campo correspondiente, separadas por una coma. Puede añadir tantas IPs como necesite.
13. Tiene que seleccionar un paquete de instalación para la implementación actual. Haga clic en la lista **Usar paquete** y seleccione el paquete de instalación que desee. Aquí puede encontrar todos los paquetes de instalación creados con anterioridad para su cuenta y también el paquete de instalación por defecto disponible con Control Center.
14. Si es necesario, puede modificar algunos de los ajustes del paquete de instalación seleccionado haciendo clic en el botón **Personalizar** junto al campo **Usar paquete**.

    Abajo aparecerán los ajustes del paquete de instalación y puede hacer los cambios que precise. Para más información sobre la modificación de los paquetes de instalación, consulte la Guía de instalación de GravityZone.

    Si desea guardar las modificaciones como un paquete nuevo, seleccione la opción **Guardar como paquete**, situada en la parte inferior de la lista de ajustes de paquetes, e introduzca un nombre para el nuevo paquete de instalación.
15. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

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

Importante
Si utiliza la administración de VMware Horizon View Persona, se recomienda configurar la política de grupo de Active Directory para excluir los siguientes procesos de Bitdefender (sin la ruta completa):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Estas exclusiones deben aplicarse siempre que el agente de seguridad se ejecute en el endpoint. Para más información, consulte esta página de la documentación de VMware Horizon.

Migrar cliente

Esta tarea solo está disponible cuando el agente Endpoint Security está instalado y se detecta en la red. Bitdefender recomienda actualizar de Endpoint Security al nuevo Bitdefender Endpoint Security Tools, para disfrutar de una protección de endpoints de última generación.

Para encontrar fácilmente los clientes que no están actualizados, puede generar un informe de estado de actualización. Para obtener más información sobre cómo crear informes, consulte "Creando Informes" (p. 444).

Desinstalar cliente

Para desinstalar de forma remota la protección de Bitdefender:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione las casillas de verificación correspondientes a los equipos de los que desee desinstalar el agente de seguridad de Bitdefender.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Desinstalar el cliente**.

6. Se muestra una ventana de configuración que le permite hacer los siguientes ajustes:
   - Puede optar por conservar los elementos en la cuarentena de la máquina cliente.
   - En el caso de entornos integrados vShield, debe seleccionar las credenciales necesarias para cada máquina, pues de lo contrario fallará la desinstalación. Seleccione **Usar credenciales para integración vShield** y, a continuación, marque todas las credenciales apropiadas en la tabla del Gestor de credenciales que se muestra debajo.
7. 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 "Ver y administrar tareas" (p. 210).

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

Actualizar cliente

Consulte el estado de los equipos periódicamente. Si observa un equipo con problemas de seguridad, haga clic en su nombre para mostrar la página **Información**. Para más información, diríjase a "Estado de seguridad" (p. 51).

Los clientes obsoletos o los contenidos de seguridad sin actualizar representan problemas de seguridad. En estos casos, debería ejecutar una actualización del cliente 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 los contenidos de seguridad de forma remota en equipos administrados:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de los equipos donde quiere realizar la actualización del cliente.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar**. Aparecerá una nueva ventana de configuración.

6. Puede optar por actualizar solo el producto, solo los contenidos de seguridad o ambos.
7. En el caso de máquinas integradas con vShield o con el sistema operativo Linux, es obligatorio seleccionar también las credenciales necesarias. Marque la opción **Usar credenciales para integración vShield** y, a continuación, seleccione las credenciales apropiadas en la tabla del Gestor de credenciales que se muestra a continuación.
8. 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 "Ver y administrar tareas" (p. 210).

Reconfigurar cliente

Los módulos de protección del agente de seguridad, los roles y los modos de análisis se configuran inicialmente en el paquete de instalación. Después de que haya instalado el agente de seguridad en su red, puede cambiar en cualquier momento los ajustes iniciales mediante el envío de una tarea remota **Reconfigurar el cliente** a los endpoints administrados que le interesen.

Aviso
Tenga en cuenta que la tarea **Reconfigurar el cliente** sobrescribe todos los ajustes de instalación y no se conserva ninguno de los ajustes iniciales. Al usar esta tarea, asegúrese de volver a configurar todos los ajustes de instalación de los endpoints objetivo.

Nota
La tarea **Reconfigurar el cliente** eliminará todos los módulos incompatibles de las instalaciones existentes en Windows heredado.

Puede cambiar los ajustes de instalación desde el área **Red** o desde el informe **Estado de los módulos de endpoint**.

Para cambiar los ajustes de instalación de uno o varios equipos:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.

4. Marque las casillas de verificación de los equipos a los que desea cambiar los ajustes de instalación.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reconfigurar el cliente**.
6. Seleccione una de las siguientes acciones:
   - **Añadir**. Añadir nuevos módulos a los ya existentes.
   - **Eliminar**. Eliminar módulos concretos ya existentes.
   - **Lista de coincidencias**. Ajustar los módulos instalados a los que seleccione.
7. Seleccione los módulos y roles que desea instalar o eliminar en los endpoints objetivo.

   Aviso
   Solo se instalarán los módulos compatibles. Por ejemplo, el Cortafuego se instala solo en las estaciones de trabajo compatibles con Windows.
   Para obtener más información, consulte la disponibilidad de las capas de protección de GravityZone.

8. Seleccione **Eliminar productos de la competencia en caso necesario** para asegurarse de que los módulos seleccionados no entren en conflicto con otras soluciones de seguridad instaladas en los endpoints objetivo.
9. Elija uno de los modos de análisis disponibles:
   - **Automática**. El agente de seguridad detecta qué motores de análisis son adecuados para los recursos del endpoint.
   - **Personal**. Usted elige explícitamente qué motores de análisis usar.

     Para obtener más información sobre las opciones disponibles, consulte la sección Crear paquetes de instalación de la Guía de instalación.

   Nota
   Esta sección está disponible solo con la **Lista de coincidencias**.

10. En la sección **Programador**, elija cuándo se ejecutará la tarea:
    - **Ahora**, para poner en marcha la tarea de inmediato.
    - **Programado**, para configurar el intervalo de recurrencia de la tarea.

En este caso, seleccione el intervalo de tiempo (cada hora, a diario o semanalmente) y configúrelo según sus necesidades.

11. 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 "Ver y administrar tareas" (p. 210).

Reparar cliente

Utilice la tarea Reparar cliente como tarea inicial de resolución de problemas para cualquier número de problemas de endpoints. Dicha tarea descarga el último paquete de instalación en el endpoint objetivo y luego realiza una reinstalación del agente.

Nota

- The modules currently configured on the agent will not be changed.
- La tarea Reparar equipo restablecerá el agente de seguridad a la versión publicada en la página **Configuración > Actualización > Componentes**.

Para enviar una tarea Reparar cliente al cliente debe hacer lo siguiente:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de los equipos donde quiera ejecutar la reparación del cliente.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reparar cliente**. Aparecerá una ventana de configuración.
6. Marque la casilla **Lo entiendo y estoy de acuerdo** y haga clic en el botón **Guardar** para ejecutar la tarea.

   Nota
   Para finalizar la tarea de reparación, puede que sea necesario reiniciar el cliente.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Reiniciar máquina

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. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación correspondientes a los equipos que quiere reiniciar.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reiniciar máquina**.
6. 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.
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 "Ver y administrar tareas" (p. 210).

Descubrimiento de red

Los agentes de seguridad con rol de relay realizan automáticamente la detección de redes. Si no tiene un agente de relay instalado en su red, tendrá que enviar manualmente una tarea de detección de redes desde un endpoint protegido.

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

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.

4. Marque la casilla de verificación correspondiente al equipo con el que quiere llevar a cabo la detección de redes.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Detección de redes**.
6. 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 "Ver y administrar tareas" (p. 210).

Detección de aplicaciones

Para detectar las aplicaciones en su red:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione los equipos en los que desea realizar la detección de aplicaciones.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Detección de aplicaciones**.

   Nota
   Bitdefender Endpoint Security Tools con Control de aplicaciones debe estar instalado y activado en los equipos seleccionados. De lo contrario, la tarea estará en gris. Cuando un grupo seleccionado contiene tanto objetivos válidos como no válidos, la tarea se enviará solo a los endpoints válidos.

6. Haga clic en **Sí** en la ventana de confirmación para continuar.

Las aplicaciones y procesos detectados se muestran en la página **Red > Inventario de aplicaciones**. Para más información, diríjase a "Inventario de aplicaciones" (p. 196).

Nota
La tarea de **Detección de aplicaciones** puede tardar cierto tiempo, dependiendo del número de aplicaciones instaladas. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Actualizar Security Server

El Security Server instalado se puede ver y administrar también desde **Equipos y máquinas virtuales** en la carpeta **Grupos personalizados**.

Si un Security Server se queda obsoleto, puede enviarle una tarea de actualización:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo donde está instalado el Security Server.

   Para localizar fácilmente el Security Server, puede utilizar el menú **Filtros** como se indica a continuación:

   - Acceda a la pestaña **Seguridad** y seleccione **Servidores de seguridad**.
   - Acceda a la pestaña **Profundidad** y seleccione **Todos los elementos recursivamente**.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar Security Server**.
5. Tendrá que confirmar esta acción. Haga clic en **Sí** para crear la tarea.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Importante
Se recomienda utilizar este método para actualizar Security Server para NSX; de lo contrario perderá la cuarentena guardada en el appliance.

Herramienta personalizada de inyección

Para inyectar herramientas en los sistemas operativos del guest objetivo:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de los endpoints objetivo.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Herramienta personalizada de inyección**. Se muestra una ventana de configuración.

6. En el menú desplegable, seleccione todas las herramientas que desee inyectar. Para cada herramienta seleccionada, se muestra una sección contraíble con sus ajustes.

   Estas herramientas se cargaron previamente en GravityZone. Si no consigue encontrar la herramienta adecuada en la lista, acceda al **Centro de administración de herramientas** y añádala desde allí. Para más información, diríjase a "Inyección de herramientas personalizadas con HVI" (p. 494).

7. Para cada herramienta visualizada en la ventana:

   a. Haga clic en el nombre de la herramienta para ver u ocultar su sección.

   b. Introduzca la línea de comando de la herramienta, junto con todos los parámetros de entrada necesarios, como hace en el símbolo del sistema o el terminal. Por ejemplo:

      ```
      bash script.sh <param1> <param2>
      ```

      En el caso de las herramientas de reparación de BD, solo puede seleccionar la acción de reparación y la acción de reparación de copia de seguridad en los dos menús desplegables.

   c. Indique la ubicación desde donde Security Server debe reunir los registros:

      - **stdout**. Marque esta casilla de verificación para capturar los registros del canal de comunicación de salida estándar.
      - **Archivo de salida**. Marque esta casilla de verificación para recopilar el archivo de registro guardado en el endpoint. En este caso, debe introducir la ruta donde Security Server puede encontrar el archivo. Puede utilizar rutas absolutas o variables del sistema.

        Aquí tiene una opción adicional: **Eliminar los archivos de registro del guest después de haberlos transferido**. Selecciónela si ya no necesita los archivos en el endpoint.

8. Si desea transferir el archivo de registros desde Security Server a otra ubicación, debe proporcionar la ruta de acceso a la ubicación de destino y las credenciales de autenticación.

9. A veces la herramienta puede requerir más tiempo de lo esperado para terminar su trabajo, o puede incluso dejar de responder. Para evitar problemas en estas situaciones, en la sección **Configuración de seguridad**, elija después de cuántas

horas Security Server debe finalizar automáticamente el proceso de la herramienta.

10. Haga clic en **Guardar**.

    Puede ver el estado de la tarea en la página **Tareas**. Para obtener más información, también puede consultar el informe de **Estado de inyección de terceros de HVI**.

6.2.6. Crear informes rápidos

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

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel de la derecha.

   Opcionalmente, puede filtrar los contenidos del grupo seleccionado solo por los equipos administrados.
4. Marque las casillas de verificación correspondientes a los equipos que desea incluir en el informe.
5. Haga clic en el botón **Informe** de la zona superior de la tabla y seleccione en el menú el tipo de informe.

   Para más información, diríjase a "Informes de equipos y máquinas virtuales" (p. 424).
6. Configure las opciones del informe. Para más información, diríjase a "Creando Informes" (p. 444).
7. Haga clic en **Generar**. El informe se mostrará inmediatamente.

   El tiempo necesario para crear los informes puede variar dependiendo del número de equipos seleccionados.

6.2.7. Asignando Políticas

Puede administrar los ajustes de seguridad en los equipos mediante políticas.

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

Nota
Los ajustes de seguridad solo están disponibles para los equipos administrados. Para ver y administrar los ajustes de seguridad con mayor facilidad, puede filtrar el inventario de red para que aparezcan solo los equipos administrados.

Para ver la política asignada a un equipo concreto:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
4. Haga clic en el nombre del equipo administrado en el que está interesado. Aparecerá una ventana de información.
5. En la sección **Seguridad** de la pestaña **General**, haga clic en el nombre de la política actual para consultar sus ajustes.
6. 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 equipos que tengan la misma política asignada.

   Para obtener más información sobre los ajustes de políticas de equipos, consulte "Políticas de equipos y máquinas virtuales" (p. 238).

Para asignar una política a un equipo o grupo:

1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
4. Marque la casilla de verificación del equipo o grupo que desee. Puede seleccionar uno o varios objetos del mismo tipo solamente desde el mismo nivel.
5. Haga clic en el botón **Asignar política** de la zona superior de la tabla.
6. Haga los ajustes necesarios en la ventana **Asignación de política**. Para más información, diríjase a "Asignando Políticas" (p. 226).

Uso del Gestor de recuperación con volúmenes cifrados

Cuando los usuarios de endpoints olviden sus contraseñas de cifrado y dejen de poder acceder a los volúmenes cifrados de sus máquinas, puede ayudarles obteniendo las claves de recuperación en la página **Red**.

Para obtener una clave de recuperación:

1. Diríjase a la página **Red**.
2. Haga clic en el botón **Gestor de recuperación** en la barra de herramientas de acción del panel de la izquierda. Aparecerá una nueva ventana.
3. En la sección **Identificador** de la ventana, introduzca los siguientes datos:
   a. El ID de la clave de recuperación del volumen cifrado. El ID de la clave de recuperación es una cadena de números y letras disponible en el endpoint, en la pantalla de recuperación de BitLocker.

      En Windows, el ID de la clave de recuperación es una cadena de números y letras disponible en el endpoint, en la pantalla de recuperación de BitLocker.

      Como alternativa, puede usar la opción de **Recuperación** en la pestaña **Protección** de los detalles del equipo para rellenar automáticamente el ID de la clave de recuperación, tanto para los endpoints de Windows como de macOS.

   b. La contraseña de su cuenta de GravityZone.
4. Haga clic en **Mostrar**. La ventana se expande.

   En **Información de volumen** se le presentan los siguientes datos:

   a. Nombre del volumen

   b. Tipo de volumen (de arranque o no).

   c. Nombre del endpoint (como aparece en el inventario de red)

   d. Clave de recuperación. En Windows, la clave de recuperación es una contraseña generada automáticamente cuando se cifra el volumen. En Mac, la clave de recuperación es la contraseña de la cuenta de usuario.
5. Envíe la clave de recuperación al usuario del endpoint.

Para obtener más información sobre el cifrado y descifrado de volúmenes con GravityZone, consulte "Cifrado" (p. 389).

6.2.9. Sincronizar con Active Directory

El inventario de red se sincroniza automáticamente con Active Directory con un intervalo de tiempo especificado en la sección de configuración de Control Center. Para más información, consulte el capítulo Instalación y configuración de GravityZone de la Guía de instalación de GravityZone.

Para sincronizar manualmente con Active Directory el inventario de red mostrado actualmente:

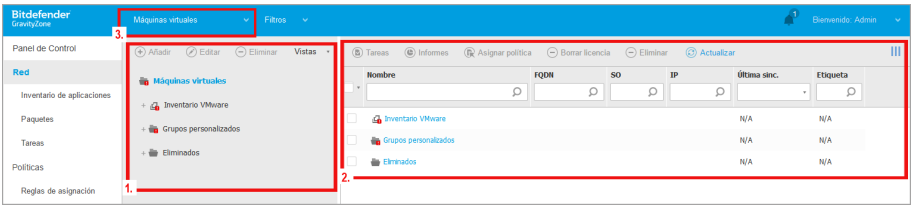
1. Diríjase a la página **Red**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Haga clic en el botón **Sincronizar con Active Directory** de la zona superior de la tabla.
4. Tendrá que confirmar esta acción haciendo clic en **Sí**.

> **Nota**
> En redes grandes con Active Directory, la sincronización puede tardar mucho tiempo en completarse.

6.3. Máquinas virtuales

Para ver la infraestructura virtual de su cuenta, diríjase a la página **Red** y seleccione **Máquinas virtuales** desde el Selector de vistas.

> **Nota**
> Puede administrar máquinas virtuales también desde la vista **Equipos y máquinas virtuales**, pero solo puede ver su infraestructura virtualizada y filtrar su contenido utilizando criterios específicos desde la vista **Máquinas virtuales**.
> Para más información acerca del trabajo con vistas de red, consulte “Trabajar con vistas de red” (p. 45).



La vista Red - Máquinas virtuales

Puede ver las redes de máquinas virtuales disponibles en el panel izquierdo y consultar detalles sobre cada máquina virtual en el panel derecho.

Para personalizar los detalles de la máquina virtual que se muestran en la tabla:

1. Haga clic en el botón **Columnas** de la esquina superior derecha del panel derecho.
2. Seleccione las columnas que desea ver.
3. Haga clic en el botón **Restablecer** para volver a la vista predeterminada de columnas.

El panel del lateral izquierdo muestra una vista con forma de árbol de la infraestructura virtual. La raíz del árbol se llama **Máquinas virtuales** y las máquinas virtuales se agrupan bajo la raíz, según las siguientes categorías basadas en el proveedor de la tecnología de virtualización:

- **Inventario Nutanix.** Contiene la lista de sistemas Nutanix Prism Element a los que tiene acceso.
- **Inventario VMware.** Contiene la lista de servidores vCenter a los que tiene acceso.
- **Inventario Citrix.** Contiene la lista de sistemas XenServer a los que tiene acceso.
- **Grupos personalizados.** Contiene los servidores de seguridad y las máquinas virtuales detectadas en su red fuera de cualquier sistema XenServer o vCenter Server.

El panel del lateral izquierdo también contiene un menú llamado **Vistas** desde donde el usuario puede seleccionar el tipo de vista para cada proveedor de virtualización.

Para acceder a la infraestructura virtualizada integrada con Control Center, debe proporcionar sus credenciales de usuario para cada sistema vCenter Server

disponible. Una vez introducidas las credenciales, se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez. Para más información, diríjase a "Administrador de Credenciales" (p. 219).

Desde la sección **Red** puede administrar las máquinas virtuales de la forma siguiente:

- Comprobar el estado de las máquinas virtuales
- Ver detalles de la máquina virtual
- Organizar las máquinas virtuales en grupos
- Ordenar, filtrar y buscar.
- Ejecutar tareas.
- Crear informes rápidos
- Asignar políticas
- Liberar puestos de licencia

En la sección **Configuración > Ajustes de red**, puede configurar las reglas programadas para la eliminación automática de máquinas virtuales sin uso del inventario de red.

6.3.1. Comprobar el estado de las máquinas virtuales

Las máquinas virtuales están representadas en la página de red mediante el icono correspondiente a su tipo y estado.

Consulte "Tipos y estados de los objetos de red" (p. 525) para ver una lista con todos los tipos de iconos y estados disponibles.

Para obtener información detallada sobre el estado, consulte:

- Estado de administración
- Estado de conexión
- Estado de seguridad

Estado de administración

Las máquinas virtuales pueden tener los siguientes estados de administración:

- **Administradas** - Máquinas virtuales en las que se ha instalado la protección de Bitdefender.
- **Reinicio pendiente** - Máquinas virtuales que requieren un reinicio del sistema después de instalar o actualizar la protección de Bitdefender.

- **No administradas** - máquinas virtuales detectadas en las que no se ha instalado todavía la protección de Bitdefender.
- **Eliminadas**: máquinas virtuales que ha eliminado de Control Center. Para más información, diríjase a "Eliminación de endpoints del inventario de red" (p. 214).

Estado de conexión

El estado de conexión se refiere a los Security Server y máquinas virtuales administradas. Desde este punto de vista, las máquinas virtuales administradas pueden estar:

- **Online**. Un icono azul indica que la máquina está online (conectada).
- **Offline (desconectada)**. Un icono gris indica que la máquina está offline (desconectada).

Una máquina virtual se considera desconectada (offline) si el agente de seguridad permanece inactivo durante más de 5 minutos. Posibles razones por las cuales las máquinas virtuales aparecen offline:

- La máquina virtual está apagada, en suspensión o hibernando.

  Nota
  Las máquinas virtuales aparecen online incluso cuando están bloqueadas o el usuario ha terminado la sesión.

- El agente de seguridad no tiene conexión con el Servidor de comunicaciones de GravityZone:
  - La máquina virtual puede estar desconectada de la red.
  - Un router o un cortafuego de red pueden estar bloqueando la comunicación entre el agente de seguridad y Bitdefender Control Center o el Endpoint Security Relay asignado.
  - La máquina virtual se encuentra detrás de un servidor proxy y los ajustes del proxy no se han configurado correctamente en la política aplicada.

    Aviso
    En el caso de máquinas virtuales detrás de un servidor proxy, los ajustes de éste deben estar configurados correctamente en el paquete de instalación del agente de seguridad, pues de lo contrario la máquina virtual no se comunicará con la consola de GravityZone y siempre aparecerá desconectada

(offline), aunque se aplique una política con los ajustes de proxy adecuados después de la instalación.

- El agente de seguridad se ha desinstalado manualmente de la máquina virtual mientras ésta carecía de conexión con Bitdefender Control Center o con el Endpoint Security Relay asignado. Normalmente, cuando el agente de seguridad se desinstala manualmente de una máquina virtual, se le notifica a Control Center y la máquina virtual se marca como no administrada.
- Puede que el agente de seguridad no esté funcionando adecuadamente.

Para averiguar cuánto tiempo han estado inactivas las máquinas virtuales:

1. Mostrar sólo las máquinas virtuales administradas. Haga clic en el menú **Filtros** situado en la zona superior de la tabla, seleccione en la pestaña **Seguridad** todas las opciones "Administrados" que precise, elija **Todos los elementos recursivamente** en la pestaña **Profundidad** y haga clic en **Guardar**.
2. Haga clic en el encabezado de la columna **Visto última vez** para organizar las máquinas virtuales por periodo de inactividad.

Puede ignorar periodos de inactividad más cortos (minutos, horas) pues probablemente sean resultado de una situación temporal. Por ejemplo, la máquina virtual está actualmente apagada.

Los periodos de inactividad más largos (días, semanas) normalmente indican un problema con la máquina virtual.

Nota
Se recomienda actualizar la tabla de red de vez en cuando para actualizar la información de los endpoints con los últimos cambios.

Estado de seguridad

El estado de seguridad se refiere a los Security Server y máquinas virtuales administradas. Los iconos de estado muestran un símbolo de advertencia que le permite identificar las máquinas virtuales o los Security Server con problemas de seguridad:

- Con problemas.
- Sin problemas.

Una máquina virtual o un Security Server tiene problemas de seguridad siempre que se dé al menos una de las siguientes situaciones:

- La protección antimalware está desactivada (solo para máquinas virtuales).
- Si la licencia ha caducado.
- El producto Bitdefender no está actualizado.
- Los contenidos de seguridad no están actualizados.
- El paquete suplementario HVI no está actualizado.
- Se ha detectado malware (solo para máquinas virtuales).
- No se pudo establecer la conexión con Bitdefender Cloud Services debido a una de las siguientes razones:
  - La máquina virtual tiene problemas de conexión a Internet.
  - Un cortafuego de red bloquea la conexión con Bitdefender Cloud Services.
  - El puerto 443, necesario para la comunicación con Bitdefender Cloud Services, está cerrado.

  En este caso, la protección antimalware se basa únicamente en los motores locales, mientras que el análisis en la nube está desconectado, lo que significa que el agente de seguridad no puede proporcionar protección completa en tiempo real.

Si observa una máquina virtual con problemas de seguridad, haga clic en su nombre para mostrar la ventana **Información**. Puede identificar los problemas de seguridad mediante el icono **!**. Asegúrese de revisar la información de seguridad de todas las pestañas de la página de información. Muestre la información sobre herramientas del icono para conocer más detalles. Puede ser necesaria más investigación local.

Nota
Se recomienda actualizar la tabla de red de vez en cuando para actualizar la información de los endpoints con los últimos cambios.
Los endpoints que no hayan recibido ninguna actualización durante las últimas 24 horas se marcarán automáticamente como **Con problemas**, independientemente de la versión de los contenidos de seguridad presente en el relay o en GravityZone Update Server.

6.3.2. Consulta de los detalles de la máquina virtual

Puede obtener información detallada sobre cada máquina virtual en la página **Red** de la siguiente manera:

- Comprobación de la página **Red**
- Comprobación de la ventana **Información**

Comprobación de la página Red

Para conocer más detalles sobre una máquina virtual, consulte la información disponible en la tabla del panel derecho de la página **Red**.

Puede añadir o eliminar columnas con información de máquinas virtuales haciendo clic en el botón **Columnas** de la esquina superior derecha del panel.

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.

   Todas las máquinas virtuales disponibles en el grupo seleccionado se muestran en la tabla del panel lateral derecho.
4. Puede identificar fácilmente el estado de la máquina virtual consultando el icono correspondiente. Para información detallada, diríjase a "Comprobar el estado de las máquinas virtuales" (p. 109).
5. Consulte la información mostrada en las columnas de la tabla para cada máquina virtual.

   Utilice la fila de encabezado para ir buscando máquinas virtuales concretas mientras escribe, en función de los criterios disponibles:

   - **Nombre**: nombre de la máquina virtual
   - **FQDN**: Nombre de dominio completo que incluye el nombre del host y el del dominio.
   - **SO**: sistema operativo instalado en la máquina virtual.
   - **IP**: dirección IP de la máquina virtual.
   - **Visto por última vez**: fecha y hora en la que la máquina virtual fue vista por última vez conectada.

     Nota
     Es importante supervisar el campo **Visto por última vez** dado que largos periodos de inactividad podrían indicar un problema de comunicación o una máquina virtual desconectada.

   - **Etiqueta**: una cadena personalizada con información adicional sobre el endpoint. Puede añadir una etiqueta en la ventana **Información** de la máquina virtual y luego usarla en las búsquedas.

- **Política**: la política aplicada a la máquina virtual, con un enlace para ver o cambiar los ajustes de esta.

Comprobación de la ventana Información

En el panel derecho de la página **Red**, haga clic en el nombre de la máquina virtual que le interese para mostrar la ventana **Información**. Esta ventana muestra solo los datos disponibles para la máquina virtual seleccionada, agrupados en varias pestañas.

A continuación encontrará la lista exhaustiva de datos que puede hallar en la ventana **Información**, de acuerdo con el tipo de máquina virtual (máquina virtual, instancia de Security Server) y su información de seguridad concreta.

Pestaña General

- Información general de la máquina virtual, como nombre, información FQDN (nombre completo), dirección IP, sistema operativo, infraestructura, grupo padre y estado de conexión actual.

  En esta sección puede asignar una etiqueta a la máquina virtual. Podrá encontrar rápidamente máquinas virtuales con la misma etiqueta y adoptar acciones sobre ellas, independientemente de dónde se encuentren en la red. Para obtener más información sobre el filtrado de máquinas virtuales, consulte "Clasificación, filtrado y búsqueda de máquinas virtuales" (p. 123).

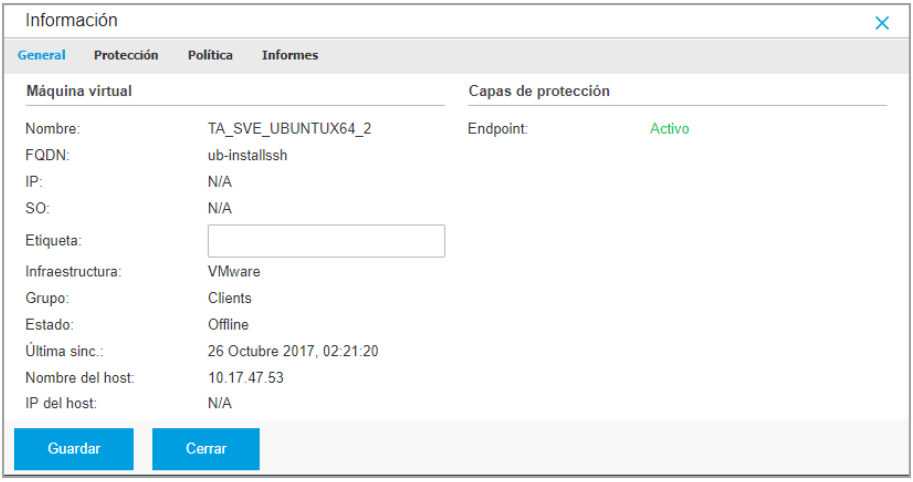
- **Requisitos de HVI**, que contiene información acerca de si puede utilizar el Security Server para implementar la protección HVI o no. Por lo tanto, si el host de Security Server se ejecuta en una versión de XenServer compatible y el paquete suplementario está instalado, puede activar HVI en las máquinas virtuales desde ese host.

- Información sobre las capas de protección, incluida la lista de tecnologías de seguridad adquiridas con su solución GravityZone y su estado de licencia, que puede ser:

  - **Disponible/Activo**: la clave de licencia de esta capa de protección está activa en la máquina virtual.
  - **Caducado**: la clave de licencia de esta capa de traducción ha caducado.
  - **Pendiente**: La clave de licencia no está confirmada aún.

Nota
Hay disponible información adicional sobre las capas de protección en la pestaña **Protección**.

- **Conexión del relay**: el nombre, IP y etiqueta del relay al que está conectado la máquina virtual, si es el caso.



Ventana de Información - pestaña General

Pestaña Protección

Esta pestaña contiene información sobre cada capa de protección con licencia en el endpoint. La información se refiere a:

- Información del agente de seguridad, como el nombre y versión del producto, la configuración de los motores de análisis y el estado de actualización. Para la protección de Exchange, también están disponibles el motor antispam y las versiones de firmas.
- Estado de seguridad para cada capa de protección. Este estado aparece a la derecha del nombre de la capa de protección:
  - **Seguro**, cuando no se ha informado de ningún problema de seguridad en los endpoints a los que se ha aplicado la capa de protección.

  - **Vulnerable**, cuando se ha informado de algún problema de seguridad en los endpoints a los que se ha aplicado la capa de protección. Para obtener más información, consulte "Estado de seguridad" (p. 111).

- Security Server asociado. Cada Security Server asignado se muestra en caso de implementaciones sin agente o cuando los motores de análisis de los agentes de seguridad se configuran para utilizar el análisis remoto. La información del Security Server ayuda a identificar el dispositivo virtual y conocer su estado de actualización.
- Información relacionada con NSX, como el estado de la etiqueta de virus y el grupo de seguridad al que pertenece la máquina virtual. La aplicación de una etiqueta de seguridad indica que la máquina está infectada. De lo contrario, puede que la máquina esté limpia o que no se hayan utilizado etiquetas de seguridad.
- El estado de los módulos de protección. Puede ver fácilmente qué módulos de protección se han instalado en el endpoint, así como el estado de los módulos disponibles (**Activado/Desactivado**) que se ha establecido mediante la política aplicada.
- Una rápida visión de conjunto sobre la actividad de los módulos y los informes de malware de ese día.

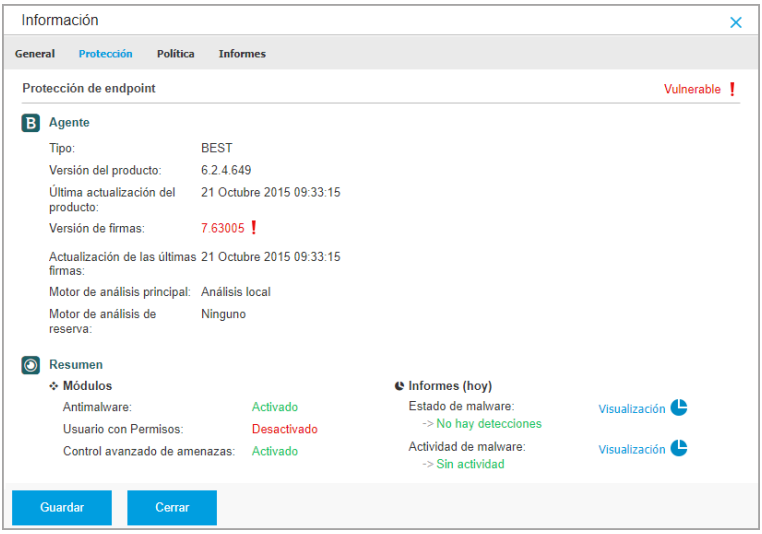
  Haga clic en el enlace **Ver** para acceder a las opciones de informes y, a continuación, generar el informe. Para obtener más información, consulte "Creando Informes" (p. 444).
- Información sobre la capa de protección Sandbox Analyzer:
  - El estado de uso de Sandbox Analyzer en la máquina virtual; se muestra a la derecha de la ventana:
    - **Activo**: Sandbox Analyzer cuenta con licencia (disponible) y se ha activado mediante la política en la máquina virtual.
    - **Inactivo**: Sandbox Analyzer cuenta con licencia (disponible) pero no se ha activado mediante la política en la máquina virtual.
  - Nombre del agente que actúa como sensor de alimentación.
  - Estado del módulo en la máquina virtual:
    - **Activado**: Sandbox Analyzer está activado mediante la política en la máquina virtual.

- **Desactivado**: Sandbox Analyzer no está activado mediante la política en la máquina virtual.

– Detecciones de amenazas durante la última semana, haciendo clic en el enlace **Ver** para acceder al informe.

- Información adicional sobre el módulo de Cifrado, como por ejemplo:
  – Volúmenes detectados (mencionando la unidad de arranque).
  – Estado de cifrado de cada volumen (que puede ser **Cifrado**, **Cifrado en curso**, **Descifrado en curso**, **Sin cifrar**, **Bloqueado** o **En pausa**).

    Haga clic en el enlace **Recuperar** para obtener la clave de recuperación correspondiente al volumen cifrado. Para obtener más información sobre cómo conseguir las claves de recuperación, consulte "Uso del Gestor de recuperación con volúmenes cifrados" (p. 167).



Ventana Información - pestaña Protección

Para Security Server, esta pestaña contiene información sobre el módulo de Protección de almacenamiento. La información se refiere a:

- Estado de servicios:

  - **N/D**: La Protección de almacenamiento cuenta con licencia, pero el servicio aún no está configurado.
  - **Habilitado**: El servicio está habilitado en la política y funciona.
  - **Desactivado**: El servicio no funciona porque se ha desactivado en la política o porque la clave de licencia ha caducado.
- Lista de dispositivos de almacenamiento compatibles con ICAP conectados con los siguientes datos:
  - Nombre del dispositivo de almacenamiento
  - IP del dispositivo de almacenamiento
  - Tipo del dispositivo de almacenamiento
  - The date and time of the last communication between the storage device and Security Server.

Pestaña Protección

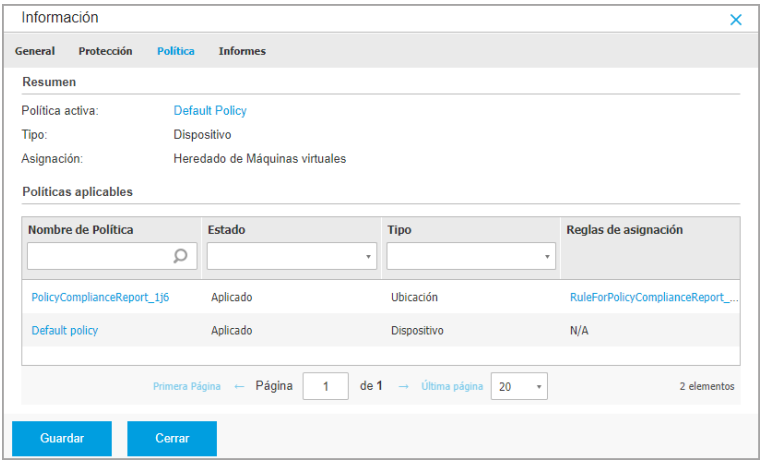
A una máquina virtual se le pueden aplicar una o varias políticas, pero solo una de ellas puede estar activa simultáneamente. La pestaña **Política** muestra información sobre todas las políticas que se aplican a la máquina virtual.

- El nombre de la política activa. Haga clic en el nombre de la política para abrir la plantilla de política y ver sus ajustes.
- El tipo de política activa, que puede ser:
  - **Dispositivo**: cuando el administrador de la red asigna manualmente la política a la máquina virtual.
  - **Ubicación**: una política basada en reglas asignada automáticamente a la máquina virtual si los ajustes de red de la VM cumplen las condiciones dadas de una regla de asignación existente.
  - **Usuario**: una política basada en reglas asignada automáticamente al endpoint si cumple con el objetivo de Active Directory especificado en una regla de asignación existente.

    Por ejemplo, una máquina puede tener asignadas dos políticas en función del usuario: una para los administradores y otra para los demás empleados. Cada una de las políticas se activa cuando el usuario con los privilegios apropiados inicia la sesión.
  - **Externo (NSX)**: cuando la política se define en el entorno VMware NSX.
- El tipo de asignación de política activa, que puede ser:

- **Directo**: cuando la política se aplica directamente a la máquina virtual.
- **Heredado**: cuando la máquina virtual hereda la política de un grupo padre.

- **Políticas aplicables**: muestra la lista de políticas vinculadas a las reglas de asignación existentes. Estas políticas pueden aplicarse a la máquina virtual cuando cumple las condiciones dadas de las reglas de asignación vinculadas.

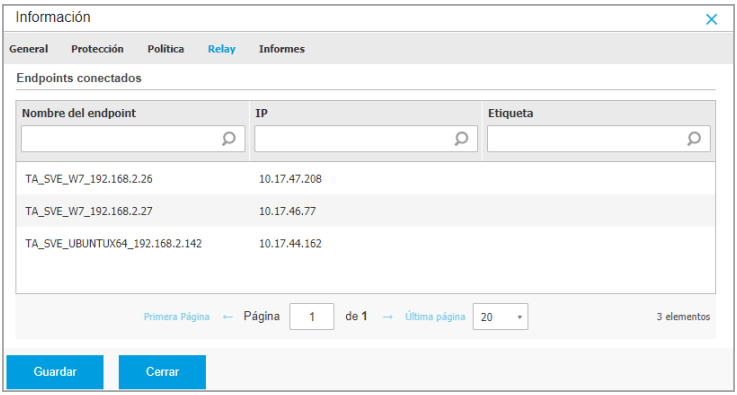


Ventana Información - pestaña Política

Para obtener más información con respecto a las políticas, consulte"Administrando las Políticas" (p. 223)

Pestaña Relay

La pestaña **Relay** solo está disponible para las máquinas virtuales con rol de relay. Esta pestaña muestra información sobre los endpoints conectados al relay actual, como son el nombre, la IP y la etiqueta.



Ventana Información - pestaña Relay

Pestaña Registros de análisis

La pestaña **Registros de análisis** muestra información detallada sobre todas las tareas de análisis ejecutadas en la máquina virtual.

Los registros se agrupan por capa de protección y se puede elegir, en el menú desplegable, de qué capa mostrar los registros.

Haga clic en la tarea de análisis que le interese y se abrirá el registro en una página nueva del navegador.

Cuando hay muchos registros de análisis disponibles, puede que tengan varias páginas. 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.

Ventana Información - pestaña Registros de análisis

Cada propiedad de esta ventana que genere problemas de seguridad se marca con el icono **!**. Consulte el tooltip del icono para conocer más detalles. Puede ser necesaria más investigación local.

6.3.3. Organizar las máquinas virtuales en Grupos

Puede administrar los grupos de máquinas virtuales en el panel lateral izquierdo de la página **Red** bajo la carpeta **Grupos personalizados**.

Las máquinas virtuales importadas desde Nutanix Prism Element se agrupan en la carpeta **Inventario Nutanix**. Las máquinas virtuales importadas desde VMware vCenter se agrupan bajo la carpeta **Inventario VMware**. Las máquinas virtuales importadas desde XenServer se agrupan bajo la carpeta **Inventario Citrix**. No puede editar el inventario de VMware, Citrix o Nutanix. Sólo puede consultar y administrar las máquinas virtuales correspondientes.

La Detección de redes detecta todas las máquinas virtuales que no están administradas por los sistemas vCenter, XenServer o Nutanix Prism y se colocan en **Grupos personalizados**, donde podrá organizarlas en grupos como desee. La ventaja principal es que puede usar las políticas de grupo para cumplir distintos requisitos de seguridad.

Bajo **Grupos personalizados** puede crear, eliminar, renombrar y mover grupos de máquinas virtuales dentro de una estructura de árbol personalizada.

Nota

- Un grupo puede contener tanto máquinas virtuales como otros grupos.
- Cuando selecciona un grupo en el panel lateral izquierdo, puede ver todas las máquinas virtuales excepto las ubicadas en sus subgrupos. Para ver todas las

máquinas virtuales incluidas en el grupo y sus subgrupos, haga clic en el menú **Filtros** situado en la zona superior 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 las máquinas virtuales basándose en solo uno o 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 **Grupos personalizados** en el panel lateral izquierdo.
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**. El nuevo grupo se muestra bajo **Grupos personalizados**.

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 máquinas virtuales

Puede mover entidades a cualquier lugar dentro de la jerarquía de **Grupos personalizados**. Para mover una entidad, arrástrela desde el panel de la derecha y suéltela en el grupo que desee en el de la izquierda.

Nota

La entidad movida heredará los ajustes de políticas del nuevo grupo padre, a no ser que la herencia de políticas se haya desactivado y se haya asignado una política diferente a la entidad. Para obtener más información sobre la herencia de políticas, consulte "Políticas de Seguridad" (p. 222).

Eliminando Grupos

No puede eliminarse un grupo si contiene al menos una máquina virtual. Mueva todas las máquinas virtuales del grupo que quiera eliminar a otros grupos. Si el grupo incluye subgrupos, puede elegir mover los subgrupos completos en lugar de máquinas virtuales individuales.

Para eliminar un grupo:

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

6.3.4. Clasificación, filtrado y búsqueda de máquinas virtuales

Dependiendo del número de máquinas virtuales, la tabla de máquinas virtuales puede ampliarse a varias páginas (solo se muestran de forma predeterminada 20 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 zona superior de la página para mostrar solo las entidades que le interesen. Por ejemplo, puede buscar una máquina virtual específica o elegir ver únicamente las máquinas virtuales administradas.

Ordenar máquinas virtuales

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

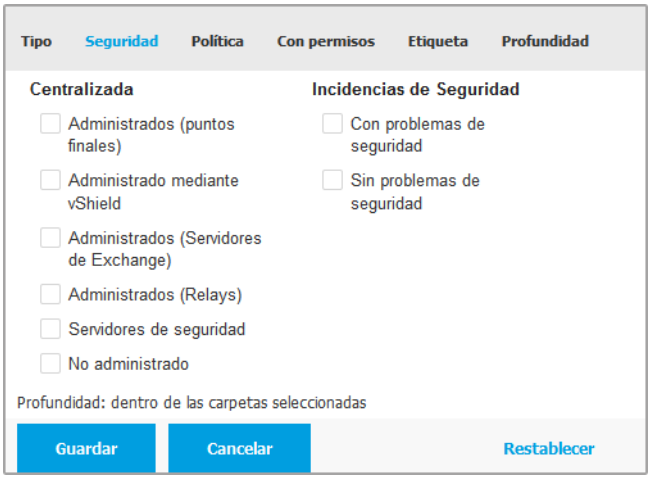
Ordenar equipos

Filtrado de máquinas virtuales

1. Seleccione el grupo que desee en el panel de la izquierda.
2. Haga clic en el menú **Filtros** de la zona superior del área de paneles de red.
3. Use el criterio de filtrado de la siguiente manera:
   - **Tipo**. Seleccione el tipo de entidades virtuales a mostrar.

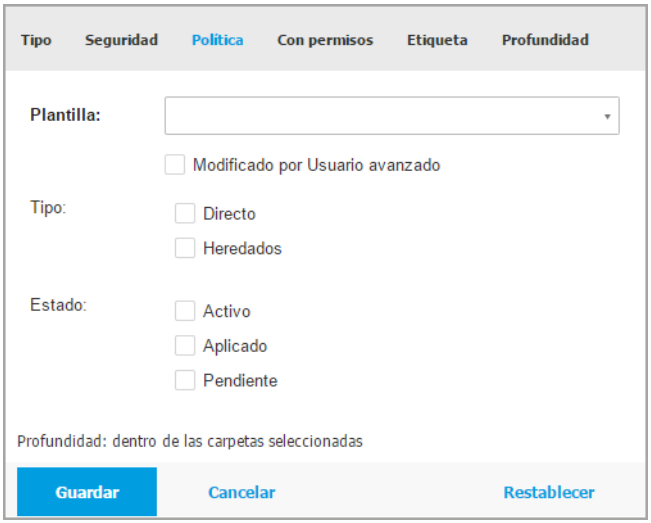
Máquinas virtuales - Filtrar por tipo

   - **Seguridad**. Seleccione el estado de seguridad y/o administración de la protección para filtrar los objetos de red. Por ejemplo, puede elegir ver solo las máquinas Security Server, o únicamente los endpoints con problemas de seguridad.



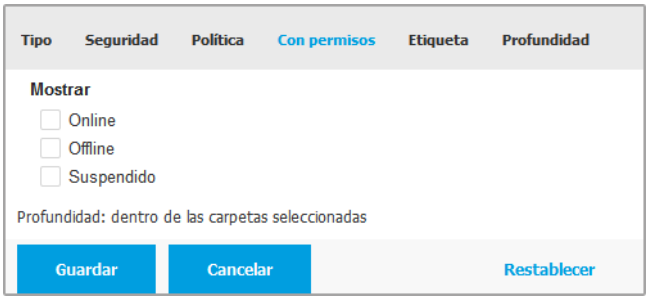
Máquinas virtuales - Filtrar por seguridad

- **Política**. Seleccione la plantilla de política según la cual quiere filtrar las máquinas virtuales, el tipo de asignación de política (directa o heredada), así como el estado de asignación de la política (activo, aplicado o pendiente).



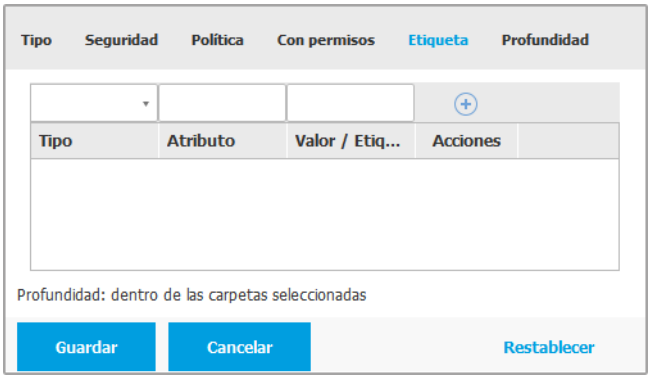
Máquinas virtuales - Filtrar por política

- **ON-OFF**. Puede optar entre mostrar máquinas virtuales conectadas, desconectadas y suspendidas.



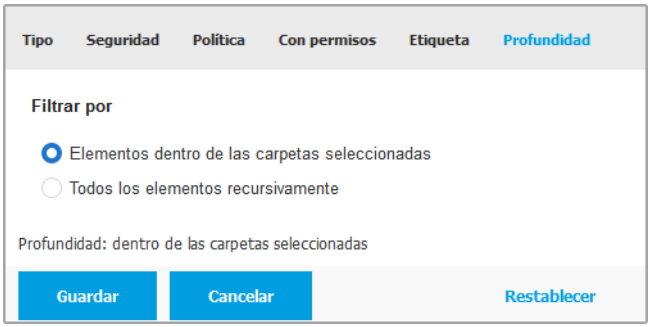
Máquinas virtuales - Filtrar por encendida

- **Etiquetas**. Puede escoger filtrar las máquinas virtuales por las etiquetas y atributos que haya definido en su entorno de virtualización.



Máquinas virtuales - Filtrar por etiquetas

- **Profundidad**. Cuando administra una red de máquinas virtuales con estructura de árbol, por omisión no se muestran las máquinas virtuales incluidas en subgrupos. Seleccione **Todos los elementos recursivamente** para ver todas las máquinas virtuales incluidas en el grupo actual y en sus subgrupos.



Máquinas virtuales - Filtrar por profundidad

Nota
Haga clic en **Restablecer** para borrar el filtro y mostrar todas las máquinas virtuales.

4. Haga clic en **Guardar** para filtrar las máquinas virtuales por el criterio seleccionado.

Buscar máquinas virtuales

1. Seleccione el contenedor deseado en 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 de la máquina virtual que está consultando en el campo **IP**. Sólo aparecerá en la tabla la máquina virtual coincidente.

   Vacíe el cuadro de búsqueda para mostrar la lista completa de máquinas virtuales.

6.3.5. Ejecución de tareas en máquinas virtuales

Desde la página **Red** puede ejecutar de forma remota un determinado número de tareas administrativas en las máquinas virtuales.

Esto es lo que puede hacer:

- “Analizar” (p. 129)
- “Tareas de parches” (p. 139)
- “Análisis de Exchange” (p. 142)
- “Instalar” (p. 147)
- “Desinstalar cliente” (p. 151)
- “Actualizar” (p. 152)
- “Reconfigurar cliente” (p. 153)
- “Descubrimiento de red” (p. 155)
- “Detección de aplicaciones” (p. 155)
- “Reiniciar máquina” (p. 156)
- “Instalar Security Server” (p. 157)
- “Desinstalar Security Server” (p. 160)
- “Actualizar Security Server” (p. 160)
- “Instalar el paquete suplementario de HVI” (p. 161)
- “Desinstalar el paquete suplementario de HVI” (p. 162)
- “Actualizar el paquete suplementario de HVI” (p. 163)

Puede elegir crear tareas individuales para cada máquina virtual o para grupos de máquinas virtuales. Por ejemplo, puede instalar de forma remota Bitdefender Endpoint Security Tools en un grupo de máquinas virtuales no administradas. En

otro momento posterior, puede crear una tarea de análisis para una determinada máquina virtual del mismo grupo.

Para cada máquina virtual, sólo puede ejecutar tareas compatibles. Por ejemplo, si selecciona una máquina virtual no administrada, solo puede elegir instalar el agente de seguridad; todas las demás tareas aparecen desactivadas.

Para un grupo, la tarea seleccionada se creará únicamente para las máquinas virtuales compatibles. Si ninguna de las máquinas virtuales en el grupo es compatible con la tarea seleccionada, se le notificará que la tarea no pudo crearse.

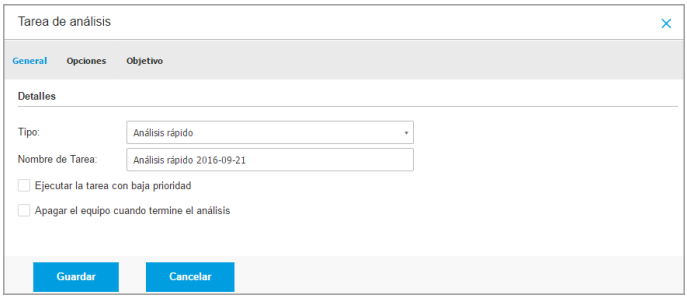
Una vez creada, la tarea se iniciará inmediatamente en las máquinas virtuales conectadas. Si una máquina virtual no está conectada, la tarea se ejecutará tan pronto como vuelva a conectarse.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Analizar

Para ejecutar de forma remota una tarea de análisis en una o varias máquinas virtuales:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.
4. Marque las casillas de verificación correspondientes a los objetos que desea analizar.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Analizar**. Aparecerá una nueva ventana de configuración.
6. 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 sirve para ayudarle a identificar fácilmente el análisis actual en la página **Tareas**.



Tarea de análisis de máquinas virtuales - Configuración de ajustes generales

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

- **Quick Scan** está preconfigurado para analizar únicamente ubicaciones vitales del sistema y nuevos archivos. 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.

  Cuando se encuentran rootkits o malware, Bitdefender procede automáticamente a la desinfección. Si por alguna razón no se pudiese desinfectar el archivo, este se trasladará a la cuarentena. Este tipo de análisis ignora los archivos sospechosos.

- **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.

  Bitdefender trata automáticamente de desinfectar los archivos en los que se ha detectado malware. En caso de que no se pueda eliminar el malware, se recluye en la cuarentena, donde no puede causar ningún daño. Los archivos sospechosos se ignoran. Si quiere actuar también sobre los archivos sospechosos, o si desea escoger otras acciones por defecto para los archivos infectados, efectúe un Análisis personalizado.

- **Análisis de memoria** comprueba los programas que se ejecutan en la memoria de la máquina virtual.

- El **Análisis de red** es un tipo de análisis personalizado que permite analizar unidades de red utilizando el agente de seguridad de Bitdefender instalado en la máquina virtual objetivo.

  Para que funcione la tarea de análisis de red:

- Tiene que asignar la tarea a un solo endpoint de su red.
- Ha de introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red objetivo para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red. Las credenciales requeridas se pueden configurar en la pestaña **Objetivo** de la ventana de tareas.

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

Para los análisis de memoria, red y personalizados, dispone también de estas opciones:

– **Ejecutar la tarea con baja prioridad**. Marque esta casilla de verificación para disminuir la prioridad del proceso de análisis y permitir que otros programas se ejecuten más rápido. Esto aumentará el tiempo necesario para que finalice el proceso de análisis.

> **Nota**
> Esta opción se aplica solo a Bitdefender Endpoint Security Tools y Endpoint Security (agente antiguo).

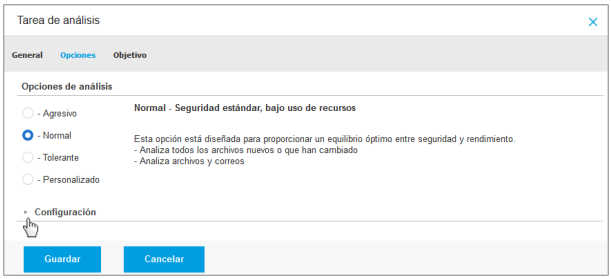
– **Apagar el equipo cuando termine el análisis**. Marque esta casilla de verificación para apagar su máquina si no va a utilizarla durante un tiempo.

> **Nota**
> Esta opción se aplica a Bitdefender Endpoint Security Tools, Endpoint Security (agente antiguo) y Endpoint Security for Mac.

Para análisis personalizados, configure los siguientes ajustes:

– Acceda 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, seleccione la opción **Personalizado** y despliegue la sección **Ajustes**.



Tarea de análisis de máquinas virtuales - Configuración de un análisis personalizado

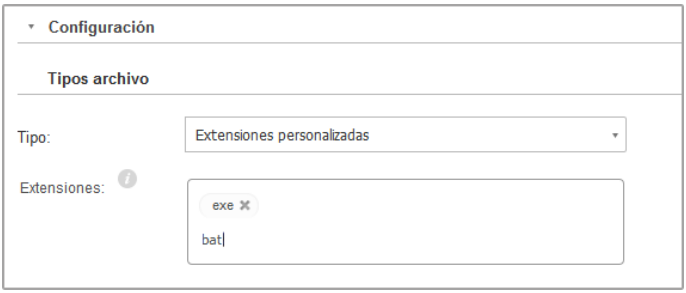
Tiene las siguientes opciones a su disposición:

- **Tipos archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede ajustar el agente de seguridad para analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación 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 "Tipos de archivos de aplicación" (p. 527).

  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.

  Importante
  Los agentes de seguridad de Bitdefender instalados en los sistemas operativos Windows y Linux analizan la mayoría de los formatos .ISO, pero no llevan a cabo ninguna acción sobre ellos.



Opciones de tarea de análisis de máquinas virtuales - 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. No obstante, se recomienda analizar los archivos empaquetados con el fin de detectar y eliminar cualquier amenaza potencial, incluso aunque no se trate de una amenaza inmediata.

  Importante
  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.

  Importante
  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 de máquina virtual 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. Los keyloggers no son aplicaciones maliciosas en sí mismas, pero se pueden utilizar con intenciones maliciosas. El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.
  - **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 las máquinas virtuales.
- **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.
- **Análisis de dispositivos extraíbles.** Seleccione esta opción para analizar cualquier unidad de almacenamiento extraíble conectada a la máquina virtual.

- **Acciones.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
  - **Al encontrar un archivo infectado.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA). El agente de seguridad de Bitdefender 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, el agente de seguridad de Bitdefender 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 se detectan como sospechosos mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos). 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.

Cuando se encuentra un virus en una máquina virtual NSX, Security Server la marca automáticamente con una etiqueta de seguridad, siempre y cuando se haya seleccionado esta opción en la integración de vCenter Server.

A tal fin, NSX incluye tres etiquetas de seguridad, según la gravedad de la amenaza:

- `ANTI_VIRUS.VirusFound.threat=low`, se aplica a la máquina cuando Bitdefender encuentra malware de bajo riesgo, que puede eliminar.

- `ANTI_VIRUS.VirusFound.threat=medium`, se aplica a la máquina si Bitdefender no puede eliminar los archivos infectados, pero sí desinfectarlos.
- `ANTI_VIRUS.VirusFound.threat=high`, se aplica a la máquina si Bitdefender no puede ni eliminar ni desinfectar los archivos infectados, pero sí bloquear el acceso a ellos.

Puede aislar las máquinas infectadas mediante la creación de grupos de seguridad con pertenencia dinámica en función de las etiquetas de seguridad.

Importante

- Si Bitdefender encuentra amenazas de diferentes niveles de gravedad en una máquina, aplicará todas las etiquetas correspondientes.
- Una etiqueta de seguridad solo se elimina de una máquina después de que se realice un análisis completo y la máquina haya sido desinfectada.

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 las máquinas virtuales objetivo.

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 todas las máquinas virtuales. Para obtener más información respecto a las variables del sistema, consulte "Variables del sistema" (p. 529).

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

Para editar una ubicación existente, haga clic en ella. Para eliminar una ubicación de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente.

Para las tareas de análisis de red, tiene que introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red objetivo, para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red.

Haga clic en la sección **Excepciones** si desea definir excepciones de objetivos.

Tarea de análisis de máquinas virtuales - 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. 293).

7. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Nota
Para programar una tarea de análisis, acceda a la página **Políticas**, seleccione la política asignada a las máquinas virtuales en las que está interesado, y añada una tarea de análisis en la sección **Antimalware > Bajo demanda**. Para más información, diríjase a "Bajo demanda" (p. 272).

Tareas de parches

Se recomienda comprobar regularmente las actualizaciones de software y aplicarlas lo antes posible. GravityZone automatiza este proceso a través de políticas de seguridad, pero si necesita actualizar el software inmediatamente en ciertas máquinas virtuales, ejecute las siguientes tareas por este orden:

1. Análisis de parches
2. Instalación de parches

Requisitos

- El agente de seguridad con el módulo de Administración de parches está instalado en las máquinas objetivo.
- Para que las tareas de análisis e instalación tengan éxito, las máquinas Windows deben cumplir estas condiciones:
  - Las **entidades de certificación raíz de confianza** almacenan el certificado **DigiCert Assured ID Root CA**.
  - Las **entidades de certificación intermedias** incluyen **DigiCert SHA2 Assured ID Code Signing CA**.
  - Los endpoints han instalado los parches para Windows 7 y Windows Server 2008 R2 mencionados en este artículo de Microsoft: Aviso de seguridad de Microsoft 3033929

Análisis de parches

Las máquinas virtuales con software obsoleto son vulnerables a los ataques. Se recomienda comprobar regularmente el software instalado en sus máquinas virtuales y actualizarlo lo antes posible. Para analizar sus máquinas virtuales en busca de parches que falten:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione los endpoints objetivo.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Análisis de parches**. Aparecerá una ventana de configuración.
6. Haga clic en **Sí** para crear la tarea de análisis.

   Cuando la tarea finaliza, GravityZone añade al Inventario de parches todos los que su software necesita. Para obtener más información, consulte “Inventario de parches” (p. 201).

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a “Ver y administrar tareas” (p. 210).

Nota
Para programar el análisis de parches, edite las políticas asignadas a las máquinas virtuales objetivo y configure los ajustes en la sección **Administración de parches**. Para más información, diríjase a "Administración de parches" (p. 341).

Instalación de parches

Para instalar uno o más parches en las máquinas virtuales objetivo:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Instalación de parches**.

   Aparecerá una nueva ventana de configuración. Aquí puede ver todos los parches que faltan en las máquinas virtuales objetivo.
5. Si es necesario, use las opciones de clasificación y filtrado de la parte superior de la tabla para encontrar parches concretos.
6. Haga clic en el botón **Columnas** de la esquina superior derecha del panel para ver solo la información relevante.
7. Seleccione los parches que desea instalar.

   Ciertos parches dependen de otros. En tal caso, se seleccionan automáticamente con el parche.

   Al hacer clic en los números de **CVE** o de **Productos,** se mostrará un panel en el lado izquierdo. Dicho panel contiene información adicional, como por ejemplo las CVE que resuelve el parche o los productos a los que se aplica. Cuando termine de leer, haga clic en **Cerrar** para ocultar el panel.
8. Seleccione **En caso necesario, reiniciar los endpoints después de instalar el parche** para reiniciar los endpoints inmediatamente después de la instalación del parche, en caso de que sea necesario reiniciar el sistema. Tenga en cuenta que esta acción puede interrumpir la actividad del usuario.
9. Haga clic en **Instalar**.

Se crea la tarea de instalación junto con las subtareas para cada máquina virtual objetivo.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Nota

- Para programar la implementación de parches, edite las políticas asignadas a las máquinas virtuales objetivo y configure los ajustes en la sección **Administración de parches**. Para más información, diríjase a "Administración de parches" (p. 341).
- Asimismo, puede instalar un parche desde la página **Inventario de parches**, a partir de un cierto parche que le interese. En tal caso, seleccione el parche de la lista, haga clic en el botón **Instalar** en la parte superior de la tabla y configure los detalles de instalación del parche. Para obtener más información, consulte "Instalación de parches" (p. 205).
- Tras instalar un parche, recomendamos enviar una tarea de Análisis de parches a los endpoints objetivo. Dicha acción actualizará la información del parche almacenada en GravityZone para sus redes administradas.

Puede desinstalar parches:

- De forma remota, enviando una tarea de Desinstalación de parche desde GravityZone.
- Localmente en la máquina. En tal caso, debe iniciar sesión como administrador en el endpoint y ejecutar el desinstalador manualmente.

Análisis de Exchange

Puede analizar de forma remota la base de datos de un servidor de Exchange mediante la ejecución de una tarea **Análisis de Exchange**.

Para poder analizar la base de datos de Exchange, debe habilitar el análisis bajo demanda proporcionando las credenciales de un administrador de Exchange. Para más información, diríjase a "Análisis del almacén de Exchange" (p. 366).

Para analizar una base de datos de servidor de Exchange:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. En el panel de la izquierda, seleccione el grupo que contiene el servidor de Exchange objetivo. Puede encontrar el servidor en el panel de la derecha.

Nota
Opcionalmente, puede aplicar filtros para encontrar rápidamente el servidor objetivo:
- Haga clic en el menú **Filtros** y seleccione las siguientes opciones: **Administrados (Servidores de Exchange)** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.
- Introduzca el nombre de host del servidor o su IP en los campos de los encabezados de las columnas correspondientes.

4. Marque la casilla de verificación del servidor de Exchange cuya base de datos quiera analizar.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y elija **Análisis de Exchange**. Aparecerá una nueva ventana de configuración.
6. Configure las opciones de análisis:
   - **General.** Escriba un nombre descriptivo para la tarea.

     Con bases de datos grandes, la tarea de análisis puede tardar mucho tiempo y es posible que afecte al rendimiento del servidor. En tales casos, marque la casilla de verificación **Detener el análisis si tarda más de** y seleccione un intervalo de tiempo oportuno en los menús correspondientes.
   - **Objetivo.** Seleccione los contenedores y objetos que desea analizar. Puede optar por analizar los buzones, las carpetas públicas o ambos. Además de los correos electrónicos, puede optar por analizar otros objetos como **Contactos**, **Tareas**, **Citas** y **Elementos para exponer**. Además, puede establecer las siguientes restricciones a los contenidos que se analizarán:
     – Solo los mensajes no leídos.
     – Solo los elementos con adjuntos.
     – Solo los elementos nuevos recibidos en un intervalo de tiempo determinado.

     Por ejemplo, puede elegir analizar solo los mensajes de correo electrónico de los buzones de los usuarios recibidos en los últimos siete días.

     Marque la casilla de verificación **Exclusiones** si desea definir excepciones de análisis. Para crear una excepción, utilice los campos del encabezado de la tabla de la siguiente manera:
     a. Seleccione el tipo de repositorio en el menú.
     b. Dependiendo del tipo de repositorio, indique el objeto que haya que excluir:

Tipo de repositorio	Formato de objeto
Buzón de Correo	Dirección de correo:
Carpeta pública	Ruta de la carpeta, a partir de la raíz
Base de Datos	La identidad de la base de datos

Nota
Para obtener la identidad de la base de datos, utilice el comando shell de Exchange:
```
Get-MailboxDatabase | fl name,identity
```

Solo puede indicar los elementos uno a uno. Si tiene varios elementos del mismo tipo, debe definir tantas reglas como elementos tenga.

c. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para guardar la excepción y añadirla a la lista.

Para eliminar una regla de excepción de la lista, haga clic en el botón ⊖ **Eliminar** correspondiente.

- **Opciones.** Configure las opciones de análisis para mensajes de correo electrónico que cumplan la regla:
  - **Tipos de archivos analizados.** Utilice esta opción para especificar los tipos de archivo que desee analizar. Puede optar por analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación o extensiones de archivo concretas que considere peligrosas. Analizar todos los archivos aporta la mayor protección, mientras que se recomienda analizar solo las aplicaciones para 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 "Tipos de archivos de aplicación" (p. 527).

    Si desea analizar solo los archivos con determinadas extensiones, tiene dos alternativas:
    - **Extensiones definidas por el usuario**, donde debe proporcionar solo las extensiones que se analizarán.
    - **Todos los archivos, excepto extensiones concretas**, donde debe introducir solo las extensiones que no se analizarán.

- **Tamaño máximo del adjunto/cuerpo del mensaje (MB).** Marque esta casilla de verificación e introduzca un valor en el campo correspondiente para establecer el tamaño máximo aceptado de un archivo adjunto o del cuerpo del mensaje de correo electrónico que se va a analizar.
- **Profundidad de archivo máxima (niveles).** Marque la casilla de verificación y elija la profundidad máxima del archivo comprimido en el campo correspondiente. Cuanto menor sea el nivel de profundidad, mayor será el rendimiento, pero menor el grado de protección.
- **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Marque esta casilla de verificación para buscar aplicaciones maliciosas o potencialmente no deseadas, como por ejemplo adware, que pueden instalarse en los sistemas sin el consentimiento del usuario, cambiar el comportamiento de diversos productos de software y reducir el rendimiento del sistema.

- **Acciones.** Puede especificar diferentes acciones para que el agente de seguridad las aplique automáticamente a los archivos, en función del tipo de detección.

  El tipo de detección divide los archivos en tres categorías:
  - **Archivos infectados.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA).
  - **Archivos sospechosos.** Estos archivos se detectan mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos).
  - **Archivos no analizables.** Estos archivos no se pueden analizar. Los archivos que no se pueden analizar incluyen, pero no se limitan, a los archivos protegidos con contraseña, cifrados o sobrecomprimidos.

  Para cada tipo de detección, dispone de una acción por defecto o principal y de una acción alternativa por si falla la principal. Aunque no es recomendable, puede cambiar estas acciones mediante los menús correspondientes. Elija la acción a adoptar:
  - **Desinfectar.** Elimina el código de malware de los archivos infectados y reconstruye el archivo original. Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. Se recomienda siempre mantener esta como la primera acción

a aplicar en los archivos infectados. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.
- **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Eliminar archivo.** Elimina los archivos adjuntos problemáticos sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Reemplazar archivo.** Elimina los archivos problemáticos e inserta un archivo de texto que comunica al usuario las acciones adoptadas.
- **Mover archivo a la cuarentena.** Mueve los archivos detectados a la carpeta de cuarentena e inserta un archivo de texto que comunica al usuario las acciones adoptadas. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de la cuarentena desde la página **Cuarentena**.

  Nota
  Tenga en cuenta que la cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad. El tamaño de la cuarentena depende del número de elementos almacenados y de su tamaño.

- **No realizar ninguna acción.** No se realizará ninguna acción sobre los archivos detectados. Estos archivos solo aparecerán en el log de análisis. 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.
- Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

7. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Instalar

Para proteger sus máquinas virtuales con Security for Virtualized Environments, debe instalar el agente de seguridad de Bitdefender en cada una de ellas. El agente de seguridad de Bitdefender administra la protección en las máquinas virtuales. También se comunica con Control Center para recibir los comandos del administrador y enviar los resultados de sus acciones. Una vez que haya instalado un agente de seguridad de Bitdefender en una red, éste detectará las máquinas virtuales sin protección en esa red. La protección de Security for Virtualized Environments puede instalarse en esas máquinas virtuales de forma remota desde Control Center. La instalación remota se ejecuta en segundo plano, sin que el usuario lo perciba.

En redes aisladas que carecen de conexión directa con el appliance GravityZone, puede instalar el agente de seguridad con rol de relay. En tal caso, la comunicación entre el appliance GravityZone y los demás agentes de seguridad se efectuará a través del agente de relay, que actuará también como servidor de actualizaciones local para los agentes de seguridad que protegen la red aislada.

Nota
Se recomienda que la máquina en que instale el agente de relay esté siempre encendida.

Aviso
Antes de realizar la instalación, asegúrese de desinstalar software antimalware y cortafuego ya existente en las máquinas virtuales. Instalar la protección de Bitdefender sobre software de seguridad existente puede afectar al funcionamiento y causar problemas importantes en 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 Virtualized Environments en una o varias máquinas virtuales:

1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.
3. Seleccione **Máquinas virtuales** desde el selector de vistas.
4. Seleccione el contenedor que desee del 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 las máquinas no administradas. Haga clic en el menú **Filtros** y seleccione las siguientes opciones: **No administrados** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.

5. Seleccione las entidades (máquinas virtuales, hosts, clusters o grupos) en las que desee instalar la protección.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Instalar > BEST**.

   El asistente de **Instalar cliente** se está mostrando.

Instalación de Bitdefender Endpoint Security Tools desde el menú Tareas

7. En la sección **Opciones**, configure 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.

8. Si quiere que los endpoints objetivo se reinicien automáticamente para completar la instalación, seleccione **Reiniciar automáticamente (si es necesario)**.
9. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los endpoints objetivo. Puede añadir las credenciales escribiendo el usuario y contraseña para 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 Bitdefender Endpoint Security Tools en los endpoints.

   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 del encabezado de la tabla de credenciales. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta.

      Si las máquinas están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

      Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

      - Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
      - Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

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

> **Nota**
> Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez. Para acceder al Gestor de credenciales, haga clic en su nombre de usuario en la esquina superior derecha de la consola.

> **Importante**
> Si las credenciales proporcionadas no son válidas, la implementación del cliente fallará en los endpoints correspondientes. Asegúrese de actualizar las credenciales del SO introducidas en el Gestor de credenciales cuando éstas cambien en los endpoints objetivo.

c. Marque las casillas de verificación correspondientes a las cuentas que desee usar.

10. En la sección **Implementador**, seleccione la entidad a la que se conectarán las máquinas objetivo para instalar y actualizar el cliente:

- **Appliance GravityZone**, cuando las máquinas se conectan directamente al appliance GravityZone.

  En este caso, también puede definir un Servidor de comunicaciones personalizado introduciendo su IP o nombre de host, de ser necesario.

- **Endpoint Security Relay**, si desea conectar las máquinas a un cliente de relay instalado en su red. Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla que se muestra a continuación. Seleccione la máquina de relay que desee. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.

> **Importante**
> - El puerto 7074 debe estar abierto para que funcione la implementación mediante el agente de relay.
> - Para implementar el agente a través de un relay de Linux, deben cumplirse las siguientes condiciones:
>   - El endpoint de relay debe tener instalado el paquete Samba (`smbclient`) versión 4.1.0 o superior y el comando/binario `net` para poder implementar agentes de Windows.

Nota
El comando/binario `net` viene generalmente con los paquetes samba-client o samba-common. En algunas distribuciones de Linux (como CentOS 7.4), el comando `net` solo se instala cuando se instala la suite completa de Samba (Common + Client + Server). Asegúrese de que su endpoint de relay disponga del comando `net`.

- Los endpoints de Windows objetivo deben tener habilitados el Recurso compartido de red y el Recurso compartido administrativo.
- Los endpoints objetivo de Linux y Mac deben tener habilitado SSH y el cortafuego desactivado.

11. Tiene que seleccionar un paquete de instalación para la implementación actual. Haga clic en la lista **Usar paquete** y seleccione el paquete de instalación que desee. Aquí puede encontrar todos los paquetes de instalación creados anteriormente para su empresa.
12. Si es necesario, puede modificar algunos de los ajustes del paquete de instalación seleccionado haciendo clic en el botón **Personalizar** junto al campo **Usar paquete**.

    Abajo aparecerán los ajustes del paquete de instalación y puede hacer los cambios que precise. Para más información sobre la modificación de los paquetes de instalación, consulte la Guía de instalación de GravityZone.

    Aviso
    Tenga en cuenta que el módulo de Cortafuego solo está disponible para estaciones de trabajo Windows.

    Si desea guardar las modificaciones como un paquete nuevo, seleccione la opción **Guardar como paquete**, situada en la parte inferior de la lista de ajustes de paquetes, e introduzca un nombre para el nuevo paquete de instalación.
13. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Desinstalar cliente

Para desinstalar de forma remota la protección de Bitdefender:

1. Diríjase a la página **Red**.

2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Seleccione las casillas de verificación correspondientes a las máquinas virtuales de las que desee desinstalar el agente de seguridad de Bitdefender.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Desinstalar el cliente**.
6. Se muestra una ventana de configuración que le permite hacer los siguientes ajustes:
   - Puede optar por conservar los elementos en la cuarentena de la máquina cliente.
   - En el caso de entornos integrados vShield, debe seleccionar las credenciales necesarias para cada máquina, pues de lo contrario fallará la desinstalación. Seleccione **Usar credenciales para integración vShield** y, a continuación, marque todas las credenciales apropiadas en la tabla del Gestor de credenciales que se muestra debajo.
7. 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 "Ver y administrar tareas" (p. 210).

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

Actualizar

Consulte el estado de las máquinas virtuales periódicamente. Si observa una máquina virtual con problemas de seguridad, haga clic en su nombre para mostrar la página **Información**. Para más información, diríjase a "Estado de seguridad" (p. 111).

Los clientes obsoletos o los contenidos de seguridad sin actualizar representan problemas de seguridad. En estos casos, debería ejecutar una actualización del cliente en las máquinas virtuales correspondientes. Esta tarea puede realizarse localmente desde la máquina virtual, o bien de forma remota desde Control Center.

Para actualizar el cliente y los contenidos de seguridad de forma remota en máquinas virtuales administradas:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de las máquinas virtuales donde quiera realizar la actualización del cliente.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar**. Aparecerá una nueva ventana de configuración.
6. Puede optar por actualizar solo el producto, solo los contenidos de seguridad o ambos.
7. En el caso de máquinas integradas con vShield o con el sistema operativo Linux, es obligatorio seleccionar también las credenciales necesarias. Marque la opción **Usar credenciales para integración vShield** y, a continuación, seleccione las credenciales apropiadas en la tabla del Gestor de credenciales que se muestra a continuación.
8. 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 "Ver y administrar tareas" (p. 210).

Reconfigurar cliente

Los módulos de protección del agente de seguridad, los roles y los modos de análisis se configuran inicialmente en el paquete de instalación. Después de que haya instalado el agente de seguridad en su red, puede cambiar en cualquier momento los ajustes iniciales mediante el envío de una tarea remota **Reconfigurar el cliente** a los endpoints administrados que le interesen.

Aviso
Tenga en cuenta que la tarea **Reconfigurar el cliente** sobrescribe todos los ajustes de instalación y no se conserva ninguno de los ajustes iniciales. Al usar esta tarea, asegúrese de volver a configurar todos los ajustes de instalación de los endpoints objetivo.

Para cambiar los ajustes de instalación de una o varias máquinas virtuales:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de las máquinas virtuales a las que desea cambiar los ajustes de instalación.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reconfigurar el cliente**.
6. En la sección **General**, configure el momento en que se ejecutará la tarea:
   - **Ahora**, para poner en marcha la tarea de inmediato.
   - **Programado**, para configurar el intervalo de recurrencia de la tarea. 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 también se requiere la ejecución de otros procesos importantes en la máquina objetivo, puede programar que la tarea se ejecute cada dos horas. La tarea se lanzará en las máquinas objetivo cada dos horas hasta que culmine correctamente.

7. Configure los módulos, roles y modos de análisis del endpoint objetivo como desee. Para más información, consulte la Guía de instalación de GravityZone.

   Aviso
   - Solo se instalarán los módulos soportados por cada sistema operativo.

     Tenga en cuenta que el módulo de Cortafuego solo está disponible para estaciones de trabajo Windows.
   - Bitdefender Tools (agente antiguo) solo es compatible con el análisis centralizado.

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 "Ver y administrar tareas" (p. 210).

Descubrimiento de red

Solo los agentes de seguridad con rol de relay realizan automáticamente la detección de redes. Si no tiene un agente de relay instalado en su red, tendrá que enviar manualmente una tarea de detección de redes desde un endpoint protegido.

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

Importante
Si utiliza un relay de Linux para detectar otros endpoints de Linux o Mac, debe instalar Samba en los endpoints objetivo, o incorporarlos a Active Directory y utilizar DHCP. De esta forma, NetBIOS se configurará automáticamente para ellos.

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque la casilla de verificación correspondiente a la máquina con la que quiere llevar a cabo la detección de redes.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Detección de redes**.
6. 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 "Ver y administrar tareas" (p. 210).

Detección de aplicaciones

Para detectar las aplicaciones en su red:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las máquinas virtuales del contenedor seleccionado se muestran en la tabla del panel lateral derecho.

4. Seleccione las máquinas virtuales en las que desea realizar la detección de aplicaciones.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Detección de aplicaciones**.

> **Nota**
> Bitdefender Endpoint Security Tools con Control de aplicaciones debe estar instalado y activado en las máquinas virtuales. De lo contrario, la tarea estará en gris. Cuando un grupo seleccionado contiene tanto objetivos válidos como no válidos, la tarea se enviará solo a los endpoints válidos.

6. Haga clic en **Sí** en la ventana de confirmación para continuar.

Las aplicaciones y procesos detectados se muestran en la página **Red > Inventario de aplicaciones**. Para más información, diríjase a "Inventario de aplicaciones" (p. 196).

> **Nota**
> La tarea de **Detección de aplicaciones** puede tardar cierto tiempo, dependiendo del número de aplicaciones instaladas. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Reiniciar máquina

Puede elegir reiniciar de forma remota las máquinas virtuales administradas.

> **Nota**
> Consulte la página **Red > Tareas** antes de reiniciar determinadas máquinas virtuales. Las tareas creadas previamente pueden estar todavía en proceso en las máquinas objetivo.

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las entidades del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación correspondientes a las máquinas virtuales que quiere reiniciar.

5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reiniciar máquina**.
6. Seleccione la opción reiniciar programación:
   - Seleccione **Reiniciar ahora** para reiniciar las máquinas virtuales inmediatamente.
   - Seleccione **Reiniciar el** y use los campos inferiores para programar el reinicio en la fecha y hora deseadas.
7. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

   Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte Ver y administrar tareas.

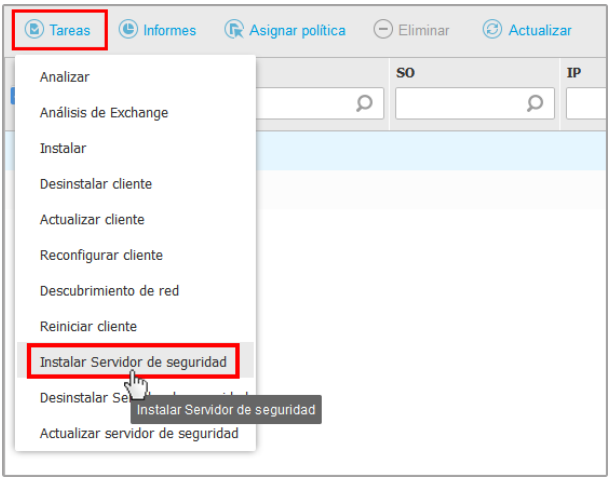
Instalar Security Server

Para instalar un Security Server en su entorno virtual:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Examine el inventario de Nutanix, Citrix o VMware y marque las casillas de selección correspondientes a los contenedores o hosts deseados (Nutanix Prism, vCenter Server, XenServer o centro de datos). Para una selección rápida, puede escoger directamente el contenedor raíz (inventario de VMware, Nutanix o Citrix). Podrá seleccionar hosts individualmente en el asistente de instalación.

   Nota
   No puede seleccionar los hosts de distintas carpetas.

4. Haga clic en el botón **Tareas** de la parte superior de la tabla y seleccione **Instalar Security Server** en el menú. Se muestra la ventana **Instalación de Security Server**.



Instalación de Security Server desde el menú Tareas

5. Todos los hosts detectados en el contenedor seleccionado aparecerán en la lista. Seleccione los hosts en los que quiera instalar las instancias Security Server.
6. Elija los ajustes de configuración que quiera emplear.

> **Importante**
> Utilizar ajustes comunes para la implementación simultánea de instancias en múltiples Security Server requiere que los hosts compartan el mismo almacenamiento, tengan sus direcciones IP asignadas por un servidor DHCP y formen parte de la misma red.

7. Haga clic en **Siguiente**.
8. Proporcione las credenciales VMware vShield correspondientes para cada máquina vCenter.
9. Escriba un nombre descriptivo para Security Server.
10. Para entornos VMware, seleccione el contenedor en el que quiere incluir el Security Server desde el menú **Implementar contenedor**.
11. Seleccione el almacenamiento de destino.

12. Elija el tipo de provisión de disco. Se recomienda implementar el appliance usando aprovisionamiento con discos thick.

    Importante
    Si utiliza aprovisionamiento con discos thin y se queda sin espacio en disco en el datastore, el Security Server se detendrá y, en consecuencia, el host se quedará sin protección.

13. Configure la asignación de recursos de CPU y memoria basándose en el ratio de consolidación de la MV en el host. Escoja **Bajo**, **Medio** o **Alto** para cargar los ajustes de asignación de recursos recomendados o **Manual** para configurar la asignación de recursos manualmente.
14. Debe establecer una contraseña de administrador para la consola de Security Server. Establecer una contraseña administrativa anula la contraseña raíz predeterminada ("sve").
15. Establezca la zona horaria del appliance.
16. Seleccione el tipo de configuración de red para la red de Bitdefender. La dirección IP de Security Server no debe cambiarse a lo largo del tiempo, ya que los agentes de Linux la utilizan para comunicarse.

    Si escoge DHCP, asegúrese de configurar el servidor DHCP para que reserve una dirección IP para el appliance.

    Si escoge fija, debe introducir la información sobre la dirección IP, máscara de subred, puerta de enlace y DNS.
17. Seleccione la red vShield e introduzca las credenciales vShield. La etiqueta predeterminada para la red vShield es `vmservice-vshield-pg`.
18. Haga clic en **Guardar** para crear la tarea. Aparecerá un mensaje de confirmación.

    Importante
    - Los paquetes de Security Server no se incluyen de forma predeterminada en el appliance GravityZone. Dependiendo de los ajustes realizados por el administrador root, o se descarga el paquete Security Server necesario para su entorno cuando se ejecute una tarea de instalación de Security Server, o el administrador recibirá una notificación indicando que falta una imagen y la instalación no se realizará. Si falta el paquete, el administrador root lo tendrá que descargar manualmente antes de que pueda realizarse la instalación.

- La instalación de Security Server en Nutanix a través de una tarea a distancia puede fallar si el cluster de Prism Element está registrado en Prism Central o por algún otro motivo. En estas situaciones, se recomienda realizar una implementación manual de Security Server. Para obtener más información, consulte este artículo de la base de conocimientos.

19. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Desinstalar Security Server

Para desinstalar un Security Server:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el centro de datos o carpeta que contiene el host en el que se ha instalado el Security Server .
4. Marque la casilla de verificación correspondiente al host en que está instalado el Security Server.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Desinstalar Security Server**.
6. Introduzca las credenciales de vShield y haga clic en **Sí** para crear la tarea.
7. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Actualizar Security Server

Para actualizar un Security Server:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el host en el que está instalado el Security Server .

   Para localizar fácilmente el Security Server, puede utilizar el menú **Filtros** como se indica a continuación:

   - Acceda a la pestaña **Seguridad** y seleccione **Servidores de seguridad**.
   - Acceda a la pestaña **Profundidad** y seleccione **Todos los elementos recursivamente**.

Nota
Si está utilizando una herramienta de administración de virtualización que no se halle integrada actualmente con Control Center, el Security Server se situará en **Grupos personalizados**.
Para más información relativa a las plataformas de virtualización compatibles, consulte la Guía de instalación de GravityZone.

4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar Security Server**.
5. Tendrá que confirmar esta acción haciendo clic en **Sí**.
6. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Importante
Se recomienda utilizar este método para actualizar Security Server para NSX; de lo contrario perderá la cuarentena guardada en el appliance.

Instalar el paquete suplementario de HVI

Para proteger máquinas virtuales con HVI debe instalar un paquete suplementario en el host. El papel de este paquete es garantizar la comunicación entre el hipervisor y el Security Server instalado en el host. Una vez instalado, HVI protegerá a las máquinas virtuales que tienen HVI habilitado en la política.

Importante
- HVI protege las máquinas virtuales exclusivamente en hipervisores Citrix Xen.
- No necesita desinstalar el agente de seguridad existente de las máquinas virtuales.

Para instalar el paquete suplementario en un host:

1. Acceda a la página **Configuración > Actualización**.
2. Seleccione el paquete suplementario de HVI en la lista de **Componentes** y haga clic en el botón **Descargar** de la zona superior de la tabla.
3. Acceda a la página **Red** y seleccione **Máquinas virtuales** en el selector de vistas.
4. Seleccione **Servidor** en el menú de **Vistas** del panel izquierdo.
5. Seleccione uno o más hosts Xen del inventario de red. Puede ver fácilmente los hosts disponibles seleccionando la opción **Tipo > Hosts** en el menú **Filtros**.

6. Haga clic en el botón **Tareas** del panel derecho y seleccione **Instalar el paquete suplementario de HVI**. Se abre la ventana de instalación.
7. Programe cuándo debe ejecutarse la tarea de instalación. Puede optar por ejecutar la tarea inmediatamente después de guardarla, o en un momento determinado. En caso de que no se pueda completar la instalación en el momento especificado, la tarea se repite automáticamente según los ajustes de recurrencia. Por ejemplo, si selecciona varios hosts y uno no está disponible cuando esté programada la instalación del paquete, la tarea se ejecutará de nuevo a la hora especificada.
8. Debe reiniciarse el host para aplicar los cambios y completar la instalación. Si desea que el host se reinicie de forma desatendida, seleccione **Reiniciar automáticamente (si es necesario)**.
9. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

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

Desinstalar el paquete suplementario de HVI

Para desinstalar el paquete suplementario de los hosts:

1. Acceda a la página **Red** y seleccione **Máquinas virtuales** en el selector de vistas.
2. Seleccione **Servidor** en el menú de **Vistas** del panel izquierdo.
3. Seleccione uno o más hosts Xen del inventario de red. Puede ver fácilmente los hosts disponibles seleccionando la opción **Tipo > Hosts** en el menú **Filtros**.
4. Haga clic en el botón **Tareas** del panel derecho y seleccione **Desinstalar el paquete suplementario de HVI**. Se abre la ventana de configuración.
5. Programe cuándo eliminar el paquete. Puede optar por ejecutar la tarea inmediatamente después de guardarla, o en un momento determinado. En caso de que no se pueda completar la desinstalación en el momento especificado, la tarea se repite automáticamente según los ajustes de recurrencia. Por ejemplo, si selecciona varios hosts y uno no está disponible cuando esté programada la desinstalación del paquete, la tarea se ejecutará de nuevo a la hora especificada.
6. Se debe reiniciar el host para completar la eliminación. Si desea que el host se reinicie de forma desatendida, seleccione **Reiniciar automáticamente (si es necesario)**.
7. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

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

Actualizar el paquete suplementario de HVI

Para actualizar el paquete suplementario en los hosts:

1. Instale el último paquete suplementario de HVI disponible.

   Para más información, diríjase a "Instalar el paquete suplementario de HVI" (p. 161).
2. Diríjase a la página **Red**.
3. Seleccione **Máquinas virtuales** desde el selector de vistas.
4. Seleccione **Servidor** en el menú de **Vistas** del panel izquierdo.
5. Seleccione uno o más hosts Xen del inventario de red.

   Puede ver fácilmente los hosts disponibles seleccionando la opción **Tipo > Hosts** en el menú **Filtros**.
6. Haga clic en el botón **Tareas** del panel derecho y seleccione **Actualizar el paquete suplementario de HVI**. Se abre la ventana de configuración.
7. Programe cuándo actualizar el paquete. Puede optar por ejecutar la tarea inmediatamente después de guardarla, o en un momento determinado.

   En caso de que no se pueda completar la actualización en el momento especificado, la tarea se repite automáticamente según los ajustes de recurrencia. Por ejemplo, si selecciona varios hosts y uno no está disponible cuando esté programada la actualización del paquete, la tarea se ejecutará de nuevo a la hora especificada.
8. Seleccione **Reiniciar automáticamente (si es necesario)** si desea reiniciar el host sin supervisión. De lo contrario, debe reiniciar el host manualmente para aplicar la actualización.
9. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Puede comprobar el estado de la tarea en la página **Red > Tareas**.

Herramienta personalizada de inyección

Para inyectar herramientas en los sistemas operativos del guest objetivo:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.

3. Seleccione el grupo que desee del panel de la izquierda. Todos los endpoints del contenedor seleccionado se muestran en la tabla del panel de la derecha.
4. Marque las casillas de verificación de los endpoints objetivo.
5. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Herramienta personalizada de inyección**. Se muestra una ventana de configuración.
6. En el menú desplegable, seleccione todas las herramientas que desee inyectar. Para cada herramienta seleccionada, se muestra una sección contraíble con sus ajustes.

   Estas herramientas se cargaron previamente en GravityZone. Si no consigue encontrar la herramienta adecuada en la lista, acceda al **Centro de administración de herramientas** y añádala desde allí. Para más información, diríjase a "Inyección de herramientas personalizadas con HVI" (p. 494).
7. Para cada herramienta visualizada en la ventana:
   a. Haga clic en el nombre de la herramienta para ver u ocultar su sección.
   b. Introduzca la línea de comando de la herramienta, junto con todos los parámetros de entrada necesarios, como hace en el símbolo del sistema o el terminal. Por ejemplo:

      ```
      bash script.sh <param1> <param2>
      ```

      En el caso de las herramientas de reparación de BD, solo puede seleccionar la acción de reparación y la acción de reparación de copia de seguridad en los dos menús desplegables.
   c. Indique la ubicación desde donde Security Server debe reunir los registros:
      - **stdout**. Marque esta casilla de verificación para capturar los registros del canal de comunicación de salida estándar.
      - **Archivo de salida**. Marque esta casilla de verificación para recopilar el archivo de registro guardado en el endpoint. En este caso, debe introducir la ruta donde Security Server puede encontrar el archivo. Puede utilizar rutas absolutas o variables del sistema.

        Aquí tiene una opción adicional: **Eliminar los archivos de registro del guest después de haberlos transferido**. Selecciónela si ya no necesita los archivos en el endpoint.

8. Si desea transferir el archivo de registros desde Security Server a otra ubicación, debe proporcionar la ruta de acceso a la ubicación de destino y las credenciales de autenticación.
9. A veces la herramienta puede requerir más tiempo de lo esperado para terminar su trabajo, o puede incluso dejar de responder. Para evitar problemas en estas situaciones, en la sección **Configuración de seguridad**, elija después de cuántas horas Security Server debe finalizar automáticamente el proceso de la herramienta.
10. Haga clic en **Guardar**.

    Puede ver el estado de la tarea en la página **Tareas**. Para obtener más información, también puede consultar el informe de **Estado de inyección de terceros de HVI**.

6.3.6. Crear informes rápidos

Puede elegir crear informes instantáneos de las máquinas virtuales administradas empezando desde la página **Red**:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las máquinas virtuales del contenedor seleccionado se muestran en la tabla del panel lateral derecho.
4. Filtre los contenidos del grupo seleccionado sólo por las máquinas virtuales administradas.
5. Marque las casillas de verificación correspondientes a las máquinas virtuales que se incluirán en el informe.
6. Haga clic en el botón **Informe** de la zona superior de la tabla y seleccione en el menú el tipo de informe. Para más información, diríjase a "Informes de equipos y máquinas virtuales" (p. 424).
7. Configure las opciones del informe. Para obtener más información, consulte"Creando Informes" (p. 444)
8. Haga clic en **Generar**. El informe se mostrará inmediatamente. El tiempo requerido para crear los informes puede variar dependiendo del número de máquinas virtuales seleccionadas.

6.3.7. Asignando Políticas

Puede administrar los ajustes de seguridad en las máquinas virtuales mediante políticas.

Desde la página **Red** puede consultar, modificar y asignar políticas para cada máquina virtual o grupo de máquinas virtuales.

Nota
Los ajustes de seguridad solo están disponibles para las máquinas virtuales administradas. Para ver y administrar los ajustes de seguridad con mayor facilidad, puede filtrar el inventario de red para que aparezcan solo las máquinas virtuales.

Para ver la configuración de seguridad asignada a una máquina virtual determinada:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las máquinas virtuales del contenedor seleccionado se muestran en la tabla del panel lateral derecho.
4. Haga clic en el nombre de la máquina virtual en la que está interesado. Aparecerá una ventana de información.
5. En la sección **Seguridad** de la pestaña **General**, haga clic en el nombre de la política actual para consultar sus ajustes.
6. 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 todas las demás máquinas virtuales que tengan la misma política asignada.

   Para obtener más información sobre los ajustes de políticas de máquinas virtuales, consulte"Políticas de Seguridad" (p. 222)

Para asignar una política a una máquina virtual o a un grupo de ellas:

1. Diríjase a la página **Red**.
2. Seleccione **Máquinas virtuales** desde el selector de vistas.
3. Seleccione el contenedor que desee del panel de la izquierda. Todas las máquinas virtuales del contenedor seleccionado se muestran en la tabla del panel lateral derecho.

4. Marque la casilla de verificación de la entidad que desee. Puede seleccionar uno o varios objetos del mismo tipo solamente desde el mismo nivel.
5. Haga clic en el botón **Asignar política** de la zona superior de la tabla.
6. Haga los ajustes necesarios en la ventana **Asignación de política**.

   Para más información, diríjase a "Asignando Políticas" (p. 226).

Aviso
En el caso de políticas con Hypervisor Memory Introspection activado, las máquinas objetivo pueden requerir un reinicio justo después de la asignación de políticas. Las máquinas en este estado se marcan en la página **Red** con el icono **Reinicio pendiente**.

6.3.8. Uso del Gestor de recuperación con volúmenes cifrados

Cuando los usuarios de endpoints olviden sus contraseñas de cifrado y dejen de poder acceder a los volúmenes cifrados de sus máquinas, puede ayudarles obteniendo las claves de recuperación en la página **Red**.

Para obtener una clave de recuperación:

1. Diríjase a la página **Red**.
2. Haga clic en el botón **Gestor de recuperación** en la barra de herramientas de acción del panel de la izquierda. Aparecerá una nueva ventana.
3. En la sección **Identificador** de la ventana, introduzca los siguientes datos:
   a. El ID de la clave de recuperación del volumen cifrado. El ID de la clave de recuperación es una cadena de números y letras disponible en el endpoint, en la pantalla de recuperación de BitLocker.

      En Windows, el ID de la clave de recuperación es una cadena de números y letras disponible en el endpoint, en la pantalla de recuperación de BitLocker.

      Como alternativa, puede usar la opción de **Recuperación** en la pestaña **Protección** de los detalles de la máquina virtual para rellenar automáticamente el ID de la clave de recuperación, tanto para los endpoints de Windows como de macOS.

   b. La contraseña de su cuenta de GravityZone.
4. Haga clic en **Mostrar**. La ventana se expande.

   En **Información de volumen** se le presentan los siguientes datos:

a. Nombre del volumen
b. Tipo de volumen (de arranque o no).
c. Nombre del endpoint (como aparece en el inventario de red)
d. Clave de recuperación. En Windows, la clave de recuperación es una contraseña generada automáticamente cuando se cifra el volumen. En Mac, la clave de recuperación es la contraseña de la cuenta de usuario.

5. Envíe la clave de recuperación al usuario del endpoint.

Para obtener más información sobre el cifrado y descifrado de volúmenes con GravityZone, consulte "Cifrado" (p. 389).

6.3.9. Liberación de puestos de licencia

En inventarios de Xen Server, vCenter Server (sin vShield, NSX o HVI) y Active Directory, puede liberar fácilmente los puestos de licencia utilizados por las máquinas virtuales de las que se haya eliminado el agente de seguridad sin ejecutar el programa de desinstalación.

Tras hacer esto, las máquinas objetivo pasan a figurar como no administradas en el inventario de la red.

Para liberar un puesto de licencia:

1. Diríjase a la página **Red**.
2. Seleccione **Equipos y máquinas virtuales** o **Máquinas virtuales** en el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda. Se mostrarán todas las máquinas virtuales en la tabla de la derecha.
4. Seleccione la máquina virtual de la que desee eliminar la licencia.
5. Haga clic en el botón ⊖ **Borrar licencia** de la zona superior de la tabla.
6. Haga clic en **Sí** en la ventana de confirmación para continuar.

6.4. Dispositivos móviles

Para administrar la seguridad de dispositivos móviles utilizados en su empresa, primero tiene que vincularlos a usuarios determinados en Control Center, y luego instalar y activar la aplicación GravityZone Mobile Client en cada uno de ellos.

Los dispositivos móviles pueden ser propiedad de la empresa o personal de los usuarios. Puede instalar y activar GravityZone Mobile Client en cada dispositivo móvil y luego entregarlo al usuario correspondiente. Los usuarios también pueden instalar y activar GravityZone Mobile Client por sí mismos, siguiendo las instrucciones recibidas por email. Para más información, consulte la Guía de instalación de GravityZone.

Para ver los dispositivos móviles de los usuarios bajo su cuenta, diríjase a sección **Red** y seleccione **Dispositivos móviles** desde el Selector de servicios. La página **Red** muestra los grupos de usuarios disponibles en el panel del lateral izquierdo, y los usuarios correspondientes y los dispositivos en el panel del lateral derecho.

Si se ha configurado la integración con Active Directory, puede añadir dispositivos móviles a los usuarios existentes de Active Directory. También puede crear usuarios desde **Grupos personalizados** y añadirles dispositivos móviles.

Puede cambiar la vista del panel derecho a **Usuarios** o a **Dispositivos** mediante la pestaña **Vistas** del menú **Filtros** localizado en la parte superior de la tabla. La vista **Usuarios** le permite administrar usuarios en Control Center; por ejemplo, añadir usuarios y dispositivos móviles, y consultar el número de dispositivos para cada usuario. Use la vista **Dispositivos** para administrar y consultar fácilmente los detalles de cada dispositivo móvil en Control Center.

Puede administrar los usuarios y dispositivos móviles en Control Center de la forma siguiente:

- Añadir usuarios personalizados
- Añadir dispositivos móviles a los usuarios
- Organizar los usuarios personalizados en grupos
- Filtrar y buscar usuarios y dispositivos
- Consultar el estado y los datos de usuarios o dispositivos
- Ejecutar tareas en dispositivos móviles
- Crear informes rápidos de dispositivos móviles
- Consultar y modificar los ajustes de seguridad de los dispositivos
- Sincronizar el inventario de Control Center con Active Directory
- Eliminar usuarios y dispositivos móviles

6.4.1. Añadir usuarios personalizados

Si se ha configurado la integración con Active Directory, puede añadir dispositivos móviles a los usuarios existentes de Active Directory.

En situaciones sin Active Directory, primero debe crear usuarios personalizados para disponer de un medio para identificar a los propietarios de los dispositivos móviles.

Existen dos formas de crear usuarios personalizados. Puede añadirlos uno a uno o importarlos desde un archivo CSV.

Para añadir un usuario personalizado:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de servicios.
3. Haga clic en el menú **Filtros** de la zona superior de la tabla y acceda a la pestaña **Ver**. Asegúrese de que esté seleccionada la opción **Usuarios**.
4. En el panel izquierdo, seleccione **Grupos personalizados**.
5. Haga clic en el botón **Añadir usuario** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.
6. Especifique los detalles de usuario necesarios:
   - Un nombre de usuario descriptivo (por ejemplo, el nombre completo del usuario)
   - La dirección de correo del usuario

   Importante
   - Asegúrese de proporcionar una dirección de correo válida. Se enviarán al usuario las instrucciones de instalación por correo cuando añada un dispositivo.
   - Cada dirección de email puede asociarse únicamente a un usuario.

7. Haga clic en **Aceptar**.

Para importar usuarios de dispositivos móviles:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de servicios.
3. Haga clic en el menú **Filtros** de la zona superior de la tabla y acceda a la pestaña **Ver**. Asegúrese de que esté seleccionada la opción **Usuarios**.
4. En el panel izquierdo, seleccione **Grupos personalizados**.
5. Haga clic en **Importar usuarios**. Se abre una nueva ventana.

6. Seleccione el archivo CSV y haga clic en **Importar**. La ventana se cierra y la tabla se rellena con los usuarios importados.

> **Nota**
> Si se produce algún error, se muestra un mensaje y la tabla se rellena solo con los usuarios válidos. Los usuarios existentes se omiten.

Posteriormente puede crear grupos de usuarios desde **Grupos personalizados**.

La política y tareas asignadas a un usuario se aplicarán a todos los dispositivos propiedad del usuario correspondiente.

6.4.2. Añadir dispositivos móviles a usuarios

Un usuario puede tener un número ilimitado de dispositivos móviles. Puede añadir dispositivos a uno o varios usuarios, pero solo puede haber un dispositivo por usuario al mismo tiempo.

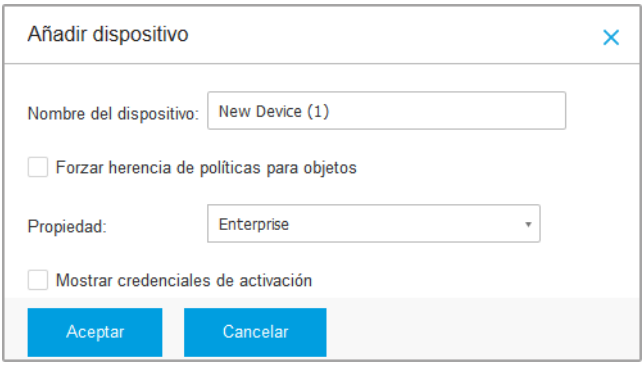
Añadir un dispositivo a un solo usuario

Para añadir un dispositivo a un usuario específico:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Localice el usuario en el grupo de **Active Directory** o en los **Grupos personalizados** y marque la casilla de verificación correspondiente en el panel del lateral derecho.

> **Nota**
> Los **Filtros** deben estar establecidos en **Usuarios** en la pestaña **Ver**.

4. Haga clic en el botón **Añadir dispositivo** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.



Añadir un dispositivo móvil a un usuario

5. Configure los detalles del dispositivo móvil:
   a. Escriba un nombre descriptivo para el dispositivo.
   b. Utilice la opción **Autoconfigurar nombre** si desea que el nombre del dispositivo se genere automáticamente. Al añadirlo, el dispositivo tiene un nombre genérico. Una vez que se activa el dispositivo, se renombra automáticamente con la información correspondiente de fabricante y modelo.
   c. Seleccione el tipo de propiedad del dispositivo (empresa o personal). Puede filtrar en cualquier momento los dispositivos móviles por el tipo de propiedad y administrarlos según sus necesidades.
   d. Seleccione la opción **Mostrar credenciales de activación** si va a instalar el GravityZone Mobile Client en el dispositivo del usuario.
6. Haga clic en **OK** para añadir el dispositivo. Se envía inmediatamente un correo al usuario con las instrucciones de instalación y los detalles de activación para configurarlos en el dispositivo. Los detalles de activación incluyen el token de activación y la dirección del servidor de comunicaciones (y el código QR correspondiente).
7. Si ha seleccionado la opción **Mostrar credenciales de activación**, aparecerá la ventana **Detalles de activación**, que muestra el token de activación único, la dirección del servidor de comunicaciones y el código QR correspondiente para el nuevo dispositivo.

Información sobre la activación de dispositivos móviles

Tras instalar GravityZone Mobile Client, cuando se le pida activar el dispositivo, introduzca el token de activación y la dirección del Servidor de comunicaciones o escanee el código QR proporcionado.

Añadir dispositivos a varios usuarios

Para añadir dispositivos móviles a una selección de usuarios y grupos:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Localice el usuario o grupos en las carpetas de **Active Directory** o en los **Grupos personalizados** y marque las casillas de verificación correspondientes en el panel del lateral derecho.

> **Nota**
> Los **Filtros** deben estar establecidos en **Usuarios** en la pestaña **Ver**.

4. Haga clic en el botón **Añadir dispositivo** del lateral derecho de la tabla. En este caso, debe definir en la ventana de configuración solo la propiedad del dispositivo.

Si existen usuarios sin dirección de correo electrónico especificada, se le notificará inmediatamente con un mensaje. La lista de usuarios correspondientes estará disponible en el área de **Notificación** de Control Center.

Los dispositivos móviles creados por selección múltiple tienen un nombre genérico por defecto en Control Center. Una vez que se activa un dispositivo, se renombra automáticamente con la información correspondiente de fabricante y modelo.

5. Haga clic en **Aceptar** para añadir los dispositivos. Se envía inmediatamente un mensaje de correo electrónico a los usuarios con las instrucciones de instalación y la información de activación para la configuración de sus dispositivos. Los detalles de activación incluyen el token de activación y la dirección del servidor de comunicaciones (y el código QR correspondiente).

Puede consultar el número de dispositivos asignados a cada usuario en el panel del lateral derecho, en la columna **Dispositivos**.

6.4.3. Organizar los usuarios personalizados en grupos

Puede ver los grupos de usuarios disponibles en el panel izquierdo de la página **Red**.

Los usuarios de Active Directory se agrupan bajo **Active Directory**. No puede editar los grupos Active Directory. Sólo puede consultar y añadir dispositivos a los usuarios correspondientes.

Puede colocar todos los usuarios no Active Directory en **Grupos personalizados**, donde puede crear y organizar grupos como desee. La ventaja principal es que puede usar las políticas de grupo para cumplir distintos requisitos de seguridad.

En **Grupos personalizados** puede crear, eliminar, renombrar y mover grupos de usuarios dentro de una estructura de árbol personalizada.

Importante
Por favor, tenga en cuenta lo siguiente:

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

Creando Grupos

Para crear un grupo personalizado:

1. Seleccione **Grupos personalizados** en el panel lateral izquierdo.
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**. El nuevo grupo se muestra bajo **Grupos personalizados**.

Renombrando Grupos

Para renombrar un grupo personalizado:

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 usuarios

Puede mover grupos y usuarios a cualquier lugar dentro de la jerarquía de **Grupos personalizados**. 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 no ser que la herencia de políticas se haya desactivado y se haya asignado una política diferente a la entidad.

Eliminando Grupos

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

Para eliminar un grupo:

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

6.4.4. Comprobación del estado de los dispositivos móviles

Los dispositivos móviles están representados en la página de red mediante el icono correspondiente a su tipo y estado.

Consulte "Tipos y estados de los objetos de red" (p. 525) para ver una lista con todos los tipos de iconos y estados disponibles.

Los dispositivos móviles pueden tener los siguientes estados de administración:

- **Administrado (Activo)**, cuando se satisfacen todas las condiciones siguientes:
  - GravityZone Mobile Client está activado en el dispositivo.
  - GravityZone Mobile Client se ha sincronizado con Control Center en las últimas 48 horas.
- **Administrado (Inactivo)**, cuando se satisfacen todas las condiciones siguientes:
  - GravityZone Mobile Client está activado en el dispositivo.
  - GravityZone Mobile Client no se ha sincronizado con Control Center desde hace más de 48 horas.
- **No administrados**, en las siguientes situaciones:
  - GravityZone Mobile Client todavía no se ha instalado y activado en el dispositivo móvil.
  - GravityZone Mobile Client se ha desinstalado del dispositivo móvil (solo para dispositivos Android).
  - El perfil MDM de Bitdefender se ha eliminado del dispositivo (solo para dispositivos iOS).

Para consultar el estado de administración de los dispositivos:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione el grupo en el que está interesado.
4. Haga clic en el menú **Filtros** situado en la parte superior de la tabla y lleve a cabo los siguientes ajustes:
   a. Acceda a la pestaña **Ver** y seleccione **Dispositivos**.

b. Acceda a la pestaña **Seguridad** y seleccione el estado que le interesa en la sección **Administración**. Puede seleccionar uno o varios criterios de filtrado al mismo tiempo.

c. También puede escoger ver todos los dispositivos recursivamente, seleccionando la opción correspondiente en la pestaña **Profundidad**.

d. Haga clic en **Guardar**.

Se mostrarán en la tabla todos los dispositivos móviles correspondientes al criterio seleccionado.

También puede generar un informe del estado de sincronización del dispositivo para uno o varios dispositivos móviles. Este informe proporciona información detallada sobre el estado de sincronización de cada dispositivo seleccionado, incluyendo la fecha y hora de la última sincronización. Para obtener más información, consulte"Crear informes rápidos" (p. 191)

6.4.5. Dispositivos conformes y no conformes

Una vez que la aplicación GravityZone Mobile Client se ha activado en un dispositivo móvil, Control Center comprueba si el dispositivo correspondiente cumple todos los requisitos de conformidad. Los dispositivos móviles pueden tener los siguientes estados de seguridad:

- **Sin problemas de seguridad**, cuando se satisfacen todos los requisitos de conformidad.
- **Con problemas de seguridad**, cuando no se cumple al menos uno de los requisitos de conformidad. Cuando se declara no conforme un dispositivo, se pide al usuario que resuelva los problemas de disconformidad. El usuario debe realizar los cambios requeridos dentro de un periodo de tiempo determinado, de lo contrario se aplicará la acción definida en la política para los dispositivos no conformes.

  Para obtener más información acerca de las acciones y criterios para dispositivos no conformes, consulte "Conformidad" (p. 404).

Para consultar el estado de conformidad de los dispositivos:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione el grupo en el que está interesado.

4. Haga clic en el menú **Filtros** situado en la parte superior de la tabla y lleve a cabo los siguientes ajustes:
   a. Acceda a la pestaña **Ver** y seleccione **Dispositivos**.
   b. Acceda a la pestaña **Seguridad** y seleccione el estado que le interesa en la sección **Problemas de seguridad**. Puede seleccionar uno o varios criterios de filtrado al mismo tiempo.
   c. También puede escoger ver todos los dispositivos recursivamente, seleccionando la opción correspondiente en la pestaña **Profundidad**.
   d. Haga clic en **Guardar**.

      Se mostrarán en la tabla todos los dispositivos móviles correspondientes al criterio seleccionado.
5. Puede ver la tasa de conformidad de los dispositivos para cada usuario:
   a. Haga clic en el menú **Filtros** situado en la parte superior de la tabla y seleccione **Usuarios** de la categoría **Ver**. Se mostrarán en la tabla todos los usuarios del grupo seleccionado.
   b. Consulte la columna **Conforme** para ver cuántos dispositivos son conformes del número total de dispositivos propiedad del usuario.

También puede generar un informe de Conformidad de dispositivo para uno o varios dispositivos móviles. Este informe proporciona información detallada sobre el estado de conformidad de cada dispositivo seleccionado, incluyendo el motivo de la no conformidad. Para obtener más información, consulte"Crear informes rápidos" (p. 191)

6.4.6. Consultar detalles de usuarios y dispositivos móviles

Puede obtener información detallada sobre cada usuario y dispositivo móvil desde la página **Red**.

Consulta de detalles de usuarios

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo deseado desde el panel lateral izquierdo.
4. Haga clic en el menú **Filtros** situado en la parte superior de la tabla, acceda a la pestaña **Ver** y seleccione **Usuarios**. Para mostrar recursivamente los usuarios,

acceda a la pestaña **Profundidad** y seleccione **Todos los elementos recursivamente**. Haga clic en **Guardar**. Se muestran en la tabla todos los usuarios del grupo seleccionado.

5. Consulte la información mostrada en las columnas de la tabla para cada usuario:
   - **Nombre**. El nombre del usuario.
   - **Dispositivos**. El número de dispositivos conectados al usuario. Haga clic en el número para cambiar a la vista **Dispositivos** y muestre únicamente los dispositivos correspondientes.
   - **Conformidad**. La tasa de dispositivos conformes del total de dispositivos conectados al usuario. Haga clic en el primer valor para cambiar a la vista **Dispositivos** y mostrar únicamente los dispositivos conformes.
6. Haga clic en el nombre del usuario en el que está interesado. Aparece una ventana de configuración, donde puede ver y editar el nombre del usuario y la dirección de correo

Consultar detalles del dispositivo

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo deseado desde el panel lateral izquierdo.
4. Haga clic en el menú **Filtros** situado en la parte superior de la tabla, acceda a la pestaña **Ver** y seleccione **Dispositivos**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos pertenecientes a los usuarios del grupo seleccionado.
5. Consulte la información mostrada en las columnas de la tabla para cada dispositivo:
   - **Nombre**. El nombre del dispositivo.
   - **Usuario**. El nombre del usuario al que pertenece el dispositivo correspondiente.
   - **SO**. El sistema operativo del dispositivo correspondiente.
6. Haga clic en el nombre del dispositivo para obtener más detalles. Aparece la ventana **Detalles de dispositivos móviles**, donde puede verificar la siguiente información agrupada en las pestañas **Resumen** y **Detalles**:

- **General**.
  - **Nombre**. El nombre especificado cuando se añade el dispositivo a Control Center.
  - **Usuario**. El nombre del propietario del dispositivo.
  - **Grupos**. El grupo padre del dispositivo móvil en el inventario de red.
  - **SO**. El sistema operativo del dispositivo móvil.
  - **Propiedad**. El tipo de propiedad del dispositivo móvil (empresa o personal).
- **Seguridad**.
  - **Versión del cliente**. La versión de la aplicación GravityZone Mobile Client instalada en el dispositivo, solo detectada tras la inscripción.
  - **Política**. La política asignada actualmente al dispositivo móvil. Haga clic en el nombre de la política para ir a la página **Política** correspondiente y consultar los ajustes de seguridad.

    Importante

    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. Los cambios realizados en la política afectarán a todos los dispositivos que tienen dicha política asignada. Para más información, diríjase a "Asignando Políticas" (p. 192).

  - **Estado de licencia**. Ver la información de licencia para el dispositivo correspondiente.
  - **Estado de cumplimiento**. El estado de conformidad está disponible para dispositivos móviles administrados. Un dispositivo móvil puede ser Conforme o No conforme.

    Nota

    Para los dispositivos móviles no conformes, se mostrará un icono de notificación ! . Consulte el tooltip del icono para conocer el motivo de la falta de conformidad.
    Para obtener más información sobre la conformidad de dispositivos móviles, consulte "Conformidad" (p. 404).

- **Actividad malware (últimas 24 H)**. Un resumen rápido acerca del número de detecciones de malware para el equipo correspondiente en el día actual.
- **Contraseña de bloqueo**. Una contraseña única generada automáticamente al registrar el dispositivo, que se utiliza para bloquear de forma remota el dispositivo (sólo para dispositivos Android).
- **Estado de encriptación**. Algunos dispositivos Android 3.0 o superior soportan la opción de cifrado de dispositivo. Marque el estado de cifrado en la página de detalles del dispositivo para averiguar si el dispositivo correspondiente soporta la opción de cifrado. Si se ha requerido el cifrado por política en el dispositivo, también puede ver el estado de activación del cifrado.

- **Detalles de activación**
  - **Código de activación**. El token de activación exclusivo asignado al dispositivo.
  - La dirección del servidor de comunicaciones.
  - **Código QR**. El Código QR único que contiene el código de activación y la dirección del servidor de comunicación.
- **Hardware**. Puede ver aquí la información sobre el hardware del dispositivo, disponible solo para dispositivos administrados (activados). La información sobre el hardware se comprueba cada 12 horas y se actualiza si se produce cualquier cambio.

  Importante
  A partir de Android 10, GravityZone Mobile Client no tiene acceso al número de serie, IMEI, IMSI ni a la dirección MAC del dispositivo. Esta restricción conduce a las siguientes situaciones:
  - Si el dispositivo móvil, que ya tenga GravityZone Mobile Client instalado, se actualiza de una versión anterior de Android a Android 10, Control Center mostrará los datos correctos del dispositivo. Antes de la actualización, el dispositivo debe ejecutar la última versión de GravityZone Mobile Client.
  - Si GravityZone Mobile Client se instala en un dispositivo Android 10, Control Center mostrará datos inexactos sobre ese dispositivo debido a la limitación impuesta por el sistema operativo.

- **Red**. Puede ver aquí la información sobre la conectividad de red, disponible solo para dispositivos administrados (activados).

6.4.7. Clasificación, filtrado y búsqueda de dispositivos móviles

La tabla de inventario de Dispositivos móviles puede ocupar varias páginas, dependiendo del número de usuarios o dispositivos (de forma predeterminada 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.

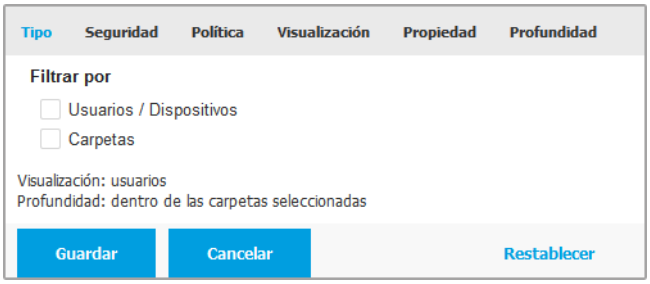
Si hay muchas entradas, puede usar las opciones de filtrado disponibles para mostrar únicamente las entradas en las que está interesado. Por ejemplo, puede buscar un dispositivo móvil concreto o elegir ver únicamente los dispositivos móviles administrados.

Ordenar el inventario de dispositivos móviles

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

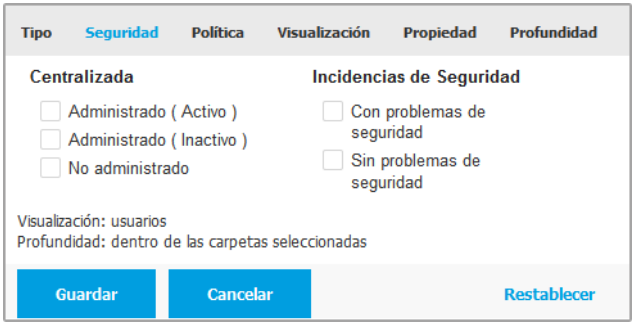
Filtrado del inventario de dispositivos móviles

1. Seleccione el grupo que desee en el panel de la izquierda.
2. Haga clic en el menú **Filtros** de la zona superior del área de paneles de red.
3. Use el criterio de filtrado de la siguiente manera:
   - **Tipo**. Seleccione el tipo de entidades que desea mostrar (usuarios/dispositivos y carpetas).



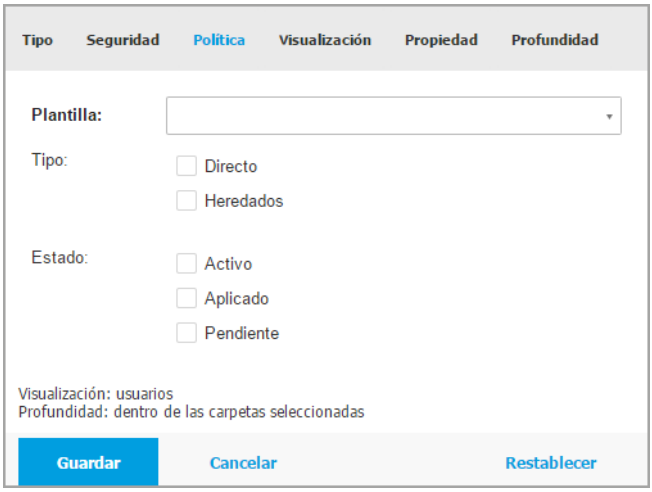
Dispositivos móviles - Filtrar por tipo

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



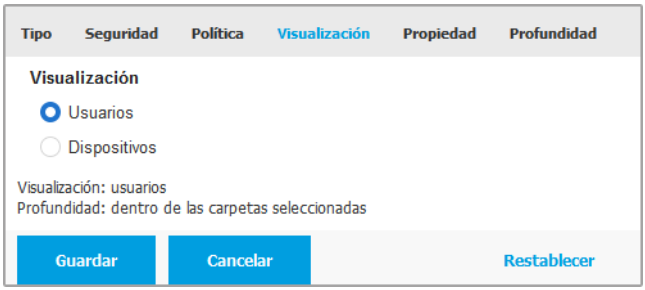
Dispositivos móviles - Filtrar por seguridad

- **Política**. Seleccione la plantilla de política según la cual quiere filtrar los dispositivos móviles, el tipo de asignación de política (directa o heredada), así como el estado de asignación de la política (activo, aplicado o pendiente).



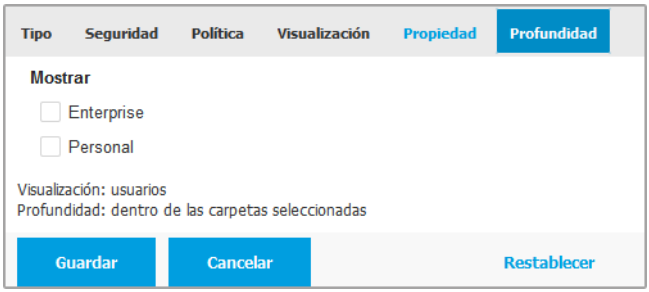
Dispositivos móviles - Filtrar por política

- **Ver**. Seleccione **Usuarios** para mostrar solamente los usuarios del grupo seleccionado. Seleccione **Dispositivos** para mostrar solamente los dispositivos del grupo seleccionado.



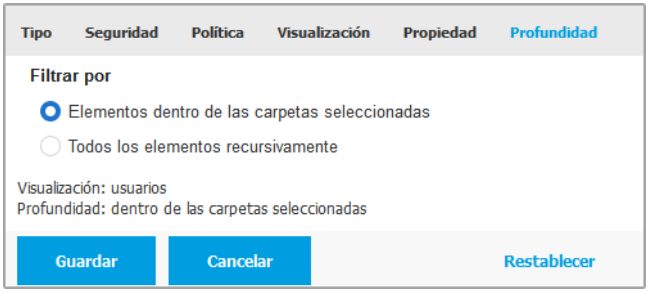
Dispositivos móviles - Filtrar por vista

- **Propiedad**. Puede filtrar los dispositivos móviles por propiedad, escogiendo mostrar dispositivos de **Empresa** o **Personales**. El atributo de propiedad se define en los datos de los dispositivos móviles.



Dispositivos móviles - Filtrar por propietario

- **Profundidad**. Al administrar una red con estructura de árbol, los dispositivos móviles o usuarios incluidos en subgrupos no se muestran cuando se selecciona el grupo raíz. Seleccione **Todos los elementos recursivamente** para ver todas las entidades incluidas en el grupo actual y en sus subgrupos.



Dispositivos móviles - Filtrar por profundidad

4. Haga clic en **Guardar** para filtrar el inventario de dispositivos móviles por el criterio seleccionado.

   El filtro permanece activo en la página **Red** hasta que cierra la sesión o restablece el filtro.

Búsqueda de dispositivos móviles

La tabla del panel derecho proporciona información específica de usuarios y dispositivos móviles. Puede usar las categorías disponibles en cada columna para filtrar los contenidos de la tabla.

1. Seleccione el grupo deseado desde el panel lateral izquierdo.
2. Cambie a la vista que desee (usuarios o dispositivos móviles) mediante el menú **Filtros** de la parte superior del área de paneles de red.
3. Busque las entidades que desee utilizando los campos de búsqueda de los encabezados de columna del panel de la derecha:
   - Introduzca el término que desea buscar en el campo de búsqueda correspondiente.

     Por ejemplo, cambie a la vista **Dispositivos** y escriba el nombre del usuario que esté buscando en el campo **Usuario**. Sólo aparecerán en la tabla los dispositivos que coincidan con el criterio.
   - Seleccione el atributo que desee buscar en los cuadros de lista desplegables correspondientes.

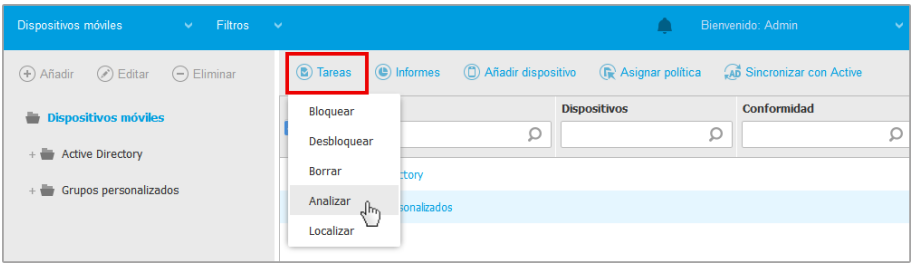
     Por ejemplo, cambie a la vista **Dispositivos**, haga clic en el cuadro de lista **SO** y seleccione **Android** para ver solo los dispositivos móviles Android.

   Nota
   Para vaciar el término de búsqueda y mostrar todas las entradas, coloque el cursor sobre el cuadro correspondiente y haga clic en el icono ×.

6.4.8. Ejecutar tareas en los dispositivos móviles

Desde la página **Red**, puede ejecutar de forma remota un determinado número de tareas administrativas en los dispositivos móviles. Esto es lo que puede hacer:

- “Bloquear” (p. 187)
- “Borrar” (p. 188)
- “Analizar” (p. 189)
- “Localizar” (p. 190)



Tareas de dispositivos móviles

Para ejecutar tareas remotas en los dispositivos móviles, deben cumplirse determinados requisitos previos. Para más información, consulte el capítulo Requisitos de instalación de la Guía de instalación de GravityZone.

Puede elegir crear tareas individuales para cada dispositivo móvil, para cada usuario o para grupos de usuarios. Por ejemplo, puede analizar en busca de malware de forma remota los dispositivos móviles de un grupo de usuarios. También puede ejecutar una tarea de localización para un dispositivo móvil específico.

El inventario de red puede contener dispositivos móviles activos, inactivos o no administrados. Una vez creada, las tareas se iniciarán inmediatamente en los dispositivos móviles activos. Para dispositivos inactivos, las tareas se iniciarán tan pronto como vuelvan a estar conectados. No se crearán tareas para dispositivos móviles no administrados. En este caso se mostrará una notificación indicando que la tarea no ha podido crearse.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

Bloquear

La tarea Bloquear bloquea inmediatamente la pantalla de los dispositivos móviles objetivo. El comportamiento de la tarea Bloquear depende del sistema operativo:

- La tarea de bloqueo para dispositivos Android (7.0 o superior) aplicará la contraseña configurada en su consola GravityZone solo si no se ha configurado una protección de bloqueo en el dispositivo. De lo contrario, se utilizarán las opciones de bloqueo de pantalla existentes, como Patrón, PIN, Contraseña, Huella dactilar o Smart Lock, para proteger el dispositivo.

Nota

- La contraseña de bloqueo de la pantalla generada por Control Center se muestra en la ventana Detalles del dispositivo móvil.
- La tarea de desbloqueo ya no está disponible para dispositivos Android (7.0 o superior). En cambio, los usuarios pueden desbloquear sus dispositivos manualmente. Sin embargo, debe asegurarse de antemano de que esos dispositivos admitan los requisitos de complejidad esperados para la contraseña de desbloqueo.
- Debido a limitaciones técnicas, la tarea de bloqueo no está disponible en Android 11.

- Si el dispositivo, en iOS, posee una contraseña de bloqueo de la pantalla, se solicita para desbloquearlo.

Para bloquear de forma remota dispositivos móviles:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Usuarios** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los usuarios del grupo seleccionado.
5. Marque las casillas de verificación correspondientes a los usuarios en los que tenga interés. Puede seleccionar uno o varios usuarios al mismo tiempo.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Bloquear**.
7. Tendrá que confirmar esta acción haciendo clic en **Sí**. Un mensaje le informará si la tarea se creó o no.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a “Ver y administrar tareas” (p. 210).

Borrar

La tarea **Borrar** restaura los dispositivos móviles objetivo a los ajustes de fábrica. Ejecute esta tarea para borrar toda la información sensible y las aplicaciones almacenadas en los dispositivos móviles objetivo.

Aviso

Utilice la tarea **Borrar** con cuidado. Compruebe la propiedad de los dispositivos objetivo (si quiere evitar borrar dispositivos móviles de propiedad personal) y asegúrese de que realmente quiere borrar el contenido de los dispositivos seleccionados. Una vez enviada, la tarea **Borrar**no puede deshacerse.

Nota

Debido a limitaciones técnicas, la tarea de borrado no está disponible en Android 11.

Para borrar de forma remota un dispositivo móvil:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos del grupo seleccionado.

   Nota

   También puede seleccionar **Todos los dispositivos recursivamente** en la sección **Profundidad** para ver todos los dispositivos en el grupo actual.

5. Marque la casilla de verificación correspondiente al dispositivo que quiere borrar.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Borrar**.
7. Tendrá que confirmar esta acción haciendo clic en **Sí**. Un mensaje le informará si la tarea se creó o no.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a “Ver y administrar tareas” (p. 210).

Analizar

La tarea **Analizar** le permite comprobar la existencia de malware en los dispositivos móviles seleccionados. El usuario del dispositivo recibe una notificación relativa al malware detectado y se le solicita que lo elimine. El análisis se ejecuta desde la nube; por ello el dispositivo debe tener conexión a Internet.

Nota
El análisis remoto no funciona en dispositivos iOS (limitación de la plataforma).

Para analizar de forma remota dispositivos móviles:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos del grupo seleccionado.

   Nota
   También puede seleccionar **Todos los dispositivos recursivamente** en la sección **Profundidad** para ver todos los dispositivos en el grupo actual.
   Para mostrar solamente dispositivos Android en el grupo seleccionado, diríjase al encabezado de columna **SO** en el panel derecho y seleccione **Android** en el cuadro de lista correspondiente.

5. Marque las casillas de verificación correspondientes a los equipos que quiere analizar.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Analizar**.
7. Tendrá que confirmar esta acción haciendo clic en **Sí**. Un mensaje le informará si la tarea se creó o no.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Puede consultar un informe de análisis que aparece disponible cuando se completa la tarea. Haga clic en el icono correspondiente de la columna **Informes** para generar un informe instantáneo.

   Para más información, diríjase a “Ver y administrar tareas” (p. 210).

Localizar

La tarea Localizar abre un mapa que le muestra la localización de los dispositivos seleccionados. Puede localizar uno o varios dispositivos al mismo tiempo.

Para que funcione la tarea Localizar, los servicios de localización deben estar activados en los dispositivos móviles.

Para localizar dispositivos móviles:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos del grupo seleccionado.

   Nota
   También puede seleccionar **Todos los dispositivos recursivamente** en la sección **Profundidad** para ver recursivamente todos los dispositivos en el grupo actual.

5. Marque la casilla de verificación correspondiente al dispositivo que quiera localizar.
6. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Localizar**.
7. Se abre la ventana **Localización**, que muestra la siguiente información:
   - Un mapa mostrando la posición de los dispositivos móviles seleccionados. Si un dispositivo no está sincronizado, el mapa mostrará la última ubicación conocida.
   - Una tabla mostrando los detalles de los dispositivos seleccionados (nombre, usuario, fecha y hora de la última sincronización. Para ver la localización en el mapa de un determinado dispositivo mostrado en la lista, simplemente marque su casilla de verificación. El mapa se centrará instantáneamente en la ubicación del dispositivo correspondiente.
   - La opción **Actualizar automáticamente** actualiza de forma automática las ubicaciones de los dispositivos móviles seleccionados cada 10 segundos.
8. Puede ver y administrar las tareas en la página **Red > Tareas**. Para más información, diríjase a "Ver y administrar tareas" (p. 210).

6.4.9. Crear informes rápidos

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

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Seleccione el grupo que desee del panel de la izquierda.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. También puede seleccionar las opciones administradas de la pestaña **Seguridad**, para filtrar el grupo seleccionado solamente por dispositivos administrados. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos que corresponden a los criterios de filtrado del grupo seleccionado.
5. Marque las casillas de verificación correspondientes a los dispositivos móviles que le interesen. Puede seleccionar uno o varios dispositivos al mismo tiempo.
6. Haga clic en el botón **Informe** de la zona superior de la tabla y seleccione en el menú el tipo de informe. Para obtener más información, consulte"Informes de Dispositivos móviles" (p. 442)
7. Configure las opciones del informe. Para obtener más información, consulte"Creando Informes" (p. 444)
8. Haga clic en **Generar**. El informe se mostrará inmediatamente. El tiempo requerido para crear los informes puede variar dependiendo del número de dispositivos móviles seleccionados.

6.4.10. Asignando Políticas

Puede administrar los ajustes de seguridad en los dispositivos móviles mediante políticas.

Desde la sección **Red** puede consultar, modificar y asignar políticas para dispositivos móviles de su cuenta.

Puede asignar políticas a grupos, usuarios o dispositivos específicos.

Nota

Una política asignada a un usuario afecta a todos los dispositivos propiedad de ese usuario. Para más información, diríjase a "Asignación de políticas locales" (p. 226).

Para ver la configuración de seguridad asignada a un dispositivo móvil:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.

3. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos pertenecientes a los usuarios del grupo seleccionado.
4. Haga clic en el nombre del dispositivo móvil en el que esté interesado. Aparecerá una ventana de detalles.
5. En la sección **Seguridad** de la página **Resumen**, haga clic en el nombre de la política asignada actualmente para consultar sus ajustes.
6. Puede cambiar los ajustes de seguridad como precise. Por favor, tenga en cuenta que cualquier cambio que haga se aplicará también a todos los otros dispositivos en los que esté activa la política.

   Para obtener más información, consulte"Políticas de dispositivos móviles" (p. 398)

Para asignar una política a un dispositivo móvil:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione el grupo en el que está interesado.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**. Haga clic en **Guardar**. Se muestran en la tabla todos los dispositivos pertenecientes a los usuarios del grupo seleccionado.
5. En el panel derecho, marque la casilla de verificación del dispositivo móvil en el que esté interesado.
6. Haga clic en el botón **Asignar política** de la zona superior de la tabla.
7. Haga los ajustes necesarios en la ventana **Asignación de política**. Para más información, diríjase a "Asignación de políticas locales" (p. 226).

6.4.11. Sincronizar con Active Directory

El inventario de red se sincroniza automáticamente con Active Directory con un intervalo de tiempo especificado en la sección de configuración de Control Center. Para más información, consulte el capítulo Instalación y configuración de GravityZone de la Guía de instalación de GravityZone.

Para sincronizar manualmente los usuarios mostrados actualmente con Active Directory:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Haga clic en el botón **Sincronizar con Active Directory** de la zona superior de la tabla.
4. Tendrá que confirmar esta acción haciendo clic en **Sí**.

Nota

En redes grandes con Active Directory, la sincronización puede tardar mucho tiempo en completarse.

6.4.12. Eliminación de usuarios y dispositivos móviles

Cuando el inventario de red contiene usuarios o dispositivos móviles obsoletos, se recomienda eliminarlos.

Eliminación de dispositivos móviles del inventario de red

Cuando elimina un dispositivo de Control Center:

- Se desvincula GravityZone Mobile Client, pero no se elimina del dispositivo.
- En los dispositivos iOS, se elimina el perfil MDM. Si el dispositivo no está conectado a Internet, el perfil MDM permanece instalado hasta que haya una nueva conexión disponible.
- Todos los registros relacionados con el dispositivo eliminado siguen estando disponibles.
- Su información personal y sus aplicaciones no se ven afectados.

Aviso

- No puede restaurar los dispositivos móviles eliminados.
- Si elimina accidentalmente un dispositivo bloqueado, tendrá que reestablecer los ajustes de fábrica en el dispositivo para desbloquearlo.

Para eliminar un dispositivo móvil:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione el grupo en el que está interesado.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Dispositivos** de la categoría **Ver**.
5. Haga clic en **Guardar**.
6. Marque la casilla de verificación correspondiente a los dispositivos móviles que desea eliminar.
7. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

Eliminar usuarios del inventario de red

Los usuarios vinculados actualmente a dispositivos móviles no pueden eliminarse. Primero tendrá que eliminar los dispositivos móviles correspondientes.

Nota
Sólo puede eliminar usuarios de los Grupos personalizados.

Para eliminar un usuario:

1. Diríjase a la página **Red**.
2. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. En el panel izquierdo, seleccione el grupo en el que está interesado.
4. Haga clic en el menú **Filtros** de la parte superior de la tabla del área de paneles de red y seleccione **Usuarios** de la categoría **Ver**.
5. Haga clic en **Guardar**.
6. Marque la casilla de verificación correspondiente al usuario que desea eliminar.
7. Haga clic en el botón ⊖ **Eliminar** del lateral derecho de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

6.5. Inventario de aplicaciones

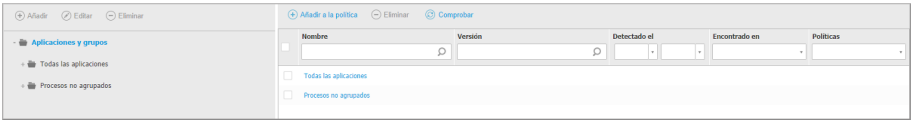
En la sección **Aplicaciones y grupos** puede ver todas las aplicaciones que la tarea de **Detección de aplicaciones** ha detectado en su red. Para más información, diríjase a "Detección de aplicaciones" (p. 101).

Las aplicaciones y los procesos se añaden automáticamente a la carpeta **Aplicaciones y grupos**, en el panel de la izquierda.

Puede organizar las aplicaciones y los procesos en grupos personalizados.

Todas las aplicaciones o procesos de una carpeta seleccionada se muestran en la tabla del panel lateral derecho. Puede buscar por nombre, versión, editor/autor, actualizador, ubicación y política.

Para ver la última información en la tabla, haga clic en el botón **Refrescar** de su parte superior. Esto puede ser necesario cuando dedique más tiempo a la página.



Inventario de aplicaciones

Importante
Las nuevas aplicaciones que se detectan cada vez que se ejecuta la tarea de **Detección de aplicaciones** van a parar automáticamente a la carpeta **Aplicaciones no agrupadas**. Los procesos que no están relacionados con aplicaciones concretas, se ubican en la carpeta **Procesos no agrupados**.

Árbol de aplicaciones y grupos

Para añadir un grupo personalizado al árbol de **Aplicaciones y grupos**:

1. Seleccione la carpeta **Todas las aplicaciones**.
2. Haga clic en el botón **Añadir** de la parte superior del árbol.
3. Introduzca un nombre en la nueva ventana.
4. Haga clic en **Aceptar** para crear el nuevo grupo.
5. Seleccione la carpeta **Aplicaciones no agrupadas**. Todas las aplicaciones agrupadas en una carpeta seleccionada se muestran en la tabla del panel lateral derecho.

6. Seleccione las aplicaciones deseadas en la tabla del panel lateral derecho. Arrastre y suelte los elementos seleccionados del panel lateral derecho para moverlos al grupo personalizado que desee en el panel de la izquierda.

Para añadir una aplicación personalizada:

1. Seleccione la carpeta objetivo en **Todas las aplicaciones**.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior del árbol.
3. Introduzca un nombre en la nueva ventana.
4. Haga clic en **Aceptar** para crear la aplicación personalizada.
5. Puede añadir procesos relacionados con la nueva aplicación personalizada desde la carpeta **Procesos no agrupados**, o desde otras carpetas que aparecen en el árbol de **Aplicaciones y grupos**. Después de seleccionar la carpeta, todos los procesos se muestran en la tabla del panel de la derecha.
6. Seleccione los procesos deseados en la tabla del panel lateral derecho. Arrastre y suelte los elementos seleccionados en el panel del lado izquierdo para moverlos a la aplicación personalizada.

Nota
Una aplicación solo puede formar parte de un grupo.

Para modificar el nombre de una aplicación o de una carpeta:

1. Selecciónelo en el árbol de **Aplicaciones y grupos**.
2. Haga clic en el botón ✎ **Editar** de la parte superior del árbol.
3. Cambie el nombre por el que desee.
4. Haga clic en **Aceptar**.

Puede mover grupos y aplicaciones a cualquier lugar dentro de la jerarquía de **Aplicaciones y grupos**. Para mover un grupo o una aplicación, arrastre y suelte desde la ubicación actual a la nueva.

Para eliminar una aplicación o una carpeta personalizada, selecciónela en el árbol de **Aplicaciones y grupos** y, a continuación, haga clic en el botón ⊖ **Eliminar** de la parte superior del árbol.

Añadir aplicaciones a las políticas

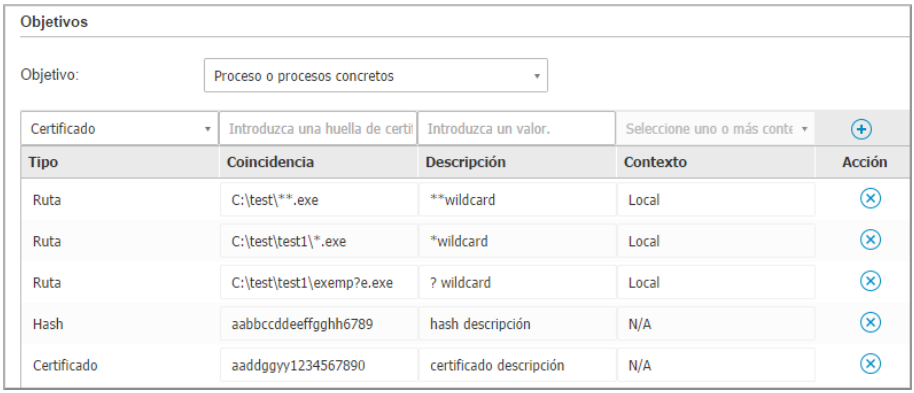
Para añadir una aplicación o un proceso a una regla directamente desde el Inventario de aplicaciones:

1. Seleccione la carpeta deseada en el árbol de **Aplicaciones y grupos**. Los contenidos de la carpeta aparecen en el panel de la derecha.
2. Seleccione los procesos o aplicaciones que desee del panel de la derecha.
3. Haga clic en el botón ⊕ **Añadir a la política** para abrir la ventana de configuración.
4. En la sección **Aplicar la regla a estas políticas**, introduzca un nombre de política existente. Utilice el cuadro de búsqueda para buscar por nombre de política o por propietario.
5. En la sección **Detalles de la regla**, introduzca el **Nombre de la regla**.
6. Seleccione la casilla de verificación **Activada** para activar la regla.
7. El tipo de objetivo se reconoce automáticamente. De ser necesario, modifique los criterios existentes:
   - **Proceso o procesos concretos**, para definir un proceso cuyo inicio se permite o deniega. Puede autorizar por ruta, hash o certificado. Las condiciones dentro de la regla se verifican mediante AND lógico.
     - Para autorizar una aplicación de una ruta determinada:
       a. Seleccione **Ruta** en la columna **Tipo**. Especifique la ruta de acceso al objeto. Puede proporcionar una ruta absoluta o relativa y utilizar caracteres comodín. El símbolo asterisco (*) se aplica a cualquier archivo dentro de un directorio. Un asterisco doble (**) se aplica a todos los archivos y directorios en el directorio indicado. Un signo de interrogación (?) sustituye a un solo carácter. También puede añadir una descripción que ayude a identificar el proceso.
       b. En el menú desplegable **Seleccione uno o más contextos** puede elegir entre local, CD-ROM, extraíble y red. Puede bloquear una aplicación ejecutada desde un dispositivo extraíble, o permitirla si la aplicación se ejecuta localmente.
     - Para autorizar una aplicación en función del hash, seleccione **Hash** en la columna **Tipo** e introduzca un valor hash. También puede añadir una descripción que ayude a identificar el proceso.

Importante
Para generar el valor hash, descargue la herramienta Fingerprint. Para más información, diríjase a "Herramientas del Control de aplicaciones" (p. 530)

– Para autorizar en función de un certificado, seleccione **Certificado** en la columna **Tipo** e introduzca una huella digital de certificado. También puede añadir una descripción que ayude a identificar el proceso.

Importante
Para obtener la huella digital del certificado, descargue la herramienta Thumbprint. Para más información, diríjase a "Herramientas del Control de aplicaciones" (p. 530)



Reglas de aplicación

Haga clic en ⊕ **Añadir** para añadir la regla. La regla recién creada tendrá la mayor prioridad en esta política.

- **Grupos o aplicaciones del inventario**, para añadir un grupo o una aplicación detectada en su red. Puede ver las aplicaciones que se ejecutan en su red en la página **Red > Inventario de aplicaciones**.

  Inserte en el campo los nombres de los grupos o aplicaciones, separados por una coma. La función de autorrellenar muestra sugerencias a medida que escribe.

8. Seleccione la casilla de verificación **Incluir subprocesos** para aplicar la regla a los procesos secundarios generados.

   Aviso
   Al establecer reglas para las aplicaciones de navegador, se recomienda desactivar esta opción para evitar riesgos de seguridad.

9. Opcionalmente, también puede definir exclusiones de la regla de inicio de procesos. La operación de añadir es similar a la descrita en los pasos anteriores.
10. En la sección de **Permisos**, elija si desea permitir o denegar la ejecución de la regla.
11. Haga clic en **Guardar** para aplicar los cambios.

Para eliminar una aplicación o un proceso:

1. Seleccione la carpeta deseada en el árbol de **Aplicaciones y grupos**.
2. Seleccione los procesos o aplicaciones que desee del panel de la derecha.
3. Haga clic en el botón **Borrar**.

Actualizadores

Debe definir actualizadores para las aplicaciones detectadas en la red.

Aviso
Si no asigna actualizadores, no se permitirá la actualización de las aplicaciones de la lista blanca.

Para asignar un actualizador:

1. Seleccione la carpeta deseada en el árbol de **Aplicaciones y grupos**. Los contenidos de la carpeta aparecen en el panel de la derecha.
2. En el panel derecho, seleccione el archivo que desea utilizar como actualizador.
3. Haga clic en el botón **Asignar actualizadores**.
4. Haga clic en **Sí** para confirmar la asignación. Los actualizadores están marcados con un icono concreto:

Actualizador

Para descartar un actualizador:

1. Seleccione la carpeta deseada en el árbol de **Aplicaciones y grupos**. Los contenidos de la carpeta aparecen en el panel de la derecha.
2. En el panel derecho, seleccione el actualizador que desea descartar.
3. Haga clic en el botón **Descartar actualizador**.
4. Haga clic en **Sí** para confirmar.

6.6. Inventario de parches

GravityZone descubre los parches que necesita su software mediante las tareas de **Análisis de parches** y luego los añade al inventario de parches.

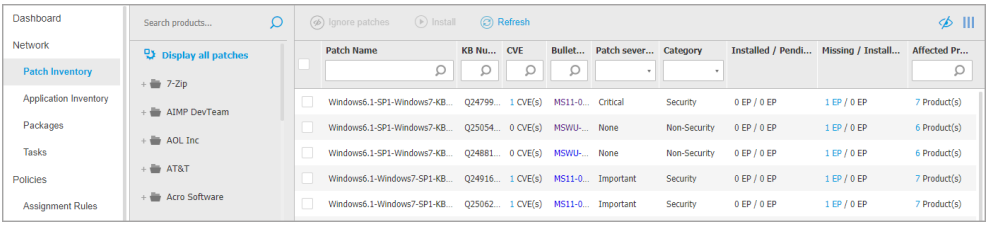
La página **Inventario de parches** muestra todos los detectados para el software instalado en sus endpoints y ofrece varias acciones que puede adoptar respecto a estos parches.

Utilice el Inventario de parches siempre que necesite implementar inmediatamente algún parche. Esta alternativa le permite resolver fácilmente ciertos problemas que conozca. Por ejemplo, si ha leído un artículo sobre una vulnerabilidad de software y conoce el ID de la CVE. Puede buscar en el inventario los parches que abordan esa CVE y luego ver qué endpoints han de actualizarse.

Para acceder al inventario de parches, haga clic en la opción **Red > Inventario de parches** en el menú principal de Control Center.

La página se organiza en dos paneles:

- El izquierdo muestra los productos de software instalados en su red, agrupados por proveedor.
- El derecho muestra una tabla con los parches disponibles e información sobre ellos.



Inventario de parches

A continuación, aprenderá a usar el inventario. Esto es lo que puede hacer:

- Consultar información de parche
- Buscar y filtrar parches
- Ignorar parches
- Instalar parches
- Desinstalar parches
- Crear estadísticas de parches

6.6.1. Consulta de la información de parches

La tabla de parches proporciona información que le ayuda a identificar parches, evaluar su importancia y ver su estado de instalación y su ámbito de aplicación. Los detalles se describen aquí:

- **Nombre del parche.** Es el nombre del archivo ejecutable que contiene el parche.
- **Número de BC.** Este número identifica el artículo de la base de conocimientos que anuncia la publicación del parche.
- **CVE.** Es el número de CVE abordadas por el parche. Al hacer clic en el número, se mostrará la lista de los ID de las CVE.
- **ID del boletín.** Es el ID del boletín de seguridad emitido por el proveedor. Este ID se vincula al artículo real, que describe el parche y proporciona información sobre la instalación.
- **Importancia del parche.** Este dato le informa sobre la importancia del parche en relación con los daños que previene.

- **Categoría.** Según el tipo de problemas que resuelvan, los parches se agrupan en dos categorías: de seguridad y ajenos a ella. Este campo le informa de la categoría a la que pertenece el parche.
- **Instalados/Pendientes de instalación.** Estos números muestran cuántos endpoints tienen el parche instalado y cuántos están pendientes de ello. Los números enlazan con la lista de estos endpoints.
- **Carencia/Instalación fallida.** Estos números muestran cuántos endpoints carecen del parche y en cuántos ha fallado su instalación. Los números enlazan con la lista de estos endpoints.
- **Productos afectados.** Este es el número de productos para los que se lanzó el parche. El número enlaza con la lista de estos productos de software.
- **Eliminable.** Si precisa revertir un determinado parche, primero debe comprobar que el parche se pueda desinstalar. Use este filtro para descubrir qué parches se pueden eliminar (revertir). Para obtener más información, consulte Desinstalar parches.

Para personalizar los datos que se muestran en la tabla:

1. Haga clic en el botón **Columnas** de la derecha de la barra de herramientas de acción.
2. Seleccione las columnas que desea ver.
3. Haga clic en el botón **Restablecer** para volver a la vista predeterminada de columnas.

Mientras está en la página, los procesos de GravityZone que se ejecutan en segundo plano pueden afectar a la base de datos. Asegúrese de ver la información más reciente en la tabla haciendo clic en el botón **Actualizar** de su parte superior.

GravityZone revisa una vez a la semana la lista de parches disponibles y elimina los que ya no son aplicables porque las aplicaciones o endpoints correspondientes ya no existen.

GravityZone también revisa y elimina diariamente los parches que no están disponibles en la lista, aunque pueden estar presentes en algunos endpoints.

6.6.2. Búsqueda y filtrado de parches

Por defecto, Control Center muestra todos los parches disponibles para su software. GravityZone le brinda varias opciones para encontrar rápidamente los parches que necesita.

Filtrado de parches por producto

1. Busque el producto en el panel de la izquierda.

   Puede hacer esto desplazándose por la lista para encontrar su proveedor o escribiendo su nombre en el cuadro de búsqueda de la zona superior del panel.

2. Haga clic en el nombre del proveedor para expandir la lista y ver sus productos.

3. Seleccione el producto para ver los parches disponibles o anule la selección para ocultar sus parches.

4. Repita los pasos anteriores para los otros productos que le interesen.

Si desea volver a ver los parches de todos los productos, haga clic en el botón **Mostrar todos los parches** de la zona superior del panel izquierdo.

Filtrado de parches por utilidad

Un parche se vuelve innecesario si, por ejemplo, ya está implementada en el endpoint esa misma versión del parche u otra más reciente. Dado que el inventario puede contener en algún momento esos parches, GravityZone le permite ignorarlos. Seleccione esos parches y haga clic en el botón **Ignorar parches** de la zona superior de la tabla.

Control Center muestra los parches ignorados en una vista diferente. Haga clic en el botón **Administrado/Ignorado** del lado derecho de la barra de herramientas de acción para alternar entre las vistas:

- - Para ver los parches ignorados.
- - Para ver los parches administrados.

Filtrado de parches por detalles

Utilice las posibilidades de búsqueda para filtrar parches según ciertos criterios o detalles conocidos. Introduzca los términos de búsqueda en los cuadros de búsqueda de la zona superior de la tabla de parches. Los parches que cumplen los criterios se muestran en la tabla a medida que escribe o una vez realizada la selección.

Si borra los campos de búsqueda se restablecerá esta.

6.6.3. Ignorar parches

Es posible que deba excluir ciertos parches del inventario de parches, si no piensa instalarlos en sus endpoints, utilizando el comando **Ignorar parches**.

Un parche ignorado se excluirá de las tareas de parches automáticos y de los informes de parches y, además, no se contará como parche que falte.

Para ignorar un parche:

1. En la página **Inventario de parches**, seleccione uno o varios parches que desee ignorar.
2. Haga clic en el botón **Ignorar parches** en la zona superior de la tabla.

   Aparecerá una ventana de configuración donde podrá ver información sobre los parches seleccionados, junto con los posibles parches subordinados.
3. Haga clic en **Ignorar**. El parche se eliminará de la lista del inventario de parches.

Puede encontrar los parches ignorados en una vista específica y realizar acciones en relación con ellos:

- Haga clic en el botón **Mostrar parches ignorados** en la zona superior derecha de la tabla. Verá la lista con todos los parches ignorados.
- Puede obtener más información sobre determinado parche ignorado generando un informe de estadísticas de parches. Seleccione el parche ignorado que desee y haga clic en el botón **Estadísticas de parches** en la zona superior de la tabla. Para obtener más información, consulte "Crear estadísticas de parches" (p. 209)
- Para restaurar los parches ignorados, selecciónelos y haga clic en el botón **Restaurar parches** en la zona superior de la tabla.

  Aparecerá una ventana de configuración donde podrá ver información sobre los parches seleccionados.

  Haga clic en el botón **Restaurar** para reponer el parche en el inventario.

6.6.4. Instalación de parches

Para instalar parches desde el Inventario de parches:

1. Acceda a **Red > Inventario de parches**.
2. Busque los parches que desea instalar. Si es necesario, use las opciones de filtrado para encontrarlos rápidamente.

3. Seleccione los parches y, a continuación, haga clic en el botón **Instalar** de la zona superior de la tabla. Aparecerá una ventana de configuración en la que puede editar los detalles de instalación del parche.

   Verá los parches seleccionados, junto con los posibles parches subordinados.

   - Seleccione los grupos de endpoints objetivo.
   - **En caso necesario, reiniciar los endpoints después de instalar el parche**. Esta opción reiniciará los endpoints inmediatamente después de la instalación del parche, en caso de que sea necesario reiniciar el sistema. Tenga en cuenta que esta acción puede interrumpir la actividad del usuario.

     Dejar esta opción desactivada implica que, en caso de ser preciso reiniciar el sistema en los endpoints objetivo, estos mostrarán el icono de estado de reinicio pendiente en el inventario de red de GravityZone. En este caso, dispone de las siguientes opciones:

     – Envíe una tarea **Reiniciar máquina** a los endpoints pendientes de reinicio cuando considere oportuno. Para obtener más información, consulte "Reiniciar máquina" (p. 100).

     – Configure la política activa para notificar al usuario del endpoint que es necesario reiniciar. Para ello, acceda a la política activa en el endpoint objetivo, vaya a **General > Notificaciones** y habilite la opción **Notificación de reinicio de endpoint**. En este caso, el usuario verá una ventana emergente cada vez que se precise un reinicio debido a los cambios realizados por los componentes especificados de GravityZone (en este caso, la Administración de parches). La ventana emergente brinda la opción de posponer el reinicio. Si el usuario elige posponer, la notificación de reinicio aparecerá en la pantalla periódicamente, hasta que el usuario reinicie el sistema o hasta que haya transcurrido el tiempo establecido por el administrador de la empresa.

       Para obtener más información, consulte "Notificación de reinicio de endpoint" (p. 244).

4. Haga clic en **Instalar**.

   Se crea la tarea de instalación junto con las subtareas para cada endpoint objetivo.

Nota

- También puede instalar un parche desde la página **Red**, comenzando por los endpoints concretos que desea administrar. En este caso, seleccione los endpoints del inventario de red, haga clic en el botón **Tareas** en la zona superior de la tabla y elija **Instalación de parches**. Para más información, diríjase a "Instalación de parches" (p. 83).
- Tras instalar un parche, recomendamos enviar una tarea de Análisis de parches a los endpoints objetivo. Dicha acción actualizará la información del parche almacenada en GravityZone para sus redes administradas.

6.6.5. Desinstalación de parches

Puede que deba eliminar los parches que hayan ocasionado un mal funcionamiento de los endpoints objetivo. GravityZone ofrece la posibilidad de revertir los parches instalados en su red, lo que restaura el software a su estado anterior antes de aplicar el parche.

La opción de desinstalación solo está disponible para parches eliminables. El inventario de parches de GravityZone incluye una columna **Eliminable** que le permite filtrar los parches por este criterio.

Nota
La posibilidad de eliminación depende del fabricante del parche o de los cambios realizados por el parche en el software. En el caso de parches que no sea posible eliminar, puede que deba volver a instalar el software.

Para desinstalar un parche:

1. Acceda a **Red > Inventario de parches**.
2. Seleccione el parche que desea desinstalar. Para buscar un parche concreto, emplee los filtros disponibles en las columnas, como el número de KB o CVE. Utilice la columna **Eliminable** para mostrar solo los parches disponibles que se pueden desinstalar.

   Nota
   Puede desinstalar solo un parche a la vez para uno o varios endpoints.

3. Haga clic en el botón **Desinstalar** en la zona superior de la tabla. Aparecerá una ventana de configuración en la que puede editar los detalles de la tarea de desinstalación.

- **Nombre de la tarea**. Si lo desea, puede editar el nombre por defecto de la tarea de desinstalación del parche. Así, identificará más fácilmente la tarea en la página de **Tareas**.
- **Añadir el parche a la lista de parches ignorados**. Por lo general, no volverá a necesitar un parche que desee desinstalar. Esta opción añade automáticamente el parche a la lista de ignorados una vez que se desinstala.
- **En caso necesario, reiniciar los endpoints después de desinstalar el parche**. Esta opción reiniciará los endpoints inmediatamente después de la desinstalación del parche, en caso de que sea necesario reiniciar el sistema. Tenga en cuenta que esta acción puede interrumpir la actividad del usuario.

  Dejar esta opción desactivada implica que, en caso de ser preciso reiniciar el sistema en los endpoints objetivo, estos mostrarán el icono de estado de reinicio pendiente en el inventario de red de GravityZone. En este caso, dispone de las siguientes opciones:

  – Envíe una tarea **Reiniciar máquina** a los endpoints pendientes de reinicio cuando considere oportuno. Para obtener más información, consulte "Reiniciar máquina" (p. 100).

  – Configure la política activa para notificar al usuario del endpoint que es necesario reiniciar. Para ello, acceda a la política activa en el endpoint objetivo, vaya a **General > Notificaciones** y habilite la opción **Notificación de reinicio de endpoint**. En este caso, el usuario verá una ventana emergente cada vez que se precise un reinicio debido a los cambios realizados por los componentes especificados de GravityZone (en este caso, la Administración de parches). La ventana emergente brinda la opción de posponer el reinicio. Si el usuario elige posponer, la notificación de reinicio aparecerá en la pantalla periódicamente, hasta que el usuario reinicie el sistema o hasta que haya transcurrido el tiempo establecido por el administrador de la empresa.

    Para obtener más información, consulte "Notificación de reinicio de endpoint" (p. 244).
- En tabla **Revertir objetivos**, seleccione los endpoints en los que desea desinstalar el parche.

  Puede seleccionar uno o varios endpoints de su red. Utilice los filtros disponibles para ubicar el endpoint que desee.

Nota
La tabla muestra solo los endpoints donde está instalado el parche seleccionado.

4. Haga clic en **Confirmar**. Se creará una tarea de **Desinstalación de parche** y se enviará a los endpoints objetivo.

   Para cada tarea de desinstalación de parche finalizada, se genera automáticamente un informe de **Desinstalación de parche** que proporciona información sobre el parche, los endpoints objetivo y el estado de la tarea desinstalación de parche.

Nota
Tras desinstalar un parche, recomendamos enviar una tarea de Análisis de parches a los endpoints objetivo. Dicha acción actualizará la información del parche almacenada en GravityZone para sus redes administradas.

6.6.6. Crear estadísticas de parches

Si precisa información detallada sobre el estado de un determinado parche para todos los endpoints, recurra a **Estadísticas de parches**, que genera un informe instantáneo sobre el parche seleccionado:

1. En la página **Inventario de parches**, seleccione el parche que desee en el panel derecho.
2. Haga clic en el botón **Estadísticas de parches** en la zona superior de la tabla.

   Aparece un informe de estadísticas de parches que proporciona diversos detalles sobre el estado del parche, entre los que se incluyen los siguientes:

   - Un gráfico circular que muestra el porcentaje de estados de parches instalados, fallidos, ausentes y pendientes en los endpoints que han informado del parche.
   - Una tabla que muestra la siguiente información:
     - **Nombre**, **FQDN**, **IP** y **sistema operativo** de cada endpoint que ha informado del parche.
     - **Última comprobación**: La hora a la que se comprobó el parche por última vez en el endpoint.
     - **Estado del parche**: Instalado, fallido, ausente o ignorado.

Nota
La opción de estadísticas de parches está disponible tanto para parches administrados como para los ignorados.

6.7. 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.

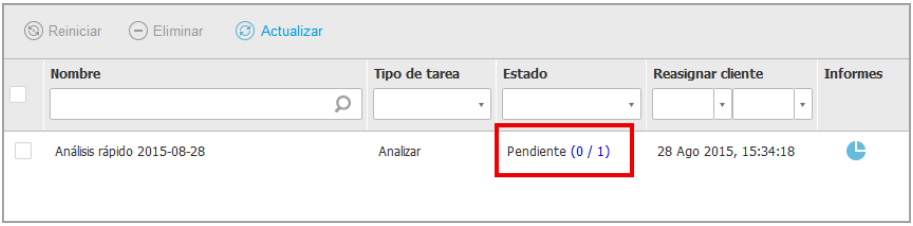
Desde la página **Red > Tareas** puede hacer lo siguiente:

- Comprobar el estado de la tarea
- Ver informes de tareas
- Reiniciar tareas
- Detener tareas de análisis de Exchange
- Eliminar Tareas

6.7.1. 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 ninguna de las subtareas se ha iniciado aún o cuando se ha superado el número de implementaciones simultáneas. El número máximo de implementaciones simultáneas puede establecerse desde el menú **Configuración**. Para más información, consulte la Guía de instalación de GravityZone.
- **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.

    Además, para las tareas de análisis bajo demanda de Exchange, también puede ver el estado de finalización.

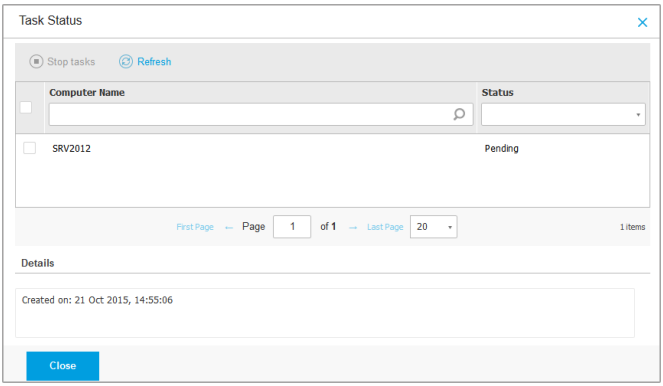
  - **Finalizado**, cuando la subtarea ha finalizado correctamente.

  - **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.
    - El dispositivo objetivo está inactivo (desconectado), en el caso de dispositivos móviles. La tarea se ejecutará en el dispositivo objetivo tan pronto como vuelva a estar conectado.

- **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.
- **Deteniendo**, cuando el análisis bajo demanda está tardando demasiado y ha elegido detenerlo.

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.

6.7.2. 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. Elija el objeto de red deseado en el selector de vistas.
3. Marque la casilla de verificación correspondiente a la tarea de análisis que le interese.

4. 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. 423).

6.7.3. Reinicio de tareas

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

1. Diríjase a la página **Red > Tareas**.
2. Elija el objeto de red deseado en el selector de vistas.
3. Marque las casillas de verificación correspondientes a las tareas fallidas.
4. Haga clic en el botón **Reiniciar** de la zona superior de la tabla. Se reiniciarán las tareas fallidas y su estado cambiará a **Intentando de nuevo**.

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

6.7.4. Detención de tareas de análisis de Exchange

Analizar el almacén de Exchange puede tardar un tiempo considerable. Si por cualquier motivo desea detener una tarea de análisis bajo demanda de Exchange, siga los pasos descritos en este documento:

1. Diríjase a la página **Red > Tareas**.
2. Elija la vista de red deseada en el selector de vistas.
3. Haga clic en la columna **Estado** para abrir la ventana **Estado de la tarea**.
4. Marque la casilla de verificación correspondiente a las subtareas pendientes o en ejecución que desee detener.
5. Haga clic en el botón **Detener tareas** en la zona superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

Nota
También puede detener un análisis bajo demanda del almacén de Exchange desde el área de eventos de Bitdefender Endpoint Security Tools.

6.7.5. Eliminar Tareas

GravityZone borra automáticamente las tareas pendientes transcurridos dos días, y las tareas finalizadas después de treinta días. Si aun así tuviera muchas tareas, le recomendamos que elimine las que ya no necesite, para que no tenga una lista excesivamente larga.

1. Diríjase a la página **Red > Tareas**.
2. Elija el objeto de red deseado en el selector de vistas.
3. Marque la casilla de verificación correspondiente a la tarea que desee eliminar.
4. Haga clic en el botón ⊖ **Eliminar** de la parte superior 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.

6.8. Eliminación de endpoints del inventario de red

El inventario de red contiene por defecto la carpeta **Eliminados**, destinada al almacenamiento de los endpoints que no desee administrar.

La acción **Eliminar** tiene los siguientes efectos:

- Cuando se eliminan los endpoints no administrados, se mueven directamente a la carpeta **Eliminados**.
- Cuando se eliminan los endpoints administrados:
  - Se crea una tarea de desinstalación del cliente.
  - Se libera un puesto de licencia.
  - Los endpoints se mueven a la carpeta **Eliminados**.

Para eliminar endpoints del inventario de red:

1. Diríjase a la página **Red**.
2. Elija la vista de red adecuada desde el selector de vistas.
3. Seleccione **Grupos personalizados** en el panel lateral izquierdo. Todos los endpoints de este grupo se muestran en la tabla del panel derecho.

Nota
Solo puede eliminar los endpoints mostrados en **Grupos personalizados**, que se detectan fuera de cualquier infraestructura de red integrada.

4. En el panel de la derecha, marque la casilla de verificación del endpoint que desee eliminar.
5. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

   Si el endpoint eliminado está administrado, se creará una tarea **Desinstalar el cliente** en la página **Tareas** y se desinstalará el agente de seguridad del endpoint, con lo que se liberará un puesto de licencia.
6. El endpoint se moverá a la carpeta **Eliminados**.

En cualquier momento, puede mover endpoints de la carpeta **Eliminados** a **Grupos personalizados** con arrastrar y soltar.

Nota
- Si desea excluir permanentemente ciertos endpoints de la administración, debe mantenerlos en la carpeta **Eliminados**.
- Si elimina los endpoints de la carpeta **Eliminados**, se eliminarán por completo de la base de datos de GravityZone. No obstante, los endpoints excluidos que estén conectados se detectarán en la próxima tarea de Detección de redes y aparecerán en el inventario de red como nuevos endpoints.

6.9. Configuración de los ajustes de red

En la página **Configuración > Ajustes de red**, puede configurar los ajustes relativos al inventario de red, como guardar filtros, retener la última ubicación explorada o crear y administrar reglas programadas para eliminar máquinas virtuales sin uso.

Las opciones se organizan en las siguientes categorías:

- Ajustes de inventario de red
- Limpieza de máquinas sin conexión

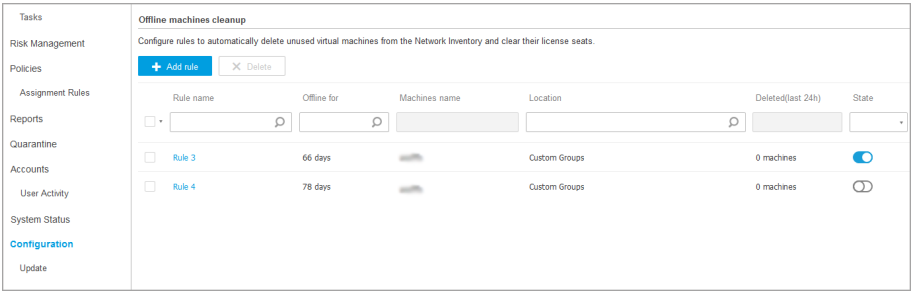
6.9.1. Ajustes del inventario de red

En la sección **Ajustes del inventario de red** se dispone de las siguientes opciones:

- **Guardar filtros del inventario de red**. Marque esta casilla de verificación para guardar sus filtros en la página **Red** entre sesiones de Control Center.
- **Recordar la última ubicación visitada en el Inventario de red hasta que cierre la sesión**. Marque esta casilla de verificación para guardar la última ubicación a la que ha accedido al abandonar la página **Red**. La ubicación no se guarda entre sesiones.
- **Evitar duplicados de endpoints clonados**. Seleccione esta opción para habilitar un nuevo tipo de objetos de red en GravityZone, llamados imágenes maestras. De esta manera, puede diferenciar los endpoints de origen de sus clones. Más adelante, debe marcar todos los endpoints que clone de la siguiente manera:
  1. Diríjase a la página **Red**.
  2. Seleccione el endpoint que desea clonar.
  3. Desde su menú contextual, seleccione **Marcar como imagen maestra**.

6.9.2. Limpieza de máquinas sin conexión

En la sección **Limpieza de máquinas sin conexión**, puede programar reglas para la eliminación automática de máquinas virtuales sin uso del inventario de red.



Configuración - Ajustes de red - Limpieza de máquinas sin conexión

Creando Reglas

Para crear una regla de limpieza:

1. En la sección **Limpieza de máquinas sin conexión**, haga clic en el botón **Añadir regla**.
2. En la página de configuración:

a. Escriba un nombre de regla.

b. Seleccione una hora para la limpieza diaria.

c. Defina los criterios de limpieza:

- El número de días en que las máquinas estuvieron sin conexión (de 1 a 90).
- Un patrón de nombre, que puede aplicarse a una sola máquina virtual o a varias máquinas virtuales.

  Por ejemplo, use `nombrevm_1` para eliminar la máquina con este nombre. Como alternativa, añada `nombrevm_*` para eliminar todas las máquinas cuyo nombre comience por `nombrevm_`.

  Este campo distingue entre mayúsculas y minúsculas y acepta solo letras, dígitos y los caracteres especiales asterisco (*), guion bajo (_) y guion (-). El nombre no puede empezar por un asterisco (*).

d. Seleccione los grupos de endpoints objetivo en el inventario de red donde desea aplicar la regla.

3. Haga clic en **Guardar**.

Visualización y administración de reglas

La sección **Ajustes de red > Limpieza de máquinas sin conexión** muestra todas las reglas que ha creado. Una tabla le proporciona la siguiente información:

- Nombre de la regla.
- El número de días transcurridos desde que las máquinas no se conectan.
- Patrón de nombre de máquinas.
- Ubicación en el inventario de red.
- El número de máquinas eliminadas durante las últimas 24 horas.
- Estado: habilitada, inhabilitada o no válida.

> **Nota**
> Una regla no es válida cuando los objetivos ya no son válidos debido a ciertas razones. Por ejemplo, las máquinas virtuales se han eliminado o ya no tiene acceso a ellas.

Una regla recién creada queda habilitada por defecto. Puede habilitar e inhabilitar reglas en cualquier momento utilizando el conmutador de Activar/Desactivar de la columna **Estado**.

Si es necesario, use las opciones de clasificación y filtrado de la parte superior de la tabla para encontrar reglas concretas.

Para modificar una regla:

1. Haga clic en el nombre de la regla.
2. En la página de configuración, edite los detalles de la regla.
3. Haga clic en **Guardar**.

Para eliminar una o más reglas:

1. Use las casillas de verificación para seleccionar una o más reglas.
2. Haga clic en el botón **Eliminar** de la zona superior de la tabla.

6.10. Configuración de los ajustes de Security Server

Security Server utiliza su mecanismo de almacenamiento en caché para deduplicar el análisis antimalware, con lo que se optimiza este proceso. Un paso más en la optimización de análisis es compartir esta caché con otros Security Server.

El uso compartido de caché solo funciona entre Security Server que sean del mismo tipo. Por ejemplo, un Security Server Multiplataforma compartirá su caché solo con otro Security Server Multiplataforma y no con un Security Server para NSX.

Para habilitar y configurar el uso compartido de la caché:

1. Acceda a la página **Configuración > Ajustes de Security Server**.
2. Marque la casilla de verificación **Uso compartido de caché de Security Server**.
3. Elija el ámbito de aplicación del uso compartido:
   - Todos los Security Server disponibles.

     Se recomienda utilizar esta opción si todos los Security Server están en la misma red.
   - Security Server disponibles en la lista de asignación.

     Use esta opción cuando los Security Server se distribuyan en diferentes redes y el uso compartido de la caché pueda generar un gran volumen de tráfico.

4. Si limita el ámbito de aplicación, cree el grupo de Security Server. Seleccione los Security Server en la lista desplegable y haga clic en **Añadir**.

   Solo los Security Server de la tabla compartirán su caché.

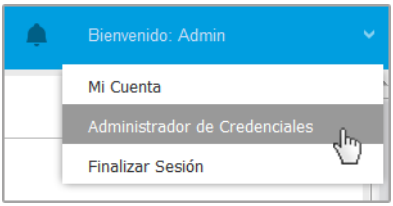
   Nota
   Los Security Server para NSX-T y NSX-V intercambian información de caché solo dentro del mismo vCenter Server.

5. Haga clic en **Guardar**.

6.11. Administrador de Credenciales

El Gestor de credenciales le ayuda a definir las credenciales necesarias para acceder a los inventarios del vCenter Server disponibles y también para la autenticación remota en los distintos sistemas operativos de su red.

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



El menú Gestor de credenciales

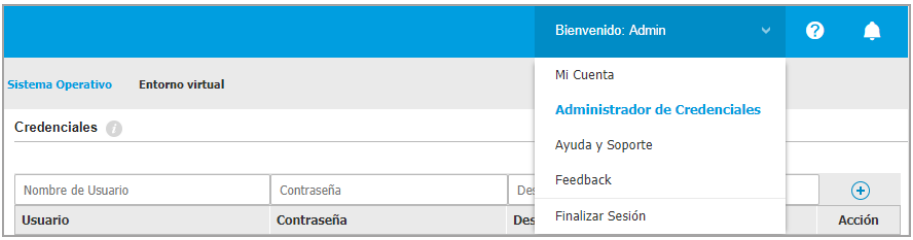
La ventana **Gestor de credenciales** contiene dos pestañas:

- Sistema Operativo
- Entorno virtual

6.11.1. Sistema Operativo

En la pestaña **Sistema operativo** puede gestionar las credenciales de administrador necesarias para la autenticación remota cuando se envían tareas de instalación a equipos y máquinas virtuales de su red.

Para añadir un conjunto 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 de la zona superior del encabezado de la tabla. 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 normas de Windows cuando introduzca el nombre de una cuenta de usuario:

   - Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
   - Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

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

6.11.2. Entorno virtual

Desde la pestaña Entorno virtual, puede administrar las credenciales de autenticación para los sistemas servidores virtualizados disponibles.

Para acceder a la infraestructura virtualizada integrada con Control Center, debe proporcionar sus credenciales de usuario para cada sistema de servidor virtualizado disponible. Control Center usa sus credenciales para conectar con la infraestructura virtualizada, mostrando solamente los recursos a los que tiene acceso (según se define en el servidor virtualizado).

Para especificar las credenciales necesarias para conectarse a un servidor virtualizado:

1. Seleccione el servidor en el menú correspondiente.

   Nota
   Si el menú no está disponible, o bien no se ha configurado todavía la integración, o todas las credenciales necesarias ya han sido configuradas.

2. Escriba su nombre de usuario y contraseña, y una descripción adecuada.
3. Haga clic en el botón ⊕ **Añadir**. El nuevo conjunto de credenciales se añade a la tabla.

   Nota
   Sí no configura sus credenciales de autenticación en el Gestor de credenciales, tendrá que introducirlas cada vez que quiera examinar el inventario de cualquier sistema servidor virtualizado. Una vez introducidas las credenciales, se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

   Importante
   Siempre que cambie su contraseña de usuario del servidor virtualizado, recuerde actualizarla también en el Gestor de credenciales.

6.11.3. 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.

7. POLÍTICAS DE SEGURIDAD

Una vez instalada, la protección de Bitdefender puede configurarse y administrarse desde Control Center usando políticas de seguridad. Una política específica las opciones de seguridad que se aplican a los elementos del inventario de red (equipos, máquinas virtuales o dispositivos móviles).

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. Siempre que esté activada la integración NSX, hay disponibles otras tres políticas de seguridad por defecto para NSX, una para cada nivel de seguridad: tolerante, normal y agresiva. Estas políticas están preconfiguradas con los ajustes de protección recomendados. No puede modificar ni borrar las políticas por defecto.

Puede crear todas las políticas que necesite basadas en requisitos de seguridad para cada tipo de elemento de red administrado.

Esto es lo que necesita saber sobre políticas:

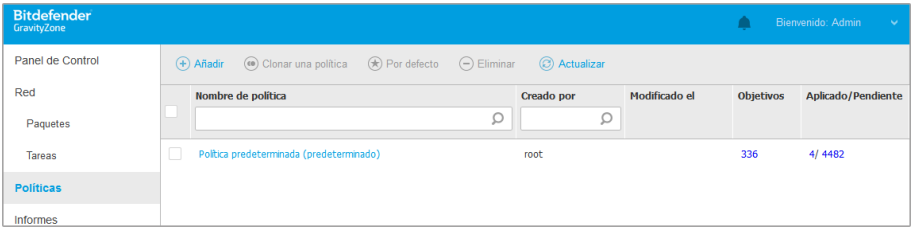
- Las políticas se crean en la página **Políticas** y se asignan a elementos de red en la página **Red**.
- Las políticas pueden heredar varios ajustes de módulos de otras políticas.
- Puede configurar la asignación de políticas a los endpoints de modo que una política se aplique solo en determinadas condiciones, en función de la ubicación o del usuario que haya iniciado sesión. Por lo tanto, un endpoint puede tener varias políticas asignadas.
- Los endpoints pueden tener una sola política activa en cada momento.
- Puede asignar una política a endpoints individuales o a grupos de endpoints. Al asignar una política, también definirá las opciones de herencia de esta. Por defecto, todos los endpoints heredan la política del grupo primario.
- 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.
- La página **Políticas** solo muestra los siguientes tipos de políticas:
  - Políticas creadas por usted.
  - Otras políticas (como la política predeterminada o plantillas creadas por otros usuarios) que se asignan a los endpoints de su cuenta.

- 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.

Aviso
Solo se aplicarán a los endpoints objetivo los módulos de políticas disponibles. Tenga en cuenta que para los sistemas operativos de servidor solo está disponible el módulo Antimalware.

7.1. Administrando las Políticas

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



La página Políticas

Cada tipo de endpoint posee unos ajustes de política concretos. Para administrar políticas, primero debe seleccionar el tipo de endpoint (**Equipos y máquinas virtuales** o **Dispositivos móviles**) en el selector de vistas.

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.*
- El número de objetivos a los que se aplicó la política o para los que está pendiente de aplicar.*

Para las políticas con el módulo NSX activado, se dispone de información adicional:

- El nombre de la política de NSX, que se utiliza para identificar la política de Bitdefender en VMware vSphere.

- La visibilidad de la política en las consolas de administración, que le permite filtrar las políticas para NSX. Así, mientras que las políticas de tipo **Local** solo son visibles en Bitdefender Control Center, las de tipo **Global** también lo son en VMware NSX.

Estos detalles están ocultos por defecto.

Para personalizar los datos de la política que se muestran en la tabla:

1. Haga clic en el botón **Columnas** de la derecha de la barra de herramientas de acción.
2. Seleccione las columnas que desea ver.
3. Haga clic en el botón **Restablecer** para volver a la vista predeterminada de columnas.

* Al hacer clic en el número se le redirigirá a la página **Red**, donde podrá ver los endpoints correspondientes. Se le pedirá que elija la vista de red. Esta acción creará un filtro utilizando los criterios de la política.

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

7.1.1. Crear políticas

Puede crear políticas ya sea añadiendo una nueva o duplicando (clonando) una existente.

Para crear una política de seguridad:

1. Diríjase a la página **Políticas**.
2. Elija el tipo de endpoint que desee en el selector de vistas.
3. Seleccione el método de creación de políticas:
   - **Añadir nueva política**.
     - Haga clic en el botón **Añadir** en la parte superior 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** de la zona superior de la tabla.

4. Configure los ajustes de la política. Para obtener más información detallada, consulte:
   - “Políticas de equipos y máquinas virtuales” (p. 238)
   - “Políticas de dispositivos móviles” (p. 398)
5. Haga clic en **Guardar** para crear la política y volver a la lista de políticas.

Cuando se definen las políticas que se utilizarán en VMware NSX, además de configurar los ajustes de la protección antimalware en GravityZone Control Center, también es necesario crear una política en NSX, dándole instrucciones para usar la política de GravityZone como perfil de servicio. Para crear una política de seguridad NSX:

1. Inicie sesión en vSphere Web Client.
2. Acceda a la pestaña **Red y seguridad > Service Composer > Políticas de seguridad**.
3. Haga clic en el botón **Crear política de seguridad** de la barra de herramientas en la zona superior de la tabla de políticas. Se muestra la ventana de configuración.
4. Introduzca el nombre de la política y haga clic en **Siguiente**.

   Opcionalmente, también puede añadir una breve descripción.
5. Haga clic en el botón **Añadir servicio Guest Introspection** en la zona superior de la tabla. Se muestra la ventana de configuración del servicio Guest Introspection.
6. Introduzca el nombre y la descripción del servicio.
7. Deje la acción por defecto seleccionada para permitir que se aplique el perfil de servicio de Bitdefender al grupo de seguridad.
8. En el menú **Nombre del servicio**, seleccione **Bitdefender**.
9. En el menú **Perfil del servicio**, seleccione una política de seguridad de GravityZone existente.
10. Deje los valores por defecto de las opciones **Estado** y **Hacer cumplir**.

> **Nota**
> Para obtener más información sobre los ajustes de las políticas de seguridad, consulte la Documentación de VMware NSX.

11. Haga clic en **OK** para añadir el servicio.
12. Haga clic en **Siguiente** hasta llegar al último paso y, a continuación, haga clic en **Finalizar**.

7.1.2. Asignando Políticas

A los endpoints se les asigna inicialmente la política por defecto. Una vez definidas las políticas necesarias en la página **Políticas**, puede asignarlas a endpoints.

El proceso de asignación de políticas va ligado a los diversos entornos con los que se integra GravityZone. Para ciertas integraciones, como por ejemplo VMware NSX, las políticas están accesibles desde fuera de GravityZone Control Center. Se conocen también como políticas externas.

Asignación de políticas locales

Puede asignar políticas locales de dos maneras:

- Asignación basada en el dispositivo, lo que significa que selecciona manualmente los endpoints objetivo a los que asignará las políticas. Estas políticas se conocen también como políticas de dispositivos.
- Asignación basada en reglas, lo que significa que una política se asigna a un endpoint administrado si los ajustes de red en el endpoint coinciden con las condiciones establecidas en una regla de asignación existente.

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**.
- En las máquinas virtuales protegidas por sí solas de HVI, solo puede asignar políticas de dispositivos. Cuando Bitdefender Endpoint Security Tools está instalado en ellas, puede asignar también políticas basadas en reglas; el agente de seguridad gestiona la activación de la política.

Asignación de políticas de dispositivos

En GravityZone, puede asignar políticas de varias maneras:

- Asignar la política directamente al objetivo.
- Asignar la política del grupo primario mediante la herencia.
- Forzar la herencia de políticas al objetivo.

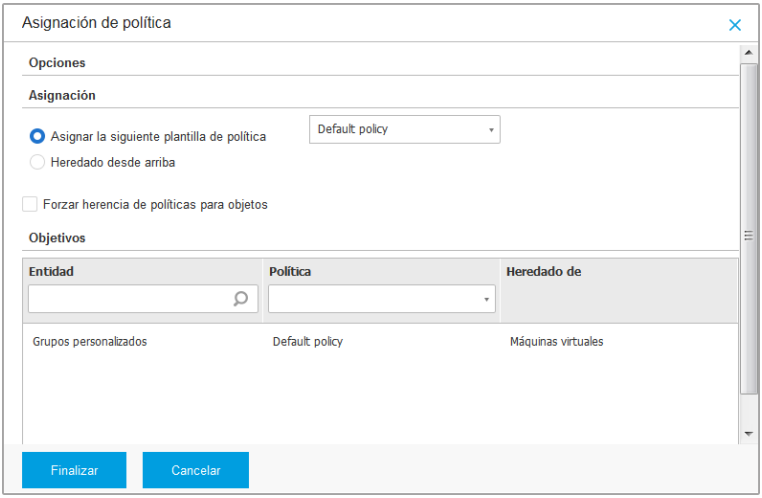
Por defecto, cada endpoint o grupo de endpoints hereda la política del grupo primario. El cambio de política del grupo primario afectará a todos los descendientes, a excepción de los que tengan una política impuesta.

Para asignar una política de dispositivo:

1. Diríjase a la página **Red**.
2. Elija la vista de red en el selector de vistas.
3. Seleccione los endpoints objetivo. Puede seleccionar uno o varios endpoints o grupos de endpoints.

   Para conservar la compatibilidad con versiones anteriores, no puede cambiar la política por defecto del grupo raíz. Por ejemplo, la **Política por defecto** siempre estará asignada a **Equipos y máquinas virtuales**.
4. Haga clic en el botón **Asignar política** de la parte superior de la tabla o seleccione la opción **Asignar política** en el menú contextual.

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



Ajustes de asignación de políticas

5. Compruebe la tabla con los endpoints objetivo. Para cada endpoint, puede ver:
   - La política asignada.

- El grupo primario del que hereda la política el objetivo, de ser el caso.

  Si el grupo está imponiendo la política, puede hacer clic en su nombre para ver la página de **Asignación de política** con este grupo como objetivo.

- El estado de imposición.

  Este estado muestra si el objetivo está imponiendo la herencia de la política o se le ha impuesto la política heredada.

  Observe los objetivos con política impuesta (estado **Está impuesta**). Sus políticas no pueden sustituirse. En tales casos, se muestra un mensaje de advertencia.

6. De aparecer una advertencia, haga clic en el enlace **Excluir estos objetivos** para continuar.
7. Elija una de las opciones disponibles para asignar la política:
   - **Asignar la siguiente plantilla de política**: para asignar determinada política directamente a los endpoints objetivo.
   - **Heredado desde arriba**: para utilizar la política del grupo primario.
8. Si decide asignar una plantilla de política:
   a. Seleccione la política en la lista desplegable.
   b. Seleccione **Forzar la herencia de políticas en grupos dependientes** para lograr lo siguiente:
      - Asignar la política a todos los descendientes de los grupos objetivo, sin excepción.
      - Evitar cambiarla desde un lugar más bajo de la jerarquía.

      Una nueva tabla muestra recursivamente todos los endpoints y grupos de endpoints afectados, junto con las políticas que se reemplazarán.
9. Haga clic en **Finalizar** para guardar y aplicar los cambios. De no ser así, haga clic en **Atrás** o **Cancelar** para volver a la página anterior.

Una vez finalizadas, las políticas se envían a los endpoints inmediatamente. La configuración debería aplicarse a los endpoints en menos de un minuto (siempre que estén conectados). Si un endpoint no está conectado, los ajustes se aplicarán tan pronto como vuelva a conectarse.

Para comprobar si la política se asignó correctamente:

1. En la página **Red**, haga clic en el nombre del endpoint que le interese. Control Center mostrará la ventana de **información**.
2. Consulte la sección de **Política** para ver el estado de la política actual. Debe mostrar **Aplicada**.

Otro método para comprobar el estado de la asignación es desde la información de la política:

1. Diríjase a la página **Políticas**.
2. Busque la política que asignó.

   En la columna **Activo/Aplicado/Pendiente**, puede ver el número de endpoints en cada uno de los tres estados.
3. Haga clic en cualquier número para ver la lista de endpoints con su estado respectivo en la página **Red**.

Asignación de políticas basadas en reglas

La página **Políticas > Reglas de asignación** le permite definir políticas en función de ubicaciones o usuarios. Por ejemplo, puede aplicar reglas de cortafuego más restrictivas cuando los usuarios se conecten a Internet desde fuera de la empresa o puede activar el Control de acceso Web para los usuarios que no formen parte del grupo de administradores.

Esto es lo que necesita saber sobre las reglas de asignación:

- Los endpoints solo pueden tener una política activa en cada momento.
- Una política aplicada a través de una regla sobrescribirá la política del dispositivo establecida en el endpoint.
- Si ninguna de las reglas de asignación fuera aplicable, entonces se aplicaría la política del dispositivo.
- Las reglas se clasifican y procesan por orden de prioridad, siendo `1` la más alta. Es posible tener varias reglas para el mismo objetivo. En tal caso, se aplicará la primera regla que cumpla con los ajustes de conexión activos en el endpoint objetivo.

  Por ejemplo, si un endpoint coincide con una regla de usuario con prioridad 4 y con una regla de ubicación con prioridad 3, se aplicará la regla de ubicación.

Aviso
Al crear reglas, asegúrese de tener en cuenta los ajustes delicados, como las exclusiones, la comunicación o la información del proxy.
Como buena práctica, se recomienda utilizar la herencia de políticas para mantener los ajustes críticos de la política del dispositivo también en la política utilizada por las reglas de asignación.

Para crear una nueva regla:

1. Diríjase a la página **Reglas de asignación**.
2. Haga clic en el botón **Añadir** en la parte superior de la tabla.
3. Seleccione el tipo de regla:
   - Regla de ubicación
   - Regla de usuario
   - Regla de etiqueta
4. Configure los ajustes de la regla según sea necesario.
5. Haga clic en **Guardar** para almacenar los cambios y aplicar la regla a los endpoints objetivo de la política.

Para cambiar los ajustes de una regla existente:

1. En la página **Reglas de asignación**, encuentre la regla que busca y haga clic en su nombre para modificarlo.
2. Configure los ajustes de la regla según sea necesario.
3. Haga clic en **Guardar** para aplicar los cambios y cierre la ventana. Para abandonar la ventana sin guardar los cambios, haga clic en **Cancelar**.

Si ya no quiere volver a utilizar una regla, selecciónela y haga clic en el botón **Eliminar** de la parte superior de la tabla. Se le pedirá que confirme esta acción haciendo clic en **Sí**.

Para asegurarse de que se está mostrando la información más reciente, haga clic en el botón **Actualizar** de la zona superior de la tabla.

Configuración de reglas de ubicación

Una ubicación es un segmento de red identificado por uno o varios ajustes de red, como por ejemplo una puerta de enlace concreta, un DNS determinado utilizado para resolver las URL, o un subconjunto de direcciones IP. Por ejemplo, puede

definir ubicaciones como la red local de la empresa, la granja de servidores o un departamento.

En la ventana de configuración de reglas, siga estos pasos:

1. Escriba un nombre adecuado y una descripción para la regla que quiere crear.
2. Establezca la prioridad de la regla. Las reglas se ordenan por prioridad, teniendo la primera regla la mayor prioridad. No se puede establecer la misma prioridad más de una vez.
3. Seleccione la política para la que ha creado la regla de asignación.
4. Defina las ubicaciones a las que se aplica la regla.
   a. Seleccione el tipo de ajustes de red en el menú de la zona superior de la tabla de ubicaciones. Estos son los tipos disponibles:

Tipo	Valor
IP/rango de direcciones IP	Direcciones IP específicas en una red o subred. Para subredes, utilice el formato CIDR. Por ejemplo: `10.10.0.12` o `10.10.0.0/16`
Dirección de la puerta de enlace	Dirección IP de la puerta de enlace
Dirección del servidor WINS	Dirección IP del servidor WINS **Importante** Esta opción no se aplica en sistemas Linux y Mac.
Dirección del servidor DNS	Dirección IP del servidor DNS
Sufijo DNS de conexión DHCP	Nombre del DNS sin el nombre de host para una conexión DHCP determinada Por ejemplo: `central.empresa.biz`
El endpoint puede resolver el host	Nombre del host. Por ejemplo: `serv.empresa.biz`
El endpoint puede conectarse a GravityZone	Sí/no

Tipo	Valor
Tipo de red	Inalámbrica/Ethernet Al elegir una red inalámbrica, también puede añadir el SSID de esta. **Importante** Esta opción no se aplica en sistemas Linux y Mac.

Nombre del host	Nombre del host
	Por ejemplo: `cmp.bitdefender.com`
	Importante
	También puede usar comodines. El asterisco (*) sustituye cero o más caracteres y el signo de interrogación (?) sustituye exactamente un carácter. Ejemplos:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

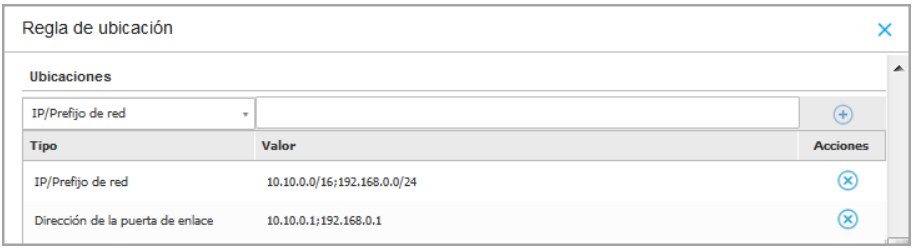
b. Introduzca el valor para el tipo seleccionado. Cuando proceda, puede introducir varios valores en el campo correspondiente, separados por punto y coma (;) y sin espacios adicionales. Por ejemplo, cuando introduce `10.10.0.0/16;192.168.0.0/24`, la regla se aplica a los endpoints cuyas IP coincidan con CUALQUIERA de estas subredes.

Aviso
Solo puede utilizar un tipo de ajuste de red por cada regla de ubicación. Por ejemplo, si añadió una ubicación con el **Prefijo de red/IP**, ya no podrá volver a utilizar este ajuste en la misma regla.

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

Para que se les aplique una regla, los ajustes de red en los endpoints deben coincidir con TODAS las ubicaciones previstas. Por ejemplo, para identificar la red de área local de la oficina puede introducir la puerta de enlace, el tipo de

red y el DNS. Además, si añade una subred, identificará un departamento dentro de la red local de la empresa.



Regla de ubicación

Haga clic en el campo **Valor** para modificar los criterios existentes y, a continuación, pulse `Intro` para guardar los cambios.

Para eliminar una ubicación, selecciónela y haga clic en el botón ⊗ **Eliminar**.

5. Desea excluir ciertas ubicaciones de la regla. Para crear una exclusión, defina las ubicaciones que se deben excluir de la regla:
   a. Marque la casilla de verificación **Exclusiones** de la tabla de Ubicaciones.
   b. Seleccione el tipo de ajustes de red en el menú de la zona superior de la tabla de Exclusiones. Para más información sobre las opciones, consulte "Configuración de reglas de ubicación" (p. 230).
   c. Introduzca el valor para el tipo seleccionado. Puede introducir varios valores en el campo correspondiente, separados por punto y coma (;) y sin espacios adicionales.
   d. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla.

   Para que se aplique una exclusión, los ajustes de red en los endpoints deben cumplir TODAS las condiciones establecidas en la tabla de Exclusiones.

   Haga clic en el campo **Valor** para modificar los criterios existentes y, a continuación, pulse `Intro` para guardar los cambios.

   Para eliminar una exclusión, haga clic en el botón ⊗ **Eliminar** del lateral derecho de la tabla.
6. Haga clic en **Guardar** para guardar la asignación y aplicar la regla.

Una vez creada, la regla de localización se aplica automáticamente a todos los endpoints objetivo administrados.

Configuración de reglas de usuario

Importante

- Solo puede crear reglas de usuario si la integración con Active Directory está disponible.
- Solo puede definir reglas de usuario para usuarios y grupos de Active Directory. Las reglas basadas en grupos de Active Directory no se admiten en sistemas Linux.

En la ventana de configuración de reglas, siga estos pasos:

1. Escriba un nombre adecuado y una descripción para la regla que quiere crear.
2. Establezca la prioridad. Las reglas se ordenan por prioridad, teniendo la primera regla la mayor prioridad. No se puede establecer la misma prioridad más de una vez.
3. Seleccione la política para la que ha creado la regla de asignación.
4. En la sección **Objetivos**, seleccione los usuarios y los grupos de seguridad a los que desea que se aplique la regla de política. Puede ver su selección en la tabla de la derecha.
5. Haga clic en **Guardar**.

   Una vez creada, la regla de usuario se aplica automáticamente a los endpoints objetivo administrados cuando el usuario inicia sesión.

Configuración de reglas de etiquetas

Importante
Si existe una integración de Amazon EC2 o Microsoft Azure, es posible crear reglas de etiquetas.

Puede usar las etiquetas definidas en las infraestructuras de la nube para asignar una política concreta de GravityZone a sus máquinas virtuales alojadas en la nube. A todas las máquinas virtuales cuyas etiquetas se especifiquen en la regla de etiquetas se les aplicará la política establecida por dicha regla.

Nota
Según la infraestructura de nube, puede definir las etiquetas de la máquina virtual de la siguiente manera:

- Para Amazon EC2, en la pestaña **Etiquetas** de la instancia de EC2.
- Para Microsoft Azure, en la sección **Resumen** de la máquina virtual.

Una regla de etiquetas puede contener una o varias etiquetas. Para crear una regla de etiquetas:

1. Escriba un nombre adecuado y una descripción para la regla que quiere crear.
2. Establezca la prioridad de la regla. Las reglas se ordenan por prioridad, teniendo la primera regla la mayor prioridad. No se puede establecer la misma prioridad más de una vez.
3. Seleccione la política para la que ha creado la regla de etiquetas.
4. En la tabla **Etiqueta**, añada una o varias etiquetas.

   Una etiqueta consiste en un par clave-valor que distingue mayúsculas de minúsculas. Asegúrese de introducir las etiquetas tal como se definen en su infraestructura de nube. Solo se tendrán en cuenta los pares clave-valor válidos.

   Para añadir una etiqueta:

   a. En el campo de **Clave de etiqueta**, introduzca el nombre de la clave.
   b. En el campo de **Valor de etiqueta**, introduzca el valor de la clave.
   c. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla.

Asignación de políticas de NSX

En NSX, las políticas de seguridad se asignan a grupos de seguridad. Un grupo de seguridad puede contener varios objetos de vCenter, como centros de datos, clusters y máquinas virtuales.

Para asignar una política de seguridad a un grupo de seguridad:

1. Inicie sesión en vSphere Web Client.
2. Acceda a **Red y seguridad > Service Composer** y haga clic en la pestaña **Grupos de seguridad**.
3. Cree tantos grupos de seguridad como precise. Para más información, consulte la documentación de VMware.

Puede crear grupos de seguridad dinámica, en función de las etiquetas de seguridad. De esta manera, puede agrupar todas las máquinas virtuales que resulten estar infectadas.

4. Haga clic con el botón derecho en el grupo de seguridad que le interese, y luego en **Aplicar política**.
5. Seleccione la política que desee aplicar y haga clic en **Aceptar**.

7.1.3. 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. Elija el tipo de endpoint que desee en el selector de vistas.
3. Encuentre la política que está buscando en la lista y haga clic en su nombre para editarla.
4. Configure las opciones de la política según sea necesario. Para obtener más información detallada, consulte:
   - “Políticas de equipos y máquinas virtuales” (p. 238)
   - “Políticas de dispositivos móviles” (p. 398)
5. 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.

7.1.4. 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. Elija el tipo de endpoint que desee en el selector de vistas.
3. Haga clic en el nombre de la política. Esto abrirá la página de políticas.
4. Introduzca el nombre de la nueva política.
5. Haga clic en **Guardar**.

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

7.1.5. 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. Al eliminar una política con secciones heredadas por otras políticas, los ajustes de las secciones heredadas se almacenan en las políticas secundarias.

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 poder eliminar una política de NSX de GravityZone Control Center, debe asegurarse de que la política no esté en uso. Por lo tanto, asigne otro perfil de seguridad al grupo de seguridad objetivo. Para más información, diríjase a "Asignación de políticas de NSX" (p. 235).

Para eliminar una política:

1. Diríjase a la página **Políticas**.
2. Elija el tipo de endpoint que desee en el selector de vistas.

3. Marque la casilla de verificación de la política que desea eliminar.
4. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

7.2. Políticas de equipos y máquinas virtuales

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. Elija **Equipos y máquinas virtuales** en el selector de vistas.
3. Haga clic en el nombre de la política. Esto abrirá la página de configuración de políticas.
4. Configure las opciones de la política según sea necesario. Los ajustes se organizan en las siguientes secciones:
   - General
   - HVI
   - Antimalware
   - Sandbox Analyzer
   - Cortafuego
   - Protección de red
   - Administración de parches
   - Control de aplicaciones
   - Control de dispositivos
   - Relay
   - Protección de Exchange
   - Cifrado
   - NSX
   - Protección de almacenamiento

   Navegue por las secciones mediante el menú de la izquierda de la página.
5. 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. 223).

7.2.1. General

Los ajustes generales le ayudan a administrar las opciones de visualización de la interfaz de usuario, la protección con contraseña, la configuración del proxy, los ajustes de Usuario avanzado, las opciones de comunicación y las preferencias de actualización de los endpoints objetivo.

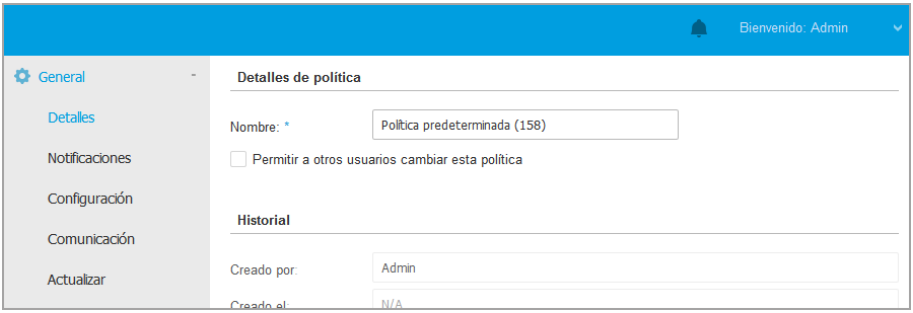
Los ajustes se organizan en las siguientes categorías:

- Detalles
- Notificaciones
- Configuración
- Comunicación
- Actualizar

Detalles

La página **Detalles** contiene los datos de la política general:

- 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 y máquinas virtuales

Puede renombrar la política escribiendo el nuevo nombre en el campo correspondiente y haciendo clic en el botón **Guardar** de la zona inferior de la página. 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.

Reglas de herencia

Puede establecer secciones para que se hereden de otras políticas. Para ello:

1. Seleccione el módulo y la sección que desea que herede la política actual. Todas las secciones se pueden heredar, excepto **General > Detalles**.
2. Especifique la sección que desea que herede la política.
3. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla.

Si se elimina una política fuente, se rompe la herencia y los ajustes de las secciones heredadas se almacenan en la política secundaria.

Las secciones heredadas no las pueden heredar a su vez otras políticas. Veamos el siguiente ejemplo:

La política A hereda la sección **Antimalware > Bajo demanda** de la política B. La política C no pueden heredar la sección **Antimalware > Bajo demanda** de la política A.

Información del soporte técnico

Puede personalizar la información de contacto y soporte técnico disponibles en la ventana **Acerca de** del agente de seguridad rellenando los campos correspondientes.

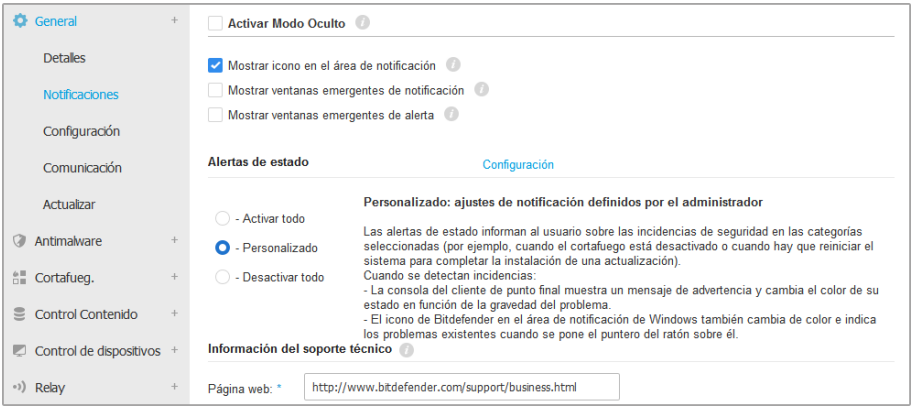
Para configurar una dirección de correo electrónico en la ventana **Acerca de** de modo que abra la aplicación de correo electrónico por defecto en el endpoint, debe añadirla en el campo **Correo electrónico** con el prefijo "mailto:". Ejemplo: `mailto:nombre@dominio.com`.

Los usuarios pueden acceder a esta información desde la consola del agente de seguridad con solo hacer doble clic en el icono de Bitdefender en la bandeja del sistema y seleccionando **Acerca de**.

Notificaciones

En esta sección puede configurar las opciones de visualización de la interfaz de usuario del agente de seguridad de Bitdefender de manera exhaustiva e intuitiva.

Con un solo clic, puede activar o desactivar todo un tipo de notificaciones, conservando solo lo que realmente le importa. Además, en la misma página, se le proporciona un control total sobre la visibilidad de las incidencias de los endpoints.



Políticas - Ajustes de visualización

- **Modo oculto.** Utilice la casilla de verificación para activar o desactivar el modo silencioso. El modo silencioso está diseñado para ayudarle a desactivar fácilmente la interacción del usuario en el agente de seguridad. 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 el botón derecho

para abrir rápidamente la ventana principal del agente de seguridad o la ventana **Acerca de**.

- **Mostrar ventanas emergentes de alerta.** Los usuarios reciben información a través de ventanas emergentes de alerta relativas a los eventos de seguridad que requieran alguna acción por su parte. Si elige no mostrar alertas emergentes, el agente de seguridad 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 Advanced Threat 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**.
- **Mostrar ventanas emergentes de notificación.** A diferencia de las ventanas emergentes de alerta, las ventanas emergentes de notificación informan a los usuarios acerca de diversos eventos de seguridad. Las ventanas emergentes desaparecen automáticamente en unos pocos segundos sin la intervención del usuario.

  Seleccione **Mostrar ventanas emergentes de notificación** y, a continuación, haga clic en el enlace **Mostrar ajustes modulares** para elegir sobre qué eventos desea informar a los usuarios, por módulo. Hay tres tipos de ventanas emergentes de notificación, en función de la gravedad de los eventos:
  - **Información**. Se informa a los usuarios acerca de eventos importantes, pero que no atentan contra la seguridad. Por ejemplo, una aplicación que se ha conectado a Internet.
  - **Bajo**. Se informa a los usuarios acerca de los eventos de seguridad importantes que puedan requerir su atención. Por ejemplo, el análisis on-access ha detectado una amenaza y el archivo ha sido eliminado o puesto en cuarentena.
  - **Crítico**. Estas ventanas emergentes de notificación informan a los usuarios acerca de situaciones peligrosas, como por ejemplo un proceso de actualización que no se pudiera finalizar, o que el análisis on-access hubiera detectado una amenaza y la política de acción por defecto fuera **No realizar ninguna acción**, por lo que el malware estaría todavía presente en el endpoint.

Marque la casilla de verificación asociada al nombre del tipo para activar esa clase de ventanas emergentes para todos los módulos a la vez. Haga clic en las casillas de verificación asociadas a los módulos individuales para activar o desactivar esas notificaciones concretas.

La lista de los módulos podría variar según su licencia.

- **Visibilidad de incidencias de endpoints.** Los usuarios saben si su endpoint 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:
  - Consultando el área de estado de la ventana principal, que 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.
  - Consultando el icono de Bitdefender en la bandeja del sistema, que cambia de aspecto cuando se detectan problemas.

  El agente de seguridad de Bitdefender utiliza el siguiente esquema de colores en el área de notificación:
  - Verde: no se han detectado problemas.
  - Amarillo: el endpoint 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 endpoint tiene problemas críticos que requieren una acción inmediata del usuario.

  Seleccione **Visibilidad de incidencias de endpoints** y, a continuación, haga clic en el enlace **Mostrar ajustes modulares** para personalizar las alertas de estado que aparecen en la interfaz de usuario del agente de Bitdefender.

  Para cada módulo, puede elegir mostrar la alerta como una advertencia o como una incidencia crítica, o bien no mostrarla de ninguna manera. Las opciones se describen aquí:
  - **General**. La alerta de estado se genera siempre que es necesario reiniciar el sistema durante o después de la instalación de un producto, y también

cuando el agente de seguridad no se pudo conectar a Cloud Services de Bitdefender.

- **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.
  - Es necesario reiniciar para completar el proceso de desinfección.
- **Cortafuegos**. Esta alerta de estado se genera cuando se desactiva el módulo de Cortafuego.
- **Control de aplicaciones**. Esta alerta de estado se genera cuando se modifica el módulo de Control de aplicaciones.
- **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.

- **Notificación de reinicio de endpoint.** Esta opción muestra una alerta de reinicio en el endpoint cada vez que se precisa reiniciar el sistema debido a cambios realizados en el endpoint por los módulos de GravityZone seleccionados en los ajustes modulares.

  Nota
  Los endpoints que requieren un reinicio del sistema tienen un icono de estado concreto ( ) en el inventario de GravityZone.

  Puede personalizar aún más las alertas de reinicio haciendo clic en **Mostrar ajustes modulares**. Tiene las siguientes opciones a su disposición:

  - **Actualizar**: Seleccione esta opción para activar las notificaciones de reinicio de actualización del agente.
  - **Administración de parches**: Seleccione esta opción para activar las notificaciones de reinicio de instalación de parches.

Nota
También puede establecer un límite para el número de horas que un usuario puede posponer un reinicio. Para ello, seleccione **Reinicio automático de la máquina después de** e introduzca un valor de 1 a 46.

La alerta de reinicio requiere que el usuario opte por una de las siguientes acciones:

- **Reiniciar ahora**. En tal caso, el sistema se reiniciará inmediatamente.
- **Posponer reinicio**. En este caso, aparecerá periódicamente una notificación de reinicio, hasta que el usuario reinicie el sistema o hasta que haya transcurrido el tiempo establecido por el administrador de la empresa.

Configuración

En esta sección puede configurar los siguientes ajustes:

- **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 ajustes de instalación** 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**.

- **Configuración proxy**

  Si la red está detrás de un servidor proxy, tiene que definir los ajustes del proxy que permitirán a sus endpoints comunicarse con los componentes de la solución GravityZone. En este caso, tiene que activar la opción **Configuración proxy** y rellenar los parámetros necesarios:
  - **Servidor**: introduzca la IP del servidor proxy.
  - **Puerto**: introduzca el puerto utilizado para conectar con el servidor proxy.
  - **Nombre de usuario**: introduzca un nombre de usuario que el proxy reconozca.
  - **Contraseña**: introduzca la contraseña válida para el usuario especificado.

- **Usuario con Permisos**

  El módulo de Usuario avanzado otorga privilegios de administración a nivel de endpoint, lo que permite al usuario de endpoint acceder y modificar los ajustes

de la política mediante una consola local, a través de la interfaz de Bitdefender Endpoint Security Tools.

Si quiere que determinados endpoints tengan privilegios de usuario avanzado, primero tiene que incluir este módulo en el agente de seguridad instalado en los endpoints objetivo. A continuación, tiene que configurar los ajustes de Usuario avanzado en la política aplicada a estos endpoints:

Importante
El módulo de Usuario avanzado solo está disponible para sistemas operativos soportados de servidor y equipos de escritorio Windows.

1. Active la opción de **Usuario avanzado**.
2. Defina una contraseña de Usuario avanzado en los campos que aparecen a continuación.

   A los usuarios que accedan al modo de Usuario avanzado desde el endpoint local se les pedirá que introduzcan la contraseña indicada.

Para acceder al módulo de Usuario avanzado, los usuarios deben hacer clic con el botón derecho en el icono de Bitdefender de la bandeja del sistema y seleccionar **Usuario avanzado** en el menú contextual. Después de proporcionar la contraseña en la ventana de inicio de sesión, se mostrará una consola que contiene los ajustes de la política aplicada actualmente, donde el usuario del endpoint podrá ver y modificar los ajustes de la política.

Nota
Solo se puede acceder localmente a ciertas características de seguridad, relacionadas con los módulos Antimalware, Cortafuego, Control de contenidos y Control de dispositivos, a través de la consola de Usuario avanzado.

Para revertir los cambios realizados en el modo de Usuario avanzado:

- En Control Center, abra la plantilla de política asignada al endpoint con privilegios de Usuario avanzado y haga clic en **Guardar**. De esta manera, se volverán a aplicar los ajustes originales al endpoint objetivo.
- Asigne una nueva política al endpoint con privilegios de Usuario avanzado.
- Inicie sesión en el endpoint local, abra la consola de Usuario avanzado y haga clic en **Resincronizar**.

Para encontrar fácilmente los endpoints con políticas modificadas en el modo de Usuario avanzado:

- En la página **Red**, haga clic en el menú **Filtros** y seleccione la opción **Modificado por Usuario avanzado** de la pestaña **Política**.
- En la página **Red**, haga clic en el endpoint que le interese para mostrar la ventana **Información**. Si la política se modificó en el modo de Usuario avanzado, se mostrará una notificación en la pestaña **General** de la sección **Política**.

> **Importante**
> El módulo de Usuario avanzado está diseñado específicamente para solucionar problemas y permite al administrador de la red ver y cambiar con facilidad los ajustes de políticas en equipos locales. La asignación de privilegios de Usuario avanzado a otros usuarios en la empresa debe limitarse al personal autorizado, para garantizar que las políticas de seguridad se aplican siempre en todos los endpoints de la red de la empresa.

- **Opciones**

  En esta sección puede definir los siguientes ajustes:

  - **Eliminar eventos con una antigüedad superior a (días).** El agente de seguridad de Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en el equipo (incluyendo también las actividades del equipo monitorizadas por el Control de contenidos). 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, si el agente de seguridad se bloquea, los informes se envíen a los laboratorios de Bitdefender para su análisis. Los informes ayudarán a nuestros ingenieros a descubrir qué causó el problema y evitar que éste vuelva a ocurrir. No sé enviará información personal.
  - **Enviar archivos ejecutables sospechosos para su análisis.** Seleccione esta opción para que los archivos que no parecen dignos de confianza o que presentan un comportamiento sospechoso se envíen a los laboratorios de Bitdefender para su análisis.
  - **Enviar infracciones de memoria de HVI a Bitdefender.** Por defecto, HVI envía a los servidores en la nube de Bitdefender información anónima relativa a

las infracciones detectadas, que se utilizarán en estadísticas y para mejorar las tasas de detección de los productos. Puede dejar sin marcar esta casilla de verificación si no desea enviar dicha información desde su red.

Comunicación

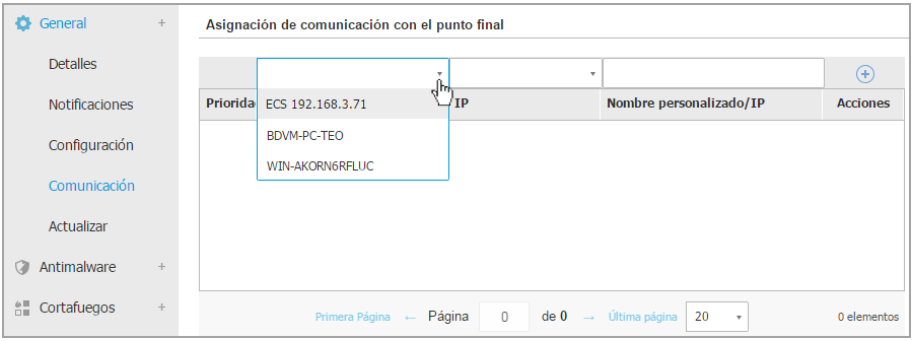
En esta sección puede asignar una o varias máquinas de relay para los endpoints objetivo y, a continuación, configurar las preferencias de proxy para la comunicación entre los endpoints objetivo y GravityZone.

Asignación de comunicación con el endpoint

Cuando hay varios servidores de comunicaciones instalados en el appliance de GravityZone, puede asignar los equipos objetivo a uno o varios servidores de comunicaciones mediante políticas. También se tienen en cuenta los endpoints de relay disponibles, que actúan como servidores de comunicaciones.

Para asignar servidores de comunicaciones a equipos objetivo:

1. En la tabla de **Asignación de comunicación de endpoint**, haga clic en el campo **Nombre**. Se mostrará la lista de servidores de comunicaciones detectados.
2. Seleccione una entidad.



Políticas de equipos y máquinas virtuales - Ajustes de comunicación

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

   El servidor de comunicaciones se añade a la lista. Todos los equipos objetivo se comunicarán con Control Center mediante el servidor de comunicaciones especificado.

4. Siga los mismos pasos para añadir varios servidores de comunicaciones, si existen.
5. Puede configurar las prioridades de servidores de comunicaciones 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.

Comunicación entre endpoints y relays con GravityZone

En esta sección puede configurar las preferencias de proxy para la comunicación entre los endpoints objetivo y las máquinas de relay asignadas, o entre los endpoints objetivo y el appliance de GravityZone (cuando no se ha asignado ningún relay):

- **Mantener los ajustes de la instalación**, para utilizar los mismos ajustes de proxy definidos en el paquete de instalación.
- **Utilizar el proxy definido en la sección General**, para usar los ajustes de proxy definidos en la política actual, en la sección **General > Ajustes**.
- **No utilizar**, cuando los endpoints objetivo no se comunican con los componentes de GravityZone a través de proxy.

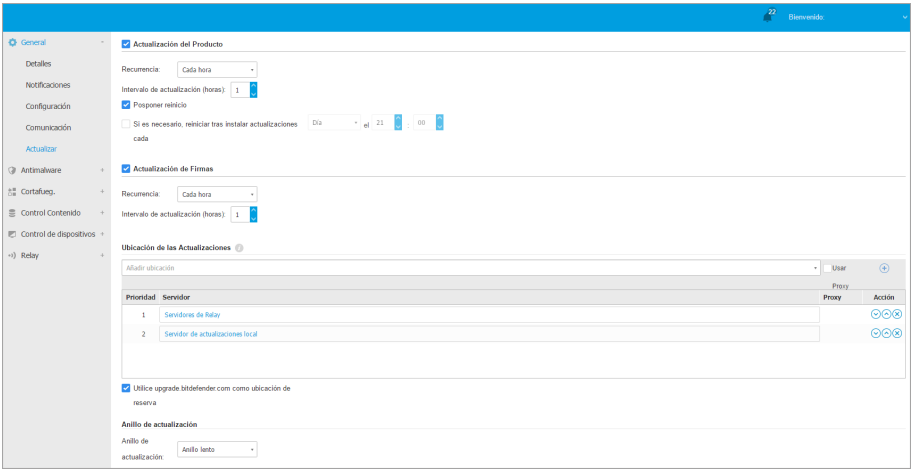
Comunicación entre los endpoints y los Servicios en la nube

En esta sección puede configurar las preferencias de proxy para la comunicación entre los endpoints objetivo y Bitdefender Cloud Services (requiere conexión a Internet):

- **Mantener los ajustes de la instalación**, para utilizar los mismos ajustes de proxy definidos en el paquete de instalación.
- **Utilizar el proxy definido en la sección General**, para usar los ajustes de proxy definidos en la política actual, en la sección **General > Ajustes**.
- **No utilizar**, cuando los endpoints objetivo no se comunican con los componentes de GravityZone a través de proxy.

Actualizar

Las actualizaciones son muy importantes ya que permiten luchar contra las últimas amenazas. Bitdefender publica todas las actualizaciones del producto y de los contenidos de seguridad a través de los servidores de Bitdefender en Internet. Todas las actualizaciones van cifradas y firmadas digitalmente, por lo que es imposible manipularlas. Cuando hay una nueva actualización disponible, el agente de seguridad de Bitdefender comprueba la autenticidad de la firma digital de la actualización, así como la integridad del contenido del paquete. A continuación, se analizan las actualizaciones y se comprueban sus versiones respecto a las instaladas. Los archivos nuevos se descargan localmente y se comprueban sus hash MD5 para cerciorarse de que no han sido alterados. En esta sección puede configurar el agente de seguridad de Bitdefender y los ajustes de actualización de contenidos de seguridad.



Políticas de equipos y máquinas virtuales - Opciones de actualización

- **Actualización del Producto.** El agente de seguridad de Bitdefender 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. Por defecto, el producto seguirá funcionando con los archivos antiguos hasta que se reinicie el equipo, después de lo cual se aplicarán las últimas actualizaciones. Una notificación de la interfaz de usuario solicitará a este el reinicio del sistema siempre que lo requiera una actualización. Se recomienda dejar activada esta opción. De lo contrario, el sistema se reiniciará automáticamente después de instalar una actualización que lo requiera. Se avisará a los usuarios para que guarden su trabajo, pero el reinicio no se podrá cancelar.
- 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 contenidos de seguridad.** Los contenidos de seguridad se refieren a medios estáticos y dinámicos de detección de amenazas, como por ejemplo, entre otros, motores de análisis, modelos de aprendizaje automático, heurísticas, reglas, firmas y listas negras. El agente de seguridad de Bitdefender comprueba automáticamente la actualización de contenidos de seguridad cada hora (configuración por defecto). 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.
- **Ubicación de las Actualizaciones**. La ubicación de actualización por defecto del agente de seguridad de Bitdefender es el Servidor de actualizaciones local de GravityZone. Añada una ubicación de actualización, ya sea eligiendo las ubicaciones predefinidas en el menú desplegable o introduciendo la IP o el nombre de host de uno o varios servidores de actualización de su red. Configure su prioridad utilizando los botones arriba y abajo que se muestran al pasar el ratón por encima. Si la primera ubicación de actualización no está disponible, se usa la siguiente y así sucesivamente.

  Para establecer una dirección de actualización local:

  1. Introduzca la dirección del servidor de actualizaciones en el campo **Añadir ubicación**. Podrá:
     - Elija una ubicación predefinida:

- **Servidores de Relay**. El endpoint se conectará automáticamente al Servidor de Relay que tenga asignado.

  Aviso
  Los servidores de relay no son compatibles con los sistemas operativos antiguos. Para más información, consulte la Guía de instalación.

  Nota
  Puede comprobar el Servidor de Relay asignado en la ventana **Información**. Para obtener más información, vea Consulta de la información del equipo.

- **Servidor de actualizaciones local**

– Introduzca la dirección IP o nombre de host de uno o varios servidores de actualizaciones de su red. Use una de estas sintaxis:

  - `update_ server_ip:port`
  - `update_ server_name:port`

  El puerto predeterminado es 7074.

  La casilla de verificación **Usar servidores de Bitdefender como ubicación de reserva** está marcada por defecto. Si no están disponibles las ubicaciones de actualización, se utilizará la de reserva.

  Aviso
  Desactivar la ubicación de reserva detendrá las actualizaciones automáticas, lo que dejará su red vulnerable cuando las ubicaciones previstas no estén disponibles.

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 y ⌄ Abajo de la columna **Acción** para establecer la prioridad de las ubicaciones de actualización definidas. Si la primera ubicación de actualización no está disponible, se comprueba la siguiente y así sucesivamente.

Para eliminar una ubicación de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente. Aunque puede eliminar la dirección de actualización predeterminada, no es recomendable que lo haga.

- **Anillo de actualización.** Puede distribuir las actualizaciones de productos por fases mediante anillos de actualización:
  - **Anillo lento**. Las máquinas con una política de anillo lento recibirán las actualizaciones en una fecha posterior, dependiendo de la respuesta recibida desde los endpoints de anillo rápido. Es una medida de precaución en el proceso de actualización. Esta es la configuración predeterminada.
  - **Anillo rápido**. Las máquinas con una política de anillo rápido recibirán las actualizaciones más recientes disponibles. Este ajuste se recomienda para máquinas que no sean críticas para producción.

Importante

- En el caso improbable de que se produjera un problema en las máquinas del anillo rápido con una configuración particular, se solucionaría antes de la actualización del anillo lento.
- BEST for Windows Legacy no es compatible con ensayos. Los endpoints antiguos en ubicaciones de ensayo deben moverse a la ubicación de producción.

Nota

Para más información sobre cómo afecta la selección de anillos a los ensayos, consulte el capítulo **Actualizar GravityZone > Ensayos** de la Guía de instalación de GravityZone.

7.2.2. HVI

Nota

HVI solo proporciona protección a las máquinas virtuales en hipervisores Citrix Xen.

Hypervisor Memory Introspection protege las máquinas virtuales contra amenazas avanzadas que los motores basados en firmas no pueden atajar. Garantiza la detección en tiempo real de los ataques, mediante la monitorización de los procesos desde fuera del sistema operativo del guest. El mecanismo de protección incluye varias opciones para bloquear los ataques en cuanto suceden y eliminar inmediatamente la amenaza.

Siguiendo el principio de separación de la memoria de los sistemas operativos, HVI incluye dos módulos de protección organizados en las siguientes categorías:

- Espacio del usuario, que aborda los procesos normales de las aplicaciones de los usuarios.
- Espacio del kernel, que aborda los procesos reservados al núcleo del sistema operativo.

Además, la política de HVI incluye dos características para ayudarle a administrar la seguridad y mantener las máquinas virtuales protegidas:

- Exclusiones, para ver y administrar procesos excluidos del análisis.
- Herramientas personalizadas, para inyectar las herramientas necesarias en actividades operativas y forenses en los sistemas operativos guest.

Espacio del usuario

En esta sección puede configurar los ajustes de protección para los procesos que se ejecutan en la memoria del espacio del usuario.

Utilice la casilla de verificación **Introspección de memoria del espacio del usuario** para activar o desactivar la protección.

La funcionalidad de este módulo se basa en reglas, lo que le permite configurar la protección para los diferentes grupos de procesos por separado. Adicionalmente, puede optar por recoger más información forense.

- Reglas del espacio del usuario
- Información forense

Reglas del espacio del usuario

El módulo viene con un conjunto de reglas predefinidas que abordan las aplicaciones más vulnerables. La tabla de esta sección enumera las reglas existentes y proporciona información importante sobre cada una de ellas:

- Nombre de la regla
- Procesos a los que se aplica la regla
- Modo de monitorización
- Acción que bloquea el ataque detectado
- Acciones para eliminar la amenaza

También puede proporcionar una lista de reglas personalizadas para los procesos que desee monitorizar. Para crear una nueva regla:

1. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Esta acción abre la ventana de configuración de reglas.
2. Configure el módulo con los siguientes ajustes de reglas:
   - **Nombre de la regla.** Escriba el nombre con el que mostrará la regla en la tabla de reglas. Por ejemplo, para procesos como `firefox.exe` o `chrome.exe`, puede llamar a la regla `Navegadores`.
   - **Procesos.** Introduzca el nombre de los procesos que desee monitorizar, separados por un punto y coma (;).
   - **Modo de monitorización.** Para una configuración rápida, 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.

     Puede configurar en detalle los ajustes del módulo mediante la selección del nivel de protección **Personalizado** y seleccionando una o más de las siguientes opciones:
     - **Enlaces establecidos en DLL críticas en modo usuario.** Detecta las inyecciones de DLL, que cargan código malicioso en el proceso de llamada.
     - **Intentos de desempaquetado/descifrado en el ejecutable principal.** Detecta intentos de descifrar el código en el ejecutable principal del proceso, y protege el proceso contra su alteración con instrucciones maliciosas.
     - **Escritura externa dentro del proceso objetivo.** Protege contra la inyección de código en el proceso protegido.
     - **Exploits.** Detecta comportamientos no intencionados de procesos causados por el aprovechamiento de un error o de una vulnerabilidad previamente revelada. Utilice esta opción si desea monitorizar la ejecución de código heap y de pila de las aplicaciones protegidas.
     - **Enganche de WinSock.** Bloquea las intercepciones de las bibliotecas de red (DLL) que utiliza el sistema operativo, lo que garantiza una comunicación TCP/IP segura.

- **Acciones.** Hay diversas acciones que puede adoptar respecto a las amenazas detectadas. Cada acción tiene, a su vez, varias opciones posibles o acciones secundarias. Se describen a continuación:
  - **Acción principal.** Esta es la acción inmediata que puede adoptar cuando se detecta un ataque contra la máquina guest, lo que le permite bloquearlo. Estas son las opciones disponibles:
    - **Registrar.** Únicamente registrar el evento en la base de datos. En este caso, solo recibirá una notificación (si está configurada) y podrá ver el incidente en el informe de **Actividad de HVI**.
    - **Denegar.** Rechazar cualquier intento de la amenaza de alterar el proceso objetivo.
    - **Apagar la máquina.** Apaga la máquina virtual en la que se ejecuta el proceso objetivo.

      Importante
      Se recomienda establecer previamente la acción principal a **Registro**. A continuación, utilice la política durante el tiempo suficiente para asegurarse de que todo funciona como cabría esperar. Más adelante, puede seleccionar cualquier acción que desee llevar a cabo en caso de detectarse una violación de memoria.

  - **Acción de reparación.** Dependiendo de la opción seleccionada, Security Server inyecta una herramienta de reparación en el sistema operativo del guest. La herramienta empieza automáticamente la exploración en busca de malware y, cuando se detecta una amenaza, procede a llevar a cabo la acción seleccionada. Estas son las opciones disponibles:
    - **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.
    - **Ignorar.** La herramienta de reparación detecta y únicamente informa de los archivos detectados.
    - **Nada.** La herramienta de reparación no se inyectará en el sistema operativo del guest.

> **Nota**
> Cerrar la herramienta también la eliminará del sistema, sin dejar huella en el sistema operativo del guest.

- **Acción de reparación de copia de seguridad.** Cuando falle la acción de reparación, puede elegir otra acción de reparación entre las opciones disponibles.

3. Haga clic en **Guardar**.

Una vez creada, puede modificar una regla en cualquier momento. Hacer clic en el nombre de la regla abre la ventana de configuración de reglas.

GravityZone también le permite configurar rápidamente el comportamiento de la Introspección de memoria ante las detecciones mediante la modificación de varias reglas a la vez. Para configurar varias reglas con las mismas acciones:

1. Seleccione las reglas que desee cambiar.
2. Haga clic en el botón **Acción y reparación** en la zona superior de la tabla.
3. Seleccione la opción que desee para cada acción.
4. Haga clic en **Guardar**. Las nuevas acciones serán efectivas una vez que guarde la política, siempre y cuando las máquinas objetivo estén online.

Para eliminar una o varias reglas de la lista, selecciónelas y haga clic en el botón ⊗ **Eliminar** de la zona superior de la tabla.

Información forense

Marque la casilla de verificación **Eventos de cierre inesperado de la aplicación** debajo de la tabla de reglas del espacio del usuario para permitir la recopilación de información detallada cuando se cierran las aplicaciones.

Puede ver esta información en el informe de actividad de HVI, y hallar la razón que ocasionó el cierre de la aplicación. Si el evento está relacionado con un ataque, sus detalles aparecerán agrupados con otros eventos bajo el incidente correspondiente que condujo al evento.

Espacio del kernel

HVI protege los elementos clave del sistema operativo, como por ejemplo:

- Controladores críticos del kernel y los objetos de controlador asociados que impliquen tablas de gestión rápida de E/S asociadas con controladores básicos.

- Controladores de red, cuya alteración permitiría a un malware interceptar el tráfico e inyectar componentes maliciosos en el flujo de tráfico.
- Imagen del kernel del sistema operativo, que implica lo siguiente: sección de código, sección de datos y de solo lectura, incluyendo la tabla de direcciones que importar (IAT), la tabla de direcciones que exportar (EAT) y los recursos.

En esta sección puede configurar los ajustes de protección para los procesos que se ejecutan en la memoria del espacio del kernel.

Utilice la casilla de verificación **Introspección de memoria del espacio del kernel** para activar o desactivar la protección.

Para una configuración rápida, 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.

Puede configurar en detalle los ajustes del módulo mediante la selección del nivel de protección **Personalizado** y seleccionando una o más de las siguientes opciones:

- **Registros de control**. Los registros de control (CR) son registros del procesador que controlan el comportamiento general de un procesador u otro dispositivo digital. Seleccione esta opción para detectar los intentos de carga de valores no válidos en determinados registros de control.
- **Registros específicos del modelo**. Estos registros se refieren a cualquiera de los diversos registros de control en el conjunto de instrucciones x86 utilizado para la depuración, el trazado de la ejecución del programa, la monitorización del rendimiento del equipo, y la activación o desactivación de determinadas características de la CPU. Seleccione esta opción para detectar los intentos de cambiar estos registros.
- **Integridad IDT/GDT**. Las tablas de descriptores de interrupción/tablas globales de descriptores (IDT/GDT) las utiliza el procesador para determinar la respuesta correcta a las interrupciones y excepciones. Seleccione esta opción para detectar cualquier intento de cambiar estas tablas.
- **Protección de controladores antimalware.** Seleccione esta opción para detectar los intentos de alterar los controladores utilizados por el software antimalware.
- **Protección de controladores Xen.** Seleccione esta opción para detectar los intentos de alterar los controladores del hipervisor Citrix XenServer.

Hay diversas acciones que puede adoptar respecto a las amenazas detectadas. Cada acción tiene, a su vez, varias opciones posibles o acciones secundarias. Se describen a continuación:

- **Acción principal.**
  - **Registrar.** Únicamente registrar el evento en la base de datos. En este caso, solo recibirá una notificación (si está configurada) y podrá ver el incidente en el informe de **Actividad de introspección de memoria**.
  - **Denegar.** Rechazar cualquier intento de la amenaza de alterar el proceso objetivo.
  - **Apagar la máquina.** Apaga la máquina virtual en la que se ejecuta el proceso objetivo.

  Importante
  Se recomienda establecer previamente la acción principal a **Registro**. A continuación, utilice la política durante el tiempo suficiente para asegurarse de que todo funciona como cabría esperar. Más adelante, puede seleccionar cualquier acción que desee llevar a cabo en caso de detectarse una violación de memoria.

- **Acción de reparación.**
  - **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.
  - **Ignorar.** La herramienta de reparación detecta y únicamente informa de los archivos detectados.
  - **Nada.** La herramienta de reparación no se inyectará en el sistema operativo del guest.
- **Acción de reparación de copia de seguridad.** Cuando falle la acción de reparación, puede elegir otra acción de reparación entre las opciones disponibles.

Adicionalmente, puede optar por recopilar información que aumente los datos proporcionados a los equipos forenses. Marque las casillas de verificación **Eventos de fallos del sistema operativo** y **Eventos de controladores** para permitir la recopilación de información relativa a los fallos del sistema operativo guest o a

eventos generados por los módulos adicionales cargados por el sistema operativo. Estos eventos, que preceden al incidente, contribuirán a las investigaciones forenses para determinar con mayor rapidez la causa del ataque.

Estos eventos se agrupan en el informe de actividad de HVI bajo el incidente que dio lugar a ellos.

Exclusiones

GravityZone le permite excluir procesos del análisis de HVI, utilizando los informes de **Aplicaciones bloqueadas** y **HVI**. La sección de **Exclusiones** reúne todos estos procesos de los informes mencionados y los muestra en forma de tabla.

Para cada proceso excluido puede ver un comentario con el motivo de la exclusión.

Si cambia de opinión sobre un proceso excluido, haga clic en el botón **Eliminar** de la parte superior de la tabla y se incluirá en análisis futuros.

Herramientas personalizadas

En esta sección puede configurar la inyección de herramientas en los sistemas operativos guest objetivo. Estas herramientas deben cargarse en GravityZone antes de usarlas. Para más información, diríjase a "Inyección de herramientas personalizadas con HVI" (p. 494).

Para configurar las inyecciones:

1. Utilice la casilla de verificación **Activar inyecciones** para activar o desactivar esta característica.
2. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para añadir una nueva herramienta. Se muestra una ventana de configuración.
3. Seleccione la herramienta que desee utilizar en la lista desplegable **Elegir herramienta**.

   Estas herramientas se cargaron previamente en GravityZone. Si no consigue encontrar la herramienta adecuada en la lista, acceda al **Centro de administración de herramientas** y añádala desde allí. Para más información, diríjase a "Inyección de herramientas personalizadas con HVI" (p. 494).
4. En **Descripción de la herramienta**, introduzca el uso previsto de la herramienta o cualquier otra información que considere útil.

5. Introduzca la línea de comando de la herramienta, junto con todos los parámetros de entrada necesarios, como hace en el símbolo del sistema o el terminal. Por ejemplo:

   ```
   bash script.sh <param1> <param2>
   ```

   .

   En el caso de las herramientas de reparación de BD, solo puede seleccionar la acción de reparación y la acción de reparación de copia de seguridad en los dos menús desplegables.

6. Indique la ubicación desde donde Security Server debe reunir los registros:
   - **stdout**. Marque esta casilla de verificación para capturar los registros del canal de comunicación de salida estándar.
   - **Archivo de salida**. Marque esta casilla de verificación para recopilar el archivo de registro guardado en el endpoint. En este caso, debe introducir la ruta donde Security Server puede encontrar el archivo. Puede utilizar rutas absolutas o variables del sistema.

     Aquí tiene dos opciones adicionales:

     a. **Eliminar los archivos de registro del guest después de haberlos transferido**. Seleccione esta opción si ya no necesita los archivos en el endpoint.

     b. **Transferir registros a**. Seleccione esta opción para mover el archivo de registros desde Security Server a otra ubicación. En este caso, debe proporcionar la ruta de acceso a la ubicación de destino y las credenciales de autenticación.

7. Seleccione cómo se desencadenará la inyección. Dispone de las opciones siguientes:
   - **Tras detectarse una infracción en la máquina virtual guest.** La herramienta se inyecta justo cuando se detecta una amenaza en la máquina virtual.
   - **Según una programación determinada.** Utilice las opciones de programación para configurar el programa de inyección. Puede decidir ejecutar la herramienta cada pocas horas, días o semanas, a partir de una fecha y hora concreta.

Tenga en cuenta que la máquina virtual debe estar encendida a la hora programada. Una inyección no se ejecutará cuando esté programada si la máquina está apagada o en pausa. En tales situaciones, se recomienda marcar la casilla de verificación **Si se pasa el momento de inyección programado, ejecutar la tarea lo antes posible**.

- A veces la herramienta puede requerir más tiempo de lo esperado para terminar su trabajo, o puede incluso dejar de responder. Para evitar problemas en estas situaciones, en la sección **Configuración de seguridad**, elija después de cuántas horas Security Server debe finalizar automáticamente el proceso de la herramienta.
- Haga clic en **Guardar**. La herramienta se añadirá en la tabla.

Puede añadir tantas herramientas como necesite siguiendo los pasos mencionados anteriormente.

7.2.3. Antimalware

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- Linux
- macOS

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 tres categorías:

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

Cuando detecte un virus u otro malware, el agente de seguridad de Bitdefender 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.

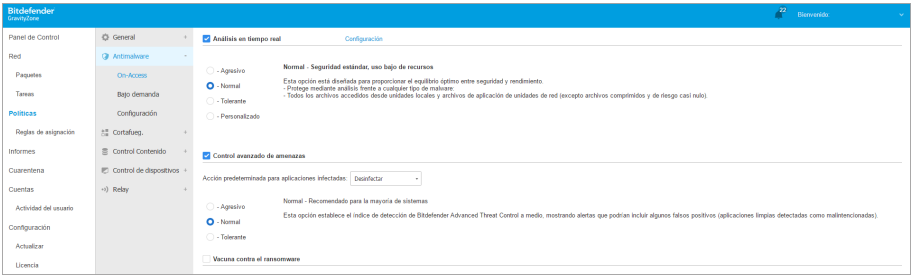
Los ajustes se organizan en las siguientes categorías:

- On-Access
- En ejecución
- Bajo demanda
- HyperDetect
- Antiexploit avanzado
- Configuración
- Servidores de seguridad

On-Access

En esta sección, puede configurar los componentes que proporcionan protección cuando se accede a un archivo o aplicación:

- Análisis en tiempo real
- Vacuna contra el ransomware



Políticas - Ajustes on-access

Análisis en tiempo real

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).

Nota
Esta característica tiene ciertas limitaciones en los sistemas basados en Linux. Para más información, consulte el capítulo dedicado a los requisitos de la Guía de instalación de GravityZone.

Para configurar el análisis on-access:

1. Utilice el conmutador para activar o desactivar el análisis on-access.

   Aviso
   Si desactiva el análisis on-access, los endpoints 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**.

   A continuación se describen las opciones de la pestaña **General**:

   - **Ubicación de archivos**. 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 endpoint 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 el agente de seguridad para analizar todos los archivos a los que se acceda (con independencia de su extensión), solamente archivos de aplicación 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 "Tipos de archivos de aplicación" (p. 527).

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.

> **Nota**
> En los sistemas basados en Linux, las extensiones de archivos distinguen entre mayúsculas y minúsculas y los archivos con el mismo nombre pero con extensiones diferentes se consideran objetos distintos. Por ejemplo, `archivo.txt` es diferente de `archivo.TXT`.

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.

- **Analizar.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.
  - **Solo los archivos nuevos o modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
  - **Sectores de arranque.** Para analizar el sector de arranque del sistema. Este sector del disco duro contiene el código 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.
  - **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.
  - **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.

- **Archivos**. Seleccione esta opción 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.
- **Análisis aplazado.** El análisis diferido mejora el rendimiento del sistema cuando se realizan operaciones de acceso a archivos. Por ejemplo, los recursos del sistema no se ven afectados cuando se copian archivos de gran tamaño. Esta opción está activada por omisión.

- **Acciones del Análisis**. Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
  - **Acción predeterminada para archivos infectados.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA). El agente de seguridad de Bitdefender puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

    Por defecto, si se detecta un archivo infectado, el agente de seguridad de Bitdefender intenta desinfectarlo automáticamente. Si falla la desinfección, el archivo se traslada a la cuarentena para contener la infección. Puede cambiar este procedimiento recomendado según sus necesidades.

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 sospechosos.** Los archivos se detectan como sospechosos mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos). 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.

Importante
Para endpoints de Mac se lleva a cabo la acción de **Mover a la cuarentena** en lugar de **Denegar acceso**.

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.

Ninguna acción
Informar solo de los archivos infectados detectados por Bitdefender.

La pestaña **Avanzado** aborda el análisis en tiempo real para máquinas Linux. Utilice la casilla de verificación para activarlo o desactivarlo.

En la siguiente tabla, puede configurar los directorios de Linux que desee analizar. Por defecto, hay cinco entradas, cada una de las cuales corresponde a una ubicación concreta en los endpoints: `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

Para añadir más entradas:

- Indique cualquier nombre de ubicación personalizada en el campo de búsqueda, en la parte superior de la tabla.
- Seleccione los directorios predefinidos en la lista que aparece cuando hace clic en la flecha de la derecha del campo de búsqueda.

Haga clic en el botón ⊕ **Añadir** para guardar una ubicación en la tabla, o en el botón ⊗ **Eliminar** para eliminarla.

Vacuna contra el ransomware

La vacuna contra ransomware inmuniza sus máquinas contra el ransomware **conocido** mediante el bloqueo del proceso de cifrado, incluso si el equipo resulta infectado. Utilice la casilla de verificación para activar o desactivar la Vacuna contra el ransomware.

La Vacuna contra el ransomware está desactivada por defecto. Los laboratorios de Bitdefender analizan el comportamiento del ransomware generalizado y se proporcionan nuevas firmas con cada actualización de contenidos de seguridad para hacer frente a las amenazas más recientes.

Aviso
Para aumentar aún más la protección contra las infecciones de ransomware, tenga cuidado con los archivos adjuntos sospechosos o no solicitados y asegúrese de que los contenidos de seguridad estén actualizados.

Nota
La vacuna contra ransomware solo está disponible con Bitdefender Endpoint Security Tools para Windows.

En ejecución

En esta sección puede configurar la protección contra procesos maliciosos que se ejecuten. Proporciona las siguientes capas de protección:

Control avanzado de amenazas

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- macOS

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

Advanced Threat Control monitoriza continuamente las aplicaciones que se están ejecutando en su endpoint, 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.

Advanced Threat Control tratará automáticamente de desinfectar el archivo detectado. Si la rutina de desinfección fracasa, Advanced Threat 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 **Antimalware > Ajustes** de los ajustes de política. Esta opción está activada por defecto en las plantillas de política.

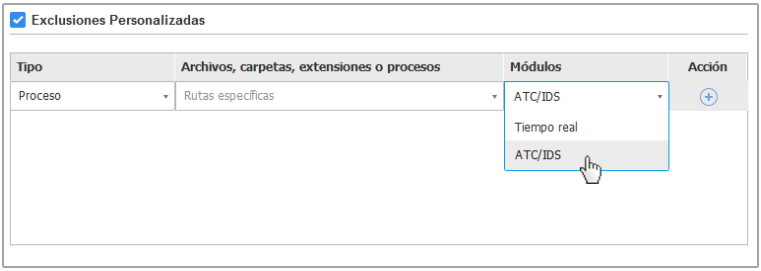
Para configurar el Advanced Threat Control:

1. Utilice la casilla de verificación para activar o desactivar el Advanced Threat Control.

Aviso
Si desactiva Advanced Threat Control, los equipos serán vulnerables al malware desconocido.

2. La acción por defecto para las aplicaciones infectadas detectadas por Advanced Threat Control es desinfectar. Puede establecer otra acción por defecto mediante el menú del que dispone:
   - **Bloquear**, para denegar el acceso a la aplicación infectada.
   - **No realizar ninguna acción**, para limitarse a informar de las aplicaciones infectadas que haya detectado Bitdefender.
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, Advanced Threat Control necesitará menos indicios de comportamiento afín al 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).
Es muy recomendable crear reglas de exclusión para las aplicaciones más conocidas o usadas, con lo que se evitan falsos positivos (detección incorrecta de aplicaciones legítimas). Acceda a la pestaña Antimalware > Ajustes y configure las reglas de exclusión de procesos ATC/IDS para las aplicaciones de confianza.



Políticas de equipos y máquinas virtuales - Exclusión de procesos ATC/IDS

Mitigación de ransomware

La Mitigación de ransomware aplica tecnologías de detección y reparación para mantener sus datos a salvo de los ataques de ransomware. Ya se trate de un ransomware nuevo o conocido, GravityZone detecta intentos de cifrado anómalos y bloquea el proceso. Posteriormente, recupera los archivos de las copias de seguridad en su ubicación original.

Importante
La Mitigación de ransomware requiere Active Threat Control.

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores

Para configurar la Mitigación de ransomware debe hacer lo siguiente:

1. Para habilitar la característica, marque la casilla de verificación **Mitigación de ransomware** en la sección de política **Antimalware > En ejecución**.
2. Seleccione los modos de monitorización que desee usar:
   - Local. GravityZone monitoriza los procesos y detecta los ataques de ransomware iniciados localmente en el endpoint. Se recomienda para estaciones de trabajo. Úselo con precaución en los servidores debido al impacto en el rendimiento.
   - Remoto. GravityZone monitoriza el acceso a las rutas de recursos compartidos y detecta los ataques de ransomware iniciados desde otra máquina. Utilice esta opción si el endpoint es un servidor de archivos o tiene recursos compartidos habilitados.
3. Seleccione el método de recuperación:
   - Bajo demanda. Debe elegir manualmente los ataques de los que desea recuperar los archivos. Puede hacerlo en cualquier momento desde la página **Informes > Actividad de ransomware**, pero tiene de plazo hasta treinta días después del ataque. Transcurrido ese tiempo, no podrá recuperarlos.
   - Automático. GravityZone recupera automáticamente los archivos después de una detección de ransomware.

   Para que la recuperación se lleve a cabo, los endpoints han de estar disponibles.

Una vez que se habilita, dispone de varias opciones para comprobar si su red está sufriendo un ataque de ransomware:

- Consulte las notificaciones y busque **Detección de ransomware**.

  Para obtener más información sobre esta notificación, consulte "Tipo de notificaciones" (p. 496).

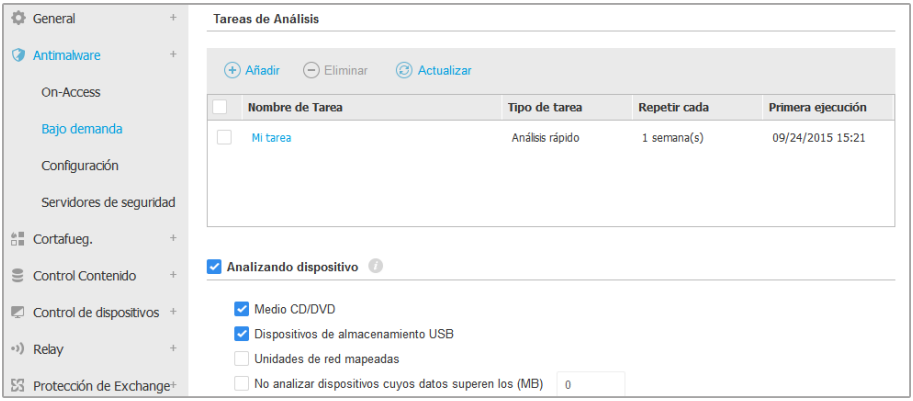
- Consulte el informe de **Auditoría de seguridad**.
- Consulte la página **Actividad de ransomware**.

  Además, desde esta página puede iniciar tareas de recuperación, de ser necesario. Para más información, diríjase a ???.

En caso de que observe una detección que sea un proceso de cifrado legítimo, tenga ciertas rutas en las que autorice el cifrado de archivos o permita el acceso remoto desde determinadas máquinas, añada exclusiones a la sección de política **Antimalware > Ajustes > Exclusiones personalizadas**. La Mitigación de ransomware permite exclusiones por carpetas, procesos e IP o máscara. Para más información, diríjase a "Exclusiones" (p. 293).

Bajo demanda

En esta sección puede añadir y configurar las tareas de análisis antimalware que se ejecutarán regularmente en los equipos objetivo según la programación definida.



Políticas de equipos y máquinas virtuales - Tareas de análisis bajo demanda

El análisis se realiza discretamente en segundo plano, tanto si ha iniciado sesión el usuario en el sistema como si no.

Aunque no es obligatorio, se recomienda programar un análisis completo del sistema que se ejecute semanalmente en todos los endpoints. Analizar los endpoints regularmente 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.

Puede añadir y configurar los siguientes tipos de tareas de análisis:

- **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.

  Cuando se encuentran rootkits o malware, Bitdefender procede automáticamente a la desinfección. Si por alguna razón no se pudiese desinfectar el archivo, este se trasladará a la cuarentena. Este tipo de análisis ignora los archivos sospechosos.

  Quick Scan es una tarea de análisis por defecto con opciones preconfiguradas que no se pueden cambiar. Puede añadir solo una tarea de Quick Scan para una misma política.

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

  Bitdefender trata automáticamente de desinfectar los archivos en los que se ha detectado malware. En caso de que no se pueda eliminar el malware, se recluye en la cuarentena, donde no puede causar ningún daño. Los archivos

sospechosos se ignoran. Si quiere actuar también sobre los archivos sospechosos, o si desea escoger otras acciones por defecto para los archivos infectados, efectúe un Análisis personalizado.

El Análisis completo es una tarea de análisis por defecto con opciones preconfiguradas que no se pueden cambiar. Puede añadir solo una tarea de Análisis completo para una misma política.

- **Análisis personalizado** le permite elegir las ubicaciones concretas a analizar y configurar las opciones de análisis.
- **Análisis de red** es un tipo de análisis personalizado que permite asignar un solo endpoint administrado para que analice unidades de red y, a continuación, configurar las opciones de análisis y las ubicaciones concretas que deben analizarse. Para las tareas de análisis de red, tiene que introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red objetivo, para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red.

  La tarea de análisis de red recurrente se enviará solo al endpoint seleccionado para realizar el análisis (analizador). Si el endpoint seleccionado no está disponible, se aplicarán los ajustes de análisis locales.

  Nota
  Puede crear tareas de análisis de red solo dentro de una política que ya se aplique a un endpoint que se pueda utilizar como analizador.

Además de las tareas de análisis predeterminadas (que no puede eliminar ni duplicar), puede crear todas las tareas de análisis de red y personalizadas que desee.

Para crear y configurar una nueva tarea de análisis de red o personalizada, haga clic en el botón ⊕ **Añadir** a la derecha 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.

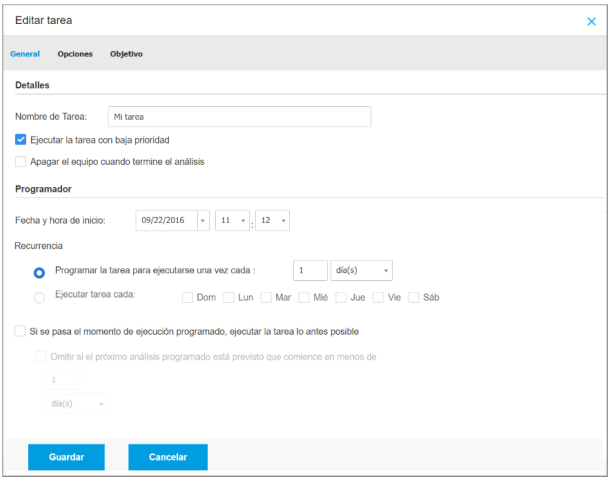
Configurando una Tarea de Análisis

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 que hay que analizar y defina las exclusiones del análisis.

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



Políticas de equipos y máquinas virtuales - 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.

  De forma predeterminada, las tareas de análisis se ejecutan con prioridad decreciente. De esta manera, Bitdefender permite que otros programas se ejecuten más rápidamente, pero aumenta el tiempo necesario para que el análisis finalice. Utilice la casilla de verificación **Ejecutar la tarea con prioridad baja** para desactivar o volver a activar esta característica.

  > **Nota**
  > Esta opción se aplica solo a Bitdefender Endpoint Security Tools y Endpoint Security (agente antiguo).

Seleccione la casilla de verificación **Apagar el equipo cuando termine el análisis** para apagar la máquina si no va a utilizarla durante un tiempo.

> **Nota**
> Esta opción se aplica a Bitdefender Endpoint Security Tools, Endpoint Security (agente antiguo) y Endpoint Security for Mac.

- **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.

  Los endpoints deben encenderse a la hora programada. Un análisis programado no se ejecutará en su momento adecuado si la máquina está apagada, hibernada o en modo suspensión. En tales situaciones, el análisis se aplazará hasta la próxima vez.

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

  Opcionalmente, puede especificar qué ocurre si la tarea de análisis no se iniciara a la hora programada (endpoint offline o apagado). Use la opción **Si se pasa el momento de ejecución programado, ejecutar la tarea lo antes posible** en función de sus necesidades:

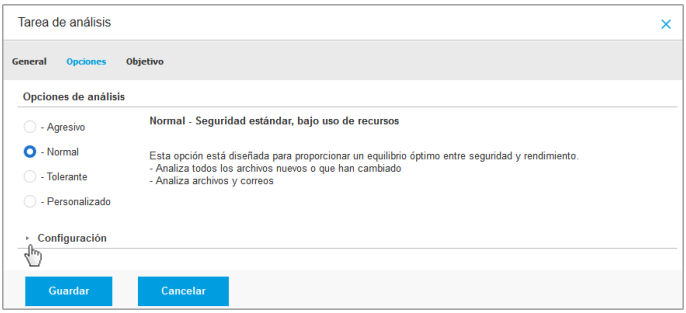
  – Cuando deje la opción desmarcada, la tarea de análisis intentará ejecutarla nuevamente en la siguiente hora programada.

  – Cuando seleccione la opción, obliga al análisis a ejecutarse tan pronto como sea posible. Para definir el mejor momento para la ejecución del análisis y evitar afectar al usuario durante las horas de trabajo, seleccione **Omitir si el próximo análisis programado está previsto que comience en menos de** y especifique el intervalo que desee.

- **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 - Configuración de un análisis personalizado

- **Tipos archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede ajustar el agente de seguridad para analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación 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 "Tipos de archivos de aplicación" (p. 527).

  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 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 recursos compartidos.** Esta opción analiza las unidades de red montadas.

  Esta opción está desactivada por defecto para los Quick Scans. Está activada por defecto para los análisis completos. Para los análisis personalizados, si establece el nivel de seguridad en **Agresivo/Normal**, la opción **Analizar recursos compartidos** se activa automáticamente. Si establece el nivel de seguridad en **Tolerante**, la opción **Analizar recursos compartidos** se desactiva automáticamente.
- **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 endpoint.
- **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.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA). El agente de seguridad 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, el agente de seguridad 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 sospechosos.** Los archivos se detectan como sospechosos mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos). 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.

- Para las tareas de análisis de red, tiene que introducir las credenciales de una cuenta de usuario con permisos de lectura/escritura en las unidades de red

objetivo, para que el agente de seguridad pueda acceder y llevar a cabo acciones en estas unidades de red.

- **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. 293).

Análisis de dispositivos

Puede configurar el agente de seguridad para que detecte y analice automáticamente dispositivos de almacenamiento externo cuando se conecten al endpoint. La detección de dispositivos se dividen en una de estas categorías:

- Cds/DVDs
- Dispositivos de almacenamiento USB, como lápices flash y discos duros externos.
- 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 algunos dispositivos, como los CD o DVD, son de solo lectura. No se puede realizar ninguna acción sobre los archivos infectados contenidos en tales soportes de almacenamiento.

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 > Notificaciones**, se le pregunta al usuario si desea 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 > Notificaciones**.

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**
- **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.

HyperDetect

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- Linux

HyperDetect añade otra capa de seguridad a las tecnologías de análisis existentes (on-access, bajo demanda y análisis del tráfico), para combatir la nueva generación de ataques informáticos, incluyendo las amenazas persistentes avanzadas. HyperDetect mejora los módulos de protección Antimalware y Control de contenido con su potente heurística basada en la inteligencia artificial y el aprendizaje automático.

Gracias a su capacidad para predecir los ataques personalizados y detectar el malware más sofisticado antes de que se ejecute, HyperDetect pone de manifiesto las amenazas mucho más rápidamente que las tecnologías de análisis basadas en firmas o en el comportamiento.

Para configurar HyperDetect:

1. Utilice la casilla de verificación **HyperDetect** para activar o desactivar el módulo.
2. Seleccione frente a qué tipo de amenazas desea proteger su red. Por defecto, se activa la protección para todo tipo de amenazas: ataques personalizados, archivos sospechosos y tráfico de red, exploits, ransomware o grayware.

Nota
La heurística para el tráfico de red requiere que se active **Control de contenido > Análisis de tráfico**.

3. Personalice el nivel de protección frente a amenazas de los tipos seleccionados.

   Utilice el conmutador general de la parte superior de la lista de amenazas para elegir un nivel único de protección para todos los tipos de amenazas, o seleccione niveles individuales para afinar la protección.

   Configurar el módulo en determinado nivel provocará que las acciones se adopten hasta ese nivel. Por ejemplo, si se establece en **Normal**, el módulo detecta y contiene amenazas que activen los umbrales **Tolerante** y **Normal**, pero no el **Agresivo**.

   La protección aumenta del nivel **Tolerante** a **Agresivo**.

   Tenga en cuenta que una detección agresiva puede conducir a falsos positivos, mientras que una tolerante podría exponer su red a algunas amenazas. Se recomienda establecer primero el nivel de protección al máximo y, luego, bajarlo en caso de que se den muchos falsos positivos, hasta lograr el equilibrio óptimo.

   Nota
   Siempre que activa la protección para un tipo de amenaza, la detección se establece automáticamente en el valor predeterminado (nivel **Normal**).

4. En la sección **Acciones**, configure cómo debe reaccionar HyperDetect ante las detecciones. Utilice las opciones del menú desplegable para establecer la acción que se debe adoptar respecto a las amenazas:
   - Para los archivos: denegar el acceso, desinfectar, eliminar, poner en cuarentena o simplemente informar del archivo.
   - Para el tráfico de red: bloquear o simplemente informar del tráfico sospechoso.
5. Marque la casilla de verificación **Ampliar informes a niveles superiores** que hay junto al menú desplegable si desea ver las amenazas detectadas en niveles de protección más altos que el establecido.

Si no está seguro de la configuración actual, puede restaurar fácilmente los ajustes iniciales haciendo clic en el botón **Restablecer a la configuración predeterminada** en la parte inferior de la página.

Antiexploit avanzado

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo

El Antiexploit avanzado es una tecnología proactiva que detecta exploits en tiempo real. Basado en el aprendizaje automático, protege contra una serie de exploits conocidos y desconocidos, incluyendo ataques sin archivos en memoria.

Para habilitar la protección contra exploits, marque la casilla de verificación **Antiexploit avanzado**.

El Antiexploit avanzado está configurado para que se ejecute con los ajustes recomendados. Puede ajustar la protección de forma diferente en caso necesario. Para restaurar los ajustes iniciales, haga clic en el enlace **Restablecer a la configuración predeterminada** a la derecha del encabezado de la sección.

Los ajustes antiexploit de GravityZone se organizan en tres secciones:

- **Detecciones en todo el sistema**

  Las técnicas antiexploit de esta sección monitorizan los procesos del sistema que son blanco de exploits.

  Para obtener más información sobre las técnicas disponibles y cómo configurar sus ajustes, consulte “Configurar la mitigación en todo el sistema” (p. 286).

- **Aplicaciones predefinidas**

  El módulo Antiexploit avanzado está preconfigurado con una lista de aplicaciones habituales, como Microsoft Office, Adobe Reader o Flash Player, que son las más expuestas a los exploits.

  Para obtener más información sobre las técnicas disponibles y cómo configurar sus ajustes, consulte “Configurar técnicas específicas de aplicaciones” (p. 286).

- **Aplicaciones adicionales**

  En esta sección puede añadir y configurar la protección para tantas otras aplicaciones como desee.

  Para obtener más información sobre las técnicas disponibles y cómo configurar sus ajustes, consulte “Configurar técnicas específicas de aplicaciones” (p. 286).

Puede expandir o contraer cada sección haciendo clic en su encabezado. De esta manera, llegará rápidamente a los ajustes que desee configurar.

Configurar la mitigación en todo el sistema

En esta sección, dispone de las siguientes opciones:

Técnica	Descripción
Escalamiento de privilegios	Evita que los procesos obtengan acceso a recursos y privilegios no autorizados. Acción por defecto: Cierra el proceso
Protección de procesos LSASS	Protege al proceso LSASS contra la filtración de secretos, como los hashes de contraseñas y los ajustes de seguridad. Acción por defecto: Bloquea el proceso

Estas técnicas antiexploit están habilitadas por defecto. Para inhabilitar cualquiera de ellas, desmarque su casilla de verificación.

Opcionalmente, puede cambiar la acción adoptada automáticamente al producirse la detección. Elija una acción disponible en el menú correspondiente:

- **Cerrar proceso**: Cierra inmediatamente el proceso sometido a exploit.
- **Bloquear proceso**: Evita que el proceso malicioso acceda a recursos no autorizados.
- **Solo informar**: GravityZone informa del evento sin adoptar ninguna acción de mitigación. Puede ver los detalles del evento en la notificación de **Antiexploit avanzado** y en los informes de auditoría de seguridad y de aplicaciones bloqueadas.

Configurar técnicas específicas de aplicaciones

Ya sean aplicaciones predefinidas o adicionales, todas comparten el mismo conjunto de técnicas antiexploit. Estos se describen a continuación:

Técnica	Descripción
ROP: Emulación	Detecta intentos de hacer ejecutables las páginas de memoria para datos utilizando la técnica de programación orientada al retorno (ROP, por sus siglas en inglés). Acción por defecto: Cerrar el proceso
ROP: Stack pivoting	Detecta los intentos de secuestrar el flujo de código mediante la técnica ROP validando la ubicación de la pila. Acción por defecto: Cerrar el proceso
ROP: Llamada ilegal	Detecta los intentos de secuestrar el flujo de código mediante la técnica ROP validando los autores de llamadas a funciones sensibles del sistema. Acción por defecto: Cerrar el proceso
ROP: Pila desalineada	Detecta los intentos de corromper la pila mediante la técnica ROP validando la alineación de la dirección de la pila. Acción por defecto: Cerrar el proceso
ROP: Retorno a la pila	Detecta los intentos de ejecutar código directamente en la pila mediante la técnica ROP validando el rango de la dirección de retorno. Acción por defecto: Cerrar el proceso
ROP: Pila ejecutable	Detecta los intentos de corromper la pila mediante la técnica ROP validando la protección de página de la pila. Acción por defecto: Cerrar el proceso
Genérico de flash	Detecta los intentos de exploit de Flash Player. Acción por defecto: Cerrar el proceso
Carga útil flash	Detecta los intentos de ejecutar código malicioso en Flash Player analizando los objetos Flash en la memoria. Acción por defecto: Cerrar el proceso
VBScript Genérico	Detecta los intentos de exploit de VBScript. Acción por defecto: Cerrar el proceso
Ejecución de shellcode	Detecta los intentos de crear nuevos procesos o descargar archivos mediante shellcode.

Técnica	Descripción
	Acción por defecto: Cerrar el proceso
Shellcode LoadLibrary	Detecta los intentos de ejecutar código a través de rutas de red mediante shellcode. Acción por defecto: Cerrar el proceso
Antidesvío	Detecta los intentos de eludir las comprobaciones de seguridad para crear nuevos procesos. Acción por defecto: Cerrar el proceso
Shellcode EAF (filtrado de direcciones de exportación)	Detecta los intentos de acceso de código malicioso a funciones sensibles del sistema en las exportaciones de DLL. Acción por defecto: Cerrar el proceso
Subproceso shellcode	Detecta los intentos de insertar código malicioso validando los subprocesos recién creados. Acción por defecto: Cerrar el proceso
Anti Meterpreter	Detecta los intentos de crear un shell inverso analizando páginas de memoria ejecutables. Acción por defecto: Cerrar el proceso
Creación de proceso obsoleto	Detecta los intentos de crear nuevos procesos utilizando técnicas obsoletas. Acción por defecto: Cerrar el proceso
Creación de proceso secundario	Bloquea la creación de cualquier proceso secundario. Acción por defecto: Cerrar el proceso
Aplicar Windows DEP	Hace cumplir la prevención de ejecución de datos (DEP, por sus siglas en inglés) para bloquear la ejecución de código desde páginas de datos. Por defecto: Inhabilitado
Aplicar la reubicación de módulos (ASLR)	Evita que el código se cargue en ubicaciones predecibles reubicando los módulos de memoria. Por defecto: Habilitado

Técnica	Descripción
Exploits emergentes	Protege contra cualquier nuevo exploit o amenaza emergente. Se utilizan actualizaciones rápidas para esta categoría antes de que se puedan realizar cambios más completos. Por defecto: Habilitado

Para monitorizar otras aplicaciones, excepto las predefinidas, haga clic en el botón **Añadir aplicación** disponible en la parte superior e inferior de la página.

Para configurar los ajustes de antiexploit para una aplicación:

1. Para aplicaciones existentes, haga clic en su nombre. Para aplicaciones nuevas, haga clic en el botón **Añadir**.

   Una nueva página muestra todas las técnicas y sus ajustes para la aplicación seleccionada.

   > **Importante**
   > Tenga cuidado al añadir nuevas aplicaciones para su monitorización. Bitdefender no puede garantizar la compatibilidad con ninguna aplicación. Por lo tanto, se recomienda probar la característica primero en algunos endpoints que no sean críticos y, luego, implementarla en la red.

2. Para añadir una nueva aplicación, introduzca su nombre y los de sus procesos en los campos correspondientes. Use el punto y coma (;) para separar los nombres de los procesos.
3. Si necesita consultar rápidamente la descripción de una técnica, haga clic en la flecha junto a su nombre.
4. Seleccione o desmarque las casillas de verificación de las técnicas de exploit, según sea preciso.

   Utilice la opción **Todas** si desea marcar todas las técnicas a la vez.
5. En caso necesario, cambie la acción adoptada automáticamente al producirse la detección. Elija una acción disponible en el menú correspondiente:
   - **Cerrar proceso**: Cierra inmediatamente el proceso sometido a exploit.

- **Solo informar**: GravityZone informa del evento sin adoptar ninguna acción de mitigación. Puede ver los detalles del evento en la notificación de **Antiexploit avanzado** y en los informes.

Por defecto, todas las técnicas para aplicaciones predefinidas están configuradas para mitigar el problema, mientras que para las aplicaciones adicionales se configuran para informar del evento únicamente.

Para cambiar rápidamente la acción adoptada para todas las técnicas a la vez, seleccione la acción en el menú correspondiente con la opción **Todas**.

Haga clic en el botón **Atrás** del lateral derecho de la página para volver a los ajustes generales de antiexploit.

Configuración

En esta sección puede configurar los ajustes de la cuarentena y las reglas de exclusión de análisis.

- Configuración de ajustes de la cuarentena
- Configurar exclusiones de análisis

Cuarentena

Puede configurar las siguientes opciones para los archivos en cuarentena de los endpoints objetivo:

- **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).** Por defecto, los archivos en cuarentena se envían automáticamente a Bitdefender Labs cada hora. 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.
- **Volver a analizar la cuarentena tras actualizar los contenidos de seguridad.** Mantenga esta opción seleccionada para analizar automáticamente los archivos de la cuarentena tras las actualizaciones de los contenidos de seguridad. 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**.
- **Permitir a los usuarios adoptar acciones en la cuarentena local.** Esta opción controla las acciones que los usuarios de endpoints pueden adoptar sobre los archivos locales en cuarentena a través de la interfaz de Bitdefender Endpoint Security Tools. Por defecto, los usuarios locales pueden restaurar o eliminar los archivos en cuarentena de su equipo mediante las opciones disponibles en Bitdefender Endpoint Security Tools. Al desactivar esta opción, los usuarios ya no tendrán acceso a los botones de acción de los archivos en cuarentena de la interfaz de Bitdefender Endpoint Security Tools.

Cuarentena centralizada

Si desea conservar los archivos en cuarentena de los endpoints administrados para un análisis posterior, utilice la opción **Cuarentena centralizada**, que envía una copia comprimida de cada archivo en cuarentena local a un recurso compartido.

Tras habilitar esta opción, cada archivo en cuarentena de los endpoints administrados se copia y se empaqueta en un archivo ZIP protegido por contraseña para dejarlo en la ubicación de red especificada. El nombre del archivo comprimido es el hash del archivo en cuarentena.

Importante
El tamaño del archivo comprimido está limitado a 100 MB. Si el archivo superase los 100 MB, no se guardará en el recurso compartido.

Para configurar los ajustes de la cuarentena centralizada, rellene los campos siguientes:

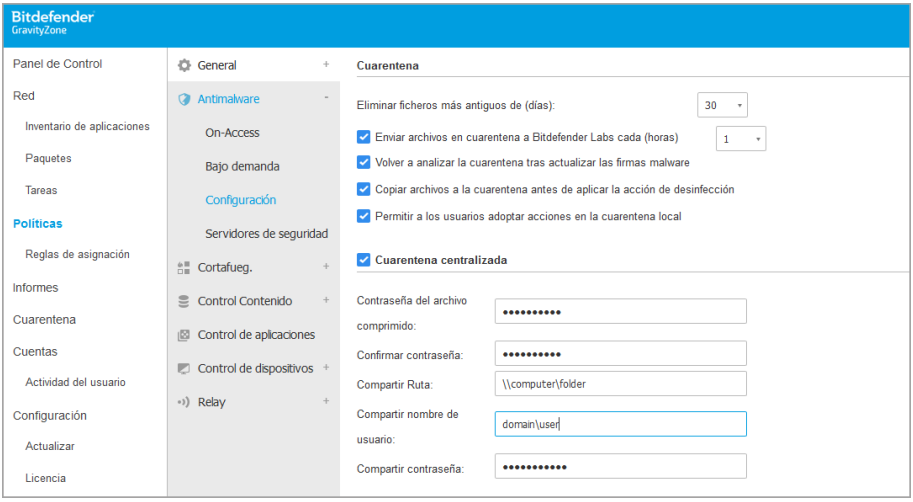
- **Contraseña del archivo comprimido**: introduzca la contraseña requerida para los archivos comprimidos de la cuarentena. La contraseña debe contener al menos un carácter en mayúsculas, uno en minúsculas, y un número o un carácter especial. Confirme la contraseña en el campo siguiente.
- **Ruta del recurso compartido**: introduzca la ruta de red donde desea almacenar los archivos comprimidos (por ejemplo, `\\equipo\carpeta`).

- Nombre de usuario y contraseña necesarios para conectarse al recurso compartido. Los formatos admitidos para el nombre de usuario son los siguientes:
  - `Usuario@dominio`
  - `dominio\ nombre de usuario`
  - `nombre de usuario`.

Para que la cuarentena centralizada funcione correctamente, asegúrese de que se cumplen las siguientes condiciones:

- La ubicación compartida es accesible en la red.
- Los endpoints pueden conectarse al recurso compartido.
- Las credenciales de inicio de sesión son válidas y proporcionan acceso de escritura al recurso compartido.
- El recurso compartido tiene suficiente espacio en disco.

Nota
La cuarentena centralizada no se aplica a la cuarentena de servidores de correo.



Cuarentena centralizada

Si tiene una instancia local de Sandbox Analyzer configurada en la sección **Sandbox Analyzer > Sensor de endpoints**, puede marcar la casilla de verificación **Enviar automáticamente los elementos de la cuarentena a Sandbox Analyzer**. Tenga en cuenta que los elementos enviados deben tener un tamaño máximo de 50 MB.

Exclusiones

El agente de seguridad de Bitdefender puede excluir del análisis ciertos tipos de objetos. Las exclusiones de antimalware son para utilizarlas en circunstancias especiales o siguiendo las recomendaciones de Microsoft o de Bitdefender. Lea este artículo para consultar una lista actualizada de exclusiones recomendadas por Microsoft.

En esta sección, puede configurar el uso de diferentes tipos de exclusiones disponibles en el agente de seguridad de Bitdefender.

- Las **exclusiones incorporadas** están activadas por defecto y se incluyen en el agente de seguridad de Bitdefender.

  Si desea analizar todo tipo de objetos, puede optar por desactivar las exclusiones incorporadas, pero esta opción tendrá un impacto considerable sobre el rendimiento de la máquina y aumentará el tiempo de análisis.

- También puede definir **Exclusiones personalizadas** para aplicaciones desarrolladas internamente o herramientas personalizadas, en función de sus necesidades concretas.

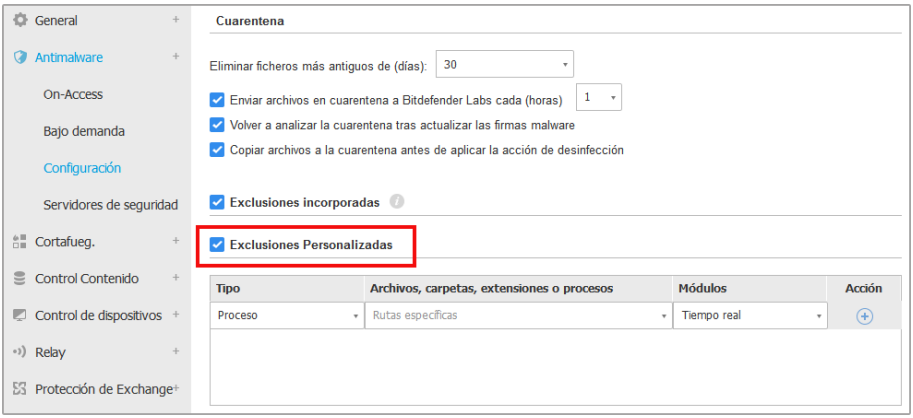
  Las exclusiones de antimalware personalizadas se aplican a uno o varios de los siguientes métodos de análisis:

  - Análisis en tiempo real
  - Análisis solicitado
  - Control avanzado de amenazas
  - Protección contra ataques sin archivos
  - Mitigación de ransomware

  Importante

  - Si dispone de un archivo de prueba de EICAR que use para probar la protección antimalware periódicamente, debería excluirlo del análisis on-access.
  - Si utiliza VMware Horizon View 7 y App Volumes AppStacks, consulte este documento de VMware.

Para excluir elementos concretos del análisis, seleccione la opción **Exclusiones personalizadas** y, luego, añada las reglas a la tabla que figura a continuación.



Políticas de equipos y máquinas virtuales - Exclusiones personalizadas

Para añadir una regla de exclusión personalizada:

1. Seleccione el tipo de exclusión desde el menú:
   - **Archivo**: Solo el archivo especificado
   - **Carpeta**: Todos los archivos y procesos dentro de la carpeta indicada y de todas sus subcarpetas
   - **Extensión**: Todos los elementos que tengan la extensión indicada
   - **Proceso**: Cualquier objeto al que acceda el proceso excluido
   - **Hash de archivo**: El archivo con el hash indicado
   - **Hash de certificado**: Todas las aplicaciones con el hash de certificado (huella digital) indicado
   - **Nombre de la amenaza**: Cualquier elemento que tenga el nombre de detección (no disponible para sistemas operativos Linux)
   - **Línea de comandos**: La línea de comandos especificada (disponible solo para sistemas operativos Windows)

Aviso
En entornos VMware sin agentes integrados con vShield, puede excluir solo carpetas y extensiones. Mediante la instalación de Bitdefender Tools en las máquinas virtuales, también puede excluir archivos y procesos.
Durante el proceso de instalación, al configurar el paquete, debe marcar la casilla de verificación **Implementar endpoint con vShield cuando se detecta un entorno VMware integrado con vShield**. Para más información, consulte la sección **Crear paquetes de instalación** de la Guía de instalación.

2. Proporcione la información específica para el tipo de exclusión seleccionado:

   Archivo, carpeta o proceso

   Introduzca la ruta al elemento que se excluirá del análisis. Dispone de varias opciones útiles para escribir la ruta:

   – Declare la ruta explícitamente.

     Por ejemplo: `C: emp`

     Para añadir exclusiones para las rutas UNC, use cualquiera de las siguientes sintaxis:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   – Utilice las variables del sistema disponibles en el menú desplegable.

     Para procesar exclusiones debe añadir también el nombre del archivo ejecutable de la aplicación.

     Por ejemplo:

     `%ProgramFiles%`: Excluye la carpeta Archivos de programa

     `%WINDIR%\system32`: Excluye la carpeta system32 dentro de la carpeta de Windows

     Nota
     Se aconseja utilizar variables del sistema (donde sea preciso) para asegurar que la ruta es válida en todos los equipos objetivo.

   – Use comodines.

     El asterisco (*) sustituye cero o más caracteres. El signo de interrogación (?) sustituye 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.

Por ejemplo:

Exclusiones de archivos:

`C:\Test\*`: Excluye todos los archivos de la carpeta Test

`C:\Test\*.png`: Excluye los archivos PNG de la carpeta Test

Exclusión de carpeta:

`C:\Test\*`: Excluye todos los archivos de la carpeta Test

Exclusión de procesos:

`C:\Archivos de programa\WindowsApps\Microsoft.Not??.exe`: Excluye los procesos de Microsoft Notes

Nota
Las exclusiones de procesos no admiten comodines en los sistemas operativos Linux.

Extensión

Introduzca una o más extensiones de archivo que deban excluirse 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
En los sistemas basados en Linux, las extensiones de archivos distinguen entre mayúsculas y minúsculas y los archivos con el mismo nombre pero con extensiones diferentes se consideran objetos distintos. Por ejemplo, `archivo.txt` es diferente de `archivo.TXT`.

Hash de archivo, hash de certificado, nombre de amenaza o línea de comandos

Introduzca el hash del archivo, la huella digital del certificado (hash), el nombre exacto de la amenaza o la línea de comandos dependiendo de la regla de exclusión. Puede utilizar un elemento por exclusión.

3. Seleccione los métodos de análisis a los que se aplica la regla. Algunas exclusiones pueden ser relevantes para el análisis on-access, el análisis bajo demanda o ATC/IDS, mientras que otras pueden recomendarse para los tres módulos.
4. Opcionalmente, haga clic en el botón **Mostrar anotaciones** para añadir una nota acerca de la regla en la columna **Notas**.
5. 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.

Importante
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 en un archivo o carpeta y seleccionando **Analizar con Bitdefender Endpoint Security Tools**.

Importación y exportación de exclusiones

Si tiene intención de volver a utilizar las reglas de exclusión en varias políticas, puede exportarlas e importarlas.

Para exportar exclusiones personalizadas:

1. Haga clic en el botón **Exportar** de la zona superior de la tabla de exclusiones.
2. Guarde el archivo CSV en su equipo. Dependiendo de la configuración de su navegador, puede que el archivo se descargue de forma automática, o que se le pida que lo guarde en alguna ubicación.

Cada fila del archivo CSV corresponde a una sola regla, cuyos campos aparecen en el orden siguiente:

```
<exclusion type>, <object to be excluded>, <modules>
```

Estos son los valores disponibles para los campos CSV:

Tipo de exclusión:

`1`, para las exclusiones de archivos

`2`, para las exclusiones de carpetas

3, para las exclusiones de extensiones

4, para las exclusiones de procesos

5, para las exclusiones de hashes de archivos

6, para las exclusiones de hashes de certificados

7, para las exclusiones de nombres de amenazas

8, para las exclusiones de líneas de comandos

Objeto que hay que excluir:
Una ruta o una extensión de archivo

Módulos:

1, para los análisis bajo demanda

2, para los análisis on-access

3, para todos los módulos

4, para ATC/IDS

Por ejemplo, un archivo CSV que contenga exclusiones antimalware podría tener este aspecto:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Nota
En las rutas de Windows hay que duplicar el carácter de barra invertida (\). Por ejemplo, `%WinDir%\\System32\\LogFiles`.

Para importar exclusiones personalizadas:

1. Haga clic en **Importar**. Se abre la ventana **Importar exclusiones de políticas**.
2. Haga clic en **Añadir** y, a continuación, seleccione el archivo CSV.
3. Haga clic en **Guardar**. La tabla se rellena con las reglas válidas. Si el archivo CSV contiene reglas no válidas, aparece una advertencia le informa de los números de fila correspondientes.

Security Servers

En este apartado puede configurar lo siguiente:

- Asignación de Security Server
- Ajustes específicos de Security Server

Política - Equipos y máquinas virtuales - Antimalware - Servidores de seguridad

Asignación de Security Server

Puede asignar uno o varios Security Server a los endpoints objetivo y establecer la prioridad con la que los endpoints elegirán un Security Server para enviar sus solicitudes de análisis.

Nota
Se recomienda usar Security Server para analizar máquinas virtuales o equipos de escasos recursos.

Para asignar un Security Server a los endpoints objetivo, añada los Security Server que desea usar en la tabla de **Asignación de Security Server** de la siguiente manera:

1. Haga clic en la lista desplegable **Security Server** y luego seleccione un Security Server.

2. Si el Security Server está en una DMZ o tras un servidor NAT, introduzca el FQDN o la IP del servidor NAT en el campo **Nombre/IP del servidor personalizado**.

   Importante
   Asegúrese de que la redirección de puertos esté correctamente configurada en el servidor NAT para que el tráfico de los endpoints pueda llegar al Security Server.

3. Haga clic en el botón ⊕ **Añadir** de la columna **Acciones**.

   El Security Server se añade a la lista.

4. Repita los pasos anteriores para añadir otros Security Server, si existen o se necesitan.

Para establecer la prioridad de los Security Server:

1. Use las flechas de arriba y abajo de la columna **Acciones** para aumentar o disminuir la prioridad de cada Security Server.

   Al asignar más Security Server, el que figure más arriba en la lista tendrá la mayor prioridad y se seleccionará primero. Si este Security Server no está disponible o se halla sobrecargado, se seleccionará el siguiente Security Server. El tráfico de análisis se redirige al primer Security Server que haya disponible y tenga una carga conveniente.

2. Seleccione **Conectarse en primer lugar al Security Server instalado en el mismo host físico, si está disponible, cualquiera que sea la prioridad asignada** para una distribución uniforme de endpoints y una latencia optimizada. Si este Security Server no está disponible, se elegirá otro Security Server de la lista por orden de prioridad.

   Importante
   Esta opción solo funciona con Security Server Multiplataforma y solo si GravityZone está integrado con el entorno virtualizado.

Para eliminar un Security Server de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente de la columna **Acciones**.

Ajustes de Security Server

Al asignar la política a los Security Server, puede configurarlos con los siguientes ajustes:

- **Limite el número de análisis bajo demanda simultáneos**.

  La ejecución de múltiples tareas de análisis bajo demanda en máquinas virtuales que compartan el mismo datastore puede crear tormentas de análisis antimalware. Para evitarlo y permitir que solo se ejecuten simultáneamente un cierto número de tareas de análisis:

  1. Seleccione la opción **Limitar el número de análisis bajo demanda simultáneos**.
  2. Seleccione en el menú desplegable el nivel de tareas de análisis concurrentes permitidas. Puede elegir un nivel predefinido o introducir un valor personalizado.

     La fórmula para hallar el límite máximo de tareas de análisis para cada nivel predefinido es la siguiente: `N = a x MAX(b ; vCPUs - 1)`, donde:

     - `N` = límite máximo de tareas de análisis
     - `a` = coeficiente multiplicador, con los siguientes valores: `1` - para Bajo; `2` - para Medio; `4` - para Alto
     - `MAX(b ; vCPU - 1)` = una función que devuelve el número máximo de slots de análisis disponibles en el Security Server.
     - `b` = el número por defecto de slots de análisis bajo demanda, que actualmente se establece en cuatro.
     - `vCPUs` = número de CPUs virtuales asignadas al Security Server

     Por ejemplo:

     Para un Security Server con 12 CPU y un límite Alto de análisis simultáneos, tenemos un límite de:

     `N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` tareas de análisis bajo demanda simultáneas.

- **Habilitar reglas de afinidad para Security Server Multiplataforma**

  Elija qué comportamiento debe tener Security Server cuando su host entre en modo de mantenimiento:

  - Si está habilitado, el Security Server permanece vinculado al host y GravityZone lo apaga. Cuando finaliza el mantenimiento, GravityZone reinicia automáticamente el Security Server.

Este es el comportamiento por defecto.

– Si está inhabilitado, el Security Server se mueve a otro host y sigue ejecutándose. En este caso, el nombre del Security Server cambia en Control Center para apuntar al host anterior. El cambio de nombre persiste hasta que el Security Server se mueva de nuevo a su host nativo.

  Si hay suficientes recursos, el Security Server puede ir a parar a un host donde haya instalado otro Security Server.

  Importante
  Esta opción no tiene efecto si HVI también usa Security Server.

- **Usar SSL**

  Habilite esta opción si desea cifrar la conexión entre los endpoints objetivo y los appliances Security Server especificados.

  GravityZone utiliza por defecto certificados de seguridad autofirmados. Puede cambiarlos por sus propios certificados en la página **Configuración > Certificados** de Control Center. Para más información, consulte el capítulo "Configurar los ajustes de Control Center" de la Guía de instalación.

- **Comunicación entre los Security Server y GravityZone**

  Escoja una de las opciones disponibles para definir sus preferencias de proxy para la comunicación entre las máquinas Security Server seleccionadas y GravityZone:

  – **Mantener los ajustes de la instalación**, para utilizar los mismos ajustes de proxy definidos en el paquete de instalación.

  – **Utilizar el proxy definido en la sección General**, para usar los ajustes de proxy definidos en la política actual, en la sección **General > Ajustes**.

  – **No usar proxy**, cuando los endpoints objetivo no se comunican con los componentes de Bitdefender a través de proxy.

7.2.4. Sandbox Analyzer

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores

Sandbox Analyzer proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender.

En esta sección puede configurar lo siguiente:

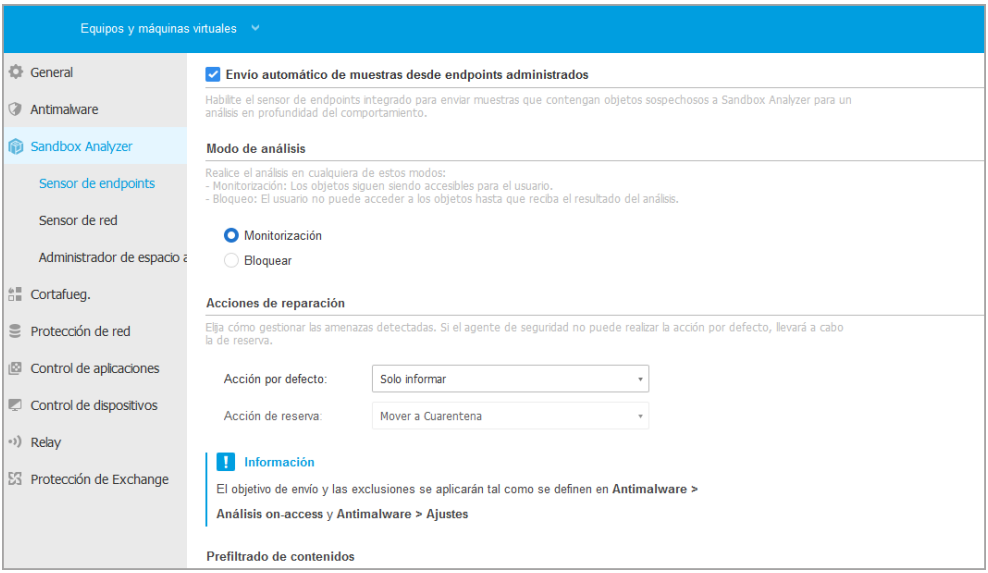
- Envío a través del sensor de endpoints
- Envío a través del sensor de red
- Envío a través del sensor ICAP
- Ajustes de Sandbox Manager

En los ajustes de la política, también puede configurar el envío automático desde la cuarentena centralizada. Para obtener información, consulte "Cuarentena centralizada" (p. 291).

Para obtener información sobre el envío manual, consulte "Envío manual" (p. 484). Para obtener más información sobre el envío a través de API, consulte los capítulos sobre **Sandbox** y **Portal de Sandbox** en la Guía de la API de GravityZone (on-premise).

Sensor de endpoints

Bitdefender Endpoint Security Tools puede actuar como un sensor de alimentación de Sandbox Analyzer desde los endpoints de Windows.



Políticas > Sandbox Analyzer > Sensor de endpoints

Para configurar el envío automático a través del sensor de endpoints:

1. En **Ajustes de conexión**, seleccione una de las opciones:
   - **Usar Sandbox Analyzer en la nube**: El sensor del endpoint enviará muestras a una instancia de Sandbox Analyzer alojada por Bitdefender, según su región.
   - **Usar la instancia local de Sandbox Analyzer**: El sensor de endpoints enviará muestras a una instancia de Sandbox Analyzer On-Premises. Elija en el menú desplegable la instancia de Sandbox Analyzer que prefiera.

   Si su red está detrás de un servidor proxy o un cortafuego, puede configurar un proxy para que se conecte a Sandbox Analyzer marcando la casilla de verificación **Usar configuración proxy**.

   Ha de rellenar los siguientes campos:
   - **Servidor**: La IP del servidor proxy.
   - **Puerto**: El puerto utilizado para conectar con el servidor proxy.
   - **Nombre de usuario**: Un nombre de usuario que el proxy reconozca.

- **Contraseña**: La contraseña válida para el usuario especificado.

2. Marque la casilla de verificación **Envío automático de muestras desde endpoints administrados** para permitir el envío automático de archivos sospechosos a Sandbox Analyzer.

   Importante

   - Sandbox Analyzer requiere el análisis on-access. Asegúrese de tener el módulo **Antimalware > Análisis on-access** activado.
   - Sandbox Analyzer utiliza los mismos objetivos y exclusiones definidos en **Antimalware > Análisis on-access**. Revise cuidadosamente los ajustes de análisis on-access al configurar Sandbox Analyzer.
   - Para evitar falsos positivos (la detección errónea de aplicaciones legítimas), puede configurar exclusiones por nombre, extensión, tamaño y ruta de acceso al archivo. Para obtener más información sobre el análisis on-access, consulte "Antimalware" (p. 262).
   - El límite de carga de cualquier archivo (comprimido o no) es de 50 MB.

3. Elija el **Modo de análisis**. Hay dos opciones disponibles:
   - **Monitorización**. El usuario puede acceder al archivo durante el análisis en el espacio aislado, pero se le recomienda no ejecutarlo hasta recibir el resultado del análisis.
   - **Bloqueo**. El usuario no puede ejecutar el archivo hasta que el resultado del análisis llegue al endpoint desde el clúster de Sandbox Analyzer a través del portal de Sandbox Analyzer.
4. Especifique las **Acciones de reparación**. Estas se adoptan cuando Sandbox Analyzer detecta una amenaza. Para cada modo de análisis se proporciona una doble configuración, que consiste en una acción por defecto y otra alternativa. Sandbox Analyzer realiza inicialmente la acción por defecto y, a continuación, la de reserva, si no puede llevar a cabo la primera.

   Al acceder a esta sección por primera vez, están disponibles las siguientes configuraciones:

   Nota
   Se recomienda utilizar acciones de reparación en esta configuración.

- En el modo de **Monitorización**, la acción por defecto es **Solo informar**, con la acción de reserva desactivada.
- En el modo de **Bloqueo**, la acción por defecto es **Cuarentena**, mientras que la de reserva es **Eliminar**.

Sandbox Analyzer le ofrece las siguientes acciones de reparación:

- **Desinfectar**. Elimina el código de malware de los archivos infectados.
- **Eliminar**. Elimina todo el archivo detectado del disco.
- **Cuarentena**. Traslada 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 la cuarentena desde la página **Cuarentena** de Control Center.
- **Solo informar**. Sandbox Analyzer solo informa de las amenazas detectadas, sin adoptar ninguna otra acción respecto a ellas.

Nota
Dependiendo de la acción por defecto, puede que no haya disponible ninguna acción de reserva.

5. Tanto las acciones de reparación por defecto como las alternativas están configuradas en el modo **Solo informar**.
6. En **Prefiltrado de contenidos**, personalice el nivel de protección contra amenazas potenciales. El sensor de endpoints ha incorporado un mecanismo de filtrado de contenidos que determina si es necesario detonar un archivo sospechoso en Sandbox Analyzer.

   Los tipos de objetos admitidos son los siguientes: aplicaciones, documentos, scripts, archivos y mensajes de correo electrónico. Para obtener más información sobre los tipos de objetos admitidos, consulte "Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos" (p. 532).

   Utilice el conmutador principal de la parte superior de la lista de amenazas para elegir un nivel único de protección para todos los tipos de objetos o seleccione niveles individuales para afinar la protección.

   Configurar el módulo en determinado nivel ocasionará el envío de cierta cantidad de muestras:

- **Tolerante**. El sensor del endpoint envía automáticamente a Sandbox Analyzer solo los objetos con más probabilidades de ser maliciosos e ignora el resto.
- **Normal**. El sensor del endpoint busca un equilibrio entre los objetos enviados e ignorados y envía a Sandbox Analyzer tanto objetos con más probabilidades de ser maliciosos como otros con menos.
- **Agresivo**. El sensor del endpoint envía a Sandbox Analyzer casi todos los objetos, independientemente de su riesgo potencial.

En un campo al efecto, puede definir excepciones para los tipos de objetos que no desea enviar a Sandbox Analyzer.

También puede definir los límites de tamaño de los objetos enviados marcando la casilla de verificación correspondiente e introduciendo cualquier valor deseado entre 1 KB y 50 MB.

7. En **Perfil de detonación**, ajuste el nivel de complejidad del análisis de comportamiento, lo cual afecta al rendimiento de Sandbox Analyzer. Por ejemplo, si se fija en **Alto**, Sandbox Analyzer realizará, en el mismo intervalo, un análisis más preciso sobre menos muestras que si está en **Medio** o **Bajo**.

Sandbox Analyzer admite el envío local de archivos a través de endpoints con rol de relay, que pueden conectarse a diferentes direcciones del Portal de Sandbox Analyzer dependiendo de la región. Para más información sobre los ajustes para la configuración del relay, consulte “Relay” (p. 355).

Nota
Un proxy configurado en los ajustes de conexión de Sandbox Analyzer anulará cualquier endpoint con rol de relay.

Sensor de red

En esta sección, puede configurar el envío automático de muestras del tráfico de red a Sandbox Analyzer a través del sensor de red. Este módulo requiere que el Network Security Virtual Appliance se implemente y configure con Sandbox Analyzer On-Premises.

Para configurar el envío automático a través del sensor de red:

1. Marque la casilla de verificación **Envío automático de muestras desde el sensor de red** para permitir el envío automático de archivos sospechosos a Sandbox Analyzer.

2. En **Prefiltrado de contenidos**, personalice el nivel de protección contra amenazas potenciales. El sensor de red ha incorporado un mecanismo de filtrado de contenidos que determina si es necesario detonar un archivo sospechoso en Sandbox Analyzer.

   Los tipos de objetos admitidos son los siguientes: aplicaciones, documentos, scripts, archivos y mensajes de correo electrónico. Para obtener más información sobre los tipos de objetos admitidos, consulte "Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos" (p. 532).

   Utilice el conmutador general de la parte superior de la lista de amenazas para elegir un nivel único de protección para todos los tipos de objetos o seleccione niveles individuales para afinar la protección.

   Configurar el módulo en determinado nivel ocasionará el envío de cierta cantidad de muestras:

   - **Tolerante**. El sensor de red envía automáticamente a Sandbox Analyzer solo los objetos con más probabilidades de ser maliciosos e ignora el resto.
   - **Normal**. El sensor de red busca un equilibrio entre los objetos enviados e ignorados y envía a Sandbox Analyzer tanto objetos con más probabilidades de ser maliciosos como otros con menos.
   - **Agresivo**. El sensor de red envía a Sandbox Analyzer casi todos los objetos, independientemente de su riesgo potencial.

   En un campo al efecto, puede definir excepciones para los tipos de objetos que no desea enviar a Sandbox Analyzer.

   También puede definir los límites de tamaño de los objetos enviados marcando la casilla de verificación correspondiente e introduciendo cualquier valor deseado entre 1 KB y 50 MB.

3. En **Ajustes de conexión**, seleccione la instancia de Sandbox Analyzer a la que prefiera enviar los contenidos de la red.

   Si su red está detrás de un servidor proxy o un cortafuego, puede configurar un proxy para que se conecte a Sandbox Analyzer marcando la casilla de verificación **Usar configuración proxy**.

   Ha de rellenar los siguientes campos:

   - **Servidor**: La IP del servidor proxy.
   - **Puerto**: El puerto utilizado para conectar con el servidor proxy.

- **Nombre de usuario**: Un nombre de usuario que el proxy reconozca.
- **Contraseña**: La contraseña válida para el usuario especificado.

4. En **Perfil de detonación**, ajuste el nivel de complejidad del análisis de comportamiento, lo cual afecta al rendimiento de Sandbox Analyzer. Por ejemplo, si se fija en **Alto**, Sandbox Analyzer realizará, en el mismo intervalo, un análisis más preciso sobre menos muestras que si está en **Medio** o **Bajo**.

Sensor ICAP

En esta sección, puede configurar el envío automático a Sandbox Analyzer a través del sensor ICAP.

Nota
Sandbox Analyzer requiere la configuración de un Security Server para analizar los dispositivos de almacenamiento conectado a la red (NAS) que utilicen el protocolo ICAP. Para obtener información, consulte"Protección de almacenamiento" (p. 394)

1. Marque la casilla de verificación **Envío automático de muestras desde el sensor ICAP** para permitir el envío automático de archivos sospechosos a Sandbox Analyzer.
2. En **Prefiltrado de contenidos**, personalice el nivel de protección contra amenazas potenciales. El sensor de red ha incorporado un mecanismo de filtrado de contenidos que determina si es necesario detonar un archivo sospechoso en Sandbox Analyzer.

   Los tipos de objetos admitidos son los siguientes: aplicaciones, documentos, scripts, archivos y mensajes de correo electrónico. Para obtener más información sobre los tipos de objetos admitidos, consulte "Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos" (p. 532).

   Utilice el conmutador general de la parte superior de la lista de amenazas para elegir un nivel único de protección para todos los tipos de objetos o seleccione niveles individuales para afinar la protección.

   Configurar el módulo en determinado nivel ocasionará el envío de cierta cantidad de muestras:

   - **Tolerante**. El sensor ICAP envía automáticamente a Sandbox Analyzer solo los objetos con más probabilidades de ser maliciosos e ignora el resto.

- **Normal**. El sensor del ICAP busca un equilibrio entre los objetos enviados e ignorados y envía a Sandbox Analyzer tanto objetos con más probabilidades de ser maliciosos como otros con menos.
- **Agresivo**. El sensor ICAP envía a Sandbox Analyzer casi todos los objetos, independientemente de su riesgo potencial.

En un campo al efecto, puede definir excepciones para los tipos de objetos que no desea enviar a Sandbox Analyzer.

También puede definir los límites de tamaño de los objetos enviados marcando la casilla de verificación correspondiente e introduciendo cualquier valor deseado entre 1 KB y 50 MB.

3. En **Ajustes de conexión**, seleccione la instancia de Sandbox Analyzer a la que prefiera enviar los contenidos de la red.

   Si su red está detrás de un servidor proxy o un cortafuego, puede configurar un proxy para que se conecte a Sandbox Analyzer marcando la casilla de verificación **Usar configuración proxy**.

   Ha de rellenar los siguientes campos:

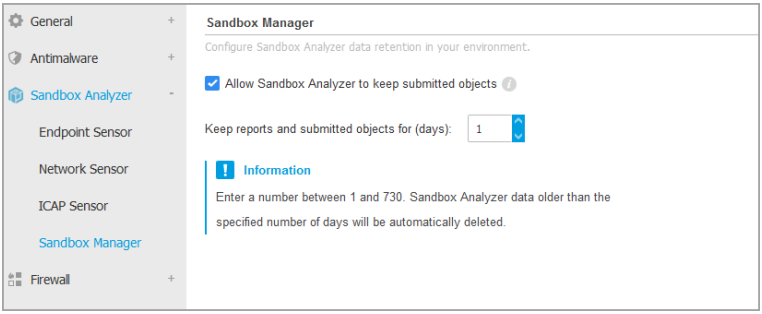
   - **Servidor**: La IP del servidor proxy.
   - **Puerto**: El puerto utilizado para conectar con el servidor proxy.
   - **Nombre de usuario**: Un nombre de usuario que el proxy reconozca.
   - **Contraseña**: La contraseña válida para el usuario especificado.
4. En **Perfil de detonación**, ajuste el nivel de complejidad del análisis de comportamiento, lo cual afecta al rendimiento de Sandbox Analyzer. Por ejemplo, si se fija en **Alto**, Sandbox Analyzer realizará, en el mismo intervalo, un análisis más preciso sobre menos muestras que si está en **Medio** o **Bajo**.

Administrador de espacio aislado

En esta sección, configurará la retención de datos para sus instancias de Sandbox Analyzer:

- Marque la casilla de verificación **Permitir que Sandbox Analyzer conserve los objetos enviados**. Este ajuste le permite utilizar la opción **Volver a enviar para analizar** en la zona de tarjetas de envío de la interfaz de informes de Sandbox Analyzer.

- Especifique el número de días que desea que Sandbox Analyzer conserve los informes y los objetos enviados en el datastore. El dato máximo que puede introducir es 730. Cuando expire el período establecido, se eliminarán todos los datos.



Políticas > Sandbox Analyzer > Sandbox Manager

7.2.5. Cortafuego

Nota
Este módulo está disponible para Windows para estaciones de trabajo.

El cortafuego protege el endpoint frente a 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.

El cortafuego detecta cualquier nueva conexión, compara la información del adaptador para esa conexión con la información de los perfiles existentes y aplica el perfil correcto. Para obtener más información sobre cómo se aplican los detalles, vea "Configuración de la red" (p. 314).

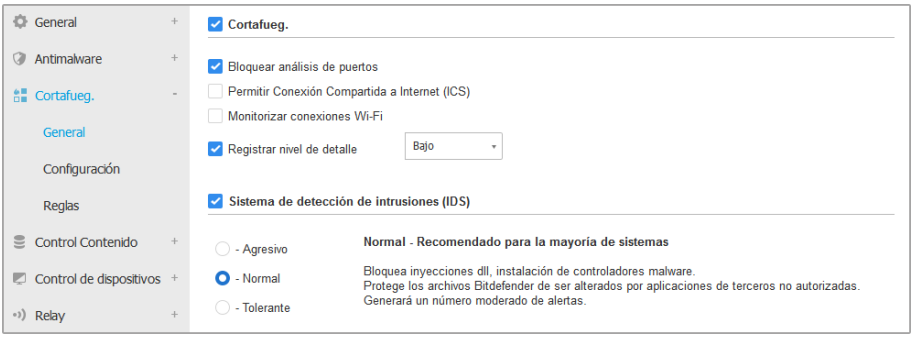
Importante
El módulo de Cortafuego solo está disponible para estaciones de trabajo Windows.

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 y máquinas virtuales - Ajustes generales del cortafuego

- **Cortafuego.** Utilice el conmutador para activar o desactivar el cortafuego.

  Aviso
  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.** El agente de seguridad de Bitdefender puede informar a los usuarios conectados a una red Wi-Fi de cuándo se une un nuevo equipo a la red. Para mostrar dichas notificaciones en la pantalla del usuario, seleccione esta opción.

- **Nivel de detalle del registro.** El agente de seguridad de Bitdefender 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 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.).

  Nota
  Los ajustes de la política del sistema de detección de intrusos (IDS) solo se aplican a Endpoint Security (agente de seguridad antiguo). El agente Bitdefender Endpoint Security Tools integra las capacidades del sistema de detección de intrusos basadas en el host en su módulo Advanced Threat Control (ATC).

  Para configurar el sistema de detección de intrusos:

  1. Marque la casilla de verificación para activar o desactivar el sistema de detección de intrusiones.
  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 intrusos, añada una **regla de exclusión de proceso ATC/IDS** para esa aplicación en la sección **Antimalware > Ajustes > Exclusiones personalizadas**.

Importante
El sistema de detección de intrusos solo está disponible para clientes Endpoint Security.

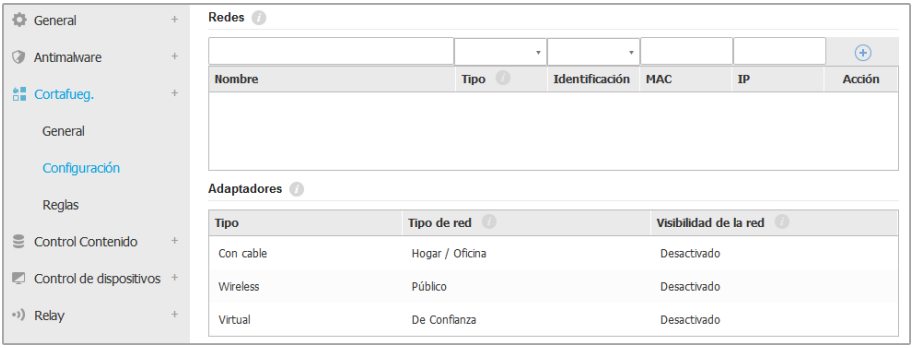
Configuración

El cortafuego aplica automáticamente un perfil basado en el nivel de confianza. Puede tener diferentes niveles de confianza para conexiones de red, dependiendo de la arquitectura de la red o del tipo de adaptador utilizado para establecer la

conexión de red. Por ejemplo, si tiene subredes dentro de la red de su empresa, puede establecer un nivel de confianza para cada subred.

Los ajustes aparecen detallados en las siguientes tablas:

- Redes
- Adaptadores



Políticas - Ajustes del cortafuego

Configuración de la red

Si desea que el cortafuego aplique diferentes perfiles a varios segmentos de red de su empresa, debe especificar las redes gestionadas en la tabla **Redes**. Rellene los campos de la tabla **Redes** como se describe a continuación:

- **Nombre.** Introduzca el nombre que identifique la red en la lista.
- **Tipo.** Seleccione desde el menú el tipo de perfil asignado a la red.

  El agente de seguridad de Bitdefender aplica automáticamente uno de los cuatro perfiles de red para cada conexión de red detectada en el endpoint, con el fin de definir las opciones básicas de filtrado del tráfico. Los tipos de perfiles son:

  - Red de **confianza**. Desactiva el cortafuego para los adaptadores correspondientes.
  - Redes **domésticas/oficina**. Permite todo el tráfico entrante y saliente entre equipos de la red local, mientras que se filtra el resto del tráfico.
  - Red **pública**. Se filtrará todo el tráfico.

  - Red **insegura**. Bloquea completamente el tráfico de red y de Internet a través de los adaptadores correspondientes.

- **Identificación.** Seleccione en el menú el método a través del cual el agente de seguridad de Bitdefender identificará la red. La red puede identificarse mediante tres métodos: **DNS**, **Puerta de enlace** y **Red**.
  - **DNS**: identifica todos los endpoints mediante el DNS especificado.
  - **Puerta de enlace**: identifica todos los endpoints que se comunican a través de la puerta de enlace especificada.
  - **Red**: identifica todos los endpoints del segmento de red especificado, definido por su dirección de red.
- **MAC**. Utilice este campo para especificar la dirección MAC de un servidor DNS o de una puerta de enlace que delimite la red, dependiendo del método de identificación seleccionado.

  Debe introducir la dirección MAC en formato hexadecimal, con separación de guiones (-) o dos puntos (:). Por ejemplo, tanto `00-50-56-84-32-2b` como `00:50:56:84:32:2b` son direcciones válidas.
- **IP.** Utilice este campo para definir la dirección IP específica en una red. El formato de IP depende del método de identificación como se indica a continuación:
  - **Red.** Introduzca el número de red en formato CIDR. Por ejemplo, `192.168.1.0/24`, donde `192.168.1.0` es la dirección de red y `/24` es la máscara de red.
  - **Puerta de enlace.** Introduzca la dirección IP de la puerta de enlace.
  - **DNS.** Introduzca la dirección IP de la MV del servidor DNS.

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**, el agente de seguridad de Bitdefender detecta el tipo de adaptador de red y aplica el consiguiente perfil a la conexión.

Los campos de la tabla **Adaptadores** se describen a continuación:

- **Tipo.** Muestra el tipo de adaptadores de red. El agente de seguridad de Bitdefender 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 perfiles de red se describen en la sección Ajustes de red. Hacer clic en el campo tipo de red le permite cambiar la configuración.

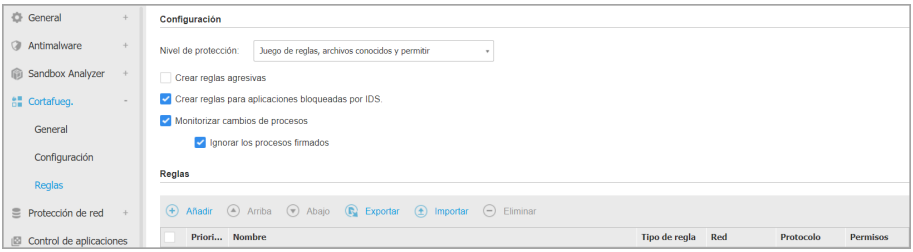
  Si selecciona **Dejar que decida Windows**, para cualquier nueva conexión de red detectada una vez aplicada la política, el agente de seguridad de Bitdefender aplica un perfil de cortafuego basado en la clasificación de la red en Windows, ignorando los ajustes de la tabla **Adaptadores**.

  Si la detección basada en Windows Network Manager falla, se intenta una detección básica. Se utiliza un perfil genérico cuando el perfil de red se considera **Público** y los ajustes de ocultación se configuran como **Activos**.

  Cuando el endpoint unido a Active Directory se conecta al dominio, el perfil del cortafuego se configura automáticamente en **Hogar/Oficina** y los ajustes de invisibilidad se establecen en **Remoto**. Si los equipos no están en un dominio, esta condición no es aplicable.
- **Descubrimiento de red.** Oculta el equipo ante software malintencionado y hackers en la red o en Internet. Configure la visibilidad del equipo en la red según sea necesario, para cada tipo de adaptador, seleccionando una de las siguientes opciones:
  - **Sí.** Cualquier usuario de la red local o Internet puede hacer ping y detectar el equipo.
  - **No.** El equipo no es visible ni en la red local ni en Internet.
  - **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 **Home/Office** y **Público**.



Políticas de equipos y máquinas virtuales - 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 está permitido.

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 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 endpoints. 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** de la zona superior de la tabla. Consulte el siguiente tema para obtener más información.

Para eliminar una regla, selecciónela y haga clic en el botón ⊖ **Eliminar** de la zona superior 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** de la zona superior de la tabla, y seleccione el tipo de regla deseado en 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.

Reglas de importación y exportación

Puede exportar e importar reglas de cortafuego para usarlas en otras políticas o empresas. Para exportar reglas:

1. Haga clic en **Exportar** en la zona superior de la tabla de reglas.

2. Guarde el archivo CSV en su equipo. Dependiendo de la configuración de su navegador, puede que el archivo se descargue de forma automática, o que se le pida que lo guarde en alguna ubicación.

Importante

- Cada fila del archivo CSV corresponde a una sola regla y tiene varios campos.
- La posición de las reglas de cortafuego en el archivo CSV determina su prioridad. Puede cambiar la prioridad de una regla moviendo toda la fila.

Para el conjunto de reglas por defecto, puede modificar solo los siguientes elementos:

- **Prioridad**: Establezca la prioridad de la regla en el orden que desee moviendo la fila del CSV.
- **Permiso**: Modifique el campo `set.Permission` utilizando los permisos disponibles:
  - 1 para **Permitir**
  - 2 para **Denegar**

Cualquier otro ajuste se descarta en la importación.

Para las reglas de cortafuego personalizadas, todos los valores de campos son configurables de la siguiente manera:

Campo	Nombre y valor
`ruleType`	**Tipo de regla**: 1 para la **Regla de aplicación** 2 para la **Regla de conexión**
`tipo`	El valor de este campo es opcional.
`details.name`	**Nombre de la regla**
`details.applictionPath`	**Ruta de aplicación** (sólo para reglas basadas en aplicaciones)
`details.commandLine`	**Línea de comando** (sólo para reglas basadas en aplicaciones)

Campo	Nombre y valor
`details.applicationMd5`	**Application MD5** (sólo para reglas basadas en aplicaciones)
`settings.protocol`	**Protocolo** 1 para **Cualquiera** 2 para **TCP** 3 para **UDP** 4 para **Otro**
`settings.customProtocol`	Solo se requiere si el **Protocolo** se establece en **Otro**. Para valores específicos, consulte esta página. No se admiten los valores 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143.
`settings.direction`	**Dirección**: 1 para **Ambos** 2 para **Entrante** 3 para **Saliente**
`settings.ipVersion`	**Versión de IP**: 1 para **Cualquiera** 2 para **IPv4** 3 para **IPv6**
`settings.localAddress.any`	La **Dirección local** se establece en **Cualquiera**: 1 para verdadero 0 o vacío para falso
`settings.localAddress.ipMask`	La **Dirección local** se establece en **IP o IP/máscara**

Campo	Nombre y valor
`settings.remoteAddress.portRange`	La **Dirección remota** se establece en **Puerto o rango de puertos**
`settings.directlyConnected.enable`	**Aplicar regla sólo a los equipos conectados directamente**: 1 para habilitado 0 o vacío para inhabilitado
`settings.directlyConnected.remoteMac`	**Aplicar regla solo a los equipos conectados directamente** con filtro de **dirección MAC**.
`permission.home`	La **Red** a la que se aplica la regla es **Hogar/Oficina**: 1 para verdadero 0 o vacío para falso
`permiso.public`	La **Red** a la que se aplica la regla es **Pública**: 1 para verdadero 0 o vacío para falso
`permission.setPermission`	Permisos disponibles: 1 para **Permitir** 2 para **Denegar**

Para importar reglas:

1. Haga clic en **Importar** en la zona superior de la tabla Reglas.
2. En la nueva ventana, haga clic en **Añadir** y seleccione el archivo CSV.
3. Haga clic en **Guardar**. La tabla se rellena con las reglas válidas.

7.2.6. Protección de red

Use la sección Protección de red para configurar sus preferencias con respecto al filtrado de contenidos, a la protección de datos sobre la actividad del usuario, incluida la navegación por Internet, el correo electrónico y las aplicaciones de

software, y a la detección de técnicas de ataque de red que intentan acceder a endpoints concretos. 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.

Tenga en cuenta que los ajustes de la Protección de red se aplican a todos los usuarios que inician sesión en los equipos objetivo.

Los ajustes se organizan en las siguientes categorías:

- General
- Control de Contenido
- Protección Web
- Ataques de red

Nota

- El módulo de Control de contenido está disponible para:
  - Windows para estaciones de trabajo
  - macOS
- El módulo Network Attack Defense está disponible para:
  - Windows para estaciones de trabajo

Importante

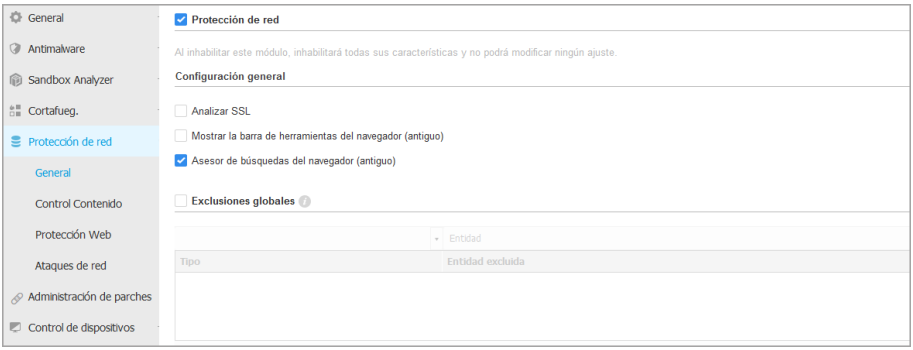
Para macOS, el Control de contenido depende de una extensión del kernel. La instalación de extensiones del kernel requiere su aprobación en macOS High Sierra (10.13) y posteriores. El sistema notifica al usuario que se ha bloqueado una extensión del sistema de Bitdefender. El usuario puede permitirla desde las preferencias de **Seguridad y privacidad**. Este módulo no funcionará mientras el usuario no apruebe la extensión del sistema de Bitdefender, y la interfaz de usuario de Endpoint Security for Mac mostrará un problema crítico que solicitará su aprobación.
Para eliminar la intervención del usuario, puede aprobar previamente la extensión del kernel de Bitdefender incluyéndola en una lista blanca mediante una herramienta de administración de dispositivos móviles. Para obtener más información sobre las extensiones del kernel de Bitdefender, consulte este artículo de la base de conocimientos.

General

En esta página, puede configurar opciones como habilitar o inhabilitar funcionalidades y configurar exclusiones.

Los ajustes se organizan en las siguientes categorías:

- Configuración general
- Exclusiones globales



Políticas de máquinas virtuales y equipos - Protección de la red - General

Configuración general

- **Analizar SSL**. Seleccione esta opción si desea que los módulos de protección del agente de seguridad de Bitdefender inspeccionen el tráfico Web de capa de conexión segura (SSL).
- **Mostrar la barra de herramientas del navegador (antiguo)**. 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.

  Nota
  – Esta opción no está disponible para macOS.

- Esta opción se elimina de Windows a partir de las nuevas instalaciones de Bitdefender Endpoint Security Tools versión 6.6.5.82.

- **Asesor de búsquedas del navegador (antiguo).** 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.

  Nota
  - Esta opción no está disponible para macOS.
  - Esta opción se elimina de Windows a partir de las nuevas instalaciones de Bitdefender Endpoint Security Tools versión 6.6.5.82.

Exclusiones globales

Puede escoger omitir el análisis en busca de malware para determinado tráfico mientras las opciones de **Protección de red** permanecen habilitadas.

Nota
Estas exclusiones se aplican al **Análisis de tráfico** y **Antiphishing**, en la sección **Protección web**, y a **Network Attack Defense**, en la sección **Ataques de red**. Las exclusiones de **Protección de datos** se pueden configurar por separado, en la sección **Control de contenido**.

Para definir un exclusión:

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/Máscara**. Introduzca la dirección IP o la máscara de IP para la que no desee analizar ni el tráfico entrante ni el saliente, lo que incluye técnicas de ataques de red.

- **URL**. Excluye del análisis la dirección Web especificada. Tenga en cuenta que las exclusiones de análisis según las URL se aplican de manera diferente a las conexiones HTTP y a las HTTPS, tal como se explica a continuación.

  Puede definir una exclusión de análisis según la URL de la siguiente manera:

  – Introduzca una URL determinada, como por ejemplo `www.ejemplo.com/ejemplo.html`

    - En el caso de las conexiones HTTP, solo se excluye del análisis esa URL concreta.
    - Para las conexiones HTTPS, al añadir una URL determinada se excluye todo el dominio y sus subdominios. Por lo tanto, en este caso, puede especificar directamente el dominio que se excluirá del análisis.

  – Use caracteres comodín para definir patrones de dirección web (solo para conexiones HTTP).

  > **Importante**
  > Las excepciones con caracteres comodín no funcionan con conexiones HTTPS.

  Puede utilizar los siguientes carácteres comodín:

  - 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 ver distintos ejemplos de sintaxis para especificar direcciones web (URL).

Sintaxis:	Aplicación de excepciones
`www.ejemplo*`	Cualquier URL 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`.

Sintaxis:	Aplicación de excepciones
`*ejemplo.com`	Cualquier URL que acabe en `ejemplo.com`, incluyendo sus subdominios.
`*ejemplo.com*`	Cualquier URL que contenga la cadena especificada.
`*.com`	Cualquier sitio web con la extensión de dominio `.com`, incluyendo sus subdominios. Utilice esta sintaxis para excluir del análisis dominios enteros de nivel superior.
`www.ejemplo?.com`	Cualquier dirección web que comience por `www.ejemplo?.com`, donde `?` puede reemplazarse por cualquier carácter. Estos sitios Web podrían incluir: `www.ejemplo1.com` o `www.ejemploA.com`.

Nota
Puede usar URL relativas de protocolo.

- **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".

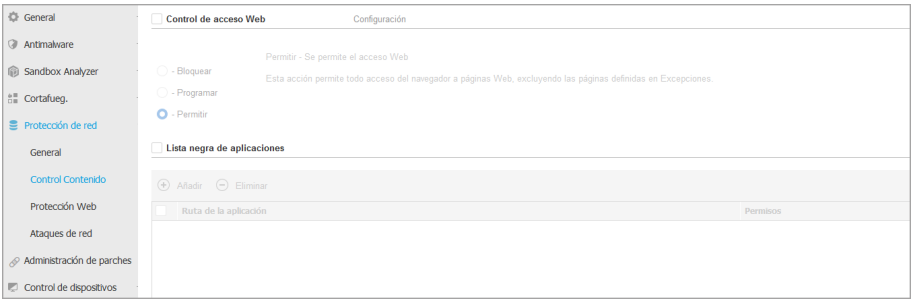
3. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla.

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

Control de Contenido

Los ajustes del Control de contenido se organizan en las siguientes secciones:

- Control de acceso Web
- Lista negra de aplicaciones
- Protección de datos



Control de acceso Web

El Control de acceso Web le ayuda a permitir o bloquear el acceso Web a usuarios o aplicaciones durante intervalos de tiempo específicos.

Las páginas Web bloqueadas por el Control de acceso no se muestran en el navegador. En su lugar, se muestra una página Web predeterminada informando al usuario de que el Control de acceso Web ha bloqueado la página Web solicitada.

Use el conmutador para activar o desactivar el **Control de acceso 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
El agente de seguridad de Bitdefender realizará actualizaciones cada hora, ya esté bloqueado el acceso Web o no.

Categorías

El Filtro de categorías Web filtra dinámicamente el acceso a sitios Web basándose en su contenido. Puede utilizar el filtro de categorías Web para definir excepciones a la acción de control de acceso 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. Active el **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 desplegando la sección **Reglas Web** situada debajo.
3. Si no le satisfacen los ajustes predeterminados, puede definir un filtro personalizado:
   a. Seleccione **Personalizado**.
   b. Haga clic en **Reglas Web** para desplegar la sección correspondiente.

c. Busque en la lista la categoría que quiera y escoja la acción deseada en el menú. Para obtener más información sobre las categorías disponibles de sitios web, consulte este artículo de la base de conocimientos.

4. También puede seleccionar la opción **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. El mensaje por defecto que se muestra al usuario que accede a los sitios web restringidos indica también la categoría a la que pertenece el contenido del sitio web. Desmarque la opción **Mostrar alertas detalladas en el cliente** si desea ocultar esta información al usuario.

   Nota
   Esta opción no está disponible para macOS.

6. 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 de acceso Web.
- **Permitir** permisos funciona solo cuando el acceso Web está bloqueado por el Control de acceso Web, mientras que **Bloquear** permisos funciona solo cuando el Control de acceso Web permite el acceso 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 de acceso Web existentes. Así, por ejemplo, los usuarios podrán acceder a páginas Web específicas incluso cuando la navegación Web esté bloqueada por el Control de acceso Web.

Para crear una regla Web:

1. Active la opción de **Usar excepciones**.
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, haga clic en el botón ⊗ **Eliminar** correspondiente.

Lista negra de aplicaciones

En esta sección puede configurar la Lista negra de aplicaciones, que le ayuda a bloquear por completo o restringir el acceso de los usuarios a las aplicaciones en 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.

Para configurar la Lista negra de aplicaciones:

1. Active la opción **Lista negra de aplicaciones**.
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** en la parte superior 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 del sistema (donde sea preciso) 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, selecciónela y haga clic en el botón ⊗ **Eliminar** de la zona superior de la tabla. Para modificar una regla existente, haga clic en ella para abrir su ventana de configuración.

Protección de datos

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

Nota
Esta característica no está disponible para macOS.

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.

Bitdefender Endpoint Security Tools analiza la Web y el tráfico de correo saliente 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. Al usuario se le informa inmediatamente de la acción tomada por Bitdefender Endpoint Security Tools a través de una página Web de alerta o de un mensaje de correo electrónico.

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** en la parte superior 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. Seleccione el tipo de datos que desee proteger.
   d. 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 cifrados en los endpoints protegidos, pero puede verlos 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**.

   e. Configure las opciones de análisis del tráfico como sea necesario.
      - **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
      - **Analizar SMTP** - analiza el tráfico SMTP (mail) y bloquea los mensajes salientes que coinciden 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.
   f. 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** en la parte superior 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.

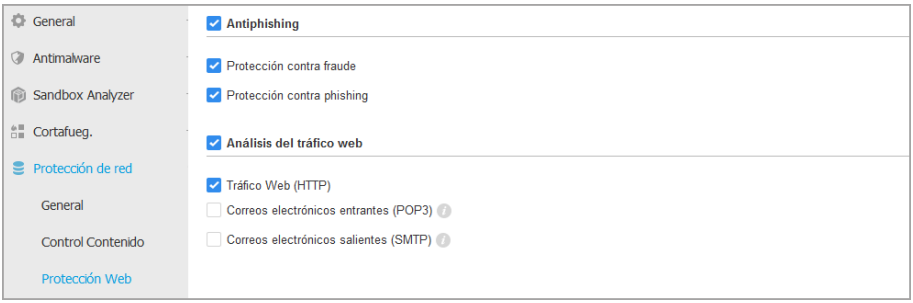
Nota
Si se envía un email que contenga información bloqueada a múltiples receptores, lo recibirán aquellos para los cuales se hayan definido exclusiones.

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

Protección Web

En esta página, los ajustes se organizan en las siguientes secciones:

- Antiphishing
- Análisis del tráfico web



Políticas de máquinas virtuales y equipos - Protección de la red - Protección web

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. Acceda a los ajustes de **General** y haga clic en **Exclusiones globales**.
2. Introduzca la dirección Web y pulse el botón ⊕ **Añadir**.

   Si desea excluir un sitio Web completo, escriba el nombre de dominio, como por ejemplo `http://www.sitioweb.com` y, si desea excluir solamente una página Web, escriba la dirección Web exacta de esa página.

   Nota
   No se aceptan comodines para la definición de URLs.

3. Para eliminar una excepción de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente.
4. Haga clic en **Guardar**.

Análisis del tráfico web

Los mensajes de correo entrante (POP3) y el tráfico Web se analizan en tiempo real para evitar que se descargue malware en el endpoint. Los mensajes de correo saliente (SMTP) se analizan para evitar que el malware infecte otros endpoints.

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.

Nota
Las opciones de **correos entrantes** y **correos salientes** no están disponibles para macOS.

Ataques de red

Network Attack Defense proporciona una capa de seguridad basada en una tecnología de Bitdefender que detecta y adopta medidas contra los ataques de red diseñados para acceder a los endpoints a través de técnicas específicas como ataques de fuerza bruta, exploits de red y ladrones de contraseñas.

Políticas de máquinas virtuales y equipos - Protección de la red - Ataques de red

Para configurar Network Attack Defense:

1. Marque la casilla de verificación **Network Attack Defense** para activar el módulo.
2. Mas las casillas de verificación correspondientes para habilitar la protección contra cada categoría de ataque de red. Las técnicas de ataque de red se agrupan según la base de conocimientos ATT&CK de MITRE de la siguiente manera:
   - **Acceso inicial**: El atacante consigue acceder a una red por diversos medios, que incluyen las vulnerabilidades de los servidores web públicos. Por ejemplo: exploits de divulgación de información, exploits de inyección de código SQL y vectores de inserción por descargas ocultas.
   - **Acceso a credenciales**: El atacante roba credenciales como nombres de usuario y contraseñas para lograr acceder a los sistemas. Por ejemplo: ataques de fuerza bruta, exploits de autenticación no autorizados y ladrones de contraseñas.
   - **Detección**: El atacante, una vez infiltrado, intenta obtener información sobre los sistemas y la red interna antes de decidir qué hacer a continuación. Por ejemplo: exploits de ruta transversal y exploits de ruta transversal HTTP.
   - **Movimiento lateral**: El atacante explora la red, a menudo moviéndose por varios sistemas, para encontrar el objetivo principal. El atacante puede usar herramientas específicas para lograr su objetivo. Por ejemplo: exploits de inserción de comandos, exploits de Shellshock y exploits de doble extensión.
   - **Crimeware**: Esta categoría comprende técnicas diseñadas para automatizar los delitos informáticos. Las técnicas de crimeware son, por ejemplo, exploits nucleares y varios programas de malware como troyanos y bots.
3. Seleccione las acciones que desea llevar a cabo contra cada categoría de técnicas de ataque de red entre las siguientes opciones:
   a. **Bloquear**: Network Attack Defense detiene el intento de ataque una vez detectado.
   b. **Solo informar**: Network Attack Defense le informará sobre el intento de ataque detectado, pero no intentará detenerlo.

Puede restaurar fácilmente los ajustes iniciales haciendo clic en el botón **Restablecer la configuración por defecto** en la parte inferior de la página.

Los detalles sobre los intentos de ataque de red están disponibles en el informe de incidentes de red y en la notificación de eventos de incidentes de red.

7.2.7. Administración de parches

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores

El módulo de Administración de parches le libera de la carga de mantener los endpoints actualizados con los últimos parches de software, distribuyendo e instalando automáticamente parches para una amplia variedad de productos.

Nota
Puede consultar la lista de proveedores y productos compatibles en este artículo de la base de conocimientos.

Esta sección de la política contiene los ajustes para la implementación automática de parches. Primero, configurará cómo se descargan los parches en los endpoints y, luego, qué parches instalar y cuándo hacerlo.

Configuración de los ajustes de descarga de parches

El proceso de difusión de parches utiliza servidores de almacenamiento en caché de parches para optimizar el tráfico de la red. Los endpoints se conectan a estos servidores y descargan los parches por la red local. Para una gran disponibilidad de los parches, se recomienda usar más de un servidor.

Para asignar servidores de almacenamiento en caché de parches a los endpoints objetivo:

1. En la sección **Ajustes de descarga de parches**, haga clic en el campo de la zona superior de la tabla. Se mostrará la lista de servidores de almacenamiento en caché de parches detectados.

   Si la lista está vacía, necesitará instalar el rol de servidor de almacenamiento en caché de parches en los relays de su red. Para más información, consulte la Guía de instalación.
2. Seleccione el servidor que desee de la lista.
3. Haga clic en el botón ⊕ **Añadir**.
4. Repita los pasos anteriores para añadir más servidores en caso necesario.

5. Use las flechas arriba y abajo del lado derecho de la tabla para establecer la prioridad del servidor. La prioridad disminuye de arriba abajo de la lista.

   Un endpoint solicita un parche de los servidores asignados por orden de prioridad. El endpoint descarga el parche del servidor donde antes lo encuentra. Un servidor que carezca de un parche solicitado lo descargará automáticamente del proveedor, para que esté disponible para futuras solicitudes.

Para eliminar servidores que ya no necesite, haga clic en el botón ⊖ Eliminar correspondiente del lateral derecho de la tabla.

Seleccione la opción **Utilizar sitios web de proveedores como ubicación de reserva para descargar parches** para asegurarse de que sus endpoints reciban los parches de software en caso de que los servidores de almacenamiento en caché de parches no estén disponibles.

Configuración del análisis y la instalación de parches

GravityZone realiza la implementación de parches en dos fases independientes:

1. Análisis. Cuando se solicita a través de la consola de administración, los endpoints analizan los parches que faltan e informan de ello.
2. Instalación. La consola envía a los agentes una lista de los parches que desea instalar. El endpoint descarga los parches desde el servidor de almacenamiento en caché de parches y los instala.

La política proporciona los ajustes para automatizar estos procesos, parcial o totalmente, de modo que se ejecuten periódicamente según la programación que se prefiera.

Para configurar el análisis automático de parches:

1. Marque la casilla de verificación **Análisis automático de parches**.
2. Utilice las opciones de programación para configurar la recurrencia de análisis. Puede configurar el análisis para que se ejecute, diariamente o en ciertos días de la semana, en un momento determinado.
3. Seleccione **Análisis inteligente cuando se instala una nueva aplicación o programa** para detectar cuándo se ha instalado una nueva aplicación en el endpoint y qué parches hay disponibles para ella.

Para configurar la instalación automática de parches:

1. Marque la casilla de verificación **Instalar parches automáticamente después del análisis**.
2. Seleccione qué tipos de parches desea instalar: de seguridad, ajenos a ella o ambos.
3. Utilice las opciones de programación para configurar cuándo ejecutar las tareas de instalación. Puede configurar el análisis para que se ejecute inmediatamente después de que finalice el análisis de parches, diariamente o en ciertos días de la semana, en un momento determinado. Recomendamos instalar los parches de seguridad en cuanto se tenga conocimiento de su existencia.
4. Por defecto, se pueden aplicar parches en todos los productos. Si desea actualizar automáticamente solo un conjunto de productos que considere esenciales para su negocio, siga estos pasos:
   a. Marque la casilla de verificación **Producto y proveedor específicos**.
   b. Haga clic en el campo **Proveedor** de la zona superior de la tabla. Se mostrará una lista con todos los proveedores admitidos.
   c. Desplácese por la lista y seleccione un proveedor para los productos que desee parchear.
   d. Haga clic en el campo **Productos** de la zona superior de la tabla. Se mostrará una lista con todos los productos del proveedor seleccionado.
   e. Seleccione todos los productos que desea parchear.
   f. Haga clic en el botón ⊕ **Añadir**.
   g. Repita los pasos anteriores para los proveedores y productos restantes.

      Si ha olvidado añadir un producto o si desea eliminar alguno, busque el proveedor en la tabla, haga doble clic en el campo **Productos** y seleccione o anule la selección del producto en la lista.

   Para eliminar un proveedor con todos sus productos, encuéntrelo en la tabla y haga clic en el botón ⊖ **Eliminar** del lateral derecho de la tabla.
5. Por diversas razones, un endpoint podría estar desconectado cuando esté programada la ejecución de la instalación del parche. Seleccione la opción **Si no se ejecuta, hacerlo lo antes posible** para instalar los parches inmediatamente después de que el endpoint vuelva a estar conectado.

6. Algunos parches pueden requerir el reinicio del sistema para finalizar su instalación. Si desea hacer esto manualmente, seleccione la opción **Posponer reinicio**.

Importante
Para que el análisis y la instalación tengan éxito en los endpoints de Windows, debe asegurarse de que se cumplan los siguientes requisitos:

- Las **entidades de certificación raíz de confianza** almacenan el certificado **DigiCert Assured ID Root CA**.
- Las **entidades de certificación intermedias** incluyen **DigiCert SHA2 Assured ID Code Signing CA**.
- Los endpoints han instalado los parches para Windows 7 y Windows Server 2008 R2 mencionados en este artículo de Microsoft: Aviso de seguridad de Microsoft 3033929

7.2.8. Control de aplicaciones

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores

El módulo de Control de aplicaciones añade una capa más de protección contra todo tipo de amenazas de malware (ransomware, ataques de día cero, exploits en aplicaciones de terceros, troyanos, spyware, rootkits, adware, etc.) al bloquear la ejecución de aplicaciones y procesos no autorizados. El Control de aplicaciones reduce la superficie de ataque que pueden aprovechar las amenazas de malware en el endpoint y evita la instalación y ejecución de aplicaciones no deseadas, poco fiables o maliciosas.

El Control de aplicaciones pone en práctica políticas flexibles que le permiten establecer una lista blanca de aplicaciones y gestionar los permisos de actualización.

Control de aplicaciones

Importante

- Para activar el **Control de aplicaciones** para sus clientes instalados actualmente, ejecute la tarea **Reconfigurar el cliente**. Después de instalar el módulo, puede ver su estado en la ventana **Información**.
- El Control de aplicaciones afecta en gran medida al modo de Usuario avanzado tras la actualización de aplicaciones. Por ejemplo, cuando se actualiza una aplicación de la lista blanca, el endpoint envía la nueva información. GravityZone actualiza la regla con los nuevos valores y vuelve a enviar la política.

Debe ejecutar la tarea de **Detección de aplicaciones** para ver las aplicaciones y procesos que se ejecutan en su red. Para más información, diríjase a "Detección de aplicaciones" (p. 101). A continuación, puede definir las reglas del Control de aplicaciones.

El Control de aplicaciones se ejecuta en dos modos:

- **Modo de prueba**. El Control de aplicaciones solo detecta e informa de las aplicaciones en Control Center, pero permite su ejecución. Puede configurar y probar sus políticas y reglas de lista blanca sin que se bloqueen las aplicaciones.
- **Modo de producción**. El Control de aplicación bloquea todas las aplicaciones desconocidas. Los procesos del sistema operativo de Microsoft y de Bitdefender están por defecto en la lista blanca. Se permitirá la ejecución de las aplicaciones definidas en la lista blanca. Para actualizar las aplicaciones de la lista blanca, debe definir actualizadores. Se trata de procesos específicos que tienen permiso para cambiar las aplicaciones existentes. Para más información, diríjase a "Inventario de aplicaciones" (p. 196).

Aviso

- Para asegurarse de que las aplicaciones legítimas no se vean restringidas por el Control de aplicaciones, debe empezar por ejecutar el Control de aplicaciones en

modo de prueba. De esta manera, puede asegurarse de que las políticas y reglas de lista blanca se han definido correctamente.

- Los procesos que ya estén ejecutándose cuando el Control de aplicaciones pasa al **modo de producción** se bloquearán tras el siguiente reinicio del proceso.

Para administrar los permisos de ejecución de las aplicaciones:

1. Marque la casilla de verificación **Control de aplicaciones** para activar este módulo.
2. Utilice la casilla de verificación **Ejecutar en modo de prueba** para activar o desactivar el modo de prueba.

   Nota

   - En el modo de prueba, se le notificará si el Control de aplicaciones habría bloqueado una aplicación determinada. Para más información, diríjase a "Tipo de notificaciones" (p. 496).
   - Las notificaciones de **Aplicación bloqueada** se mostrarán en el área de notificación cuando se detecten nuevas aplicaciones y cuando se bloqueen las aplicaciones de la lista negra.

3. Defina reglas de inicio de procesos.

Reglas de inicio de procesos

El Control de aplicaciones le permite autorizar manualmente aplicaciones y procesos concretos, según el hash del ejecutable, la huella digital del certificado, y la ruta de la aplicación. También pueden definir exclusiones de la regla.

Nota
Para obtener los valores personalizados del hash del ejecutable y la huella digital del certificado utilice"Herramientas del Control de aplicaciones" (p. 530)

La tabla de **Reglas de inicio de procesos** le informa de las reglas existentes y le proporciona información importante:

- Prioridad de reglas. La regla con mayor prioridad es la más próxima al principio de la lista.
- Nombre de la regla y estado.

- Aplicaciones objetivo y su autorización para ejecutarse. El objetivo representa el número de condiciones que se deben cumplir para que se aplique la regla, o el número de aplicaciones o grupos a los que se aplica esta.

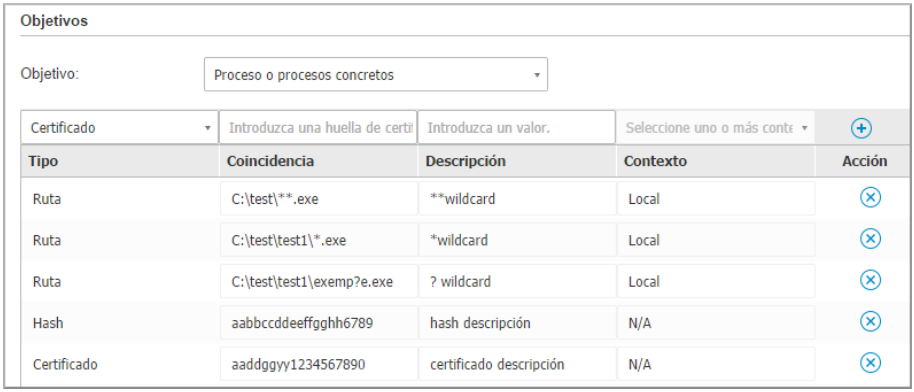
Para crear una regla de inicio de procesos:

1. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para abrir la ventana de configuración.
2. En la sección **General**, introduzca el **Nombre de la regla**.
3. Seleccione la casilla de verificación **Activada** para activar la regla.
4. En la sección **Objetivos**, indique el destino de la regla:
   - **Proceso o procesos concretos**, para definir un proceso cuyo inicio se permite o deniega. Puede autorizar por ruta, hash o certificado. Las condiciones dentro de la regla se verifican mediante AND lógico.
     - Para autorizar una aplicación de una ruta determinada:
       a. Seleccione **Ruta** en la columna **Tipo**. Especifique la ruta de acceso al objeto. Puede proporcionar una ruta absoluta o relativa y utilizar caracteres comodín. El símbolo asterisco (*) se aplica a cualquier archivo dentro de un directorio. Un asterisco doble (**) se aplica a todos los archivos y directorios en el directorio indicado. Un signo de interrogación (?) sustituye a un solo carácter. También puede añadir una descripción que ayude a identificar el proceso.
       b. En el menú desplegable **Seleccione uno o más contextos** puede elegir entre local, CD-ROM, extraíble y red. Puede bloquear una aplicación ejecutada desde un dispositivo extraíble, o permitirla si la aplicación se ejecuta localmente.
     - Para autorizar una aplicación en función del hash, seleccione **Hash** en la columna **Tipo** e introduzca un valor hash. También puede añadir una descripción que ayude a identificar el proceso.

       Importante
       Para generar el valor hash, descargue la herramienta Fingerprint. Para más información, diríjase a "Herramientas del Control de aplicaciones" (p. 530)

– Para autorizar en función de un certificado, seleccione **Certificado** en la columna **Tipo** e introduzca una huella digital de certificado. También puede añadir una descripción que ayude a identificar el proceso.

> **Importante**
> Para obtener la huella digital del certificado, descargue la herramienta Thumbprint. Para más información, diríjase a "Herramientas del Control de aplicaciones" (p. 530)



Reglas de aplicación

Haga clic en ⊕ **Añadir** para añadir la regla.

- **Grupos o aplicaciones del inventario**, para añadir un grupo o una aplicación detectada en su red. Puede ver las aplicaciones que se ejecutan en su red en la página **Red > Inventario de aplicaciones**. Para más información, diríjase a "Inventario de aplicaciones" (p. 196).

  Inserte en el campo los nombres de los grupos o aplicaciones, separados por una coma. La función de autorrellenar muestra sugerencias a medida que escribe.

5. Seleccione la casilla de verificación **Incluir subprocesos** para aplicar la regla a los procesos secundarios generados.

> **Aviso**
> Al establecer reglas para las aplicaciones de navegador, se recomienda desactivar esta opción para evitar riesgos de seguridad.

6. Opcionalmente, también puede definir exclusiones de la regla de inicio de procesos. La operación de añadir es similar a la descrita en los pasos anteriores.
7. En la sección de **Permisos**, elija si desea permitir o denegar la ejecución de la regla.
8. Haga clic en **Guardar** para aplicar los cambios.

Para modificar una regla existente:

1. Haga clic en el nombre de la regla para abrir la ventana de configuración.
2. Introduzca los nuevos valores para las opciones que desee modificar.
3. Haga clic en **Guardar** para aplicar los cambios.

Para establecer la prioridad de la regla:

1. Marque la casilla de verificación de la regla deseada.
2. Use los botones de prioridad del lateral derecho de la tabla:
   - Haga clic en el botón **Arriba** para promocionar la regla seleccionada.
   - Haga clic en el botón **Abajo** para degradarla.

Puede eliminar una o varias reglas a la vez. Lo que tiene que hacer es:

1. Seleccione las reglas que desee eliminar.
2. Haga clic en el botón **Eliminar** de la parte superior de la tabla. Una vez que se elimina una regla, no puede recuperarla.

7.2.9. Control de dispositivos

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- macOS

El módulo de control de dispositivos permite evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo y exclusiones a una amplia gama de tipos de dispositivos.

Importante
Para macOS, el Control de dispositivos depende de una extensión del kernel. La instalación de extensiones del kernel requiere la aprobación del usuario en macOS High Sierra (10.13) y posteriores. El sistema notifica al usuario que se ha bloqueado una extensión del sistema de Bitdefender. El usuario puede permitirla desde las preferencias de **Seguridad y privacidad**. Este módulo no funcionará mientras el usuario no apruebe la extensión del sistema de Bitdefender, y la interfaz de usuario de Endpoint Security for Mac mostrará un problema crítico que solicitará su aprobación.
Para eliminar la intervención del usuario, puede aprobar previamente la extensión del kernel de Bitdefender incluyéndola en una lista blanca mediante una herramienta de administración de dispositivos móviles. Para obtener más información sobre las extensiones del kernel de Bitdefender, consulte este artículo de la base de conocimientos.

Para utilizar el módulo de control de dispositivos, en primer lugar es necesario incluirlo en el agente de seguridad instalado en los endpoints objetivo y, a continuación, activar la opción **Control de dispositivos** en la política aplicada a estos endpoints. Después de esto, cada vez que se conecte un dispositivo a un endpoint administrado, el agente de seguridad enviará información sobre este evento a Control Center, incluyendo el nombre del dispositivo, su clase, el ID, y la fecha y hora de conexión.

En la siguiente tabla, puede encontrar los tipos de dispositivos compatibles con el Control de dispositivos en sistemas Windows y macOS:

Tipo de dispositivo	Windows	macOS
Adaptadores de Bluetooth	x	x
Dispositivos CD-ROM	x	x
Unidades de disquete	x	N/A
IEEE 1284.4	x	
IEEE 1394	x	
Dispositivos de imágenes	x	x
Modems	x	Administrado bajo Adaptadores de red
Unidades de cinta	x	N/A
Windows Portable	x	x
Puertos COM/LPT	x	Compatible LPT a puertos serie

Tipo de dispositivo	Windows	macOS
Raid SCSI	x	
Impresoras	x	Admite solo impresoras conectadas localmente
Adaptadores de red	x	x (incluyendo llaves Wi-Fi)
Adaptadores de red inalámbrica	x	x
Almacenamiento interno	x	
Almacenamiento externo	x	x

Nota

- En macOS, si se selecciona el permiso **Personalizado** para una clase concreta de dispositivo, solo se aplicará el permiso configurado a la subcategoría **Otras**.
- En Windows y macOS, el Control de dispositivos permite o deniega el acceso a todo el adaptador Bluetooth al nivel del sistema, en función de la política. No existe la posibilidad de establecer exclusiones granulares por dispositivo emparejados.

El Control de dispositivos permite administrar permisos de dispositivos de la siguiente manera:

- Definir reglas de permisos
- Definir exclusiones de permisos

Reglas

La sección **Reglas** permite definir los permisos para los dispositivos conectados a los endpoints objetivo.

Para establecer los permisos para el tipo de dispositivo que desee:

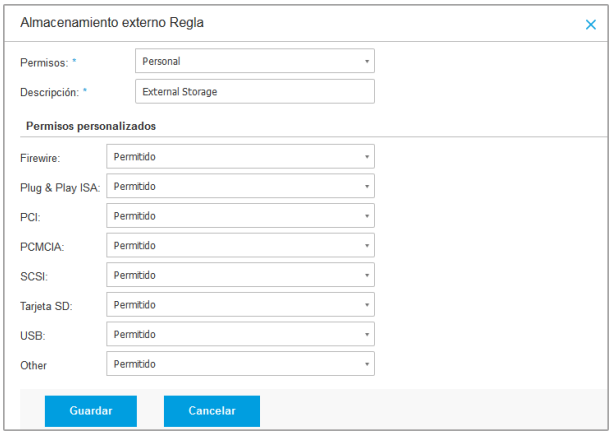
1. Acceda a **Control de dispositivos > Reglas**.
2. Haga clic en el nombre del dispositivo en la tabla correspondiente.
3. Seleccione un tipo de permiso entre las opciones disponibles. Tenga en cuenta que el conjunto de permisos a su disposición puede variar en función del tipo de dispositivo:
   - **Permitido**: el dispositivo se puede utilizar en el endpoint objetivo.
   - **Bloqueado**: el dispositivo no se puede utilizar en el endpoint objetivo. En este caso, cada vez que se conecte el dispositivo al endpoint, el agente de

seguridad presentará una notificación informándole de que el dispositivo ha sido bloqueado.

> **Importante**
> Los dispositivos conectados bloqueados previamente no se desbloquean automáticamente al cambiar el permiso a **Permitido**. El usuario debe reiniciar el sistema o volver a conectar el dispositivo para poder usarlo.

- **De solo lectura**: solo se podrán usar las funciones de lectura del dispositivo.
- **Personalizado**: defina permisos diferentes para cada tipo de puerto del mismo dispositivo, como por ejemplo Firewire, ISA Plug & Play, PCI, PCMCIA, USB, etc. En este caso, se muestra la lista de componentes disponibles para el dispositivo seleccionado, y puede establecer los permisos que desee para cada componente.

  Por ejemplo, para Almacenamiento externo, puede bloquear solamente USB y permitir que se utilicen todos los demás puertos.



Políticas de equipos y máquinas virtuales - Control de dispositivos - Reglas

Exclusiones

Tras establecer las reglas de permisos para diferentes tipos de dispositivos, puede que desee excluir ciertos tipos de productos o dispositivos de estas reglas.

Puede definir exclusiones de dispositivos:

- Por ID de dispositivo (o ID de hardware), para indicar dispositivos individuales que desee excluir.
- Por ID de producto (o PID), para indicar una gama de dispositivos producidos por el mismo fabricante.

Para definir exclusiones de reglas de dispositivos:

1. Acceda a **Control de dispositivos > Exclusiones**.
2. Active la opción de **Exclusiones**.
3. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla.
4. Seleccione el método que quiere utilizar para añadir exclusiones.
   - **Manualmente**. En este caso es necesario introducir cada ID de dispositivo o ID de producto que desee excluir, lo que supone que tenga a mano la lista de ID apropiados:
     a. Seleccione el tipo de exclusión (por ID de producto o ID de dispositivo).
     b. En el campo **Excepciones**, introduzca los ID que desea excluir.
     c. En el campo **descripción**, introduzca un nombre que le ayude a identificar el dispositivo o el conjunto de dispositivos.
     d. Seleccione el tipo de permiso para los dispositivos especificados (**Permitido** o **Bloqueado**).
     e. Haga clic en **Guardar**.

     Nota
     Puede configurar manualmente las exclusiones mediante comodines basadas en el ID del dispositivo con la sintaxis `wildcards: IDdispositivo`. Utilice el signo de interrogación (?) Para reemplazar un carácter y el asterisco (*) para reemplazar cualquier número de caracteres en el `IDdispositivo`. Por ejemplo, con `wildcards:PCI\VEN_8086*`, se excluirán de la regla de política todos los dispositivos que contengan la cadena `PCI\VEN_8086` en su ID.

   - **De dispositivos detectados**. En este caso puede seleccionar los ID de dispositivos o ID de producto que desea excluir de una lista con todos los dispositivos detectados en su red (solo en lo que se refiere a los endpoints administrados):
     a. Seleccione el tipo de exclusión (por ID de producto o ID de dispositivo).
     b. En la tabla **Exclusiones**, seleccione los ID que desea excluir:

- Para los ID de dispositivo, seleccione en la lista cada uno de los dispositivos que desea excluir.
- Para los ID de producto, al seleccionar un dispositivo excluirá todos los dispositivos que tengan el mismo ID de producto.

c. En el campo **descripción**, introduzca un nombre que le ayude a identificar el dispositivo o el conjunto de dispositivos.
d. Seleccione el tipo de permiso para los dispositivos especificados (**Permitido** o **Bloqueado**).
e. Haga clic en **Guardar**.

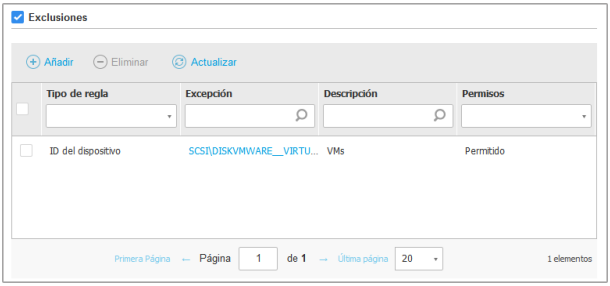
Importante

- Los dispositivos ya conectados a endpoints durante la instalación de Bitdefender Endpoint Security Tools solo se detectarán después de reiniciar los endpoints correspondientes.
- Los dispositivos conectados bloqueados previamente no se desbloquean automáticamente al establecer una excepción con el permiso en **Permitido**. El usuario debe reiniciar el sistema o volver a conectar el dispositivo para poder usarlo.

Todas las exclusiones de dispositivos aparecerán en la tabla **Exclusiones**.

Para eliminar una exclusión:

1. Selecciónela en la tabla.
2. Haga clic en el botón ⊕ **Eliminar** de la parte superior de la tabla.



Políticas de equipos y máquinas virtuales - Control de dispositivos - Exclusiones

7.2.10. Relay

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- Linux

Esta sección le permite definir los ajustes de actualización y comunicación de endpoints objetivo con función de relay.

Los ajustes se organizan en las siguientes categorías:

- Comunicación
- Actualizar

Comunicación

La pestaña **Comunicación** contiene las preferencias de proxy para la comunicación entre los endpoints de relay y los componentes de GravityZone.

De ser necesario, puede configurar de forma independiente la comunicación entre los endpoints de relay objetivo y Bitdefender Cloud Services / GravityZone mediante los siguientes ajustes:

- **Mantener los ajustes de la instalación**, para utilizar los mismos ajustes de proxy definidos en el paquete de instalación.
- **Utilizar el proxy definido en la sección General**, para usar los ajustes de proxy definidos en la política actual, en la sección **General > Ajustes**.
- **No utilizar**, cuando los endpoints objetivo no se comunican con los componentes de Bitdefender a través de proxy.

Actualizar

Esta sección le permite definir los ajustes de actualización de endpoints objetivo con función de relay:

- En la sección **Actualización** puede configurar los siguientes ajustes:
  - El intervalo de tiempo en que los endpoints de relay comprueban si hay actualizaciones.

- La carpeta ubicada en el endpoint de relay donde se descargan y reflejan las actualizaciones de producto y de firmas. Si desea definir una carpeta de descarga determinada, introduzca su ruta completa en el campo correspondiente.

  Importante
  Se recomienda definir una carpeta dedicada para las actualizaciones de producto y de firmas. No debe elegir una carpeta que contenga archivos personales o del sistema.

- **Definir ubicaciones de actualización personalizadas**. La ubicación de actualización por defecto para los agentes de relay es el Servidor de actualizaciones local de GravityZone. Puede especificar otras ubicaciones de actualización introduciendo la IP o el nombre de host local de uno o varios Servidores de actualizaciones en su red y, a continuación, configurar su prioridad mediante los botones arriba y abajo que aparecen al pasar el ratón por encima. Si la primera ubicación de actualización no está disponible, se usa la siguiente y así sucesivamente.

  Para definir una ubicación de actualización personalizada:

  1. Active la opción **Definir ubicaciones de actualización personalizadas**.
  2. Introduzca la dirección del nuevo servidor de actualizaciones en el campo **Añadir ubicación**. Use una de estas sintaxis:
     - `update_ server_ip:port`
     - `update_ server_name:port`

     El puerto predeterminado es 7074.
  3. Si el endpoint de relay se comunica con el servidor local de actualizaciones a través de un servidor proxy, seleccione **Usar proxy**. Se tendrán en cuenta los ajustes de proxy definidos en la sección **General > Ajustes**.
  4. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla.
  5. Utilice las flechas de ⌃ Arriba y ⌄ Abajo de la columna **Acción** para establecer la prioridad de las ubicaciones de actualización definidas. Si la primera ubicación de actualización no está disponible, se comprueba la siguiente y así sucesivamente.

Para eliminar una ubicación de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente. Aunque puede eliminar la dirección de actualización predeterminada, no es recomendable que lo haga.

7.2.11. Protección de Exchange

Nota
Este módulo está disponible para Windows para servidores.

Security for Exchange viene con ajustes altamente configurables, que protegen los servidores de Microsoft Exchange contra amenazas como el malware, el spam y el phishing. Con la Protección de Exchange instalada en su servidor de correo, puede filtrar también mensajes de correo electrónico que contengan adjuntos o contenidos considerados peligrosos según las políticas de seguridad de su empresa.

Para mantener el rendimiento del servidor en los niveles normales, los filtros de Security for Exchange procesan el tráfico de correo electrónico por el siguiente orden:

1. Filtrado antispam
2. Control de contenidos > Filtrado de contenidos
3. Control de contenidos > Filtrado de adjuntos
4. Filtrado antimalware

Los ajustes de Security for Exchange se organizan en las siguientes secciones:

- General
- Antimalware
- Antispam
- Control de Contenido

General

En esta sección puede crear y administrar grupos de cuentas de correo electrónico, definir la antigüedad de los elementos en cuarentena y prohibir a determinados remitentes.

Grupos de usuarios

Control Center permite la creación de grupos de usuarios para aplicar distintas políticas de análisis y filtrado a diferentes categorías de usuarios. Por ejemplo,

puede crear políticas adecuadas para el departamento de TI, para el equipo de ventas o para los directivos de la empresa.

Los grupos de usuarios están disponibles en general, independientemente de la política o del usuario que los creara.

Para facilitar la administración de grupos, el Control Center importa automáticamente los grupos de usuarios de Windows Active Directory.

Para crear un grupo de usuarios:

1. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Se muestra la ventana de información.
2. Introduzca el nombre del grupo, la descripción y las direcciones de correo electrónico de los usuarios.

   Nota
   - En caso de tener una lista de direcciones de correo electrónico muy larga, puede copiar y pegar la lista desde un archivo de texto.
   - Lista de separadores aceptados: espacio, coma, punto y coma, e intro.

3. Haga clic en **Guardar**.

Los grupos personalizados se pueden modificar. Haga clic en el nombre del grupo para abrir la ventana de configuración en la que puede cambiar los detalles del grupo o modificar la lista de usuarios.

Para eliminar un grupo personalizado de la lista, selecciónelo y haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla.

Nota
No puede modificar ni eliminar los grupos de Active Directory.

Configuración

- **Eliminar archivos en cuarentena de más de (días).** Por defecto, los archivos de más de 30 días se eliminan automáticamente. Si desea cambiar este intervalo, escriba un valor diferente en el campo correspondiente.
- **Lista negra de conexión.** Con esta opción activada, Exchange Server rechaza todos los mensajes de correo electrónico de los remitentes presentes en la lista negra.

  Para crear una lista negra:
  1. Haga clic en el enlace **Modificar elementos en la lista negra**.

2. Introduzca las direcciones de correo electrónico que desee bloquear. Al editar la lista, también puede utilizar los siguientes caracteres comodín para definir un dominio de correo electrónico completo o un patrón de direcciones de correo electrónico:
   - Asterisco (*); sustituye a cero, uno o más caracteres.
   - Signo de interrogación (?); sustituye a cualquier carácter individual.

   Por ejemplo, si introduce `*@boohouse.com`, se bloquearán todas las direcciones de correo electrónico de `boohouse.com`.
3. Haga clic en **Guardar**.

Comprobación de IP de dominio (antispoofing)

Utilice este filtro para evitar que los spammers falseen la dirección de correo electrónico del remitente y hagan que el mensaje parezca que lo ha enviado alguien de confianza (spoofing). Puede especificar las direcciones IP autorizadas para enviar correo electrónico desde sus dominios de correo electrónico y, si es necesario, para otros dominios de correo electrónico conocidos. Si un mensaje de correo electrónico parece ser de un dominio incluido en la lista, pero la dirección IP del remitente no corresponde con ninguna de las direcciones IP indicadas, se rechaza el mensaje.

Aviso
No utilice este filtro si está usando un host inteligente, un servicio de filtrado de correo electrónico alojado o una solución de filtrado de correo electrónico de puerta de enlace con sus servidores de Exchange.

Importante

- El filtro solo comprueba las conexiones de correo electrónico no autenticadas.
- Mejores prácticas:
  - Se recomienda utilizar este filtro solo en servidores de Exchange conectados directamente a Internet. Por ejemplo, si tiene servidores de transporte perimetral y de transporte de concentradores, configure este filtro solo en los perimetrales.
  - Añada a su lista de dominios todas las direcciones IP internas a las que se permita enviar correo electrónico a través de conexiones SMTP no autenticadas. Estas pueden incluir sistemas de notificación automática y equipos de red como impresoras, etc.

- En una configuración de Exchange que utilice grupos de disponibilidad de base de datos, añada también a la lista de sus dominios las direcciones IP de todos sus servidores de transporte de concentradores y buzones.
- Tenga cuidado si desea configurar direcciones IP autorizadas para dominios de correo electrónico externos concretos que no administre. Si no puede mantener al día la lista de direcciones IP, se rechazarán los mensajes de correo electrónico de esos dominios. Si utiliza una copia de seguridad de MX, debe añadir a todos los dominios de correo electrónico externos configurados las direcciones IP desde las que la copia de seguridad de MX reenvía mensajes de correo electrónico a su servidor de correo primario.

Para configurar el filtrado antispoofing, siga los pasos descritos en este documento:

1. Marque la casilla de verificación **Comprobación de IP de dominio (antispoofing)** para activar el filtro.
2. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Aparece la ventana de configuración.
3. Introduzca el dominio de correo electrónico en el campo correspondiente.
4. Indique el rango de direcciones IP autorizadas para el dominio especificado anteriormente, utilizando el formato CIDR (IP/máscara de red).
5. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla. Las direcciones IP se añaden a la tabla.
6. Para eliminar un rango de IP de la lista, haga clic en el botón ⊗ **Eliminar** correspondiente del lateral derecho de la tabla.
7. Haga clic en **Guardar**. El dominio se añade al filtro.

Para eliminar un dominio de correo electrónico del filtro, selecciónelo en la tabla de antispoofing y haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla.

Antimalware

El módulo Antimalware protege los servidores de correo de Exchange contra todo tipo de amenazas de malware (virus, troyanos, spyware, rootkits, adware, etc.) tratando de detectar los elementos infectados o sospechosos e intentando desinfectarlos o aislar la infección, según las acciones especificadas.

El análisis antimalware se realiza a dos niveles:

- Nivel de transporte

- Almacén de Exchange

Análisis de nivel de transporte

Bitdefender Endpoint Security Tools se integra con los agentes de transporte de correo para analizar todo el tráfico de correo electrónico.

Por defecto, el análisis de nivel de transporte está activado. Bitdefender Endpoint Security Tools filtra el tráfico de correo electrónico y, de ser necesario, informa a los usuarios de las acciones adoptadas añadiendo un texto al cuerpo del mensaje.

Utilice la casilla de verificación de **Filtrado antimalware** para desactivar o volver a activar esta característica.

Para configurar el texto de la notificación, haga clic en el enlace **Ajustes**. Tiene las siguientes opciones a su disposición:

- **Añadir un pie a los mensajes analizados.** Marque esta casilla de verificación para añadir una frase al pie de los mensajes analizados. Para cambiar el texto predeterminado, introduzca su mensaje en el cuadro de texto que aparece debajo.
- **Texto de sustitución.** Se puede adjuntar un archivo de notificación para los mensajes de correo electrónico cuyos adjuntos hayan sido eliminados o puestos en cuarentena. Para modificar los textos de notificación predeterminados, introduzca su mensaje en los cuadros de texto correspondientes.

El filtrado antimalware se basa en reglas. Los mensajes de correo electrónico que llegan al servidor de correo electrónico se cotejan con las reglas de filtrado antimalware, por orden de prioridad, hasta que cumplan una regla. El mensaje de correo electrónico se procesa entonces según las opciones especificadas por esa regla.

Administración de las reglas de filtrado

Puede ver todas las reglas existentes que figuran en la tabla, junto con información sobre su prioridad, estado y ámbito de aplicación. Las reglas se clasifican por prioridad, teniendo la primera regla la mayor prioridad.

Cualquier política antimalware tiene una regla por defecto que se activa en cuanto se habilita el filtrado antimalware. Lo que necesita saber sobre la regla por defecto:

- No puede copiar, desactivar ni eliminar la regla por defecto.
- Solo se pueden modificar los ajustes del análisis y las acciones.
- La prioridad de la regla por defecto es siempre la menor.

Creando Reglas

Dispone de dos alternativas para la creación de reglas de filtrado:

- Parta de los ajustes por defecto siguiendo estos pasos:
  1. Haga clic en el botón **Añadir** de la parte superior de la tabla para abrir la ventana de configuración.
  2. Configure los ajustes de la regla. Para obtener más información relativa a las opciones, consulte Opciones de reglas.
  3. Haga clic en **Guardar**. La regla aparece en primer lugar en la tabla.
- Utilice un clon de una regla personalizada como plantilla siguiendo estos pasos:
  1. Seleccione la regla que desee de la tabla.
  2. Haga clic en el botón **Clonar** de la parte superior de la tabla.
  3. Ajuste las opciones de la regla según sus necesidades.
  4. Haga clic en **Guardar**. La regla aparece en primer lugar en la tabla.

Modificación de reglas

Para modificar una regla existente:

1. Haga clic en el nombre de la regla para abrir la ventana de configuración.
2. Introduzca los nuevos valores para las opciones que desee modificar.
3. Haga clic en **Guardar**. Los cambios surten efecto tras guardar la política.

Establecimiento de la prioridad de la regla

Para cambiar la prioridad de una regla:

1. Seleccione la regla que desea mover.
2. Utilice los botones **Arriba** o **Abajo** de la parte superior de la tabla para aumentar o disminuir la prioridad de la regla.

Eliminación de reglas

Puede eliminar una o varias reglas personalizadas a la vez. Lo que tiene que hacer es:

1. Marque la casilla de verificación de las reglas que desee eliminar.
2. Haga clic en el botón **Eliminar** de la parte superior de la tabla. Una vez que se elimina una regla, no puede recuperarla.

Opciones de reglas

Tiene las siguientes opciones a su disposición:

- **General.** En esta sección debe establecer un nombre para la regla, pues de lo contrario no podrá guardarla. Marque la casilla de verificación **Activa** si desea que la regla entre en vigor tras guardar la política.

- **Ámbito de aplicación de la regla.** Puede restringir la regla para que se aplique solo a un subconjunto de mensajes de correo electrónico, mediante el establecimiento de las siguientes opciones acumulativas del ámbito de aplicación:
  - **Aplicar a (dirección).** Seleccione la dirección del tráfico de correo electrónico a la que se aplica la regla.
  - **Remitentes.** Puede decidir si la regla se aplica a cualquier remitente o solo a determinados remitentes. Para reducir el rango de remitentes, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Vea los grupos seleccionados en la tabla de la derecha.
  - **Destinatarios.** Puede decidir si la regla se aplica a cualquier destinatario o solo a determinados destinatarios. Para reducir el rango de destinatarios, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Puede ver los grupos seleccionados en la tabla de la derecha.

    La regla se aplica si alguno de los destinatarios coincide con su selección. Si desea aplicar la regla solo en caso de que todos los destinatarios estén en los grupos seleccionados, seleccione **Coincidir todos los destinatarios**.

    Nota
    Las direcciones de los campos **Cc** y **Bcc** también se consideran destinatarios.

    Importante
    Las reglas basadas en los grupos de usuarios se aplican solo a los roles de transporte de concentradores y de buzón.

- **Opciones.** Configure las opciones de análisis para mensajes de correo electrónico que cumplan la regla:
  - **Tipos de archivos analizados.** Utilice esta opción para especificar los tipos de archivo que desee analizar. Puede optar por analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación o extensiones de archivo concretas que considere peligrosas. Analizar todos los archivos aporta la mayor protección, mientras que se recomienda analizar solo las aplicaciones para 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 "Tipos de archivos de aplicación" (p. 527).

Si desea analizar solo los archivos con determinadas extensiones, tiene dos alternativas:

- **Extensiones definidas por el usuario**, donde debe proporcionar solo las extensiones que se analizarán.
- **Todos los archivos, excepto extensiones concretas**, donde debe introducir solo las extensiones que no se analizarán.

– **Tamaño máximo del adjunto/cuerpo del mensaje (MB).** Marque esta casilla de verificación e introduzca un valor en el campo correspondiente para establecer el tamaño máximo aceptado de un archivo adjunto o del cuerpo del mensaje de correo electrónico que se va a analizar.

– **Profundidad de archivo máxima (niveles).** Marque la casilla de verificación y elija la profundidad máxima del archivo comprimido en el campo correspondiente. Cuanto menor sea el nivel de profundidad, mayor será el rendimiento, pero menor el grado de protección.

– **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Marque esta casilla de verificación para buscar aplicaciones maliciosas o potencialmente no deseadas, como por ejemplo adware, que pueden instalarse en los sistemas sin el consentimiento del usuario, cambiar el comportamiento de diversos productos de software y reducir el rendimiento del sistema.

- **Acciones.** Puede especificar diferentes acciones para que el agente de seguridad las aplique automáticamente a los archivos, en función del tipo de detección.

  El tipo de detección divide los archivos en tres categorías:

  – **Archivos infectados.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA).

  – **Archivos sospechosos.** Estos archivos se detectan mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos).

  – **Archivos no analizables.** Estos archivos no se pueden analizar. Los archivos que no se pueden analizar incluyen, pero no se limitan, a los archivos protegidos con contraseña, cifrados o sobrecomprimidos.

  Para cada tipo de detección, dispone de una acción por defecto o principal y de una acción alternativa por si falla la principal. Aunque no es recomendable, puede cambiar estas acciones mediante los menús correspondientes. Elija la acción a adoptar:

- **Desinfectar.** Elimina el código de malware de los archivos infectados y reconstruye el archivo original. Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.
- **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Eliminar archivo.** Elimina los archivos adjuntos problemáticos sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Reemplazar archivo.** Elimina los archivos problemáticos e inserta un archivo de texto que comunica al usuario las acciones adoptadas.
- **Mover archivo a la cuarentena.** Mueve los archivos detectados a la carpeta de cuarentena e inserta un archivo de texto que comunica al usuario las acciones adoptadas. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de la cuarentena desde la página **Cuarentena**.

  Nota
  Tenga en cuenta que la cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad. El tamaño de la cuarentena depende del número de elementos almacenados y de su tamaño.

- **No realizar ninguna acción.** No se realizará ninguna acción sobre los archivos detectados. Estos archivos solo aparecerán en el log de análisis. 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.
- Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

Exclusiones

Si desea que las reglas de filtrado ignoren determinado tráfico de correo electrónico, puede definir exclusiones de análisis. Para crear una exclusión:

1. Expanda la sección **Exclusiones para las reglas antimalware**.
2. Haga clic en el botón ⊖ **Añadir** de la barra de herramientas de esta sección para abrir la ventana de configuración.
3. Configure los ajustes de la exclusión. Para obtener más información sobre las opciones, consulte Opciones de reglas.
4. Haga clic en **Guardar**.

Análisis del almacén de Exchange

La Protección de Exchange utiliza Exchange Web Services (EWS) de Microsoft para permitir analizar el buzón de Exchange y bases de datos de carpetas públicas. Puede configurar el módulo antimalware para ejecutar tareas de análisis bajo demanda periódicamente en las bases de datos objetivo, según la programación que especifique.

Nota

- El análisis bajo demanda está disponible únicamente para servidores de Exchange con el rol de buzón instalado.
- Tenga en cuenta que el análisis bajo demanda aumenta el consumo de recursos y, dependiendo de las opciones y del número de objetos que haya que analizar, puede tardar un tiempo considerable en completarse.

El análisis bajo demanda exige una cuenta de administrador de Exchange (cuenta de servicio) para suplantar a los usuarios de Exchange y recuperar los objetos objetivo que hay que analizar de los buzones de los usuarios y las carpetas públicas. Se recomienda crear una cuenta dedicada a tal fin.

La cuenta de administrador de Exchange debe cumplir los siguientes requisitos:

- Es miembro del grupo de Administración de la organización (Exchange 2016, 2013 y 2010)
- Ser miembro del grupo de Administradores de la organización de Exchange (Exchange 2007).
- Tener un buzón asignado.

Habilitación del análisis bajo demanda

1. En la sección **Tareas de análisis**, haga clic en el enlace **Añadir credenciales**.
2. Introduzca el nombre de usuario y contraseña de la cuenta de servicio.

3. Si el correo electrónico difiere del nombre de usuario, necesitará proporcionar también la dirección de correo electrónico de la cuenta de servicio.
4. Escriba la URL de Exchange Web Services (EWS), necesaria cuando no funciona la detección automática de Exchange.

Nota

- El nombre de usuario debe incluir el nombre de dominio, con el formato `usuario@dominio` o `dominio\usuario`.
- No olvide actualizar las credenciales en Control Center siempre que cambien.

Administración de tareas de análisis

La tabla de tareas de análisis muestra todas las tareas programadas y proporciona información sobre sus objetivos y recurrencia.

Para crear tareas con el fin de analizar el Almacén de Exchange:

1. En la sección **Tareas de análisis**, haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para abrir la ventana de configuración.
2. Configure los ajustes de la tarea según se describe en la siguiente sección.
3. Haga clic en **Guardar**. La tarea se añade a la lista y entra en vigor una vez que se guarda la política.

Puede modificar una tarea en cualquier momento haciendo clic en el nombre de la misma.

Para eliminar tareas de la lista, selecciónelas y haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla.

Ajustes de tareas de análisis

Las tareas tienen una serie de ajustes que se describen a continuación:

- **General.** Escriba un nombre descriptivo para la tarea.

  Nota
  Puede ver el nombre de la tarea en la línea de tiempo de Bitdefender Endpoint Security Tools.

- **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. Con bases de datos grandes, la tarea de análisis puede tardar mucho tiempo y es posible que afecte

al rendimiento del servidor. En tales casos, puede configurar la tarea para que se detenga tras un tiempo determinado.

- **Objetivo.** Seleccione los contenedores y objetos que desea analizar. Puede optar por analizar los buzones, las carpetas públicas o ambos. Además de los correos electrónicos, puede optar por analizar otros objetos como **Contactos**, **Tareas**, **Citas** y **Elementos para exponer**. Además, puede establecer las siguientes restricciones a los contenidos que se analizarán:
  - Solo los mensajes no leídos.
  - Solo los elementos con adjuntos.
  - Solo los elementos nuevos recibidos en un intervalo de tiempo determinado.

  Por ejemplo, puede elegir analizar solo los mensajes de correo electrónico de los buzones de los usuarios recibidos en los últimos siete días.

  Marque la casilla de verificación **Exclusiones** si desea definir excepciones de análisis. Para crear una excepción, utilice los campos del encabezado de la tabla de la siguiente manera:
  1. Seleccione el tipo de repositorio en el menú.
  2. Dependiendo del tipo de repositorio, indique el objeto que haya que excluir:

Tipo de repositorio	Formato de objeto
Buzón de Correo	Dirección de correo:
Carpeta pública	Ruta de la carpeta, a partir de la raíz
Base de Datos	La identidad de la base de datos

     Nota
     Para obtener la identidad de la base de datos, utilice el comando shell de Exchange:
     `Get-MailboxDatabase | fl name,identity`

     Solo puede indicar los elementos uno a uno. Si tiene varios elementos del mismo tipo, debe definir tantas reglas como elementos tenga.
  3. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para guardar la excepción y añadirla a la lista.

  Para eliminar una regla de excepción de la lista, haga clic en el botón ⊖ **Eliminar** correspondiente.
- **Opciones.** Configure las opciones de análisis para mensajes de correo electrónico que cumplan la regla:

- **Tipos de archivos analizados.** Utilice esta opción para especificar los tipos de archivo que desee analizar. Puede optar por analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación o extensiones de archivo concretas que considere peligrosas. Analizar todos los archivos aporta la mayor protección, mientras que se recomienda analizar solo las aplicaciones para 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 "Tipos de archivos de aplicación" (p. 527).

  Si desea analizar solo los archivos con determinadas extensiones, tiene dos alternativas:
  - **Extensiones definidas por el usuario**, donde debe proporcionar solo las extensiones que se analizarán.
  - **Todos los archivos, excepto extensiones concretas**, donde debe introducir solo las extensiones que no se analizarán.
- **Tamaño máximo del adjunto/cuerpo del mensaje (MB).** Marque esta casilla de verificación e introduzca un valor en el campo correspondiente para establecer el tamaño máximo aceptado de un archivo adjunto o del cuerpo del mensaje de correo electrónico que se va a analizar.
- **Profundidad de archivo máxima (niveles).** Marque la casilla de verificación y elija la profundidad máxima del archivo comprimido en el campo correspondiente. Cuanto menor sea el nivel de profundidad, mayor será el rendimiento, pero menor el grado de protección.
- **Analizar en busca de aplicaciones potencialmente no deseadas (APND).** Marque esta casilla de verificación para buscar aplicaciones maliciosas o potencialmente no deseadas, como por ejemplo adware, que pueden instalarse en los sistemas sin el consentimiento del usuario, cambiar el comportamiento de diversos productos de software y reducir el rendimiento del sistema.

- **Acciones.** Puede especificar diferentes acciones para que el agente de seguridad las aplique automáticamente a los archivos, en función del tipo de detección.

  El tipo de detección divide los archivos en tres categorías:
  - **Archivos infectados.** Bitdefender detecta los archivos infectados gracias a diversos mecanismos avanzados, que incluyen firmas de malware, aprendizaje automático y tecnologías basadas en la inteligencia artificial (IA).

- **Archivos sospechosos.** Estos archivos se detectan mediante el análisis heurístico y otras tecnologías de Bitdefender. Estas proporcionan una alta tasa de detección, pero los usuarios han de ser conscientes de la posibilidad de falsos positivos (archivos limpios que se identifican como sospechosos).
- **Archivos no analizables.** Estos archivos no se pueden analizar. Los archivos que no se pueden analizar incluyen, pero no se limitan, a los archivos protegidos con contraseña, cifrados o sobrecomprimidos.

Para cada tipo de detección, dispone de una acción por defecto o principal y de una acción alternativa por si falla la principal. Aunque no es recomendable, puede cambiar estas acciones mediante los menús correspondientes. Elija la acción a adoptar:

- **Desinfectar.** Elimina el código de malware de los archivos infectados y reconstruye el archivo original. Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.
- **Rechazar/Eliminar mensaje de correo electrónico.** El mensaje de correo electrónico se elimina sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Eliminar archivo.** Elimina los archivos adjuntos problemáticos sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
- **Reemplazar archivo.** Elimina los archivos problemáticos e inserta un archivo de texto que comunica al usuario las acciones adoptadas.
- **Mover archivo a la cuarentena.** Mueve los archivos detectados a la carpeta de cuarentena e inserta un archivo de texto que comunica al usuario las acciones adoptadas. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de la cuarentena desde la página **Cuarentena**.

  Nota
  Tenga en cuenta que la cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad. El tamaño de la cuarentena depende del número y del tamaño de los mensajes de correo electrónico almacenados.

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

– Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

Antispam

El módulo Antispam ofrece protección multicapa contra el spam y el phishing mediante una combinación de varios filtros y motores para determinar si los mensajes de correo electrónico son spam o no.

Nota

- El filtrado antispam está disponible para:
  - Exchange Server 2016/2013 con rol de transporte perimetral o de buzón.
  - Exchange Server 2010/2007 con rol de transporte perimetral o de transporte de concentradores.
- Si tiene roles tanto de transporte perimetral como de concentradores en su organización de Exchange, se recomienda activar el filtrado antispam en el servidor con el rol de transporte perimetral.

El filtrado de spam se activa automáticamente para los mensajes de correo electrónico entrantes. Utilice la casilla de verificación de **Filtrado antispam** para desactivar o volver a activar esta característica.

Filtros Antispam

Los mensajes se cotejan con las reglas de filtrado antispam según los grupos de remitentes y destinatarios, por orden de prioridad, hasta que cumpla una regla. El mensaje de correo electrónico se procesa entonces de acuerdo con las opciones de la regla y se adoptan las acciones sobre el spam detectado.

Algunos filtros antispam son configurables y es posible controlar si utilizarlos o no. Esta es la lista de filtros opcionales:

- **Filtro de juego de caracteres.** Muchos mensajes de spam están escritos en cirílico o en caracteres asiáticos. El Filtro de juego de caracteres detecta este tipo de mensajes y los marca como SPAM.

- **Contenido etiquetado como sexualmente explícito.** El spam con contenido sexual debe incluir la advertencia SEXUALLY-EXPLICIT: (sexualmente explícito) en la línea de asunto. Este filtro detecta correos marcados como SEXUALLY-EXPLICIT: (sexualmente explícito) en la línea de asunto y los marca como SPAM.
- **Filtro de URL.** Casi todos los mensajes de spam incluyen enlaces a varias páginas Web. Por lo general, estas páginas contienen más publicidad y ofrecen la posibilidad de comprar cosas. A veces, también se usan para el phishing.

  Bitdefender mantiene una base de datos de este tipo de enlaces. El Filtro de URL busca todos los enlaces a URLs de los mensajes en su base de datos. Si se produce una coincidencia, el mensaje se marca como SPAM.
- **Lista blackhole en tiempo real (RBL).** Se trata de un filtro que permite buscar el servidor de correo del remitente en servidores RBL de terceros. El filtro utiliza los servidores de protocolo DNSBL y RBL para filtrar el spam basándose en la reputación de los servidores de correo de los remitentes.

  La dirección del servidor de correo se extrae del encabezado del mensaje y se comprueba su validez. Si la dirección pertenece a una clase privada (`10.0.0.0`, `172.16.0.0` a `172.31.0.0` o `192.168.0.0` a `192.168.255.0`), se ignora.

  Se lleva acabo una comprobación de DNS sobre el dominio `d.c.b.a.rbl.ejemplo.com`, donde `d.c.b.a` es la dirección IP inversa del servidor y `rbl.ejemplo.com` es el servidor RBL. Si el DNS responde que el dominio es válido, significa que la IP aparece en el servidor RBL y se proporciona la puntuación del servidor. Esta puntuación va de 0 a 100, de acuerdo con el nivel de confianza que se le otorgue al servidor.

  Se consultarán todos los servidores RBL introducidos en la lista y se determinará una puntuación media a partir de la puntuación obtenida en cada uno de ellos. Cuando la puntuación llega a 100, no se llevan a cabo más consultas.

  Si la puntuación del filtro RBL es 100 o superior, el mensaje se considera spam y se adopta la acción especificada. En caso contrario, se calcula una puntuación de spam en base a la puntuación del filtro RBL y se añade a la puntuación general de spam del mensaje.
- **Filtro heurístico.** Desarrollado por Bitdefender, el filtro heurístico detecta spam nuevo y desconocido. El filtro se entrena automáticamente con gran cantidad de mensajes de correo electrónico no deseados (spam) en los laboratorios antispam de Bitdefender. Durante el entrenamiento, aprende a distinguir entre spam y mensajes legítimos y a reconocer el nuevo spam atendiendo a las

similitudes, a menudo muy sutiles, con los mensajes examinados previamente. Este filtro está diseñado para mejorar la detección basada en firmas, al tiempo que se reduce mucho el número de falsos positivos.

- **Consulta a la nube de Bitdefender.** Bitdefender mantiene en la nube una base de datos constantemente actualizada de "huellas" de correo electrónico no deseado. Se envía una consulta con la huella del mensaje a los servidores en la nube para comprobar sobre la marcha si el mensaje es spam. Incluso si no se encuentra la huella o firma en la base de datos, se comprueba con otras consultas recientes y, siempre que se cumplan determinadas condiciones, el mensaje se marca como spam.

Administración de las reglas antispam

Puede ver todas las reglas existentes que figuran en la tabla, junto con información sobre su prioridad, estado y ámbito de aplicación. Las reglas se clasifican por prioridad, teniendo la primera regla la mayor prioridad.

Cualquier política antispam tiene una regla por defecto que se activa en cuanto se habilita el módulo. Lo que necesita saber sobre la regla por defecto:

- No puede copiar, desactivar ni eliminar la regla por defecto.
- Solo se pueden modificar los ajustes del análisis y las acciones.
- La prioridad de la regla por defecto es siempre la menor.

Creando Reglas

Para crear una regla:

1. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para abrir la ventana de configuración.
2. Configure los ajustes de la regla. Para obtener más información sobre las opciones, consulte “Opciones de reglas” (p. 374).
3. Haga clic en **Guardar**. La regla aparece en primer lugar en la tabla.

Modificación de reglas

Para modificar una regla existente:

1. Haga clic en el nombre de la regla para abrir la ventana de configuración.
2. Introduzca los nuevos valores para las opciones que desee modificar.
3. Haga clic en **Guardar**. Si la regla está activa, los cambios surten efecto tras guardar la política.

Establecimiento de la prioridad de la regla

Para cambiar una prioridad de la regla, seleccione la regla que desee y utilice las flechas **Arriba** y **Abajo** de la parte superior de la tabla. Solo puede mover las reglas una a una.

Eliminación de reglas

Si ya no quiere volver a utilizar una regla, selecciónela y haga clic en el botón **Eliminar** de la parte superior de la tabla.

Opciones de reglas

Tiene las siguientes opciones a su disposición:

- **General.** En esta sección debe establecer un nombre para la regla, pues de lo contrario no podrá guardarla. Marque la casilla de verificación **Activa** si desea que la regla entre en vigor tras guardar la política.
- **Ámbito de aplicación de la regla.** Puede restringir la regla para que se aplique solo a un subconjunto de mensajes de correo electrónico, mediante el establecimiento de las siguientes opciones acumulativas del ámbito de aplicación:
  - **Aplicar a (dirección).** Seleccione la dirección del tráfico de correo electrónico a la que se aplica la regla.
  - **Remitentes.** Puede decidir si la regla se aplica a cualquier remitente o solo a determinados remitentes. Para reducir el rango de remitentes, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Vea los grupos seleccionados en la tabla de la derecha.
  - **Destinatarios.** Puede decidir si la regla se aplica a cualquier destinatario o solo a determinados destinatarios. Para reducir el rango de destinatarios, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Puede ver los grupos seleccionados en la tabla de la derecha.

    La regla se aplica si alguno de los destinatarios coincide con su selección. Si desea aplicar la regla solo en caso de que todos los destinatarios estén en los grupos seleccionados, seleccione **Coincidir todos los destinatarios**.

    Nota
    Las direcciones de los campos **Cc** y **Bcc** también se consideran destinatarios.

    Importante
    Las reglas basadas en los grupos de usuarios se aplican solo a los roles de transporte de concentradores y de buzón.

- **Ajustes.** 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.

  Además, puede activar varios filtros. Para obtener información detallada sobre estos filtros, consulte "Filtros Antispam" (p. 371).

  Importante
  El filtro RBL requiere configuración adicional. Puede configurar el filtro después de haber creado o editado la regla. Para obtener más información, consulte"Configuración del filtro RBL" (p. 376)

  En el caso de las conexiones autenticadas, puede elegir si se omite o no el análisis antispam.
- **Acciones.** Hay diversas acciones que puede adoptar respecto a los mensajes de correo electrónico detectados. Cada acción tiene, a su vez, varias opciones posibles o acciones secundarias. Se describen a continuación:

  Acciones principales:
  - **Entregar mensaje de correo electrónico.** El mensaje de correo electrónico no deseado llega a los buzones de los destinatarios.
  - **Mensaje de correo electrónico en cuarentena.** El mensaje de correo electrónico se cifra y se guarda en la carpeta de cuarentena del Exchange Server, sin entregarse a los destinatarios. Puede administrar los mensajes de correo electrónico en cuarentena desde la página **Cuarentena**.
  - **Redirigir el mensaje de correo electrónico a.** El mensaje no se entrega a los destinatarios originales sino a un buzón indicado en el campo correspondiente.
  - **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.

  Acciones secundarias:
  - **Integrar con Exchange SCL.** Añade un encabezado al mensaje de correo electrónico no deseado, dejando que sean Exchange Server o Microsoft Outlook quienes adopten las acciones de acuerdo con el mecanismo de Nivel de confianza contra correo no deseado (SCL).

- **Etiquetar el asunto del mensaje de correo electrónico como.** Puede añadir una etiqueta al asunto del mensaje para ayudar a los usuarios a filtrar los mensajes detectados en su cliente de correo electrónico.
- **Añadir un encabezado al mensaje de correo electrónico.** Se añade un encabezado a los mensajes de correo electrónico detectados como spam. Puede modificar el nombre del encabezado y su valor introduciendo los valores deseados en los campos correspondientes. Más adelante, puede utilizar este encabezado de correo electrónico para crear filtros adicionales.
- **Guardar el mensaje de correo electrónico en disco.** Se guarda una copia del mensaje de correo electrónico no deseado como archivo en la carpeta especificada. Indique la ruta absoluta de la carpeta en el campo correspondiente.

  Nota
  Esta opción solo es compatible con mensajes de correo electrónico en formato MIME.

- **Archivar en cuenta.** Se entrega una copia del mensaje detectado en la dirección de correo electrónico especificada. Esta acción añade la dirección de correo electrónico especificada a la lista CCO del mensaje.

- Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

Configuración del filtro RBL

Si desea utilizar el filtro RBL, debe proporcionar una lista de servidores RBL.

Para configurar el filtro:

1. En la página **Antispam**, haga clic en el enlace **Ajustes** para abrir la ventana de configuración.
2. Proporcione la dirección IP del servidor DNS que desea consultar y el intervalo de tiempo de espera de consulta en los campos correspondientes. Si no se configura ninguna dirección de servidor DNS, o si el servidor DNS no está disponible, el filtro RBL usa los servidores DNS del sistema.
3. Por cada servidor RBL:

a. Introduzca el nombre del servidor o la dirección IP y el nivel de confianza que ha asignado a dicho servidor en los campos del encabezado de la tabla.
b. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla.

4. Haga clic en **Guardar**.

Configuración de la lista blanca de remitentes

En el caso de remitentes de correo electrónico conocidos, puede evitar el consumo innecesario de recursos del servidor mediante su inclusión en las listas de remitentes de confianza o, por el contrario, de remitentes que no sean de fiar. De este modo, el servidor de correo aceptará o rechazará siempre los mensajes de correo electrónico procedentes de estos remitentes. Por ejemplo, si tiene una frecuente comunicación por correo electrónico con un colaborador, puede añadirlo a la lista blanca para asegurarse de que recibe todos sus mensajes.

Para crear una lista blanca de remitentes de confianza:

1. Haga clic en el enlace **Lista blanca** para abrir la ventana de configuración.
2. Marque la casilla de verificación **Lista blanca de remitentes**.
3. Introduzca la dirección de correo electrónico en el campo correspondiente. Al editar la lista, también puede utilizar los siguientes caracteres comodín para definir un dominio de correo electrónico completo o un patrón de direcciones de correo electrónico:
   - Asterisco (*); sustituye a cero, uno o más caracteres.
   - Signo de interrogación (?); sustituye a cualquier carácter individual.

   Por ejemplo, si introduce `*.gov` se aceptarán todos los correos electrónicos procedentes del dominio `.gov`.
4. Haga clic en **Guardar**.

Nota
Para incluir en la lista negra a remitentes de spam conocidos, utilice la opción **Lista negra de conexión** de la sección **Protección de Exchange > General > Ajustes**.

Control de Contenido

Utilice el Control de contenidos para mejorar la protección del correo electrónico mediante el filtrado de todo el tráfico de correo electrónico que no cumpla las políticas de su empresa (contenidos potencialmente sensibles o no deseados).

Para un control general del contenido del correo electrónico, este módulo incorpora dos opciones de filtrado del correo electrónico:

- Filtro de Contenido
- Filtro de Adjuntos

Nota
El filtrado de contenidos y el filtrado de adjuntos están disponibles para:

- Exchange Server 2016/2013 con rol de transporte perimetral o de buzón.
- Exchange Server 2010/2007 con rol de transporte perimetral o de transporte de concentradores.

Administración de las reglas de filtrado

Los filtros de control de contenidos se basan en reglas. Se pueden definir reglas distintas para diferentes usuarios y grupos de usuarios. Los mensajes de correo electrónico que llegan al servidor de correo electrónico se cotejan con las reglas de filtrado, por orden de prioridad, hasta que cumplan una regla. El mensaje de correo electrónico se procesa entonces según las opciones especificadas por esa regla.

Las reglas de filtrado de contenidos preceden a las reglas de filtrado de archivos adjuntos.

Las reglas de filtrado de contenidos y de adjuntos se incluyen en las tablas correspondientes por orden de prioridad, teniendo la primera regla la mayor prioridad. Se proporcionará la siguiente información para cada regla:

- Prioridad
- Nombre
- Dirección del tráfico.
- Grupos de destinatarios y remitentes.

Creando Reglas

Dispone de dos alternativas para la creación de reglas de filtrado:

- Parta de los ajustes por defecto siguiendo estos pasos:
  1. Haga clic en el botón ⊕ **Añadir** de la parte superior de la tabla para abrir la ventana de configuración.
  2. Configure los ajustes de la regla. Para obtener más información acerca de las opciones concretas de filtrado de adjuntos y del contenido, consulte:
     - Opciones de reglas de filtrado de contenidos
     - Opciones de reglas de filtrado de adjuntos.
  3. Haga clic en **Guardar**. La regla aparece en primer lugar en la tabla.
- Utilice un clon de una regla personalizada como plantilla siguiendo estos pasos:

1. Seleccione la regla deseada de la lista.
2. Haga clic en el botón **Clonar** de la parte superior de la tabla.
3. Ajuste las opciones de la regla conforme a sus necesidades.
4. Haga clic en **Guardar**. La regla aparece en primer lugar en la tabla.

Modificación de reglas

Para modificar una regla existente:

1. Haga clic en el nombre de la regla para abrir la ventana de configuración.
2. Introduzca los nuevos valores para las opciones que desee modificar.
3. Haga clic en **Guardar**. Los cambios surten efecto tras guardar la política.

Establecimiento de la prioridad de la regla

Para cambiar la prioridad de una regla:

1. Seleccione la regla que desea mover.
2. Utilice los botones **Arriba** o **Abajo** de la parte superior de la tabla para aumentar o disminuir la prioridad de la regla.

Eliminación de reglas

Puede eliminar una o varias reglas personalizadas. Lo que tiene que hacer es:

1. Seleccione las reglas que desee eliminar.
2. Haga clic en el botón **Eliminar** de la parte superior de la tabla. Una vez que se elimina una regla, no puede recuperarla.

Filtro de Contenido

El filtrado de contenidos le ayuda a filtrar el tráfico de correo electrónico en función de las cadenas de caracteres que haya definido previamente. Estas cadenas se comparan con el asunto del mensaje o con el texto que contiene el cuerpo del mismo. Utilizando el Filtro de Contenido, puede conseguir lo siguiente:

- Evite que los contenidos de correos no deseados lleguen a sus buzones de Exchange Server.
- Bloquee mensajes de correo electrónico salientes que contengan datos confidenciales.
- Archive mensajes de correo electrónico que cumplan las condiciones indicadas en una cuenta de correo electrónico o en el disco. Por ejemplo, puede guardar los mensajes de correo electrónico enviados a la dirección de soporte de su empresa en una carpeta en su disco local.

Activación del filtrado de contenidos

Si desea utilizar el filtrado de contenidos, marque la casilla de verificación **Filtrado de contenidos**.

Para crear y administrar reglas de filtrado de contenidos, consulte "Administración de las reglas de filtrado" (p. 378).

Opciones de reglas

- **General.** En esta sección debe establecer un nombre para la regla, pues de lo contrario no podrá guardarla. Marque la casilla de verificación **Activa** si desea que la regla entre en vigor tras guardar la política.
- **Ámbito de aplicación de la regla.** Puede restringir la regla para que se aplique solo a un subconjunto de mensajes de correo electrónico, mediante el establecimiento de las siguientes opciones acumulativas del ámbito de aplicación:
  - **Aplicar a (dirección).** Seleccione la dirección del tráfico de correo electrónico a la que se aplica la regla.
  - **Remitentes.** Puede decidir si la regla se aplica a cualquier remitente o solo a determinados remitentes. Para reducir el rango de remitentes, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Vea los grupos seleccionados en la tabla de la derecha.
  - **Destinatarios.** Puede decidir si la regla se aplica a cualquier destinatario o solo a determinados destinatarios. Para reducir el rango de destinatarios, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Puede ver los grupos seleccionados en la tabla de la derecha.

    La regla se aplica si alguno de los destinatarios coincide con su selección. Si desea aplicar la regla solo en caso de que todos los destinatarios estén en los grupos seleccionados, seleccione **Coincidir todos los destinatarios**.

    Nota
    Las direcciones de los campos **Cc** y **Bcc** también se consideran destinatarios.

    Importante
    Las reglas basadas en los grupos de usuarios se aplican solo a los roles de transporte de concentradores y de buzón.

- **Ajustes.** Configure las expresiones que hay que buscar en los mensajes de correo electrónico como se describe a continuación:
  1. Elija la parte del mensaje de correo electrónico que se debe comprobar:

- El asunto del mensaje, marcando la casilla de verificación **Filtrar por asunto**. Se filtrarán todos los mensajes de correo electrónico cuyo asunto contenga alguna de las expresiones introducidas en la tabla correspondiente.
- El cuerpo del mensaje, marcando la casilla de verificación **Filtrar por contenido del cuerpo**. Se filtrarán todos los mensajes de correo electrónico que contengan en su cuerpo alguna de las expresiones definidas.
- Tanto el asunto como el cuerpo, marcando ambas casillas de verificación. Se filtrarán todos los mensajes de correo electrónico cuyo asunto coincida con cualquier regla de la primera tabla Y cuyo cuerpo contenga cualquier expresión de la segunda tabla. Por ejemplo:

  La primera tabla contiene las expresiones: `boletín` y `semanal`. La segunda tabla contiene las expresiones: `compras`, `precio` y `oferta`.

  Coincidiría con la regla, y por tanto se filtraría, un mensaje de correo electrónico con el asunto "**Boletín** mensual de su relojería favorita" y cuyo cuerpo contuviera la frase "Tenemos el placer de presentar nuestra última **oferta** con sensacionales relojes a **precios** irresistibles". Si el tema fuera "Noticias de relojería", el mensaje no se filtraría.

2. Cree las listas de condiciones con los campos en el encabezado de la tabla. Por cada condición, siga estos pasos:
   a. Seleccione el tipo de expresión que se debe usar en las búsquedas. Puede escoger entre introducir la expresión textual exacta o crear patrones de texto mediante expresiones regulares.

      Nota
      La sintaxis de las expresiones regulares se valida conforme a la gramática de ECMAScript.

   b. Introduzca la cadena de búsqueda en el campo **Expresión**.

      Por ejemplo:

      i. La expresión `5[1-5]\d{2}([\s\-]?\d{4}){3}` coincide con las tarjetas bancarias cuyos números comienzan entre cincuenta y uno cincuenta y cinco, tienen dieciséis dígitos en grupos de cuatro, y los grupos pueden estar separados por un espacio o por un guion. Por lo tanto, se filtraría cualquier mensaje de correo electrónico que contuviera un número de tarjeta con el formato

`5257-4938-3957-3948`, `5257 4938 3957 3948` o `5257493839573948`.

ii. Esta expresión detecta mensajes de correo electrónico con las palabras `premio`, `efectivo` y `lotería`, que se encuentren exactamente en este orden:

```
(lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
```

Para detectar los mensajes de correo electrónico que contengan cada una de esas tres palabras, sin importar su orden, añada tres expresiones regulares con las palabras en diferente orden.

iii. Esta expresión detecta los mensajes de correo electrónico que incluyan tres o más apariciones de la palabra `premio`:

```
(prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
```

c. Si quiere diferenciar las mayúsculas de las minúsculas en las comparaciones de texto, marque la casilla de verificación **Coincidir mayúsculas y minúsculas**. Por ejemplo, con esa casilla de verificación marcada, `Boletín` no es lo mismo que `boletín`.

d. Si no desea que la expresión forme parte de otras palabras, marque la casilla de verificación **Palabras completas**. Por ejemplo, con la casilla de verificación marcada, la expresión `El sueldo de Luis` no coincide con `El sueldo de Luisa`.

e. Haga clic en el botón ⊕ **Añadir** del encabezado de la columna **Acción** para añadir la condición a la lista.

- **Acciones.** Hay diversas acciones que puede adoptar respecto a los mensajes de correo electrónico. Cada acción tiene, a su vez, varias opciones posibles o acciones secundarias. Se describen a continuación:

  Acciones principales:
  - **Entregar mensaje de correo electrónico.** El mensaje de correo electrónico detectado llega a los buzones de los destinatarios.
  - **Cuarentena.** El mensaje de correo electrónico se cifra y se guarda en la carpeta de cuarentena de Exchange Server, sin entregarse a los destinatarios. Puede administrar los mensajes de correo electrónico en cuarentena desde la página **Cuarentena**.

- **Redirigir a.** El mensaje no se entrega a los destinatarios originales sino a un buzón indicado en el campo correspondiente.
- **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.

Acciones secundarias:

- **Etiquetar el asunto del mensaje de correo electrónico como.** Puede añadir una etiqueta al asunto del mensaje detectado para ayudar a los usuarios a filtrar los mensajes en su cliente de correo electrónico.
- **Añadir un encabezado a los mensajes de correo electrónico.** Puede añadir un nombre de encabezado y un valor a los encabezados del mensaje de correo electrónico detectado introduciendo los valores deseados en los campos correspondientes.
- **Guardar mensaje en disco.** Se guarda una copia del mensaje de correo electrónico detectado como archivo en la carpeta especificada del servidor de Exchange. Si la carpeta no existe, se creará. Debe indicar la ruta absoluta de la carpeta en el campo correspondiente.

  Nota
  Esta opción solo es compatible con mensajes de correo electrónico en formato MIME.

- **Archivar en cuenta.** Se entrega una copia del mensaje detectado en la dirección de correo electrónico especificada. Esta acción añade la dirección de correo electrónico especificada a la lista CCO del mensaje.

- Por defecto, cuando un mensaje de correo electrónico se ajusta a las condiciones de una regla, deja de comprobarse respecto a las demás. Si desea seguir procesando reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

Exclusiones

Si desea que se entregue el tráfico de correo electrónico de remitentes o destinatarios concretos, independientemente de las reglas de filtrado de contenidos, puede definir exclusiones de filtrado.

Para crear una exclusión:

1. Haga clic en el enlace **Exclusiones** junto a la casilla de verificación **Filtrado de contenidos**. Esta acción abre la ventana de configuración.
2. Introduzca las direcciones de correo electrónico de los remitentes o destinatarios de confianza en los campos correspondientes. Cualquier mensaje de correo electrónico que provenga de un remitente de confianza o que se envíe a un destinatario de confianza quedará excluido del filtrado. Al editar la lista, también puede utilizar los siguientes caracteres comodín para definir un dominio de correo electrónico completo o un patrón de direcciones de correo electrónico:
   - Asterisco (*); sustituye a cero, uno o más caracteres.
   - Signo de interrogación (?); sustituye a cualquier carácter individual.

   Por ejemplo, si introduce `*.gov` se aceptarán todos los correos electrónicos procedentes del dominio `.gov`.
3. En el caso de mensajes de correo electrónico con varios destinatarios, puede marcar la casilla de verificación **Excluir el mensaje de correo electrónico del filtrado solo si todos los destinatarios son de confianza** para aplicar la exclusión solo si todos los destinatarios del mensaje se encuentran en la lista de destinatarios de confianza.
4. Haga clic en **Guardar**.

Filtro de Adjuntos

El módulo de filtrado de adjuntos proporciona opciones de filtrado para los archivos adjuntos a los mensajes de correo electrónico. Puede detectar adjuntos con determinados patrones de nombre o de un cierto tipo. Gracias al filtrado de adjuntos puede:

- Bloquear adjuntos potencialmente peligrosos, como los archivos `.vbs` o `.exe` o los mensajes de correo electrónico que los contengan.
- Bloquear adjuntos con nombres ofensivos o los mensajes de correo electrónico que los contengan.

Activación del filtrado de adjuntos

Si desea utilizar el filtrado de adjuntos, marque la casilla de verificación **Filtrado de adjuntos**.

Para crear y administrar reglas de filtrado de adjuntos, consulte “Administración de las reglas de filtrado” (p. 378).

Opciones de reglas

- **General.** En esta sección debe establecer un nombre para la regla, pues de lo contrario no podrá guardarla. Marque la casilla de verificación **Activa** si desea que la regla entre en vigor tras guardar la política.
- **Ámbito de aplicación de la regla.** Puede restringir la regla para que se aplique solo a un subconjunto de mensajes de correo electrónico, mediante el establecimiento de las siguientes opciones acumulativas del ámbito de aplicación:
  - **Aplicar a (dirección).** Seleccione la dirección del tráfico de correo electrónico a la que se aplica la regla.
  - **Remitentes.** Puede decidir si la regla se aplica a cualquier remitente o solo a determinados remitentes. Para reducir el rango de remitentes, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Vea los grupos seleccionados en la tabla de la derecha.
  - **Destinatarios.** Puede decidir si la regla se aplica a cualquier destinatario o solo a determinados destinatarios. Para reducir el rango de destinatarios, haga clic en el botón **Específico** y seleccione los grupos deseados de la tabla de la izquierda. Puede ver los grupos seleccionados en la tabla de la derecha.

    La regla se aplica si alguno de los destinatarios coincide con su selección. Si desea aplicar la regla solo en caso de que todos los destinatarios estén en los grupos seleccionados, seleccione **Coincidir todos los destinatarios**.

    Nota
    Las direcciones de los campos **Cc** y **Bcc** también se consideran destinatarios.

    Importante
    Las reglas basadas en los grupos de usuarios se aplican solo a los roles de transporte de concentradores y de buzón.

- **Ajustes.** Indique los archivos que se permiten o prohíben como adjuntos de correo electrónico.

  Puede realizar un filtrado de archivos adjuntos por tipo de archivo o por nombre de archivo.

  Para filtrar adjuntos por tipo de archivo, siga estos pasos:
  1. Marque la casilla de verificación **Detectar por tipo de contenido**.
  2. Seleccione la opción de detección que mejor se adapte a sus necesidades:

- **Solo las siguientes categorías**, cuando tiene una lista limitada de categorías de tipos de archivo prohibidos.
- **Todas, excepto las siguientes categorías**, cuando tiene una lista limitada de categorías de tipos de archivo permitidos.

3. Seleccione en la lista las categorías de tipos de archivo que le interesen. Para más información sobre las extensiones de cada categoría, consulte "Tipos de archivo de filtrado de adjuntos" (p. 528).

   Si está interesado únicamente en ciertos tipos de archivo, marque la casilla de verificación **Extensiones personalizadas** e introduzca la lista de extensiones en el campo correspondiente.
4. Marque la casilla de verificación **Habilitar detección de tipo real de archivo** para comprobar los encabezados de archivos e identificar correctamente el tipo de archivo adjunto al analizar las extensiones restringidas. Esto implica que no es posible cambiar simplemente el nombre de una extensión para burlar las políticas de filtrado de adjuntos.

   Nota
   La detección del tipo real de archivo puede consumir muchos recursos.

Para filtrar los adjuntos por su nombre, marque la casilla de verificación **Detectar por nombre de archivo** e introduzca los nombres de archivo que desee filtrar en el campo correspondiente. Al editar la lista, también puede utilizar los siguientes caracteres comodín para definir patrones:

- Asterisco (*); sustituye a cero, uno o más caracteres.
- Signo de interrogación (?); sustituye a cualquier carácter individual.

Por ejemplo, si introduce `base de datos.*`, se detectarán todos los archivos con el nombre `base de datos`, independientemente de su extensión.

Nota
Si activa tanto la detección por tipo de contenido como por nombre de archivo (sin detección de tipo real), el archivo debe cumplir simultáneamente las condiciones para ambos tipos de detección. Por ejemplo, ha seleccionado la categoría **Multimedia** e introducido el nombre de archivo `prueba.pdf`. En tal caso, todos los mensajes de correo electrónico pasarán la regla, dado que los archivos PDF no son archivos multimedia.

Seleccione la casilla de verificación **Analizar dentro de los archivos** para evitar que los archivos bloqueados se oculten en archivos comprimidos aparentemente inofensivos y pasen así la regla de filtrado.

El análisis es recursivo dentro de los archivos y, por defecto, llega hasta el cuarto nivel de profundidad en el archivo comprimido. Puede optimizar el análisis tal como se describe aquí:

1. Marque la casilla de verificación **Profundidad de archivo máxima (niveles)**.
2. Seleccione un valor diferente en el menú correspondiente. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.

Nota
Si ha elegido analizar los archivos comprimidos, se desactiva **Analizar dentro de los archivos** y se analizan todos los archivos.

- **Acciones.** Hay diversas acciones que puede adoptar respecto a los adjuntos detectados o a los mensajes de correo electrónico que los contengan. Cada acción tiene, a su vez, varias opciones posibles o acciones secundarias. Se describen a continuación:

  Acciones principales:
  - **Reemplazar archivo.** Elimina los archivos detectados e inserta un archivo de texto que comunica al usuario las acciones adoptadas.

    Para configurar el texto de notificación:
    1. Haga clic en el enlace **Ajustes** junto a la casilla de verificación **Filtrado de adjuntos**.
    2. Introduzca el texto de notificación en el campo correspondiente.
    3. Haga clic en **Guardar**.
  - **Eliminar archivo.** Elimina los archivos detectados sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
  - **Rechazar/Eliminar mensaje.** En los servidores con rol de transporte perimetral, se rechaza el mensaje de correo electrónico detectado con un código de error 550 SMTP. En todos los demás casos, el mensaje de correo electrónico se borra sin ninguna advertencia. Se aconseja que evite utilizar esta acción.
  - **Mensaje de correo electrónico en cuarentena.** El mensaje de correo electrónico se cifra y se guarda en la carpeta de cuarentena del Exchange Server, sin entregarse a los destinatarios. Puede administrar los

mensajes de correo electrónico en cuarentena desde la página **Cuarentena**.

- **Redirigir el mensaje de correo electrónico a.** El mensaje no se entrega a los destinatarios originales sino a una dirección de correo electrónico que indique en el campo correspondiente.
- **Entregar mensaje de correo electrónico.** Deja pasar el mensaje de correo electrónico.

Acciones secundarias:

- **Etiquetar el asunto del mensaje de correo electrónico como.** Puede añadir una etiqueta al asunto del mensaje detectado para ayudar a los usuarios a filtrar los mensajes en su cliente de correo electrónico.
- **Añadir un encabezado al mensaje de correo electrónico.** Puede añadir un nombre de encabezado y un valor a los encabezados del mensaje de correo electrónico detectado introduciendo los valores deseados en los campos correspondientes.
- **Guardar el mensaje de correo electrónico en disco.** Se guarda una copia del mensaje de correo electrónico detectado como archivo en la carpeta especificada del servidor de Exchange. Si la carpeta no existe, se creará. Debe indicar la ruta absoluta de la carpeta en el campo correspondiente.

  Nota
  Esta opción solo es compatible con mensajes de correo electrónico en formato MIME.

- **Archivar en cuenta.** Se entrega una copia del mensaje detectado en la dirección de correo electrónico especificada. Esta acción añade la dirección de correo electrónico especificada a la lista CCO del mensaje.

- Por defecto, cuando un mensaje de correo electrónico coincide con el ámbito de aplicación de una regla, se procesa exclusivamente de conformidad con la regla, sin cotejarlo con ninguna otra regla restante. Si desea seguir cotejando las otras reglas, deje sin marcar la casilla de verificación **Si las condiciones de la regla coinciden, detener el proceso de más reglas**.

Exclusiones

Si desea que se entregue el tráfico de correo electrónico de remitentes o destinatarios concretos, independientemente de las reglas de filtrado de adjuntos, puede definir exclusiones de filtrado.

Para crear una exclusión:

1. Haga clic en el enlace **Exclusiones** junto a la casilla de verificación **Filtrado de adjuntos**. Esta acción abre la ventana de configuración.
2. Introduzca las direcciones de correo electrónico de los remitentes o destinatarios de confianza en los campos correspondientes. Cualquier mensaje de correo electrónico que provenga de un remitente de confianza o que se envíe a un destinatario de confianza quedará excluido del filtrado. Al editar la lista, también puede utilizar los siguientes caracteres comodín para definir un dominio de correo electrónico completo o un patrón de direcciones de correo electrónico:
   - Asterisco (*); sustituye a cero, uno o más caracteres.
   - Signo de interrogación (?); sustituye a cualquier carácter individual.

   Por ejemplo, si introduce `*.gov` se aceptarán todos los correos electrónicos procedentes del dominio `.gov`.
3. En el caso de mensajes de correo electrónico con varios destinatarios, puede marcar la casilla de verificación **Excluir el mensaje de correo electrónico del filtrado solo si todos los destinatarios son de confianza** para aplicar la exclusión solo si todos los destinatarios del mensaje se encuentran en la lista de destinatarios de confianza.
4. Haga clic en **Guardar**.

7.2.12. Cifrado

Nota
Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores
- macOS

El módulo de cifrado gestiona el cifrado de disco completo en los endpoints mediante BitLocker en Windows y mediante FileVault y la utilidad de línea de comandos diskutil en macOS, respectivamente.

Esta filosofía de GravityZone puede proporcionar importantes ventajas:

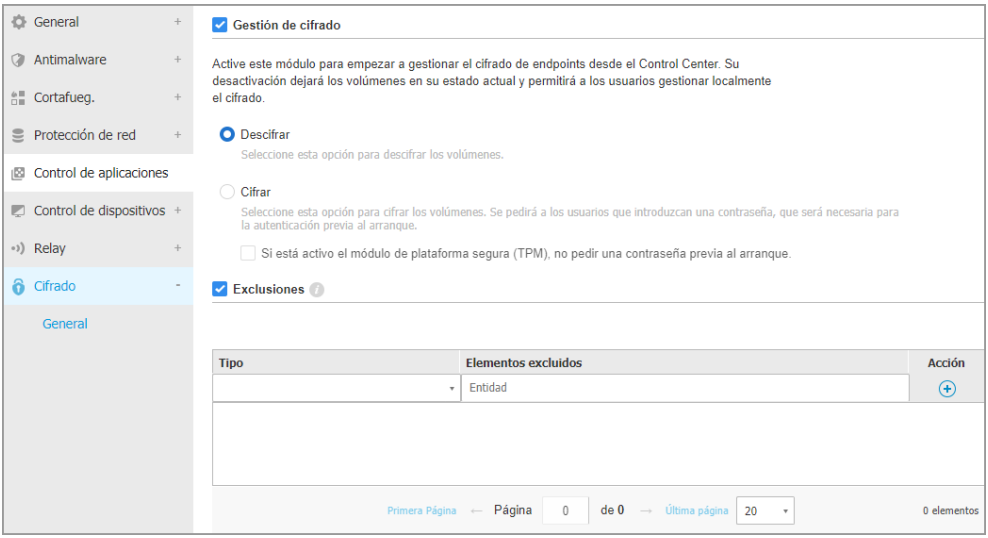
- Datos protegidos en caso de pérdida o robo de dispositivos.
- Amplia protección para las plataformas informáticas más populares del mundo, mediante el uso de estándares de cifrado recomendados con soporte completo por parte de Microsoft y Apple.

- Impacto mínimo en el rendimiento de los endpoints gracias a las herramientas de cifrado nativas.

El módulo de cifrado opera con las siguientes soluciones:

- BitLocker versión 1.2 y posterior, en los endpoints Windows con un módulo de plataforma segura (TPM), para volúmenes ya sean de arranque o no.
- BitLocker versión 1.2 y posterior, en los endpoints Windows sin un TPM, para volúmenes ya sean de arranque o no.
- FileVault en los endpoints macOS, para volúmenes de arranque.
- Diskutil en los endpoints macOS, para volúmenes que no sean de arranque.

Para ver la lista de sistemas operativos compatibles con el módulo de cifrado, consulte la Guía de instalación de GravityZone.



La página de cifrado

Para empezar a gestionar el cifrado de endpoints desde Control Center, marque la casilla de verificación **Gestión de cifrado**. Mientras este ajuste esté habilitado, los usuarios del endpoint no podrán gestionar el cifrado localmente y todas sus acciones se cancelarán o revertirán. La inhabilitación de este ajuste dejará los

volúmenes del endpoint en su estado actual (cifrado o sin cifrar) y los usuarios podrán gestionar el cifrado en sus máquinas.

Para gestionar los procesos de cifrado y descifrado, existen tres opciones:

- **Descifrar**: descifra los volúmenes y los mantiene así cuando la política está activa en los endpoints.
- **Cifrar**: cifra los volúmenes y los mantiene así cuando la política está activa en los endpoints.

  Con la opción de Cifrar, puede marcar la casilla de verificación **No solicitar contraseña para cifrar si está activo el módulo de plataforma segura (TPM)**. Este ajuste proporciona cifrado en los endpoints Windows con TPM, sin requerir una contraseña de cifrado a los usuarios. Para obtener información, consulte "Cifrado de volúmenes" (p. 391).
- **Exclusiones**

GravityZone es compatible con el método estándar de cifrado avanzado (AES) con claves de 128 y 256 bits en Windows y macOS. El algoritmo de cifrado utilizado depende de la configuración de cada sistema operativo.

Nota
GravityZone detecta y gestiona volúmenes cifrados manualmente con BitLocker, FileVault y diskutil. Para empezar a gestionar estos volúmenes, el agente de seguridad solicitará a los usuarios del endpoint que cambien sus claves de recuperación. En caso de emplear otras soluciones de cifrado, se deberán descifrar los volúmenes antes de aplicar una política de GravityZone.

Cifrado de volúmenes

Para cifrar volúmenes:

1. Marque la casilla de verificación **Gestión del cifrado**.
2. Seleccione la opción **Cifrar**.

El proceso de cifrado comienza después de activarse la política en los endpoints, con algunas particularidades en Windows y Mac.

Para Windows

Por defecto, el agente de seguridad solicitará a los usuarios que configuren una contraseña para iniciar el cifrado. Si la máquina tiene un TPM operativo, el agente de seguridad pedirá a los usuarios que configuren un número de identificación personal (PIN) para empezar el cifrado. Los usuarios deben

introducir la contraseña o el PIN configurados en este paso cada vez que se inicie el endpoint, en una pantalla de autenticación previa al arranque.

> **Nota**
> El agente de seguridad le permite configurar los requisitos de complejidad del PIN y los privilegios de los usuarios para cambiar su PIN a través de la configuración de la directiva de grupo (GPO) de BitLocker.

Para iniciar el cifrado sin requerir una contraseña a los usuarios de los endpoints, marque la casilla de verificación **Si está activo el módulo de plataforma segura (TPM), no pedir una contraseña previa al arranque**. Este ajuste es compatible con endpoints Windows que tengan TPM y UEFI.

Si está marcada la casilla de verificación **Si está activo el módulo de plataforma segura (TPM), no pedir una contraseña previa al arranque**:

- En endpoints sin cifrar:
  - El cifrado continúa sin requerir una contraseña.
  - La pantalla de autenticación previa al arranque no aparece al iniciar la máquina.
- En endpoints cifrados con contraseña:
  - Se elimina la contraseña.
  - Los volúmenes permanecen cifrados.
- En endpoints cifrados o no, sin TPM o con TPM no detectado o que no está en funcionamiento:
  - Se solicita al usuario que introduzca una contraseña para el cifrado.
  - La pantalla de autenticación previa al arranque aparece cuando se inicia la máquina.

Si no está marcada la casilla de verificación **Si está activo el módulo de plataforma segura (TPM), no pedir una contraseña previa al arranque**:

- El usuario debe introducir una contraseña para el cifrado.
- Los volúmenes permanecen cifrados.

Para Mac

Para iniciar el cifrado en volúmenes de arranque, el agente de seguridad solicitará a los usuarios que introduzcan sus credenciales del sistema. Solo pueden habilitar el cifrado los usuarios que tengan cuentas locales con privilegios administrativos.

Para iniciar el cifrado en volúmenes que no sean de arranque, el agente de seguridad solicitará a los usuarios que configuren una contraseña de cifrado. Esta contraseña será necesaria para desbloquear los volúmenes que no sean

de arranque cada vez que se inicie el equipo. Si el equipo tiene más de un volumen que no sea de arranque, los usuarios deberán configurar una contraseña de cifrado para cada uno de ellos.

Descifrado de volúmenes

Para descifrar volúmenes en los endpoints:

1. Marque la casilla de verificación **Gestión del cifrado**.
2. Seleccione la opción **Descifrar**.

El proceso de descifrado comienza después de activarse la política en los endpoints, con algunas particularidades en Windows y Mac.

Para Windows
Los volúmenes se descifran sin interacción por parte de los usuarios.

Para Mac
Para los volúmenes de arranque, los usuarios deben introducir sus credenciales del sistema. Para los volúmenes que no sean de arranque, los usuarios deben introducir la contraseña configurada durante el proceso de cifrado.

En caso de que los usuarios de los endpoints olviden sus contraseñas de cifrado, necesitarán claves de recuperación para desbloquear sus máquinas. Para obtener más información sobre cómo conseguir las claves de recuperación, consulte "" (p. 106).

Exclusión de particiones

Puede crear una lista de exclusiones del cifrado añadiendo letras de unidad, etiquetas y nombres de partición concretos y GUID de partición. Para crear una regla para excluir particiones del cifrado:

1. Marque la casilla de verificación **Exclusiones**.
2. Haga clic en **Tipo** y elija un tipo de unidad en el menú desplegable.
3. Introduzca un valor de unidad en el campo **Elementos excluidos** y tenga en cuenta las siguientes condiciones:
   - Para una **letra de unidad** introduzca `D:` o su letra de unidad seguida de dos puntos.
   - Para una **Etiqueta/Nombre**, puede introducir cualquier etiqueta, como `Trabajo`.

- Para un **GUID** de partición introduzca un valor de la siguiente manera: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.

4. Haga clic en **Añadir** ⊕ para añadir la exclusión a la lista.

Para eliminar una exclusión, elija un elemento y haga clic en **Eliminar** ⊗.

7.2.13. NSX

En esta sección puede establecer la política que se utilizará como perfil de seguridad en NSX. Para ello:

1. Marque la casilla de verificación **NSX** para establecer su visibilidad también en vSphere Web Client.
2. Introduzca el nombre con el que podrá identificar la política en NSX. Este nombre puede ser diferente del de la política en GravityZone Control Center. En vSphere aparecerá precedido del prefijo `Bitdefender_`. Elija este nombre con cuidado, ya que pasará a ser de solo lectura una vez guardada la política.

7.2.14. Protección de almacenamiento

Nota
La Protección de almacenamiento está disponible para dispositivos de almacenamiento conectados a la red (NAS) y soluciones de uso compartido de archivos compatibles con el protocolo de adaptación de contenido de Internet (ICAP).

En esta sección puede configurar Security Server como servicio de análisis para dispositivos NAS y soluciones de uso compartido de archivos que cumplan con ICAP, como Nutanix Files y Citrix ShareFile.

Security Server analiza cualquier archivos, incluidos los comprimidos, cuando lo solicitan los dispositivos de almacenamiento. Dependiendo de los ajustes, Security Server adopta las medidas oportunas sobre los archivos infectados, como desinfectarlos o denegar el acceso a ellos.

Los ajustes se organizan en las siguientes categorías:

- ICAP
- Exclusiones

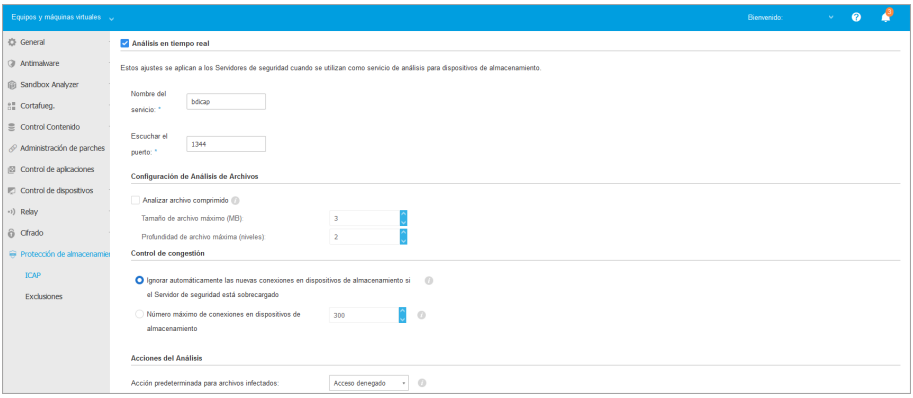
ICAP

Puede configurar las siguientes opciones para Security Server:

- Marque la casilla de verificación **Análisis on-access** para habilitar el módulo de Protección de almacenamiento. Los ajustes necesarios para la comunicación entre Security Server y los dispositivos de almacenamiento están predefinidos de la siguiente manera:
  - Nombre del servicio: `bdicap`.
  - Puerto de escucha: `1344`.
- En **Ajustes de análisis de archivos comprimidos**, marque la casilla de verificación **Analizar archivos comprimidos** para habilitar el análisis de este tipo de archivos. Configure el tamaño máximo de los archivos comprimidos que desea analizar, así como la profundidad de archivo máxima (niveles) dentro de ellos.

  Nota
  Si establece el tamaño máximo del archivo comprimido en 0 (cero), Security Server analizará todos ellos independientemente de su tamaño.

- En **Control de congestión**, elija el método que prefiere para administrar las conexiones en los dispositivos de almacenamiento en caso de sobrecarga de Security Server:
  - **Ignorar automáticamente las nuevas conexiones en dispositivos de almacenamiento si Security Server está sobrecargado**. Cuando un Security Server haya alcanzado un número máximo de conexiones, el dispositivo de almacenamiento redirigirá el excedente a otro Security Server.
  - **Número máximo de conexiones en dispositivos de almacenamiento**. Por defecto, el valor se establece en 300 conexiones.
- En **Acciones de análisis** hay disponibles las siguientes opciones:
  - **Denegar acceso**: Security Server deniega el acceso a los archivos infectados.
  - **Desinfectar**: Security Server elimina el código de malware de los archivos infectados.



Políticas - Protección de almacenamiento - ICAP

Exclusiones

Si desea excluir del análisis objetos concretos, marque la casilla de verificación **Exclusiones**.

Puede definir exclusiones:

- Por hash: Identifica el archivo excluido mediante un hash SHA-256.
- Por comodín: Identifica el archivo excluido mediante una ruta.

Configuración de exclusiones

Para añadir una 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:
   - **Hash**: Introduzca los hashes SHA-256 separados por comas.
   - **Comodín**: Especifique una ruta absoluta o relativa usando caracteres comodín. El símbolo asterisco (*) se aplica a cualquier archivo dentro de un directorio. Un signo de interrogación (?) sustituye a un solo carácter.
3. Añada una descripción para la exclusión.
4. Haga clic en el botón ⊕ **Añadir**. La nueva exclusión se añadirá a la lista.

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

Importación y exportación de exclusiones

Si tiene intención de volver a utilizar las exclusiones en varias políticas, puede exportarlas e importarlas.

Para exportar exclusiones:

1. Haga clic en el botón **Exportar** de la zona superior de la tabla de exclusiones.
2. Guarde el archivo CSV en su equipo. Dependiendo de la configuración de su navegador, puede que el archivo se descargue de forma automática, o que se le pida que lo guarde en alguna ubicación.

Cada fila del archivo CSV corresponde a una sola exclusión, cuyos campos aparecen en el orden siguiente:

```
<exclusion type>, <object to be excluded>, <description>
```

Estos son los valores disponibles para los campos CSV:

Tipo de exclusión:

`1`, para hash SHA-256

`2`, para comodín

Objeto que hay que excluir:

Un valor hash o una ruta

Descripción

Un texto para ayudar a identificar la exclusión.

Ejemplo de exclusiones en un archivo CSV:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

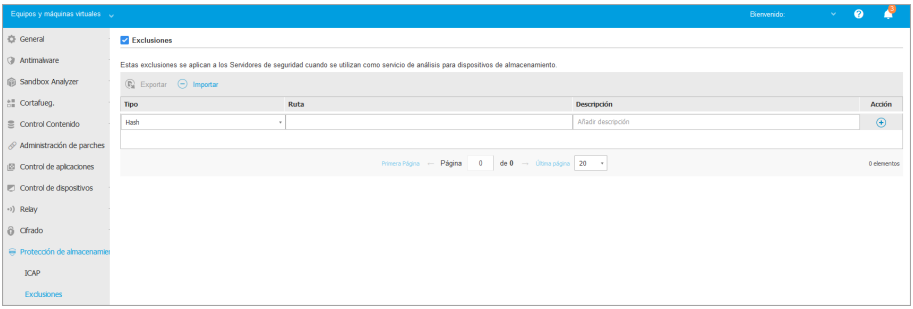
Para importar exclusiones:

1. Haga clic en **Importar**. Se abre la ventana **Importar exclusiones de políticas**.
2. Haga clic en **Añadir** y, a continuación, seleccione el archivo CSV.
3. Haga clic en **Guardar**. La tabla se rellena con las exclusiones válidas. Si el archivo CSV contiene exclusiones no válidas, aparece una advertencia que le informa de los números de fila correspondientes.

Editar exclusiones

Para editar una exclusión:

1. Haga clic en el nombre de la exclusión en la columna **Ruta** o en la descripción.
2. Edite la exclusión.
3. Pulse `Intro` cuando haya terminado.



Políticas - Protección de almacenamiento - ICAP

7.3. Políticas de dispositivos móviles

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. Seleccione **Dispositivos móviles** desde el selector de vistas.
3. Haga clic en el nombre de la política. Esto abrirá la página de configuración de políticas.
4. Configure las opciones de la política según sea necesario. Los ajustes se organizan en las siguientes categorías:
   - General
     - Detalles
   - Gestión del dispositivo
     - Seguridad
     - Contraseña

- Perfiles

Puede seleccionar la categoría de configuración usando el menú del lado izquierdo de la página.

5. Haga clic en **Guardar** para guardar los cambios y aplicarlos a los dispositivos móviles objetivos. Para abandonar la página de política sin guardar los cambios, haga clic en **Cancelar**.

7.3.1. General

La categoría **General** contiene información descriptiva con respecto a la política seleccionada.

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.

Puede renombrar la política escribiendo el nombre nuevo en el campo correspondiente. 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.

7.3.2. Gestión del dispositivo

Los ajustes de administración de dispositivos permiten definir las opciones de seguridad para dispositivos móviles, el bloqueo de pantalla mediante contraseña y también varios perfiles para cada política de dispositivo móvil.

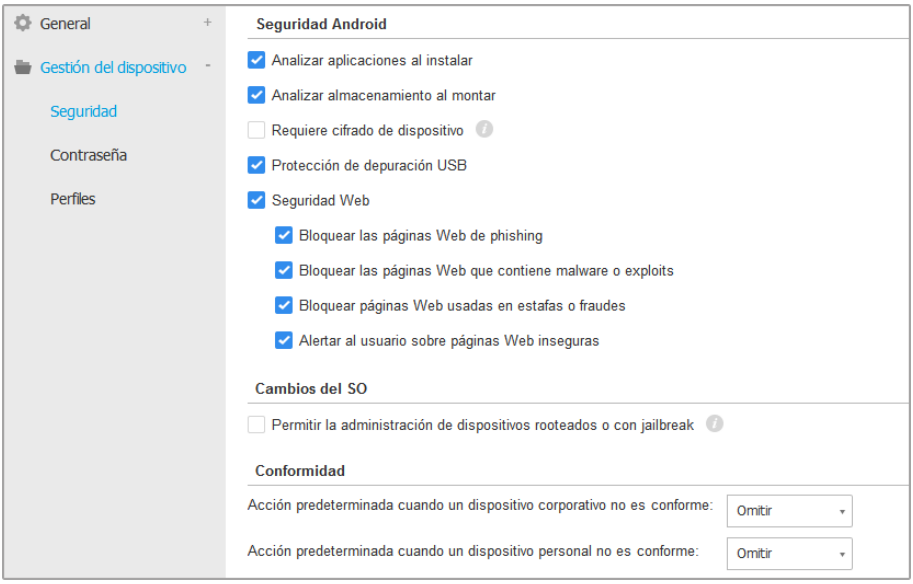
Los ajustes se organizan en las siguientes categorías:

- Seguridad
- Contraseña
- Perfiles

Seguridad

En esta sección puede configurar varios ajustes de seguridad para dispositivos móviles, incluyendo análisis antimalware para dispositivos Android, la administración de dispositivos rooteados o con jailbreak o la acción a llevar a cabo en dispositivos no conformes.

Importante
El análisis antimalware se ejecuta en la nube; por lo que los dispositivos móviles deben tener conexión a Internet.



Políticas de dispositivos móviles - Ajustes de seguridad

Seguridad Android

- Seleccione **Analizar aplicaciones al instalarse** si quiere realizar un análisis cuando se instalan nuevas aplicaciones en los dispositivos móviles administrados.
- Seleccione **Analizar almacenamiento al montarse** si quiere realizar un análisis de cada dispositivo de almacenamiento cuando se monta.

Aviso

Si se encuentra malware se pide al usuario que lo elimine. Si el usuario no elimina el malware detectado en un plazo de una hora tras la detección, el dispositivo móvil es declarado como no conforme y se le aplican automáticamente acciones para dispositivos no conformes (Ignorar, Denegar acceso, Bloquear, Borrar o Desvincular).

- Seleccione **Requiere cifrado de dispositivo** para pedir al usuario que active la opción de cifrado disponible en el sistema operativo Android. El cifrado protege los datos almacenados en dispositivos Android, incluyendo cuentas, ajustes, aplicaciones descargadas, archivos multimedia y otros archivos, frente a accesos no autorizados. Los datos cifrados solo son accesibles desde dispositivos externos proporcionando la contraseña de desbloqueo.

  Importante

  – El cifrado de dispositivo está disponible para Android 3.0 y posterior. No todos los modelos de dispositivo soportan el cifrado. Consulte la ventana de **Detalles del dispositivo móvil** para obtener información sobre el soporte del cifrado.

  – El cifrado puede afectar al rendimiento del dispositivo.

  Aviso

  – El cifrado del dispositivo es irreversible y la única manera de revertirlo al estado no cifrado es borrar el dispositivo.

  – Los usuarios deberían hacer copia de seguridad de sus datos antes de activar el cifrado del dispositivo.

  – Los usuarios no deben interrumpir el proceso de cifrado pues podrían perder algunos o todos sus datos.

  Si habilita esta opción, GravityZone Mobile Client muestra un mensaje que informa al usuario de que active el cifrado. El usuario debe tocar el botón **Resolver** para pasar a la pantalla de cifrado e iniciar el proceso. Si en siete días a partir de la notificación no se ha activado el cifrado, el dispositivo se considerará no conforme.

  Para habilitar el cifrado en un dispositivo Android:

  – La batería debe estar cargada por encima del 80%.

  – El dispositivo debe estar conectado hasta que se haya completado el cifrado.

– El usuario debe establecer una contraseña de desbloqueo que se ajuste a los requisitos de complejidad.

Nota

- Los dispositivos Android usan la misma contraseña para desbloquear la pantalla que para desbloquear el contenido cifrado.
- El cifrado requiere contraseña, PIN o reconocimiento facial para desbloquear el dispositivo, anulando los otros ajustes de bloqueo de pantalla.

El proceso de cifrado puede llevar una hora o más, tiempo durante el cual el dispositivo podría reiniciarse varias veces.

Puede comprobar el estado de cifrado de almacenamiento para cada dispositivo móvil en la ventana **Detalles del dispositivo móvil**.

- Los dispositivos Android en modo de depuración USB se pueden conectar a un PC mediante un cable USB, lo que permite un control avanzado sobre sus apps y su sistema operativo. En este caso, la seguridad de los dispositivos móviles puede estar en riesgo. La opción de **Protección de depuración USB**, activada por defecto, evita el uso de dispositivos en el modo de depuración USB. Si el usuario activa la depuración USB, el dispositivo pasa a ser automáticamente no conforme y se adopta la acción de falta de conformidad. Si la acción de falta de conformidad es **Ignorar**, se advierte al usuario acerca del ajuste inseguro.

  No obstante, puede desactivar esta opción para los dispositivos móviles que requieran trabajar en el modo de depuración USB (como por ejemplo los dispositivos móviles utilizados para desarrollar y probar aplicaciones móviles).

- Seleccione **Seguridad Web** para activar las características de seguridad Web en dispositivos Android.

  La Seguridad Web analiza en la nube todas las URL a las que se accede, respondiendo a GravityZone Mobile Client con un estado de seguridad. El estado de seguridad de la URL puede ser: limpio, fraude, malware, phishing o no fiable.

  GravityZone Mobile Client puede llevar a cabo una acción específica basándose en el estado de seguridad de la URL:

  – **Bloquear las páginas Web de phishing**. Cuando el usuario intenta acceder a un sitio Web de phishing, GravityZone Mobile Client bloquea la URL correspondiente, mostrando en su lugar una página de advertencia.

- **Bloquear las páginas Web que contiene malware o exploits**. Cuando el usuario intenta acceder a un sitio Web que difunde malware o exploits, GravityZone Mobile Client bloquea la URL correspondiente, mostrando en su lugar una página de advertencia.
- **Bloquear páginas Web usadas en estafas o fraudes**. Amplía la protección a otro tipo de fraudes además del phishing (por ejemplo, sitios de garantía falsos, falsas donaciones, amenazas para redes sociales, etc.). Cuando el usuario intenta acceder a una página Web fraudulenta, GravityZone Mobile Client bloquea la URL correspondiente, mostrando en su lugar una página de advertencia.
- **Alertar al usuario sobre páginas Web inseguras**. Cuando el usuario está accediendo a un sitio Web que sufrió anteriormente un ataque de hackers con ánimo de phishing o recientemente promovido por e-mails de phishing o spam, se mostrará una ventana con un mensaje de advertencia, sin bloquearse la página Web.

Importante
Las características de Seguridad web funcionan únicamente hasta Android 5 y solo con Chrome y con el navegador de Android incorporado.

Cambios del SO

Considerados como un riesgo de seguridad para las redes corporativas, los dispositivos rooteados o con jailbreak son declarados automáticamente no conformes.

- Seleccione **Permitir la administración de dispositivos rooteados o con jailbreak** si quiere administrar desde el Control Center dispositivos que hayan sido rooteados o se les haya aplicado un jailbreak. Tenga en cuenta que dado que esos dispositivos no son conformes de forma predeterminada, se les aplica automáticamente la acción no conforme tan pronto como son detectados. Por ello, para poder aplicarles la configuración de la política de seguridad, debe ajustarse la acción de no conformidad como Ignorar.
- Si desmarca la casilla de verificación **Permitir administración de dispositivos rooteados / jailbreak**, desvincula automáticamente estos dispositivos de la red de GravityZone. En este caso, la aplicación GravityZone Mobile Client presenta un mensaje indicando que el dispositivo está rooteado o con jailbreak. El usuario puede tocar el botón Aceptar, que redirige a la pantalla de registro. Una vez que

el dispositivo deja de estar rooteado o con jailbreak, o si la política permite la gestión de dispositivos rooteados o con jailbreak, puede reinscribirse (con el mismo token para dispositivos Android o con uno nuevo para dispositivos iOS).

Conformidad

Puede configurar acciones específicas a adoptar automáticamente con dispositivos que se detecten como no conformes basándose en la propiedad del dispositivo (empresa o personal).

Nota
Al añadir un nuevo dispositivo en Control Center se le solicita que especifique la propiedad del dispositivo (empresa o personal). Esto permitirá a GravityZone gestionar dispositivos móviles personales o de empresa por separado.

- Criterios de no conformidad
- Acciones para no conformes

Criterios de no conformidad

Un dispositivo es declarado como no conforme en las siguientes situaciones:

- **Dispositivos Android**
  - El dispositivo está rooteado.
  - GravityZone Mobile Client ya no es el administrador de dispositivos.
  - No se ha eliminado el malware tras una hora de su detección.
  - No se satisface una política:
    - El usuario no establece la contraseña de bloqueo de pantalla dentro de las 24 horas siguientes a la primera notificación.
    - El usuario no cambia la contraseña de bloqueo de pantalla en el momento especificado.
    - El usuario no activa el cifrado de dispositivo en siete días a partir de la primera notificación.
    - El modo de depuración USB está activado en el dispositivo mientras que la opción de política de Protección de depuración USB está activada.
- **Dispositivos iOS**
  - El dispositivo tiene jailbreak.

- Se ha desinstalado GravityZone Mobile Client del dispositivo móvil.
- No se satisface una política:
  - El usuario no establece la contraseña de bloqueo de pantalla dentro de las 24 horas siguientes a la primera notificación.
  - El usuario no cambia la contraseña de bloqueo de pantalla en el momento especificado.

Acción predeterminada cuando un dispositivo no es conforme

Cuando se declara no conforme un dispositivo, se pide al usuario que resuelva los problemas de disconformidad. El usuario debe hacer los cambios requeridos en un periodo de tiempo específico, de lo contrario se aplicará la acción seleccionada para los dispositivos no conformes (Ignorar, Denegar acceso, Bloquear, Borrar o Desvincular).

Puede cambiar la acción para los dispositivos no conformes en la política en cualquier momento. La nueva acción se aplica a dispositivos no conformes una vez se ha guardado la política.

Seleccione en el menú correspondiente a cada tipo de propiedad de dispositivo la acción a adoptar cuando un dispositivo se declare no conforme:

- **Ignorar**. Sólo se notifica al usuario que el dispositivo no cumple con la política de utilización de los dispositivos móviles.
- **Denegar acceso**. Bloquea el acceso del dispositivo a las redes corporativas borrando los ajustes Wi-Fi y VPN, pero manteniendo todos los demás ajustes definidos en la política. Los ajustes bloqueados se restauran tan pronto como el dispositivo se vuelve conforme.

  Importante
  Cuando el Administrador de dispositivos se desactiva para GravityZone Mobile Client, el dispositivo pasa a ser no conforme y se le aplica automáticamente la acción de **Denegar acceso**.

- **Bloquear**. Se bloquea inmediatamente la pantalla del dispositivo.
  - En Android, la pantalla se bloquea con una contraseña generada por GravityZone solo si no se ha configurado una protección de bloqueo en el dispositivo. Esto no anulará una opción de bloqueo de pantalla ya configurada, como Patrón, PIN, Contraseña, Huella dactilar o Smart Lock.

- Si el dispositivo, en iOS, posee una contraseña de bloqueo de la pantalla, se solicita para desbloquearlo.

- **Borrar**. Restaura los ajustes de fábrica del dispositivo móvil, borrando permanentemente todos los datos de usuario.

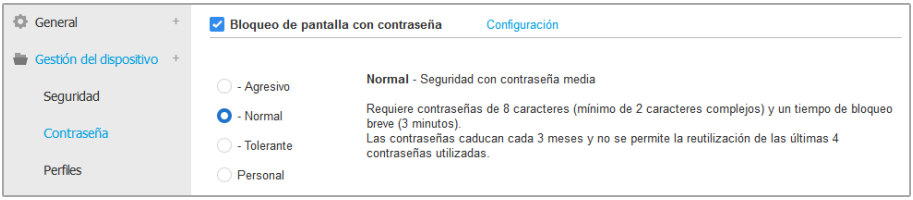
  Nota
  El borrado no elimina actualmente los datos desde los dispositivos montados (tarjetas SD).

- **Desvincular**. El dispositivo se elimina inmediatamente de la red.

  Nota
  Para reinscribir un dispositivo móvil al que se le ha aplicado la acción Desvincular, debe añadir el dispositivo otra vez desde el Centro de control. El dispositivo debe registrarse nuevamente con el nuevo token de activación. Antes de reinscribir el dispositivo, asegúrese de que ya no se dan las condiciones que llevaron a la desvinculación del dispositivo, o cambie la configuración de políticas para permitir la gestión del mismo.

Contraseña

En esta sección puede elegir activar la característica de bloqueo de pantalla con contraseña disponible en los dispositivos móviles iOS.



Políticas de dispositivos móviles - Ajustes de protección por contraseña

Una vez activada esta característica, se muestra al usuario una notificación en pantalla para definir una contraseña de bloqueo de pantalla. El usuario debe introducir una contraseña que sea conforme con el criterio de creación de contraseñas definido en la política. Una vez que el usuario ha establecido la contraseña, se borran todas las notificaciones relativas a este asunto. Se muestra un mensaje pidiendo la contraseña cada vez que se intenta desbloquear la pantalla.

Nota

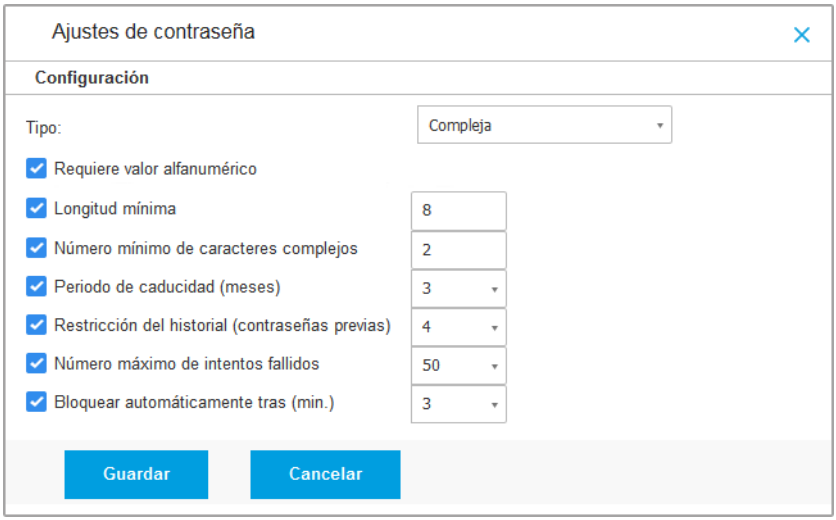
Si el usuario no establece una contraseña cuando se le solicita, el dispositivo puede utilizarse sin contraseña de bloqueo durante 24 horas tras la primera notificación. Durante este tiempo, un mensaje pide al usuario cada 15 minutos que introduzca una contraseña de bloqueo de pantalla.

Aviso

Si el usuario no establece una contraseña dentro de las 24 horas posteriores a la primera notificación, el dispositivo móvil ya no es conforme y se le aplica la acción seleccionada para dispositivos no conformes.

Para configurar los ajustes de la contraseña de bloqueo de pantalla:

1. Marque la casilla de verificación **Bloqueo de pantalla con contraseña**.
2. Haga clic en el nivel de contraseña 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.
3. Para la configuración avanzada, seleccione el nivel de protección **Personalizado** y, a continuación, haga clic en el enlace **Ajustes**.



Políticas de dispositivos móviles - Ajustes avanzados de protección por contraseña

Nota

Para ver los requisitos para la configuración de la contraseña de un nivel de seguridad predefinido, seleccione ese nivel y haga clic en el enlace **Opciones**. Si modifica cualquier opción, el nivel de seguridad de la contraseña cambiará automáticamente a **Personalizado**.

Opciones de personalización.

- **Tipo**. Puede requerir que la contraseña sea Simple o Compleja. El criterio de complejidad de la contraseña se define dentro del SO del dispositivo móvil.
  - En los dispositivos Android, las contraseñas complejas deben contener al menos una letra, un número y un carácter especial.

    Nota
    Android 3.0 y posterior soportan contraseñas complejas.

  - En los dispositivos iOS, las contraseñas complejas no permiten caracteres consecutivos ni caracteres repetidos (como abcdef, 12345 o aaaaa, 11111).

  Dependiendo de la opción seleccionada, cuando el usuario establece la contraseña de bloqueo de pantalla, el sistema operativo comprueba y avisa al usuario si no se cumplen los criterios requeridos.
- **Requerir valores alfanuméricos**. Requiera que la contraseña contenga tanto letras como números.
- **Longitud mínima**. Requerir que la contraseña contenga un número mínimo de caracteres, que puede especificar en el campo correspondiente.
- **Número mínimo de caracteres complejos**. Requerir que la contraseña contenga un número mínimo de caracteres no alfanuméricos (como @, # o $), que puede especificar en el campo correspondiente.
- **Periodo de caducidad (meses)**. Forzar al usuario a cambiar la contraseña de bloqueo de pantalla en un intervalo de tiempo determinado (en meses). Por ejemplo, si introduce 3, se le solicitará al usuario que cambie la contraseña de bloqueo de pantalla cada tres meses.

  Nota
  En Android, esta característica sólo se soporta en la versión 3.0 o posterior.

- **Restricción del historial (contraseñas previas)** Seleccione o introduzca un valor en el campo correspondiente para especificar el número de contraseñas anteriores que no pueden reutilizarse. Por ejemplo, si introduce 4, el usuario no podrá reutilizar una contraseña que coincida con alguna de las cuatro últimas utilizadas.

  Nota
  En Android, esta característica sólo se soporta en la versión 3.0 o posterior.

- **Número máximo de intentos fallidos**. Especifique cuántas veces se le permite al usuario introducir una contraseña incorrecta.

  Nota
  Cuando este número sea mayor que 6 en dispositivos iOS: tras seis intentos fallidos, se penaliza con un retardo temporal antes de que el usuario pueda introducir de nuevo la contraseña. El retardo temporal se incrementa con cada intento fallido.

  Aviso
  Si el usuario supera el número máximo de intentos fallidos para desbloquear la pantalla, se borrará el dispositivo (todos los datos y configuraciones serán eliminadas).

- **Bloquear automáticamente tras (min.)**. Establezca el periodo de inactividad (en minutos) tras el cual se bloquea automáticamente el dispositivo.

  Nota
  Los dispositivos iOS tienen una lista predefinida de tiempo de bloqueo automático y no admiten valores personalizados. Al asignar una política con un valor de bloqueo automático no compatible, el dispositivo hace cumplir el siguiente período de tiempo más restrictivo disponible en la lista. Por ejemplo, si la política fija el bloqueo automático a los tres minutos, el dispositivo se bloqueará automáticamente tras dos minutos de inactividad.

Cuando modifica la política, si elige un nivel de seguridad más alto para la contraseña de bloqueo de pantalla, se pedirá a los usuarios que cambien la contraseña según los nuevos criterios.

Si desactiva la opción **Bloqueo de pantalla con contraseña**, los usuarios volverán a conseguir acceso completo a los ajustes de bloqueo de pantalla en sus dispositivo

móvil. La contraseña existente permanece activa hasta que los usuarios decidan cambiarla o eliminarla.

Perfiles

En esta sección puede crear, modificar y borrar los perfiles de utilización para los dispositivos móviles. Los perfiles de utilización le ayudan a aplicar ajustes Wi-Fi y VPN, y reforzar el control de acceso Web en los dispositivos móviles administrados.

Políticas de dispositivos móviles - Plantillas de perfiles

Puede configurar una o varias políticas, pero sólo puede activarse una a la vez en un dispositivo.

- Si configura solamente un perfil, ese perfil se aplica automáticamente a todos los dispositivos a los que se asigna la política.
- Si configura varios perfiles, el primero en la lista se aplica automáticamente a todos los dispositivos a los que se asigna la política.

Los usuarios de dispositivos móviles pueden ver los perfiles asignados y los ajustes configurados para cada perfil en la aplicación GravityZone Mobile Client. Los usuarios no pueden modificar los ajustes existentes en un perfil, pero pueden cambiar entre perfiles si hay varios disponibles.

Nota
El cambio entre perfiles requiere conexión a Internet.

Para crear un nuevo perfil:

1. Haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla. Se muestra la página de configuración del perfil.
2. Configure los ajustes del perfil según sea necesario. Para obtener más información detallada, consulte:

- “Detalles” (p. 411)
- “Redes” (p. 411)
- “Acceso Web” (p. 415)

3. Haga clic en **Guardar**. El nuevo perfil se añade a la lista.

Para eliminar uno o varios perfiles, seleccione sus casillas de verificación correspondientes, y haga clic en el botón ⊖ **Borrar** del lateral derecho de la tabla.

Para modificar un perfil, haga clic en su nombre, cambie los ajustes según sea necesario y haga clic en **Guardar**.

Detalles

La página **Detalles** contiene información general con respecto al perfil:

- **Nombre**. Escriba el nombre del perfil deseado. Los perfiles deberían tener nombres descriptivos de forma que usted u otro administrador pueda identificarlos rápidamente.
- **Descripción**. Escriba una descripción detallada del perfil. Esta opción puede ayudar a los administradores a identificar rápidamente un perfil entre otros.

Redes

En esta sección puede especificar la configuración de una o varias redes Wi-Fi y VPN. La configuración VPN está disponible sólo para dispositivos iOS.

Políticas de dispositivos móviles - Ajustes de conexión de redes del perfil

Importante
Antes de definir las conexiones Wi-Fi y VPN, asegúrese de que tiene toda la información necesaria a mano (contraseñas, configuración del proxy, etc.).

Los dispositivos móviles asignados con el perfil correspondiente se conectan automáticamente a la red definida, cuando está dentro del alcance. Puede definir la prioridad cuando se crean varias redes, teniendo en cuenta que sólo puede usarse una red a la vez. Cuando no esté disponible la primera red, el dispositivo móvil conectará con una segunda, y así sucesivamente.

Para establecer la prioridad de redes:

1. Marque la casilla de verificación de la red deseada.
2. Use los botones de prioridad del lateral derecho de la tabla:
   - Haga clic en el botón **Arriba** para promocionar la red seleccionada.
   - Haga clic en el botón **Abajo** para degradarla.

- **Wi-Fi**

  Puede añadir tantas redes Wi-Fi como necesite. Para añadir una red Wi-Fi:

  1. En la sección **Wi-Fi**, haga clic en el botón **Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
  2. Bajo la pestaña **General** puede configurar los detalles de la conexión Wi-Fi:
     - **Nombre (SSID)**. Introduzca el nombre de la nueva red Wi-Fi.
     - **Seguridad**. Seleccione la opción correspondiente para el nivel de seguridad de red Wi-Fi:
       - **Ninguna**. Elija esta opción cuando la conexión Wi-Fi es pública (no se necesitan credenciales).
       - **WEP**. Elija esta opción para establecer una conexión Wireless Encryption Protocol (WEP). Escriba la contraseña requerida para este tipo de conexión en el campo correspondiente mostrado más abajo.
       - **WPA/WPA2 Personal**. Elija esta opción si la red Wi-Fi se asegura usando Wi-Fi Protected Access (WPA). Escriba la contraseña requerida para este tipo de conexión en el campo correspondiente mostrado más abajo.
  3. En **TCP/IP** puede configurar los ajustes TCP/IP para la conexión Wi-Fi. Cada conexión Wi-Fi puede usar IPv4, IPv6 o ambos.

- **Configure IPv4**. Si quiere usar el método IPv4, seleccione el método de asignación de IP desde el menú correspondiente:

  DHCP: si un servidor DHCP asigna automáticamente la dirección IP. Si es necesario, proporcione el ID de Cliente DHCP en el siguiente campo.

  Desactivado: seleccione esta opción si no quiere usar el protocolo IPv4.

- **Configurar IPv6**. Si quiere usar el método IPv6, seleccione el método de asignación de IP desde el menú correspondiente:

  DHCP: si un servidor DHCP asigna automáticamente la dirección IP.

  Desactivado: seleccione esta opción si no quiere usar el protocolo IPv6.

- **Servidores DNS**. Escriba la dirección de al menos un servidor DNS de la red.

4. Bajo la pestaña **Proxy**, configure los ajustes del proxy para la conexión Wi-Fi. Seleccione el método de configuración del proxy desde el menú **Tipo**:
   - **Desactivado**. Elija esta opción si la red Wi-Fi no tiene configuración proxy.
   - **Manual**. Elija esta opción para especificar la configuración proxy manualmente. Escriba el nombre del host del servidor proxy y el puerto en el que escucha conexiones. Si el servidor proxy requiere autenticación, marque la casilla de verificación **Autenticación** y proporcione el nombre de usuario y la contraseña en los campos siguientes.
   - **Automática**. Seleccione esta opción para recuperar la configuración del proxy desde el archivo Proxy Auto-Configuration (PAC) publicado en la red local. Escriba la dirección del archivo PAC en el campo **URL**.
5. Haga clic en **Guardar**. La nueva conexión Wi-Fi se añade a la lista.

- **VPN para iOS**

  Puede añadir tantas VPNs como necesite. Para añadir una VPN:

  1. En la sección **VPN para iOS**, haga clic en el botón ⊕ **Añadir** del lateral derecho de la tabla. Se muestra una ventana de configuración.
  2. Defina los ajustes VPN en la ventana **Conexión VPN**:

     General:

     - **Nombre**. Introduzca el nombre de la conexión VPN.

- **Cifrado**. El protocolo de autenticación disponible para este tipo de conexión es **IPSec**, que requiere autenticación del usuario por contraseña y autenticación de la máquina por clave secreta compartida.
- **Servidor**. Escriba la dirección del servidor VPN.
- **Usuario**. Escriba el nombre de usuario VPN.
- **Contraseña**. Escriba la contraseña VPN.
- **Nombre del grupo**. Escriba el nombre del grupo.
- **Secreto**. Escriba la clave compartida.

Proxy:

En esta sección puede configurar los ajustes del proxy para la conexión VPN. Seleccione el método de configuración del proxy desde el menú **Tipo**:

- **Desactivado**. Elija esta opción si la conexión VPN no tiene configuración proxy.
- **Manual**. Esta opción le permite especificar manualmente la configuración proxy:
  - **Servidor**: Escriba el nombre del host del proxy.
  - **Puerto**: escriba el nombre del puerto del proxy.
  - Si el servidor proxy requiere autenticación, marque la casilla de verificación **Autenticación** y proporcione el nombre de usuario y la contraseña en los campos siguientes.
- **Automática**. Seleccione esta opción para recuperar la configuración del proxy desde el archivo Proxy Auto-Configuration (PAC) publicado en la red local. Escriba la dirección del archivo PAC en el campo **URL**.

3. Haga clic en **Guardar**. La nueva conexión VPN se añadirá a la lista.

Para eliminar uno o varias redes, marque sus casillas de verificación correspondientes, y haga clic en el botón ⊖ **Borrar** del lateral derecho de la tabla.

Para modificar una red, haga clic en su nombre, cambie los ajustes según sea necesario y haga clic en **Guardar**.

Acceso Web

En esta sección puede configurar el Control de acceso Web para dispositivos Android e iOS.

Políticas de dispositivos móviles - Ajustes de acceso Web del perfil

- **Control de Acceso Web para Android.** Active esta opción para filtrar el acceso web para Chrome y para el navegador Android incorporado. Puede establecer restricciones de tiempo en el acceso Web y también bloquear o permitir explícitamente el acceso a páginas Web específicas. Las páginas Web bloqueadas por el Control de acceso no se muestran en el navegador. En su lugar, se muestra una página Web predeterminada informando al usuario de que el Control de acceso Web ha bloqueado la página Web solicitada.

  Importante
  El Control de acceso web para Android funciona únicamente hasta Android 5 y solo con Chrome y con el navegador de Android incorporado.

  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.

Políticas de dispositivos móviles - Programador para acceso Web

   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**.

Reglas Web

También puede definir reglas Web para bloquear o permitir explícitamente ciertas direcciones Web, anulando los ajustes del Control de acceso Web

existentes. Así, por ejemplo, los usuarios podrán acceder a páginas Web específicas incluso cuando la navegación Web esté bloqueada por el Control de acceso 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**.

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
`www.ejemplo*`	Cualquier sitio Web o página Web que comience por `www.ejemplo` (sin importar la extensión del dominio). La regla no se aplicará a subdominios del sitio Web especificado, tales como `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.
`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`.

- **Control de Acceso Web para iOS.** Active esta opción para administrar de forma centralizada los ajustes del navegador incorporado de iOS (Safari). Los usuarios de dispositivos móviles ya no podrán cambiar los ajustes correspondientes en su dispositivo.
  - **Permitir el uso de Safari**. Esta opción le ayuda a controlar el uso del navegador Safari en dispositivos móviles. Desactivar la opción elimina el acceso directo de Safari de la interfaz de iOS, evitando de este modo que los usuarios accedan a Internet a través de Safari.
  - **Activar autocompletar**. Desactive esta opción si quiere evitar que el navegador almacene entradas de formulario que pueden incluir información sensible.

- **Forzar advertencia de fraude**. Seleccione esta opción para garantizar que los usuarios son advertidos cuando acceden a páginas Web fraudulentas.
- **Activar Javascript**. Desactive esta opción si quiere que Safari ignore javascript en los sitios Web.
- **Bloquear ventanas emergentes**. Seleccione esta opción para evitar que se abran ventanas emergentes automáticamente.
- **Aceptar cookies**. Safari permite el uso de cookies de forma predeterminada. Desactive esta opción si quiere evitar que los sitios Web almacenen información de navegación.

Importante
El Control de acceso web para iOS no es compatible con iOS 13.

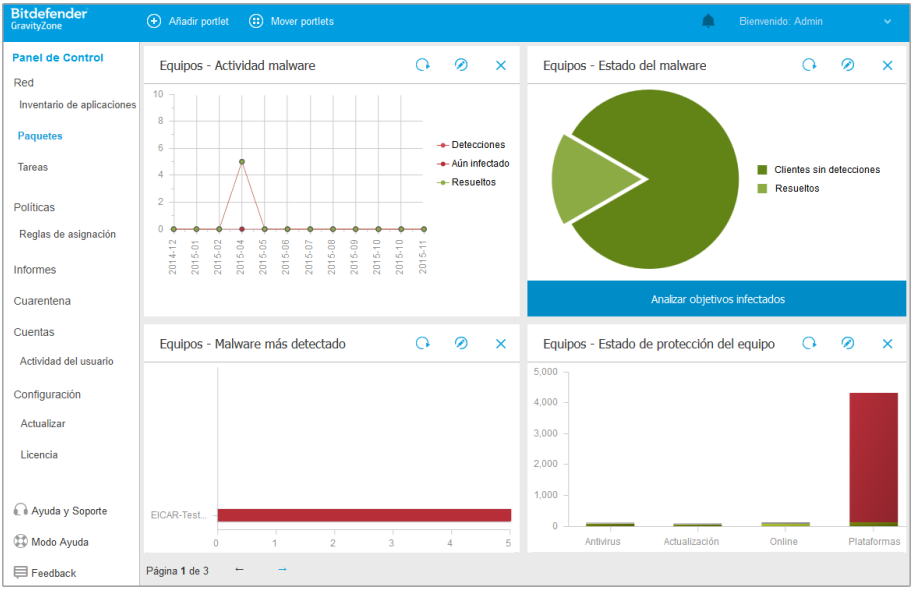
8. PANEL DE MONITORIZACIÓN

El análisis adecuado de la seguridad de su red requiere accesibilidad y correlación de datos. Tener información de seguridad centralizada le permite monitorizar y garantizar el cumplimiento de las políticas de seguridad de la organización, identificar rápidamente los problemas y analizar las amenazas y vulnerabilidades.

8.1. Panel de Control

El panel de control Control Center es una visualización personalizable que proporciona un resumen de seguridad rápido de todos los endpoints protegidos y del estado de la red.

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 endpoints, como el estado de actualización, el de malware y la actividad del cortafuego.

  Nota
  Por defecto, los portlets muestran datos del día de hoy y, a diferencia de los informes, no se pueden configurar para intervalos de más de un mes.

- La información que se muestra en los portlets se refiere solo a los endpoints de su cuenta. Puede personalizar el objetivo de cada portlet y las preferencias 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 la barra de desplazamiento vertical o las teclas de flecha arriba y abajo para navegar entre los grupos de portlets.
- En varios tipos de informes, tiene la opción de ejecutar de inmediato determinadas tareas en endpoints objetivo, sin tener que ir a la página **Red** para ejecutar la tarea (por ejemplo, analizar endpoints infectados o actualizar endpoints). Utilice el botón de la zona inferior del portlet para llevar a cabo la acción disponible.

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.

8.1.1. Actualización de los datos del portlet

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

Para actualizar la información de todos los portlets a la vez, haga clic en el botón **Actualizar portlets** de la zona superior del panel de control.

8.1.2. 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.

8.1.3. Añadir un nuevo portlet

Puede añadir otros portlets para obtener la información que necesita.

Para añadir un nuevo portlet:

1. Vaya a la página **Panel**.
2. Haga clic en el botón **Añadir** de la parte superior de la consola. Se muestra la ventana de configuración.
3. En la pestaña **Detalles**, configure los detalles del portlet:
   - Tipo de endpoint (**Equipos**, **Máquinas virtuales** o **Dispositivos móviles**)
   - Tipo de informe explicativo
   - Nombre de portlet descriptivo
   - El intervalo de tiempo para informar de los eventos

   Para obtener más información sobre los tipos de informe disponibles, consulte "Tipos de informes" (p. 423).
4. En la pestaña **Objetivos**, seleccione los objetos de red y grupos a incluir.
5. Haga clic en **Guardar**.

8.1.4. 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.

8.1.5. 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. Arrastre y suelte cada portlet en la posición deseada. Todos los demás portlets entre las posiciones de los nuevos y los viejos se mueven para conservar su orden.

> **Nota**
> Solo puede mover los portlets en las posiciones ya ocupadas.

9. 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.
- 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).

Algunos informes también le permiten solucionar rápidamente los problemas encontrados en su red. Por ejemplo, puede actualizar sin esfuerzo todos los objetos de red objetivo desde el informe, sin tener que acceder a la página **Red** y ejecutar una tarea de actualización desde la misma.

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).

9.1. Tipos de informes

Para cada tipo de endpoint hay disponibles distintos tipos de informe:

- Informes de equipos y máquinas virtuales

- Informes de Exchange
- Informes de Dispositivos móviles

9.1.1. Informes de equipos y máquinas virtuales

Estos son los tipos de informe disponibles para máquinas físicas y virtuales:

Actividad antiphishing

Le informa sobre la actividad del módulo Antiphishing de Bitdefender Endpoint Security Tools. Puede ver el número de sitios Web de phishing bloqueados en los endpoints seleccionados y el usuario que había iniciado sesión en el momento de la última detección. Al hacer clic en los enlaces de la columna **sitios Web bloqueados**, también puede ver las URLs de los sitios Web, cuántas veces fueron bloqueados y cuando se produjo el último evento de bloqueo.

Aplicaciones Bloqueadas

Le informa sobre la actividad de los siguientes módulos: Antimalware, Cortafuego, Control de contenidos, Control de aplicaciones, Antiexploit avanzado, ATC/IDS y HVI. Puede ver el número de aplicaciones bloqueadas en los endpoints seleccionados y el usuario que había iniciado sesión en el momento de la última detección.

Haga clic en el número asociado a un objetivo para ver información adicional sobre las aplicaciones bloqueadas, el número de eventos acaecidos, y la fecha y hora del último evento de bloqueo.

En este informe, puede indicar rápidamente a los módulos de protección que permitan la ejecución de la aplicación seleccionada en el endpoint objetivo:

- Haga clic en el botón **Añadir excepción** para definir excepciones en los siguientes módulos: Antimalware, ATC, Control de contenidos, Cortafuego y HVI. Aparecerá una ventana de confirmación que le informará de la nueva regla que modificará la política existente para ese endpoint concreto.
- Haga clic en el botón **Añadir regla** para definir una regla para una aplicación o un proceso en el Control de aplicaciones. En la ventana de configuración, aplique la regla a una política existente. Un mensaje le informará de la nueva regla que modificará la política asignada a ese endpoint concreto. El informe también muestra el número de intentos de acceso y si el módulo se ejecutó en modo de prueba o de producción.

Páginas Web Bloqueadas

Le informa sobre la actividad del módulo de Control de acceso Web de Bitdefender Endpoint Security Tools. Para cada objetivo, puede ver el número de sitios Web bloqueados. Haciendo clic en este número puede consultar información adicional, como por ejemplo:

- URL del sitio Web y categoría.
- Número de intentos de acceso por sitio Web.
- Fecha y hora del último intento, además del usuario que había iniciado sesión en el momento de la última detección.
- Motivo del bloqueo, que incluye acceso programado, detección de malware, filtrado de categorías y listas negras.

Protección de datos

Le informa sobre la actividad del módulo de Protección de datos de Bitdefender Endpoint Security Tools. Puede ver el número de sitios Web y mensajes de correo electrónico bloqueados en los endpoints seleccionados, así como el usuario que había iniciado sesión en el momento de la última detección.

Actividad de control de dispositivos

Le informa sobre los eventos acontecidos al acceder a los endpoints a través de los dispositivos monitorizados. Por cada endpoint objetivo, puede ver el número de eventos de solo lectura y accesos permitidos/bloqueados. Si se han producido eventos, tiene a su disposición información adicional haciendo clic en los números correspondientes. La información se refiere a:

- Usuario que ha iniciado sesión en la máquina.
- Tipo de dispositivo e ID.
- Proveedor del dispositivos e ID del producto.
- Fecha y hora del evento.

Estado de cifrado de endpoints

Le proporciona datos relativos al estado de cifrado de los endpoints. Un gráfico circular muestra el número de máquinas que cumplen y que no cumplen los ajustes de la política de cifrado.

Una tabla debajo del gráfico circular proporciona datos como por ejemplo:

- Nombre del endpoint.
- Nombre de dominio completo (FQDN).

- IP de la máquina.
- Sistema operativo.
- Cumplimiento de política del dispositivo:
  - **Cumple**: Cuando los volúmenes están cifrados o no cifrados de acuerdo con la política.
  - **No cumple**: Cuando el estado de los volúmenes no coincide con la política asignada (por ejemplo, solo está cifrado uno de los dos volúmenes, o hay un proceso de cifrado en curso en ese volumen).
- Política del dispositivo (**Cifrar** o **Descifrar**).
- Haga clic en los números de la columna Resumen de volúmenes para ver información sobre los volúmenes de cada endpoint: ID, nombre, estado de cifrado (**Cifrado** o **Descifrado**), incidencias, tipo (**Arranque** o **Sin arranque**), tamaño e ID de clave de recuperación.

Estado de los módulos de endpoint

Proporciona una visión de conjunto de la cobertura de los módulos de protección en los objetivos seleccionados. En los detalles del informe, para cada endpoint objetivo, podrá ver qué módulos están activos, desactivados o no instalados, y el motor de análisis en uso. Al hacer clic en el nombre del endpoint se mostrará la ventana **Información** con los datos del endpoint y las capas de protección instaladas.

Al hacer clic en el botón **Reconfigurar el cliente**, puede iniciar una tarea para cambiar los ajustes iniciales de uno o varios endpoints seleccionados. Para más información, consulte Reconfigurar el cliente.

Estado de la protección de endpoints

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

- Estado de protección antimalware
- Estado de actualización de Bitdefender Endpoint Security Tools
- 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.

Actividad Cortafuego

Le informa sobre la actividad del módulo de Cortafuego de Bitdefender Endpoint Security Tools. Puede ver el número de intentos de tráfico y análisis de puertos bloqueados en los endpoints seleccionados, así como el usuario que había iniciado sesión en el momento de la última detección.

Actividad de Hiperdetección

Le informa sobre la actividad del módulo HyperDetect de Bitdefender Endpoint Security Tools.

El gráfico de la parte superior de la página del informe muestra la dinámica de los intentos de ataque durante el período de tiempo especificado y su distribución por tipo de ataque. Al pasar el ratón sobre la leyenda se resalta el tipo de ataque asociado en el gráfico. Si se hace clic en un tipo concreto, se muestra u oculta en el gráfico la línea correspondiente. Al hacer clic en cualquier punto de una línea, se filtrarán los datos de la tabla en función del tipo seleccionado. Por ejemplo, si hace clic en cualquier punto de la línea naranja, la tabla solo mostrará los exploits.

Los datos de la parte inferior del informe le ayudan a identificar las vulneraciones de su red y saber si estas se abordaron. Se refieren a:

- La ruta al archivo malicioso o la URL detectada, en el caso de archivos infectados. Para los ataques sin archivos, se proporciona el nombre del ejecutable utilizado en el ataque, con un enlace a una ventana de información que muestra el motivo de la detección y la cadena de línea de comandos maliciosa.
- El endpoint en el que se produjo la detección
- El módulo de protección que detectó la amenaza. Como HyperDetect es una capa adicional de los módulos Antimalware y de Control de contenido, el informe proporcionará información sobre uno de estos dos módulos, dependiendo del tipo de detección.
- El tipo de ataque previsto (ataque selectivo, grayware, exploits, ransomware, archivos sospechosos y tráfico de red)
- El estado de la amenaza
- El nivel de protección del módulo en el que se detectó la amenaza (Tolerante, Normal o Agresivo)
- El número de veces que se detectó la amenaza.

- La detección más reciente.
- Identificación como ataque sin archivos (sí o no), para filtrar rápidamente las detecciones de ataques sin archivos

Nota
Un archivo puede utilizarse en varios tipos de ataques. Por lo tanto, GravityZone informa de él para cada tipo de ataque en el que estuvo implicado.

Basándose en este informe, puede resolver rápidamente los falsos positivos añadiendo excepciones en las políticas de seguridad asignadas. Para ello:

1. Seleccione tantas entradas de la tabla como precise.

   Nota
   Las detecciones de ataques sin archivos no se pueden añadir a la lista de excepciones debido a que el ejecutable detectado no es un malware en sí mismo, pero puede suponer una amenaza cuando se utiliza en una línea de comandos codificada maliciosamente.

2. Haga clic en el botón **Añadir excepción** de la zona superior de la tabla.
3. En la ventana de configuración, seleccione las políticas a las que debe añadirse la excepción y, a continuación, haga clic en **Añadir**.

   Por defecto, la información relativa a cada excepción añadida se envía a Bitdefender Labs, para contribuir a mejorar las capacidades de detección de los productos de Bitdefender. Puede controlar esta acción mediante la casilla de verificación **Enviar esta información a Bitdefender para un mejor análisis**.

Si la amenaza la detectó el módulo Antimalware, la excepción se aplicará a los modos de análisis on-access y bajo demanda.

Nota
Puede encontrar estas excepciones en las siguientes secciones de las políticas seleccionadas: **Antimalware > Ajustes** para los archivos y **Control de contenido > Tráfico** para las URL.

Estado del Malware

Le ayuda a encontrar cuántos y cuáles de los endpoints seleccionados han sido afectados por malware en un periodo de tiempo específico y cómo se han

tratado las amenazas. También puede ver el usuario que había iniciado sesión en el momento de la última detección.

Los endpoints se agrupan basándose en estos criterios:

- Endpoints sin detecciones (no se ha detectado ninguna amenaza de malware en el periodo de tiempo especificado).
- Endpoints con problemas de malware solucionados (todos los archivos detectados han sido desinfectados correctamente o movidos a la cuarentena).
- Endpoints con problemas de malware sin resolver (se ha denegado el acceso a algunos de los archivos detectados).

Por cada endpoint, 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.

En este informe, puede ejecutar rápidamente una tarea de Análisis completo en los objetivos sin resolver, con solo hacer clic en el botón **Analizar los objetivos infectados** de la barra de herramientas de acción sobre la tabla de datos.

Incidentes de red

Le informa sobre la actividad del módulo Network Attack Defense. Un gráfico muestra el número de intentos de ataque detectados durante un intervalo especificado. Los detalles del informe incluyen:

- Nombre del endpoint, IP y FQDN
- Usuario
- Nombre de detección
- Técnica de ataque
- Número de intentos
- IP del atacante
- IP objetivo y puerto
- Cuándo se bloqueó el ataque más recientemente

Al hacer clic en el botón **Añadir excepciones** para una detección seleccionada, se crea automáticamente una entrada en **Exclusiones globales** de la sección **Protección de red**.

Estado de parches de la red

Compruebe el estado de actualización del software instalado en su red. El informe revela los siguientes detalles:

- Máquina objetivo (nombre, IP y sistema operativo del endpoint).
- Parches de seguridad (parches instalados, parches fallidos, carencia de parches tanto de seguridad como ajenos a ella).
- Estado y última hora de modificación para los endpoints comprobados.

Estado de protección de la red

Proporciona información detallada sobre el estado de seguridad general de los endpoints objetivo. Por ejemplo, puede ver información sobre:

- Nombre, IP y FQDN
- Estado:
  - **Tiene problemas**: El endpoint tiene vulnerabilidades de protección (agente de seguridad sin actualizar, amenazas de seguridad detectadas, etc.).
  - **Sin problemas**: El endpoint está protegido y no hay motivos de preocupación.
  - **Desconocido**: El endpoint estaba desconectado cuando se generó el informe.
  - **No administrado**: El agente de seguridad aún no está instalado en el endpoint.
- Capas de protección disponibles
- Endpoints administrados y no administrados (el agente de seguridad está instalado o no)
- Tipo y estado de la licencia (por defecto se ocultan las columnas correspondientes a licencias adicionales)
- Estado de infección (el criterio de valoración es "limpio" o no)
- Estado de actualización del producto y de los contenidos de seguridad
- Estado de parches de seguridad de software (faltan parches, ya sean de seguridad o no)

Para los endpoints no administrados, verá el estado **No administrado** en otras columnas.

Análisis bajo demanda

Proporciona información acerca de los análisis bajo demanda realizados en los objetivos seleccionados. Un gráfico circular muestra las estadísticas de análisis correctos y fallidos. La tabla debajo del gráfico ofrece información sobre el tipo de análisis, incidente y último análisis con éxito para cada endpoint.

Cumplimiento de política

Proporciona información sobre las políticas de seguridad aplicadas en los objetivos seleccionados. Un gráfico circular muestra el estado de la política. En la tabla bajo el gráfico puede ver la política asignada a cada endpoint y el tipo de política, así como la fecha y el usuario que la asignó.

Envíos fallidos de Sandbox Analyzer

Muestra todos los envíos de objetos fallidos remitidos desde los endpoints a Sandbox Analyzer durante un período de tiempo determinado. Un envío se considera fallido después de varios reintentos.

El gráfico muestra la variación de los envíos fallidos durante el período seleccionado, mientras que en la tabla de detalles del informe es posible ver qué archivos no se pudieron enviar a Sandbox Analyzer, la máquina desde la que se envió el objeto, fecha y hora para cada reintento, el código de error devuelto, la descripción de cada reintento fallido y el nombre de la empresa.

Resultados de Sandbox Analyzer (en desuso)

Le proporciona información detallada relativa a los archivos de los endpoints objetivo que se analizaron en el espacio aislado de Sandbox Analyzer durante un período de tiempo determinado. Un gráfico de líneas muestra el número de archivos analizados limpios o peligrosos, mientras que la tabla presenta los detalles de cada caso.

Puede generar un informe de resultados de Sandbox Analyzer para todos los archivos analizados o solo para los que se han considerado maliciosos.

Puede ver:

- Veredicto del análisis, que indica si el archivo está limpio, es peligroso o desconocido (**Amenaza detectada** / **No se ha detectado ninguna amenaza** / **No admitido**). Esta columna solo aparece cuando selecciona el informe para mostrar todos los objetos analizados.

  Para ver la lista completa con los tipos de archivo y las extensiones compatibles con Sandbox Analyzer, consulte "Tipos de archivo y extensiones admitidas para el envío manual" (p. 531).

- Tipo de amenaza, como adware, rootkit, descargador, exploit, modificador de host, herramientas maliciosas, ladrón de contraseñas, ransomware, spam o troyano.
- Fecha y hora de la detección, que puede filtrar según el período del informe.
- Nombre de host o IP del endpoint en que se detectó el archivo.
- Nombre de los archivos, si se enviaron individualmente, o el número de archivos analizados en caso de que fueran en un paquete. Haga clic en el enlace del nombre del archivo o del paquete para ver la información detallada y las acciones adoptadas.
- Estado de la acción de reparación de los archivos enviados (**Parcial**, **Fallido**, **Solo se ha informado**, **Con éxito**).
- Nombre de la empresa.
- Para obtener más información sobre las propiedades del archivo analizado, haga clic en el botón **Más información** de la columna **Resultado del análisis**. Aquí puede ver información de seguridad e informes detallados sobre el comportamiento de la muestra.

Sandbox Analyzer captura los siguientes eventos de comportamiento:

- Escritura/borrado/traslado/duplicación/sustitución de archivos en el sistema y en unidades extraíbles.
- Ejecución de archivos recién creados.
- Cambios en el sistema de archivos.
- Cambios en las aplicaciones que se ejecutan dentro de la máquina virtual.
- Cambios en la barra de tareas de Windows y en el menú Inicio.
- Creación/terminación/inyección de procesos.
- Escritura/borrado de claves del registro.
- Creación de objetos mutex.
- Creación/inicio/parada/modificación/consulta/eliminación de servicios.
- Cambio de los ajustes de seguridad del navegador.
- Cambio de la configuración de visualización del Explorador de Windows.
- Adición de archivos a la lista de excepciones del cortafuego.
- Cambio de los ajustes de red.
- Activación de la ejecución en el inicio del sistema.
- Conexión a un host remoto.
- Acceso a determinados dominios.
- Transferencia de datos desde y hacia ciertos dominios.
- Acceso a URL, IP y puertos a través de varios protocolos de comunicación.
- Comprobación de los indicadores del entorno virtual.
- Comprobación de los indicadores de las herramientas de monitorización.

- Creación de instantáneas.
- Enlaces SSDT, IDT e IRP.
- Volcados de memoria para procesos sospechosos.
- Llamadas a funciones de la API de Windows.
- Inactividad durante un cierto período de tiempo para retrasar la ejecución.
- Creación de archivos con acciones que han de ejecutarse en determinados intervalos de tiempo.

En la ventana **Resultado del análisis**, haga clic en el botón **Descargar** para guardar en su equipo el Resumen de comportamiento con los siguientes formatos: XML, HTML, JSON y PDF.

Este informe seguirá proporcionándose por tiempo limitado. Se recomienda utilizar en su lugar las tarjetas de envíos para recopilar la información necesaria sobre las muestras analizadas. Las tarjetas de envíos se encuentran en la sección **Sandbox Analyzer**, en el menú principal de Control Center.

Audit. seguridad

Proporciona información sobre los eventos de seguridad que se produjeron en un objetivo seleccionado. La información se refiere a los siguientes eventos:

- Detección de malware
- Aplicación Bloqueada
- Análisis de puerto bloqueado
- Tráfico bloqueado
- Sitio web bloqueado
- Bloquear dispositivo
- Mensaje de correo electrónico bloqueado
- Proceso bloqueado
- Eventos de HVI
- Eventos de Antiexploit avanzado
- Eventos de Network Attack Defense
- Detección de ransomware

Estado del Security Server

Le ayuda a evaluar el estado de los Security Server objetivo. Puede identificar los problemas que podría tener cada Security Server con la ayuda de varios indicadores de estado, como por ejemplo:

- **Estado**: muestra el estado general del Security Server.
- **Estado de la máquina**: informa de qué appliances de Security Server están detenidos..

- **Estado AV**: indica si el módulo Antimalware está activado o desactivado..
- **Estado de actualización**: muestra si los appliances de Security Server están actualizados o si se han deshabilitado las actualizaciones.
- **Estado de carga**: indica el nivel de carga de análisis de un Security Server según se describe a continuación:
  - **Con escasa carga**, cuando se utiliza menos del 5% de su capacidad de análisis.
  - **Normal**, cuando la carga de análisis está equilibrada.
  - **Sobrecargado**, cuando la carga de análisis supera el 90% de su capacidad. En tal caso, compruebe las políticas de seguridad. Si todos los Security Server asignados en una política están sobrecargados, necesita añadir otro Security Server a la lista. De lo contrario, compruebe la conexión de red entre los clientes y los Security Server sin problemas de carga.
- **Máquinas virtuales protegidas por HVI**: se informa de las máquinas virtuales monitorizadas y protegidas por el módulo HVI.
- **Estado de HVI**: indica si el módulo HVI está activado o desactivado; HVI está activado si tanto este como Security Server y el paquete suplementario están instalados en el host.
- **Dispositivos de almacenamiento conectados**: Informa de cuántos dispositivos de almacenamiento compatibles con ICAP están conectados a Security Server. Al hacer clic en el número se mostrará la lista de dispositivos de almacenamiento, con información sobre cada uno: nombre, IP, tipo, fecha y hora de la última conexión.
- **Estado de análisis de almacenamiento**: Indica si el servicio Security for Storage está habilitado o no.

También puede ver cuántos agentes están conectados al Security Server. Más adelante, al hacer clic en el número de clientes conectados se mostrará la lista de endpoints. Estos endpoints pueden ser vulnerables si el Security Server tiene problemas.

Malware más detectado

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

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

Los 10 endpoints más infectados
Muestra los endpoints más infectados por el número total de detecciones durante un periodo de tiempo específico entre los endpoints seleccionados.

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

Actualización
Muestra el estado de actualización del agente de seguridad o el Security Server instalado en los objetivos seleccionados. El estado de actualización se refiere a las versiones del producto y de los contenidos de seguridad.

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

En este informe, puede actualizar rápidamente los agentes a la última versión. Para ello, haga clic en el botón **Actualizar** de la barra de herramientas de acción sobre la tabla de datos.

Estado de actualización
Muestra los agentes de seguridad instalados en los objetivos seleccionados y si hay disponible una solución más reciente.

En el caso de endpoints que tengan instalados agentes de seguridad antiguos, puede instalar rápidamente el agente de seguridad más reciente compatible haciendo clic en el botón **Actualizar**.

Nota
Este informe solo está disponible cuando se ha realizado una actualización de la solución GravityZone.

Estado de protección de la red de máquinas virtuales
Le informa sobre la cobertura de la protección de Bitdefender en su entorno virtualizado. Para cada una de las máquinas seleccionadas, puede ver qué componente resuelve los problemas de seguridad:

- Security Server, para implementaciones sin agente de VMware NSX y entornos vShield, y para HVI.

- Un agente de seguridad, en cualquier otra situación.

Actividad de HVI

Le informa sobre todos los ataques que han detectado los módulos HVI en las máquinas seleccionadas dentro de determinado periodo de tiempo.

El informe también incluye información sobre la fecha y hora del último incidente detectado que implicó al proceso monitorizado, el estado final de la acción adoptada contra el ataque, el usuario con el que se inició el proceso y la máquina objetivo.

Dependiendo de la acción adoptada, se puede informar varias veces sobre el mismo proceso. Por ejemplo, si un determinado proceso se terminó una vez y en otra ocasión se le denegó el acceso, verá dos entradas en la tabla del informe.

Para cada proceso, al hacer clic en la última fecha de detección, se mostrará un registro independiente con todos los incidentes detectados desde que se inició el proceso. El registro revela información importante, como por ejemplo el tipo de incidente y su descripción, la fuente y el objetivo del ataque, y las acciones adoptadas para remediar el problema.

En este informe, puede indicar rápidamente al módulo de protección que ignore ciertos eventos que usted considera legítimos. Para ello, haga clic en el botón **Añadir excepción** de la barra de herramientas de acción sobre la tabla de datos.

Nota
El módulo HVI puede estar disponible para su solución GravityZone con una clave de licencia independiente.

Estado de inyección de herramientas de terceros de HVI

Le ofrece un estado detallado de cada inyección ejecutada en los endpoints objetivo. La información incluye:

- El nombre del endpoint.
- El nombre de la herramienta inyectada.
- La dirección IP del endpoint.
- El sistema operativo del guest.
- El desencadenador. Este puede ser una infracción de memoria, una tarea bajo demanda o una ejecución programada.

- El número de ejecuciones correctas. Al hacer clic en el número aparecerá una ventana con la ruta de registros y la fecha y hora de cada ejecución de la herramienta. Al hacer clic en el icono situado delante de la ruta, se copiará en el portapapeles.
- El número de ejecuciones fallidas. Al hacer clic en el número aparecerá una ventana donde se puede ver el motivo del error y la fecha y hora.
- Última inyección correcta.

Las inyecciones se agrupan por endpoints objetivo. Puede filtrar el informe para ver solo los datos relacionados con una herramienta concreta mediante las opciones de filtrado en el encabezado de la tabla.

Actividad de ransomware

Le informa de los ataques de ransomware que GravityZone ha detectado en los endpoints que administra y le proporciona las herramientas necesarias para recuperar los archivos afectados por los ataques.

El informe está disponible como una página en Control Center, a diferencia de los otros informes, accesibles directamente desde el menú principal de GravityZone.

La página **Actividad de ransomware** consta de una cuadrícula que indica lo siguiente por cada ataque de ransomware:

- El nombre, la dirección IP y el FQDN del endpoint en el que tuvo lugar el ataque.
- La empresa a la que pertenece el endpoint.
- El nombre del usuario que tenía la sesión iniciada durante el ataque.
- El tipo de ataque: local o remoto.
- El proceso bajo el cual se ejecutó el ransomware para ataques locales, o la dirección IP desde la cual se inició el ataque en el caso de los remotos.
- Fecha y hora de la detección.
- Número de archivos cifrados hasta que se bloqueó el ataque.
- El estado de la operación de restauración de todos los archivos en el endpoint objetivo.

Algunos de los detalles están ocultos por defecto. Haga clic en el botón **Mostrar/Ocultar columnas** en la parte superior derecha de la página para configurar la información que desea ver en la cuadrícula. Si tiene muchas

entradas en la cuadrícula, puede optar por ocultar filtros mediante el botón **Mostrar/Ocultar filtros** de la parte superior derecha de la página.

Haciendo clic en el número de archivos puede acceder a información adicional. Puede ver una lista con la ruta completa de los archivos originales y de los restaurados, así como el estado de la restauración de todos los archivos implicados en el ataque de ransomware seleccionado.

Importante
Hay disponibles copias de seguridad durante un máximo de treinta días. Tenga en cuenta la fecha y hora hasta la cual puede todavía recuperar los archivos.

Para recuperar archivos afectados por ransomware haga lo siguiente:

1. Seleccione los ataques que desee incluir en la cuadrícula.
2. Haga clic en el botón **Restaurar archivos**. Aparecerá una ventana de confirmación.

   Se está creando una tarea de recuperación. Puede comprobar su estado en la página **Tareas**, como con cualquier otra tarea de GravityZone.

Si las detecciones son el resultado de procesos legítimos, siga los pasos que se exponen a continuación:

1. Seleccione los registros en la cuadrícula.
2. Haga clic en el botón **Añadir exclusión**.
3. En la nueva ventana, seleccione las políticas a las que se debe aplicar la exclusión.
4. Haga clic en **Añadir**.

   GravityZone aplicará a todas las posibles exclusiones: por carpeta, por proceso y por dirección IP.

   Puede comprobarlas o modificarlas en la sección de la política **Antimalware > Ajustes > Exclusiones personalizadas**.

Nota
La Actividad de ransomware mantiene un registro de eventos durante dos años.

9.1.2. Informes de servidores de Exchange

Estos son los tipos de informe disponibles para servidores de Exchange:

Exchange - Contenido y adjuntos bloqueados

Le proporciona información sobre los mensajes de correo electrónico o archivos adjuntos que el Control de contenidos eliminó de los servidores seleccionados durante un intervalo de tiempo determinado. La información incluye:

- Direcciones de correo electrónico del remitente y de los destinatarios.

  Cuando el mensaje de correo electrónico tiene varios destinatarios, en lugar de las direcciones de correo electrónico, el informe muestra el número de destinatarios con un enlace a una ventana que contiene la lista de direcciones de correo electrónico.
- Asunto del mensaje de correo electrónico.
- Tipo de detección, que indica qué filtro del Control de contenidos detectó la amenaza.
- La acción adoptada tras la detección.
- El servidor en el que se detectó la amenaza.

Exchange - Adjuntos no analizables bloqueados

Le proporciona información acerca de los mensajes de correo electrónico que contenían archivos adjuntos no analizables (sobrecomprimidos, protegidos con contraseña, etc.) bloqueados en los servidores de correo de Exchange seleccionados durante un período de tiempo determinado. Esta información se refiere a:

- Direcciones de correo electrónico del remitente y de los destinatarios.

  Cuando el mensaje de correo electrónico se envía varios destinatarios, en lugar de las direcciones de correo electrónico, el informe muestra el número de destinatarios con un enlace a una ventana que contiene la lista de direcciones de correo electrónico.
- Asunto del mensaje de correo electrónico.
- Las medidas adoptadas para eliminar los archivos adjuntos no analizables:
  - **Mensaje de correo electrónico eliminado**, lo que indica que se ha eliminado todo el mensaje de correo electrónico.
  - **Adjuntos eliminados**, un nombre genérico para todas las acciones que eliminan los archivos adjuntos del mensaje de correo electrónico, como por ejemplo eliminar el archivo adjunto, moverlo a la cuarentena o sustituirlo por un aviso.

Al hacer clic en el enlace de la columna **Acción**, puede ver información sobre cada archivo adjunto bloqueado y la correspondiente medida adoptada.

- Fecha y hora de detección.
- El servidor en el que se detectó el mensaje de correo electrónico.

Exchange - Actividad de análisis de correo electrónico

Muestra estadísticas sobre las acciones adoptadas por el módulo de Protección de Exchange durante un intervalo de tiempo determinado.

Las acciones se agrupan por tipo de detección (malware, spam, adjunto prohibido y contenido prohibido) y por servidor.

Las estadísticas se refieren a los siguientes estados de correo electrónico:

- **En cuarentena.** Estos mensajes de correo electrónico se movieron a la carpeta de cuarentena.
- **Eliminado/Rechazado.** El servidor eliminó o rechazó estos mensajes de correo electrónico.
- **Redirigido.** Estos mensajes de correo electrónico fueron redirigidos a la dirección de correo electrónico proporcionada en la política.
- **Limpiado y entregado.** Se eliminaron las amenazas de estos mensajes de correo electrónico y pasaron los filtros.

  Un mensaje de correo electrónico se considera limpiado cuando todos los archivos adjuntos detectados se han desinfectado, puesto en cuarentena, eliminado o reemplazado con texto.
- **Modificado y entregado.** Se añadió la información de análisis a los encabezados de los mensajes de correo electrónico y estos pasaron los filtros.
- **Entregado sin ninguna otra acción.** La protección de Exchange ignoró estos mensajes de correo electrónico y pasaron los filtros.

Exchange - Actividad de malware

Le proporciona información acerca de los mensajes de correo electrónico con amenazas de malware, detectados en los servidores de correo de Exchange seleccionados durante un período de tiempo determinado. Esta información se refiere a:

- Direcciones de correo electrónico del remitente y de los destinatarios.

Cuando el mensaje de correo electrónico se envía varios destinatarios, en lugar de las direcciones de correo electrónico, el informe muestra el número de destinatarios con un enlace a una ventana que contiene la lista de direcciones de correo electrónico.

- Asunto del mensaje de correo electrónico.
- Estado de correo electrónico después del análisis antimalware.

  Al hacer clic en el enlace de estado, podrá ver la información sobre el malware detectado y la acción adoptada.
- Fecha y hora de detección.
- El servidor en el que se detectó la amenaza.

Exchange - Malware más detectado

Le informa sobre las diez amenazas de malware detectadas más frecuentemente en los adjuntos de correo electrónico. Puede generar dos vistas que contengan diferentes estadísticas. Una vista muestra el número de detecciones según los destinatarios afectados y la otra según los remitentes.

Por ejemplo, GravityZone ha detectado un mensaje de correo electrónico con un archivo adjunto infectado enviado a cinco destinatarios.

- En la vista de destinatarios:
  - El informe muestra cinco detecciones.
  - Los detalles del informe muestran solo los destinatarios, no los remitentes.
- En la vista de remitentes:
  - El informe muestra una detección.
  - Los detalles del informe muestran solo el remitente, no los destinatarios.

Además de los remitentes/destinatarios y el nombre del malware, el informe le proporciona los siguientes datos:

- El tipo de malware (virus, spyware, APND, etc.)
- El servidor en el que se detectó la amenaza.
- Las medidas que ha adoptado el módulo antimalware.
- Fecha y hora de la última detección.

Exchange - Principales destinatarios de malware

Muestra los diez destinatarios de correo electrónico que han recibido más malware durante un intervalo de tiempo determinado.

Los datos del informe le proporcionan toda la lista de malware que afectó a estos destinatarios, junto con las medidas adoptadas.

Exchange - Los diez mayores destinatarios de spam

Muestra los diez principales destinatarios de correo electrónico según el número mensajes de spam o de phishing detectados durante un intervalo de tiempo determinado. El informe ofrece también información sobre las acciones aplicadas a los respectivos mensajes de correo electrónico.

9.1.3. Informes de Dispositivos móviles

Nota
La protección frente a malware y los informes relacionados sólo están disponibles para dispositivos Android.

Esta es la lista de tipos de informe disponibles para dispositivos móviles:

Estado del Malware

Le ayuda a encontrar cuántos y qué dispositivos móviles objetivo han sido afectados por malware durante un periodo de tiempo determinado y cómo se han tratado las amenazas. Los dispositivos móviles se agrupan basándose en estos criterios:

- Dispositivos móviles sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado).
- Dispositivos móviles con problemas de malware resueltos (todos los archivos detectados se han eliminado).
- Dispositivos móviles con problemas de malware existentes (algunos de los archivos detectados no se han eliminado).

Dispositivos más infectados

Le muestra los dispositivos móviles más infectados durante un periodo de tiempo determinado entre los dispositivos móviles objetivo.

Nota
La tabla de detalles muestra todo el malware detectado en los dispositivos móviles más infectados.

Malware más detectado

Le muestra las principales amenazas malware detectadas durante un periodo de tiempo determinado en los dispositivos móviles objetivo.

> **Nota**
> La tabla de detalles muestra todos los dispositivos móviles infectados por el malware más frecuentemente detectado.

Cumplimiento del dispositivo

Le informa del estado de conformidad de los dispositivos móviles objetivo. Puede ver el nombre del dispositivo, estado, sistema operativo y la razón de no conformidad.

Para más información acerca de los requisitos de conformidad, consulte "Criterios de no conformidad" (p. 404).

Sincronización de dispositivos

Le informa del estado de sincronización de los dispositivos móviles objetivo. Puede ver el nombre del dispositivo al que está asignado el usuario, además del estado de sincronización, el sistema operativo y la hora a la que el dispositivo fue visto conectado por última vez.

Para más información, diríjase a "Comprobación del estado de los dispositivos móviles" (p. 176).

Páginas Web Bloqueadas

Le informa sobre el número de intentos de acceder a sitios Web bloqueados por reglas de **Acceso Web** por parte de los dispositivos objetivo en determinado intervalo de tiempo.

Para cada dispositivo con detecciones, haga clic en el número indicado en la columna **Sitios Web bloqueados** para ver información detallada sobre cada página Web bloqueada, como por ejemplo:

- URL
- Componente de política que llevó a cabo la acción
- Número de intentos bloqueados
- Última vez que se bloqueó el sitio Web

Para obtener más información sobre los tipos de portlet del panel de control, consulte "Perfiles" (p. 410).

Actividad de Seguridad Web

Le informa sobre el número de intentos de acceder a sitios Web con amenazas para la seguridad (phishing, fraude, malware o sitios Web inseguros) por parte de los dispositivos móviles objetivo en determinado intervalo de tiempo. Para cada dispositivo con detecciones, haga clic en el número indicado en la columna Sitios Web bloqueados para ver información detallada sobre cada página Web bloqueada, como por ejemplo:

- URL
- Tipo de amenaza (phishing, malware, fraude, inseguridad)
- Número de intentos bloqueados
- Última vez que se bloqueó el sitio Web

Seguridad Web es el componente de política que detecta y bloquea sitios Web con problemas de seguridad. Para obtener más información acerca de los ajustes de política de seguridad Web, consulte "Seguridad" (p. 400).

9.2. Creando Informes

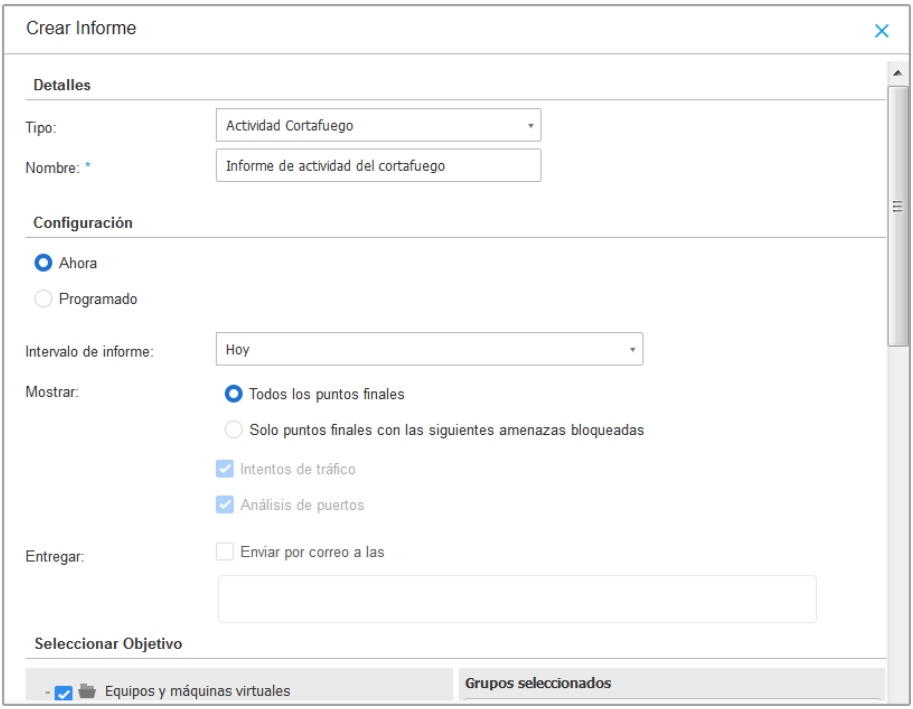
Puede crear dos categorías de informes:

- **Informes instantáneos.** Los informes instantáneos se muestran automáticamente una vez generados.
- **Informes Programados.** Los informes programados se pueden configurar para que se ejecuten periódicamente, en una fecha y hora especificadas. La página **Informes** muestra una lista de todos los informes programados.

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. Elija el tipo de objetos de red en el selector de vistas.
3. Haga clic en el botón ⊕ **Añadir** en la parte superior de la tabla. Se muestra una ventana de configuración.



Opciones de informes de equipos y máquinas virtuales

4. Seleccione el tipo de informe deseado desde el menú. Para obtener más información, consulte"Tipos de informes" (p. 423)
5. 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.
6. 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).

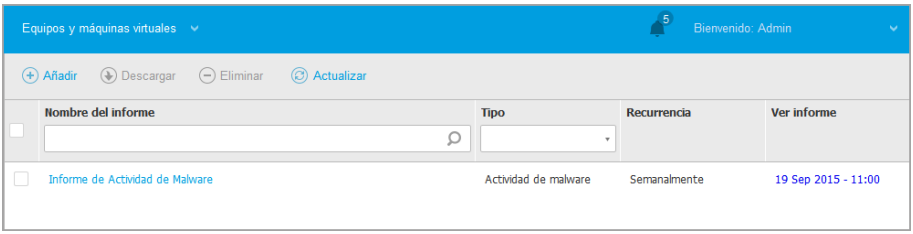
  - Semanalmente, en los días especificados de la semana y a la hora de inicio seleccionada (horas y minutos).
  - Mensualmente, en los días especificados del mes y a la hora de inicio seleccionada (horas y minutos).

7. 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.
8. 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 objetos de red que no se hayan actualizado, o los que necesiten reiniciarse para completar la actualización.
9. **Entregar**. Para recibir un informe programado por correo electrónico, marque la casilla de verificación correspondiente. Introduzca las direcciones de correo electrónico que desee en el campo de abajo. Por defecto, el mensaje de correo electrónico contiene un archivo comprimido que contiene ambos formatos de informe (PDF y CSV). Utilice las casillas de verificación de la sección **Adjuntar archivos** para personalizar qué archivos enviar por correo electrónico y cómo hacerlo.
10. **Seleccionar objetivo**. Desplácese hacia abajo para configurar el objetivo del informe. Seleccione uno o varios grupos de endpoints que desee incluir en el informe.
11. Dependiendo de la recurrencia seleccionada, haga clic en **Generar** para crear un informe instantáneo o en **Guardar** para crear un informe programado.
    - El informe instantáneo se mostrará inmediatamente tras hacer clic en **Generar**. El tiempo requerido para crear los informes puede variar dependiendo del número de objetos de red administrados. Por favor, espere a que finalice la creación del informe.
    - El informe programado se mostrará en la lista de la página **Informes**. Una vez que se ha generado el informe, puede verlo haciendo clic en su enlace correspondiente en la columna **Ver informe** de la página **Informes**.

9.3. 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 junto con información útil sobre los mismos:

- Nombre y tipo del informe.
- Recurrencia de informes
- Última instancia generada.

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.

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

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

Para asegurarse de que se está mostrando la información más reciente, haga clic en el botón **Actualizar** de la zona superior de la tabla.

9.3.1. 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. Se mostrará la instancia más reciente del informe.

   Para ver todas las instancias de un informe, consulte"Guardar Informes" (p. 451)

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 gráficas) para todos los 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 sobre cada objeto de red objetivo.

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 (sector circular o barra) que le interese para ver los detalles correspondientes en la tabla inferior.

9.3.2. 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.

9.3.3. Eliminar informes programados

Cuando ya no se necesita un informe programado, lo mejor es eliminarlo. Al eliminar un informe programado se eliminarán todas las instancias que se hayan 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 ⊖ **Eliminar** de la parte superior de la tabla.

9.4. Adopción de medidas en base a informes

Aunque la mayoría de los informes se limitan a destacar los problemas de su red, algunos de ellos también le ofrecen varias opciones para solucionar los problemas encontrados con solo hacer clic en un botón.

Para solucionar los problemas que aparecen en el informe, haga clic en el botón correspondiente de la Barra de herramientas de acción de encima de la tabla de datos.

Nota
Necesita privilegios de **Administración de red** para llevar a cabo estas acciones.

Estas son las opciones disponibles para cada informe:

Aplicaciones Bloqueadas

- **Añadir excepción**. Añade una exclusión en la política para evitar que los módulos de protección bloqueen de nuevo la aplicación.
- **Añadir regla**. Define una regla para una aplicación o un proceso en el Control de aplicaciones.

Actividad de HVI

- **Añadir excepción**. Añade una exclusión en la política para evitar que el módulo de protección informe de nuevo del incidente.

Estado del Malware

- **Analizar objetivos infectados**. Ejecuta una tarea de Análisis completo preconfigurada en los objetivos que aún se muestran como infectados.

Actualización

- **Actualizar**. Actualiza los clientes objetivo a sus últimas versiones disponibles.

Estado de actualización

- **Actualizar**. Reemplaza los clientes de endpoint antiguos con la última generación de productos disponible.

9.5. 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:

- Exportar
- Descargar

9.5.1. Exportando los Informes

Para exportar el informe a su equipo:

1. Elija un formato y haga clic en **Exportar CSV** o **Exportar PDF**.
2. 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.

9.5.2. 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.

9.6. 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**. 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 **Ajustes > 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.

Los informes se envían por correo electrónico como archivos ZIP.

9.7. 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.

9.8. Generador de informes

En Control Center, puede crear y administrar las consultas para obtener informes detallados que le permitan entender cualquier evento o cambio que se produzca en su red, en cualquier momento.

Las consultas le ofrecen la posibilidad de investigar un problema de seguridad según diversos criterios, proporcionándole una información concisa y ordenada. Con los filtros, puede agrupar los endpoints según determinados criterios y seleccionar datos relevantes para su propósito.

Mediante un informe basado en consultas, puede averiguar detalles como cuándo se produjo un incidente, cuántos endpoints se vieron afectados, qué usuarios habían iniciado sesión en el momento del incidente, qué políticas se aplicaron, el estado del agente de seguridad, y las medidas adoptadas, en un solo endpoint o en un grupo de ellos.

Todos los informes basados en consultas están disponibles en Control Center, pero puede guardarlos en su equipo o enviarlos por correo electrónico. Los formatos disponibles incluyen Portable Document Format (PDF) y Comma-Separated Values (CSV).

Con las consultas, puede aprovechar diversas ventajas respecto a los informes estándar de GravityZone:

- Abordar un gran volumen de datos para crear informes convincentes.
- Informes flexibles, debido al hecho de que los eventos no se agregan.
- Alto nivel de personalización. Mientras que los informes estándar de GravityZone le ofrecen la posibilidad de optar entre un par de opciones predefinidas, con las consultas no existe limitación en cuanto a la elección de sus filtros de datos.
- Correlación de eventos, con toda la información acompañada de datos del estado del dispositivo y del agente.
- Mínimo esfuerzo de desarrollo, dado que puede crear, guardar y reutilizar cualquier tipo de informe.
- Informes integrales que, a diferencia de los estándar, incorporan resúmenes y detalles en el mismo documento PDF.
- Las consultas pueden obtener información de los dos últimos años.

Para utilizar las consultas, debe instalar el rol de Generador de informes junto con su dispositivo virtual GravityZone. Para obtener más información sobre la

instalación del Generador de informes, consulte la Guía de instalación de GravityZone.

9.8.1. Tipos de consultas

GravityZone viene con los siguientes tipos de consultas:

- Estado de endpoints
- Eventos de endpoints
- Eventos de Exchange

Estado de endpoints

Esta consulta le proporciona información sobre el estado de seguridad en una determinada fecha de los endpoints objetivo seleccionados. De esta manera, puede saber si el agente de seguridad y los contenidos de seguridad están actualizados, obsoletos o inhabilitados. Además, puede ver si los endpoints están infectados o limpios, qué infraestructura se utiliza, y qué módulos están activados, desactivados o no instalados.

Esta consulta incluye detalles relacionados con los endpoints objetivo, como por ejemplo:

- Tipo de máquina (física, virtual o Security Server)
- Infraestructura de red a la que pertenece el endpoint (Active Directory, Nutanix Prism, VMware o Citrix Xen)
- Datos del agente de seguridad (tipo, estado, configuración de los motores de análisis, estado de seguridad)
- Estado de los módulos de protección
- Roles de endpoint (Relay, Protección de Exchange)

Eventos de endpoints

Esta consulta le permite obtener información sobre los eventos de seguridad acontecidos en los endpoints objetivo, ya sea en una fecha determinada o a lo largo de un período de tiempo. Incluye información relativa a:

- Máquina objetivo en la que se produjo el evento (nombre, tipo, IP, sistema operativo, infraestructura de red)
- Tipo, estado y configuración del agente de seguridad instalado

- Estado de los módulos de protección y roles instalados en el agente de seguridad
- Nombre y asignación de políticas
- Usuario con sesión iniciada durante el evento
- Eventos, que pueden hacer referencia a sitios Web bloqueados, aplicaciones bloqueadas, detecciones de malware o actividad del dispositivo

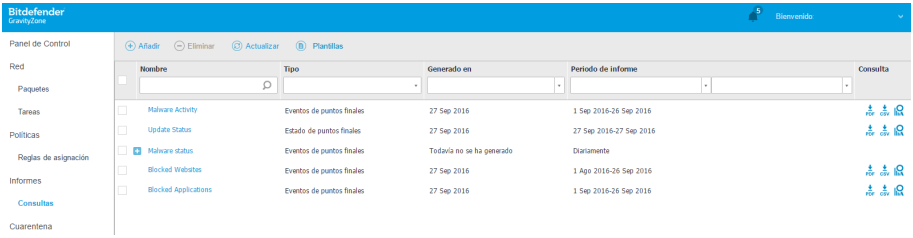
Eventos de Exchange

Le ayuda a descubrir los incidentes producidos en los servidores de Microsoft Exchange seleccionados, ya sea en una fecha determinada o a lo largo de un período de tiempo. Tiene en cuenta datos acerca de:

- Dirección del tráfico de correo electrónico
- Eventos de seguridad (como malware o detección de adjuntos)
- Medidas adoptadas en cada situación (desinfectar, eliminar, reemplazar o poner el archivo en cuarentena, eliminar o rechazar el correo electrónico)

9.8.2. Gestión de consultas

Puede crear y gestionar consultas e informes basados en consultas en la página **Informes > Consultas**.



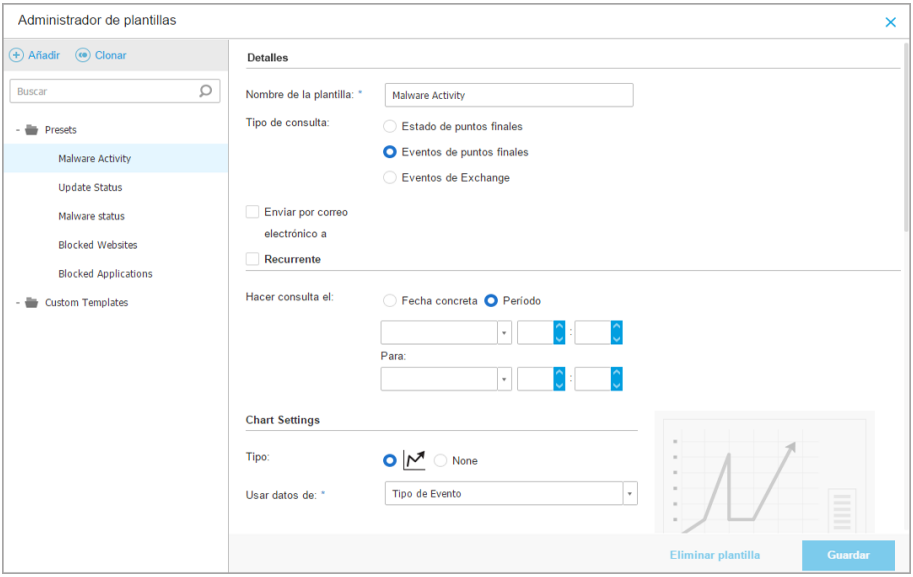
La página Consultas

Las consultas son solicitudes de información complejas cursadas a la bases de datos que utilizan un gran número de filtros, por lo que pueden tardarse varios minutos en configurarlas y crearlas. Tener que rellenar el formulario de consulta cada vez que quiere hacer un nuevo informe, parecido a los ya existentes, puede llegar a ser frustrante. GravityZone le ayuda a crear consultas fácilmente con el

uso de plantillas que rellenan automáticamente el formulario de consultas, lo que deja menos trabajo de personalización a su cargo.

Uso de plantillas

Puede añadir, clonar y buscar plantillas concretas rápidamente en la ventana **Administrador de plantillas**.



Para ver las plantillas de consulta disponibles:

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en el botón **Plantillas** de la zona superior de la tabla. Aparecerá la ventana del **Administrador de plantillas**. Todas las plantillas se muestran en el panel izquierdo, mientras que en el derecho puede ver los ajustes de la plantilla seleccionada.

Para encontrar rápidamente una plantilla, introduzca su nombre en el campo **Buscar** de la zona superior del panel izquierdo. Puede ver los resultados de la búsqueda a medida que escribe. Para borrar el campo **Buscar**, haga clic en el icono × **Eliminar** situado a su derecha.

Hay dos categorías de plantillas disponibles:

- Predefinidas. Son las plantillas predefinidas que vienen por defecto en GravityZone.
- Plantillas personalizadas. Son las plantillas que usted crea en función de sus necesidades.

Predefinidas

GravityZone incluye cinco plantillas predefinidas:

- **Actividad de malware**, le proporciona información sobre las amenazas de malware detectadas durante un período de tiempo dado en los endpoints seleccionados.

  El informe contiene el nombre de la máquina objetivo, IP, estado de infección (infectada o limpia), nombre del malware, medidas adoptadas contra la amenaza (ignorada, presente, eliminada, bloqueada, en cuarentena, limpiada o restauración), tipo de archivo, ruta del archivo y el usuario con sesión iniciada en ese momento.

- **Estado de actualizaciones**, que muestra el estado de actualización del agente de seguridad instalado en los objetivos seleccionados. El informe contiene el nombre de la máquina objetivo, IP, estado de actualización del producto (actualizado, sin actualizar o deshabilitado), estado de actualización de firmas (actualizadas, sin actualizar o deshabilitadas), tipo de agente de seguridad, versión del producto y versión de las firmas.

- **Estado del malware**, que le ayuda a encontrar cuántos y cuáles de los endpoints seleccionados han sido afectados por malware en un período de tiempo específico y cómo se han tratado las amenazas.

  El informe contiene el nombre de la máquina objetivo, IP, estado de infección (infectada o limpia), nombre del malware, medidas contra la amenaza (ignorada, presente, eliminada, bloqueada, en cuarentena, limpiada o restauración).

- **Sitios Web bloqueados**, le informa sobre la actividad del módulo de Control de acceso Web del agente de seguridad.

  El informe contiene el nombre de la máquina objetivo, IP, tipo de amenaza (phishing, fraude o no fiable), nombre de la regla, categoría del sitio Web y la URL bloqueada.

- **Aplicaciones bloqueadas**, que le ayuda a averiguar qué aplicaciones han sido bloqueadas durante un período de tiempo determinado.

El informe ofrece información sobre el nombre de la máquina objetivo, IP, nombre de la aplicación bloqueada, su ruta de archivo y cómo se atajó la amenaza: con ATC, IDS o Control de aplicaciones.

Plantillas personalizadas

Si necesita plantillas que no se encuentren entre las predefinidas de GravityZone, puede crear plantillas de consulta personalizadas. Puede guardar tantas plantillas como desee.

Para crear una plantilla personalizada:

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en el botón **Plantillas** de la zona superior de la tabla. Aparecerá la ventana de configuración del **Administrador de plantillas**.
3. Haga clic en el botón **Añadir** de la esquina superior izquierda de la ventana. Se mostrará un formulario de consulta en el panel de la derecha.
4. Rellene el formulario de consulta con la información requerida. Para obtener más información acerca de cómo rellenar un formulario de consulta, acuda a "Creación de consultas" (p. 459).
5. Haga clic en **Guardar**. La plantilla recién creada se mostrará en el panel izquierdo, en **Plantillas personalizadas**.

Como alternativa, puede crear una plantilla personalizada basándose en una predefinida.

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en el botón **Plantillas** de la zona superior de la tabla. Aparecerá la ventana de configuración del **Administrador de plantillas**.
3. Seleccione una predefinida en el panel de la izquierda. Se mostrarán los ajustes correspondientes en el panel de la derecha.
4. Haga clic en el botón **Clonar** de la esquina superior izquierda para crear una copia de la plantilla predefinida.
5. Modifique todos los ajustes que desee en el formulario de consulta. Para obtener más información acerca de cómo rellenar un formulario de consulta, acuda a "Creación de consultas" (p. 459).
6. Haga clic en **Guardar**. La plantilla recién creada se mostrará en el panel izquierdo, en **Plantillas personalizadas**.

Además, al crear una nueva consulta, puede guardarla como plantilla. Para más información, diríjase a "Creación de consultas" (p. 459).

Para eliminar una plantilla personalizada:

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en el botón ⊖ **Plantillas** de la zona superior de la tabla. Aparecerá la ventana de configuración del **Administrador de plantillas**.
3. En la sección **Plantillas personalizadas**, haga clic en la plantilla que desee eliminar. Se mostrarán los ajustes de la plantilla en el panel de la derecha.
4. Haga clic en **Eliminar plantilla** en la zona inferior de la ventana y, a continuación, confirme su acción haciendo clic en **Sí**.

Creación de consultas

Para crear una nueva consulta:

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en el botón ⊕ **Añadir** de la zona superior de la tabla. Se muestra una ventana de configuración.
3. Marque la casilla de verificación **Usar plantilla** si desea utilizar una plantilla por defecto o creada previamente.
4. En la sección **Detalles**, introduzca un nombre descriptivo para la consulta. Para elegir el nombre, tenga en cuenta el tipo de consulta, los objetivos y otros ajustes.
5. Seleccione el tipo de consulta. Para obtener más información, consulte"Tipos de consultas" (p. 454)
6. Marque la casilla de verificación **Enviar por correo a** para enviar los resultados de la consulta a determinados destinatarios. En el campo correspondiente, añada tantas direcciones de correo electrónico como desee.
7. En la sección **Recurrencia**, seleccione:
   a. **Fecha concreta** para un día determinado.
   b. **Período**, para un intervalo de tiempo prolongado.
   c. Haga clic en la casilla de verificación **Recurrente** si desea que la consulta se genere en intervalos concretos que puede establecer en **Período de informe**.

8. Configure los ajustes del gráfico.
   a. En el menú **Tipo**, seleccione el gráfico con el que desea ilustrar la consulta, o escoja **Ninguno** para omitirlo. Dependiendo del tipo de consulta y del período del informe, puede utilizar un gráfico circular, de barras o de líneas.
   b. En el campo **Tomar valores de**, seleccione las categorías de datos que desee utilizar para su consulta. Cada tipo de consulta proporciona información concreta relativa a endpoints, agentes de seguridad y eventos de seguridad. Para más información sobre los datos de los tipos, consulte "Tipos de consultas" (p. 454).
9. En la sección **Ajustes de la tabla**, seleccione las columnas que desee que tenga el informe. Los datos que puede seleccionar dependen del tipo de consulta, y pueden hacer referencia a: tipo de endpoint y sistema operativo, estado del agente de seguridad y eventos, módulos, políticas y eventos de seguridad. Todas las columnas seleccionadas se muestran en la tabla **Columnas**. Use arrastrar y soltar para cambiar el orden.

   Nota
   Tenga en cuenta el espacio disponible al crear el diseño de la tabla. Utilice un máximo de diez columnas para una buena visualización de la tabla en formato PDF.

10. En la sección **Filtros**, seleccione el conjunto de datos en el que desea que se base el informe mediante los criterios de filtrado disponibles:
    a. En el menú **Tipo de filtro**, elija un filtro y, a continuación, haga clic en ⊕ **Añadir filtro**.
    b. En la tabla inferior, haga clic en **Valor** para especificar una o más opciones de filtrado.

       Por ejemplo, el filtro **Sistema operativo del host** requiere especificar el nombre del sistema operativo, como por ejemplo Windows o Linux, mientras que el filtro del **Módulo de Control de dispositivos** le permite seleccionar en una lista desplegable los endpoints en los que está deshabilitado el módulo.
    c. Haga clic en el botón ⊖ **Eliminar** para eliminar un filtro.
11. **Seleccionar objetivos**. Desplácese hacia abajo para configurar los objetivos del informe. Seleccione uno o varios grupos de endpoints que desee incluir en

el informe. Mediante el selector de Vistas, asegúrese de haber marcado los objetivos correctos en todas las vistas de red.

12. Marque la casilla de verificación **Guardar como plantilla** para utilizar estos ajustes en consultas posteriores. En este caso, introduzca un nombre descriptivo para la plantilla.
13. Haga clic en **Generar** para crear la consulta. Una vez guardada la consulta, recibirá un mensaje en el área de **Notificaciones**.

Eliminación de consultas

Para eliminar una consulta:

1. Acceda a la página **Informes > Consultas**.
2. Seleccione el informe que desea eliminar.
3. Haga clic en el botón ⊖ **Eliminar** de la zona superior de la tabla.

Nota
Eliminar una consulta borrará también todos los informes generados.

9.8.3. Visualización y gestión informes

Todos los informes basados ??en consultas se muestran en la página **Informes > Consultas**.

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

Visualizando los Informes

Para ver un informe basado en un consulta:

1. Acceda a la página **Informes > Consultas**.
2. Ordene los informes por nombre, tipo, fecha de generación o período del informe para encontrar fácilmente lo que busca. Por defecto, los informes se ordenan por la fecha de la última instancia generada.
3. Haga clic en cualquier nombre para ver la información de la consulta en una ventana nueva. Los detalles no se pueden modificar.
4. Haga clic en el botón del signo más que precede al nombre de una consulta para desplegar la lista de instancias del informe y en el botón del signo menos para replegarla.

5. Haga clic en el icono **Ver informe** para mostrar la instancia más reciente de un informe. Las instancias más antiguas solo están disponibles en formato PDF y CSV.

Todos los informes constan de una sección de resumen, en la zona superior de la página del informe, y de una sección de detalles en su mitad inferior.

La sección de resumen le proporciona datos estadísticos (gráficos circulares, de barras o de líneas) para todos los endpoints objetivo, así como información general acerca de la consulta, como recurrencia, período de notificación, tipo de consulta y filtros utilizados.

Para configurar la información mostrada en el gráfico, haga clic en los elementos de la leyenda para mostrar u ocultar los datos seleccionados. Por otra parte, haga clic en el área del gráfico que le interese para ver los datos correspondientes en la tabla.

La sección de detalles le proporciona información sobre cada endpoint objetivo. Para encontrar rápidamente los datos que busque, haga clic en los campos de búsqueda o en las opciones de filtrado bajo los encabezados de columna.

Haga clic en el botón **Columnas** para personalizar cuáles desea ver en la tabla.

Guardar Informes

Por defecto, todos los informes se guardan automáticamente en Control Center. También puede exportarlos a su equipo, tanto en formato PDF como CSV.

Puede guardar informes en su equipo:

- Desde la página Informes.
- Desde la tabla **Consultas**.

Para guardar un informe mientras esté en su página:

1. Haga clic en el botón **Exportar** de la esquina inferior izquierda.
2. Seleccione el formato del informe deseado:
   a. Portable Document Format (PDF) o
   b. Valores separados por comas (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.

Para exportar un informe mientras está en la página **Informes > Consultas**:

1. Acceda a la página **Informes > Consultas**.
2. Haga clic en los botones **PDF** o **CSV** correspondientes a cada informe.
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.

Todos los informes exportados en PDF contienen el resumen y los detalles en el mismo documento, en páginas A4 verticales o apaisadas distintas. Los detalles se limitan a cien filas por documento PDF.

Enviar informes por correo

Tiene dos opciones para enviar informes por correo electrónico:

1. En la página del informe que está viendo, haga clic en el botón **Correo electrónico** de la esquina inferior izquierda de la página. El informe se enviará a la dirección de correo asociada a su cuenta.
2. Al crear una nueva consulta, seleccione la casilla de verificación **Enviar por correo electrónico a** e introduzca las direcciones de correo electrónico que desee en el campo correspondiente.

Imprimiendo los Informes

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

10. CUARENTENA

La cuarentena es una carpeta cifrada que contiene archivos potencialmente maliciosos, como pueden ser los sospechosos de malware, los infectados con malware u otros archivos no deseados. Cuando un virus u otra forma de malware está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

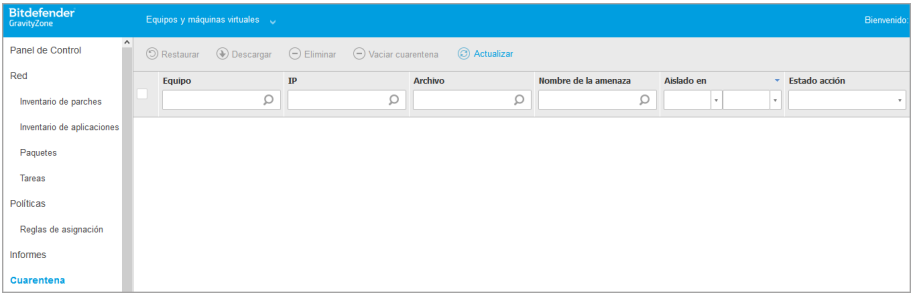
GravityZone mueve los archivos a la cuarentena según las políticas asignadas a los endpoints. Por defecto, los archivos que no se pueden desinfectar se ponen en cuarentena.

La cuarentena se guarda localmente en cada endpoint, a excepción de en el VMware vCenter Server integrado con vShield Endpoint y con NSX, en cuyo caso se guarda en el Security Server.

Importante
La cuarentena no está disponible para dispositivos móviles.

10.1. Exploración de la cuarentena

La página **Cuarentena** proporciona información detallada acerca de los archivos en cuarentena de todos los endpoints que usted administra.



La página Cuarentena

La página de cuarentena consiste en dos vistas:

- Equipos y máquinas virtuales, para los archivos detectados directamente en el sistema de archivos de los endpoints.

- Servidores de Exchange, para mensajes de correo electrónico y archivos adjuntos a mensajes de correo electrónico detectados en los servidores de correo de Exchange.

El selector de vistas de la zona superior de la página le permite pasar de una vista a otra.

La información sobre los archivos en cuarentena se muestra en una tabla. Dependiendo del número de endpoints administrados y del grado de infección, la tabla de cuarentena puede albergar un gran número de entradas. La tabla puede distribuirse en varias páginas (por defecto, únicamente se muestran 20 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.

Para una mejor visibilidad de los datos que le interesen, puede utilizar los cuadros de búsqueda de los encabezados de columna para filtrar los datos mostrados. 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 determinada.

Para asegurarse de que se está mostrando la información más reciente, haga clic en el botón **Actualizar** de la zona superior de la tabla. Esto puede ser necesario cuando dedique más tiempo a la página.

10.2. Cuarentena de equipos y máquinas virtuales

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender para que sean 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. Estas características corresponden a cada política de seguridad de la página **Políticas** y puede elegir si desea mantenerlas o desactivarlas. Para más información, diríjase a "Cuarentena" (p. 290).

10.2.1. Visualización de la información de la cuarentena

La tabla de cuarentena le proporciona la siguiente información:

- El nombre del endpoint en el que se detectó la amenaza.
- La IP del endpoint en el que se detectó la amenaza.
- La ruta al archivo sospechoso o infectado en el endpoint en que fue detectado.
- Nombre dado a la amenaza malware por los investigadores de seguridad de Bitdefender.
- La fecha y hora en la que el archivo se envió a la cuarentena.
- El estado de la acción que se ha solicitado que se aplique al archivo en cuarentena.

10.2.2. Administración de los archivos en cuarentena

El comportamiento de la cuarentena es diferente en cada entorno:

- **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.
- **Security for Virtualized Environments (Multiplataforma)** almacena los archivos de cuarentena en cada máquina virtual administrada. Usando Control Center tiene la opción de eliminar o restaurar archivos específicos de la cuarentena.
- **Security for Virtualized Environments (integrado con VMware vShield Endpoint o NSX)** almacena los archivos en cuarentena en el appliance Security Server. Usando Control Center tiene la opción de eliminar archivos de la cuarentena o descargarlos a una ubicación de su elección.

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.

Nota
Restaurar los archivos de la cuarentena sólo es posible en entornos protegidos por Security for Endpoints y Security for Virtualized Environments (Multiplataforma).

Para restaurar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas disponible en la zona superior de la página.

3. Marque las casillas de verificación correspondientes a los archivos en cuarentena que desee restaurar.
4. Haga clic en el botón **Restaurar** de la zona superior de la tabla.
5. 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 absoluta en el campo correspondiente.
6. 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.
7. Haga clic en **Guardar** para solicitar la acción de restauración del archivo. Puede observar el estado pendiente en la columna **Acción**.
8. La acción solicitada se envía a los endpoints objetivo inmediatamente o tan pronto como vuelvan a estar conectados.

   Puede ver información relativa al estado de la acción en la página **Tareas**. Una vez restaurado un archivo, la entrada correspondiente desaparece de la tabla de cuarentena.

Descarga de archivos en cuarentena

En entornos virtualizados VMware integrados con vShield Endpoint o NSX, la cuarentena se guarda en el Security Server. Si quiere examinar o recuperar datos de los archivos de la cuarentena, debe descargarlos del Security Server mediante Control Center. Los archivos en cuarentena se descargan como archivo comprimido zip protegido con contraseña y encriptado para evitar infecciones accidentales de malware.

Para abrir el archivo comprimido y extraer su contenido, debe utilizar la Quarantine Tool, una aplicación independiente de Bitdefender que no requiere instalación.

La Quarantine Tool está disponible para los siguientes sistemas operativos:

- Windows 7 o posterior
- La mayoría de distribuciones Linux de 32 bits con interfaz gráfica de usuario (GUI).

Nota
Tenga en cuenta que la Quarantine Tool carece de interfaz de línea de comandos.

Aviso
Tenga cuidado cuando extraiga los archivos en cuarentena porque pueden infectar su sistema. Se recomienda extraer y analizar los archivos en cuarentena en un sistema aislado o de prueba, preferiblemente ejecutándose en Linux. Las infecciones de malware son más fáciles de contener en Linux.

Para descargar archivos en cuarentena a su equipo:

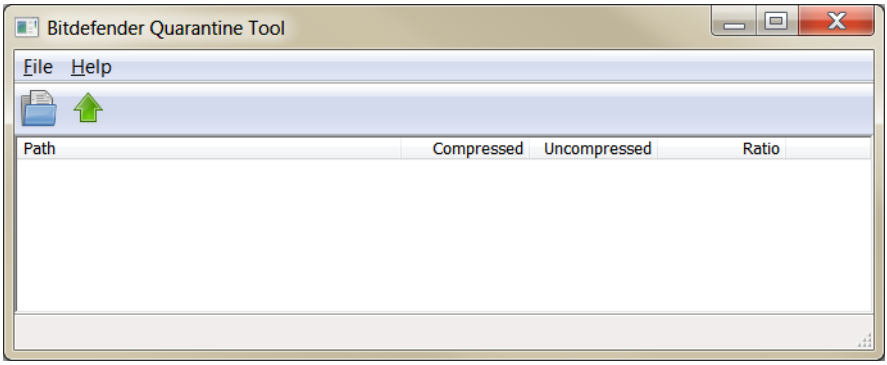
1. Vaya a la página **Cuarentena**.
2. Elija **Equipos y máquinas virtuales** en el selector de vistas disponible en la zona superior de la página.
3. Filtre los datos de la tabla introduciendo el nombre de host del Security Server o la dirección IP en el campo correspondiente del encabezado de la tabla.

   Si la cuarentena es grande, para ver los archivos que le interesen puede que tenga que aplicar filtros adicionales o aumentar el número de archivos que aparecen por página.
4. Marque las casillas de verificación correspondientes a los archivos que desee descargar.
5. Haga clic en el botón **Descargar** en la parte superior de la tabla. Dependiendo de los ajustes de su navegador, se le pedirá que guarde los archivos en una carpeta de su elección, o bien los archivos se descargarán automáticamente a la ubicación de descarga por defecto.

Para acceder a los archivos restaurados:

1. Descargue la Quarantine Tool correspondiente a su sistema operativo desde la página **Ayuda y soporte** o desde las siguientes direcciones:
   - Herramienta de cuarentena para Windows
   - Herramienta de cuarentena para Linux

   Nota
   La Quarantine Tool para Linux está comprimida en un archivo `tar`.
2. Lance el archivo ejecutable de la Quarantine Tool.



Quarantine Tool

3. En el menú **Archivo**, haga clic en **Abrir** (Ctrl + O) o haga clic en el botón **Abrir** para cargar el archivo en la herramienta.

   Los archivos se organizan en el archivo comprimido según la máquina virtual en la que se detectaron y conservando su ruta original.
4. Antes de extraer los archivos comprimidos, si está activado el análisis antimalware on-access en el sistema, asegúrese de desactivarlo o configurar una exclusión de análisis para la ubicación donde vaya a extraer los archivos. Si no, su programa antimalware detectará y adoptará medidas sobre los archivos extraídos.
5. Seleccione los archivos que desee extraer.
6. En el menú **Archivo**, haga clic en **Extraer** (CTRL + E) o haga clic en el botón **Extraer**.
7. Seleccione la carpeta de destino. Los archivos se extraerán en la ubicación seleccionada, conservando la estructura de carpetas original.

Eliminación automática de archivos de la cuarentena

Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Estos ajustes pueden cambiarse modificando la política asignada a los endpoints 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 endpoints en los que desee cambiar la configuración y haga clic en su nombre.
3. Acceda a la página **Antimalware > Ajustes**.
4. En la sección **Cuarentena**, seleccione el número de días transcurrido el cual se borrarán los archivos.
5. Haga clic en **Guardar** para aplicar los cambios.

Eliminación manual de archivos de la cuarentena

Si desea eliminar manualmente archivos en cuarentena, primero debería asegurarse de que los archivos que elige no son necesarios.

Un archivo puede ser el propio malware en sí. Si su investigación le lleva a esta situación, puede buscar esa amenaza concreta en la cuarentena y eliminarla.

Para eliminar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Seleccione **Equipos y máquinas virtuales** en el selector de vistas disponible en la zona superior de la página.
3. Marque las casillas de verificación correspondientes a los archivos en cuarentena que desee eliminar.
4. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

   Puede observar el estado pendiente en la columna **Acción**.

   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.

Vaciado de la cuarentena

Para eliminar todos los objetos en cuarentena:

1. Vaya a la página **Cuarentena**.
2. Seleccione **Equipos y máquinas virtuales** en el selector de vistas.
3. Haga clic en el botón **Vaciar cuarentena**.

   Tendrá que confirmar esta acción haciendo clic en **Sí**.

Se borrarán todos los elementos de la tabla Cuarentena. La acción solicitada se envía a los equipos de red objetivo inmediatamente o tan pronto como vuelvan a estar online.

10.3. Cuarentena de servidores de Exchange

La cuarentena de Exchange contiene mensajes de correo electrónico y archivos adjuntos. El módulo Antimalware pone en cuarentena los archivos adjuntos a los mensajes de correo electrónico, mientras que los módulos Antispam, Contenidos y Filtrado de adjuntos ponen en cuarentena todo el mensaje de correo electrónico.

Nota
Tenga en cuenta que la cuarentena para servidores de Exchange requiere espacio de disco duro adicional en la partición donde esté instalado el agente de seguridad. El tamaño de la cuarentena depende del número de elementos almacenados y de su tamaño.

10.3.1. Visualización de la información de la cuarentena

La página **Cuarentena** le ofrece información detallada sobre los objetos en cuarentena de todos los servidores de Exchange de su organización. La información está disponible en la tabla de cuarentena y en la ventana de detalles de cada objeto.

La tabla de cuarentena le proporciona la siguiente información:

- **Asunto.** El asunto del mensaje de correo electrónico en cuarentena.
- **Remitente.** La dirección de correo electrónico del remitente que aparece en el campo **De** del encabezado del mensaje de correo electrónico.
- **Destinatarios.** La lista de destinatarios que aparecen en los campos **Para** y **CC** del encabezado del mensaje de correo electrónico.
- **Destinatarios reales.** La lista de direcciones de correo electrónico de los usuarios individuales a los que iba destinado el mensaje antes de ser puesto en cuarentena.
- **Estado.** El estado del objeto después de ser analizado. El estado muestra si un correo electrónico se marca como correo no deseado o con contenido no deseado, o si un archivo adjunto está infectado por malware, es sospechoso de estar infectado, o se considera no deseado o no analizable.
- **Nombre del malware.** Nombre dado a la amenaza de malware por los investigadores de seguridad de Bitdefender.

- **Nombre del servidor.** Nombre de host del servidor en el que se detectó la amenaza.
- **Puesto en cuarentena.** Fecha y hora en la que el archivo se envió a la cuarentena.
- **Estado de la acción.** El estado de las medidas adoptadas sobre el objeto en cuarentena. De esta manera puede ver rápidamente si una acción está pendiente o ha fallado.

Nota

- Las columnas **Destinatarios reales**, **Nombre del malware** y **Nombre del servidor** están ocultas en la vista predeterminada.
- Cuando se ponen en cuarentena varios archivos adjuntos del mismo mensaje de correo electrónico, la tabla de Cuarentena muestra una entrada independiente para cada archivo adjunto.

Para personalizar los datos de la cuarentena que se muestran en la tabla:

1. Haga clic en el botón **Columnas** del lateral derecho del encabezado de la tabla.
2. Seleccione las columnas que desea ver.

   Para volver a la vista de columnas predeterminadas, haga clic en el botón **Restablecer**.

Puede obtener más información haciendo clic en el enlace **Asunto** correspondiente a cada objeto. Se muestra la ventana **Detalles del objeto**, que le proporciona la siguiente información:

- **Objeto en cuarentena.** El tipo de objeto en cuarentena, que puede ser o bien un mensaje de correo electrónico o un archivo adjunto.
- **Puesto en cuarentena.** Fecha y hora en la que el archivo se envió a la cuarentena.
- **Estado.** El estado del objeto después de ser analizado. El estado muestra si un correo electrónico se marca como correo no deseado o con contenido no deseado, o si un archivo adjunto está infectado por malware, es sospechoso de estar infectado, o se considera no deseado o no analizable.
- **Nombre del archivo adjunto.** El nombre del archivo adjunto detectado por el módulo de Filtrado de adjuntos o Antimalware.

- **Nombre del malware.** Nombre dado a la amenaza de malware por los investigadores de seguridad de Bitdefender. Esta información está disponible solo si el objeto estaba infectado.
- **Punto de detección.** Un objeto se detecta o bien en el nivel de transporte, o bien en un buzón o carpeta pública del almacén de Exchange.
- **Regla cumplida.** La regla de política que cumplió la amenaza.
- **Servidor.** Nombre de host del servidor en el que se detectó la amenaza.
- **IP del remitente.** Dirección IP del remitente.
- **Remitente (De).** La dirección de correo electrónico del remitente que aparece en el campo **De** del encabezado del mensaje de correo electrónico.
- **Destinatarios.** La lista de destinatarios que aparecen en los campos **Para** y **CC** del encabezado del mensaje de correo electrónico.
- **Destinatarios reales.** La lista de direcciones de correo electrónico de los usuarios individuales a los que iba destinado el mensaje antes de ser puesto en cuarentena.
- **Asunto.** El asunto del mensaje de correo electrónico en cuarentena.

Nota
La marca de puntos suspensivos al final del texto indica que se ha omitido una parte del mismo. En este caso, mueva el ratón sobre el texto para verlo en una caja de información.

10.3.2. Objeto en cuarentena

Los mensajes de correo electrónico y archivos puestos en cuarentena por el módulo de Protección de Exchange se almacenan localmente en el servidor como archivos cifrados. Desde el Control Center tiene la opción de restaurar los correos en cuarentena, así como eliminar o guardar cualquier archivo o mensaje de correo electrónico en cuarentena.

Restaurar mensajes de correo electrónico de la cuarentena

Si decide que un mensaje de correo electrónico en cuarentena no representa una amenaza, puede liberarlo de ésta. Si usa Exchange Web Services, la Protección de Exchange envía el mensaje de correo electrónico en cuarentena a sus destinatarios como archivo adjunto a un correo de notificación de Bitdefender.

Nota
Solo puede restaurar los mensajes de correo electrónico. Para recuperar un archivo adjunto en cuarentena, debe guardarlo en una carpeta local del servidor de Exchange.

Para restaurar uno o más mensajes de correo electrónico:

1. Vaya a la página **Cuarentena**.
2. Elija **Exchange** en el selector de vistas disponible en la zona superior de la página.
3. Marque las casillas de verificación correspondientes a los mensajes de correo electrónico que desee restaurar.
4. Haga clic en el botón **Restaurar** de la zona superior de la tabla. Aparecerá la ventana **Restaurar credenciales**.
5. Seleccione las credenciales de un usuario de Exchange autorizado para enviar los mensajes de correo electrónico que desee restaurar. Si las credenciales que va a utilizar son nuevas, tiene que añadirlas previamente al Gestor de credenciales.

   Para añadir las credenciales requeridas:

   a. Introduzca la información necesaria en los campos correspondientes del encabezado de la tabla:
      - El nombre de usuario y la contraseña del usuario de Exchange.

        Nota
        El nombre de usuario debe incluir el nombre de dominio, con el formato `usuario@dominio` o `dominio\usuario`.

      - La dirección de correo electrónico del usuario de Exchange, necesaria solo cuando la dirección de correo electrónico es diferente del nombre de usuario.
      - La URL de Exchange Web Services (EWS), necesaria cuando no funciona la detección automática de Exchange. Este suele ser el caso de los servidores de transporte perimetral en una DMZ.

   b. Haga clic en el botón **Añadir** del lateral derecho de la tabla. El nuevo conjunto de credenciales se añade a la tabla.
6. Haga clic en el botón **Restaurar**. Aparecerá un mensaje de confirmación.

La acción solicitada se envía inmediatamente a los servidores objetivo. Una vez restaurado un mensaje de correo electrónico, también se elimina de la cuarentena, por lo que la entrada correspondiente desaparecerá de la tabla de cuarentena.

Puede comprobar el estado de la acción de restauración en cualquiera de estos lugares:

- Columna **Estado de la acción** de la tabla de cuarentena.
- Página **Red > Tareas**.

Guardar archivos de la cuarentena

Si desea examinar o recuperar datos de archivos en cuarentena, puede guardar los archivos en una carpeta local en el servidor de Exchange. Bitdefender Endpoint Security Tools descifra los archivos y los guarda en la ubicación especificada.

Para guardar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Elija **Exchange** en el selector de vistas disponible en la zona superior de la página.
3. Filtre los datos de la tabla para ver todos los archivos que desee guardar, mediante la introducción de los términos de búsqueda en los campos de encabezado de columna.
4. Marque las casillas de verificación correspondientes a los archivos en cuarentena que desee restaurar.
5. Haga clic en el botón **Guardar** de la zona superior de la tabla.
6. Introduzca la ruta de la carpeta de destino en el servidor de Exchange. Si la carpeta no existe en el servidor, se creará.

   Importante
   Debe excluir esta carpeta del análisis del sistema de archivos, pues de no ser así los archivos se moverían a la Cuarentena de equipos y máquinas virtuales. Para más información, diríjase a “Exclusiones” (p. 293).

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

   Puede observar el estado pendiente en la columna **Estado de acción**. Puede ver también el estado de la acción en la página **Red > Tareas**.

Eliminación automática de archivos de la cuarentena

Los archivos en cuarentena con una antigüedad superior a 30 días se eliminan automáticamente de forma predeterminada. Puede cambiar este ajuste modificando la política asignada al servidor de Exchange administrado.

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

1. Diríjase a la página **Políticas**.
2. Haga clic en el nombre de la política asignada al servidor de Exchange administrado que le interese.
3. Acceda a la página **Protección de Exchange > General**.
4. En la sección **Ajustes**, seleccione el número de días transcurrido el cual se borrarán los archivos.
5. Haga clic en **Guardar** para aplicar los cambios.

Eliminación manual de archivos de la cuarentena

Para eliminar uno o más objetos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Seleccione **Exchange** en el selector de vistas.
3. Marque las casillas de verificación correspondientes a los archivos que desee eliminar.
4. Haga clic en el botón ⊖ **Eliminar** de la parte superior de la tabla. Tendrá que confirmar esta acción haciendo clic en **Sí**.

   Puede observar el estado pendiente en la columna **Estado de acción**.

   La acción solicitada se envía inmediatamente a los servidores objetivo. Una vez que se ha eliminado un archivo, la entrada correspondiente desaparecerá de la tabla Cuarentena.

Vaciado de la cuarentena

Para eliminar todos los objetos en cuarentena:

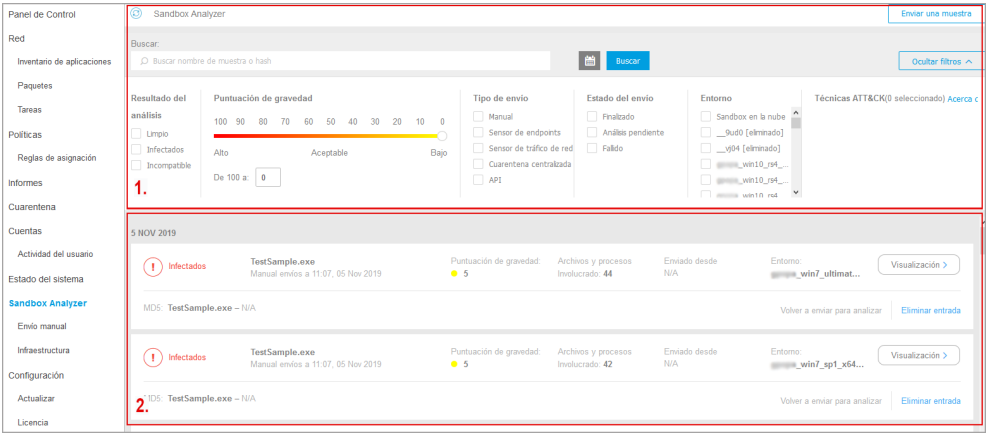
1. Vaya a la página **Cuarentena**.
2. Seleccione **Exchange** en el selector de vistas.
3. Haga clic en el botón **Vaciar cuarentena**.

Tendrá que confirmar esta acción haciendo clic en **Sí**.

Se borrarán todos los elementos de la tabla Cuarentena. La acción solicitada se envía inmediatamente a los objetos de la red objetivo.

11. USO DE SANDBOX ANALYZER

La página **Sandbox Analyzer** proporciona una interfaz unificada para ver, filtrar y buscar en envíos automáticos y manuales al entorno de espacio aislado. La página **Sandbox Analyzer** consta de dos zonas:



La página Sandbox Analyzer

1. El **área de filtrado** le permite buscar y filtrar envíos por varios criterios: nombre, hash, fecha, resultado del análisis, estado, entorno de detonación y técnicas ATT&CK de MITRE.
2. La **zona de tarjetas de envíos** muestra todos los envíos en un formato compacto con información detallada sobre cada uno de ellos.

En la página Sandbox Analyzer, puede hacer lo siguiente:

- Filtrar tarjetas de envíos
- Ver la lista de envíos y la información de análisis
- Reenviar muestras al análisis desde la tarjeta de envío
- Eliminar tarjetas de envíos
- Realizar envíos manuales

11.1. Filtrar tarjetas de envíos

En el área de filtros puede hacer lo siguiente:

- Filtra envíos por diversos criterios. La página cargará automáticamente solo las tarjetas de eventos de seguridad que cumplan los criterios seleccionados.
- Restablezca los filtros haciendo clic en el botón **Borrar filtros**.
- Oculte el área de filtros haciendo clic en el botón **Ocultar filtros**. Puede volver a mostrar las opciones ocultas haciendo clic en **Mostrar filtros**.

Puede filtrar los envíos de Sandbox Analyzer según los siguientes criterios:

- **Nombre de la muestra y hash (MD5)**. Introduzca en el campo de búsqueda el nombre completo, una parte o el hash de la muestra que está buscando y luego haga clic en el botón **Buscar** del lado derecho.
- **Fecha**. Para filtrar por fecha:
  1. Haga clic en el icono del calendario para configurar el período de la búsqueda.
  2. Defina el intervalo. Haga clic en los botones **Desde** y **Hasta** de la parte superior del calendario para seleccionar las fechas que definen el intervalo de tiempo. También puede seleccionar un período predeterminado, en la lista de opciones de la derecha, respecto al momento actual (por ejemplo, los últimos treinta días).

     Asimismo, puede especificar la hora y los minutos para cada fecha del intervalo de tiempo mediante las opciones que hay debajo del calendario.
  3. Haga clic en **Aceptar** para aplicar el filtro.
- **Resultado del análisis**. Seleccione una o varias de las siguientes opciones:
  - **Limpio**: La muestra es segura.
  - **Infectado**: La muestra es peligrosa.
  - **Incompatible**: La muestra tiene un formato que Sandbox Analyzer no ha podido detonar. Para ver la lista completa con los tipos de archivo y las extensiones compatibles con Sandbox Analyzer, consulte "Tipos de archivo y extensiones admitidas para el envío manual" (p. 531).
- **Puntuación de gravedad**. El valor indica lo peligrosa que es una muestra en una escala de 100 a 0. Cuanta más alta sea la puntuación, más peligrosa será la

muestra. La puntuación de gravedad se aplica a todas las muestras enviadas, incluidas las que tienen el estado **Limpio** o **Incompatible**.

- **Tipo de envío**. Seleccione una o varias de las siguientes opciones:
  - **Manual**. Sandbox Analyzer ha recibido la muestra mediante la opción de **Envío manual**.
  - **Sensor de endpoint**. Bitdefender Endpoint Security Tools ha enviado la muestra a Sandbox Analyzer según los ajustes de la política.
  - **Sensor de tráfico de red**. El sensor de red ha enviado la muestra a una instancia local de Sandbox Analyzer según los ajustes de la política.
  - **Cuarentena centralizada**. GravityZone ha enviado la muestra a una instancia local de Sandbox Analyzer según los ajustes de la política.
  - **API**. La muestra se ha enviado a una instancia local de Sandbox Analyzer mediante métodos de API.
  - **Sensor ICAP**. Security Server ha enviado la muestra a una instancia local de Sandbox Analyzer después de analizar un servidor ICAP.
- **Estado del envío**. Marque una o varias de las siguientes casillas de verificación:
  - **Terminado**: Sandbox Analyzer ha entregado el resultado del análisis.
  - **Análisis pendiente**: Sandbox Analyzer está detonando la muestra.
  - **Fallido**: Sandbox Analyzer no ha podido detonar la muestra.
- **Entorno**. Aquí se indican las máquinas virtuales disponibles para la detonación, incluida la instancia de Sandbox Analyzer alojada por Bitdefender. Marque una o varias casillas de verificación para ver qué muestras se han detonado en determinados entornos.
- **Técnicas ATT&CK**. Esta opción de filtrado integra la base de conocimientos ATT&CK de MITRE. Los valores de las técnicas ATT&CK cambian dinámicamente en función de los eventos de seguridad.

  Haga clic en el enlace **Acerca de** para abrir la tabla de técnicas ATT&CK en una nueva pestaña.

11.2. Consulta de los detalles del análisis

La página **Sandbox Analyzer** muestra las tarjetas de envíos por días, en orden cronológico inverso. Las tarjetas de envíos incluyen los siguientes datos:

- Resultado del análisis
- Nombre de la muestra
- Tipo de envío
- Puntuación de gravedad
- Archivos y procesos involucrados
- Entorno de detonación
- Valor hash (MD5)
- Técnicas ATT&CK
- Estado del envío, cuando no hay disponible un resultado

Cada tarjeta de envío incluye un enlace a un detallado informe HTML del análisis, caso de estar disponible. Para abrir el informe, haga clic en el botón **Ver** a la derecha de la tarjeta.

El informe HTML proporciona abundante información organizada en varios niveles, con texto descriptivo, gráficos y capturas de pantalla que ilustran el comportamiento de la muestra en el entorno de detonación. Mediante un informe HTML de Sandbox Analyzer puede averiguar lo siguiente:

- Datos generales sobre la muestra analizada, como nombre y clasificación de malware, detalles del envío (nombre de archivo, tipo y tamaño, hash, momento del envío y duración del análisis).
- Resultados del análisis de comportamiento, que incluyen todos los eventos de seguridad capturados durante la detonación, organizados en secciones. Los eventos de seguridad se refieren a:
  - Escritura/borrado/traslado/duplicación/sustitución de archivos en el sistema y en unidades extraíbles.
  - Ejecución de archivos recién creados.
  - Cambios en el sistema de archivos.
  - Cambios en las aplicaciones que se ejecutan dentro de la máquina virtual.
  - Cambios en la barra de tareas de Windows y en el menú Inicio.
  - Creación/terminación/inyección de procesos.
  - Escritura/borrado de claves del registro.
  - Creación de objetos mutex.
  - Creación/inicio/parada/modificación/consulta/eliminación de servicios.
  - Cambio de los ajustes de seguridad del navegador.
  - Cambio de la configuración de visualización del Explorador de Windows.
  - Adición de archivos a la lista de excepciones del cortafuego.
  - Cambio de los ajustes de red.
  - Activación de la ejecución en el inicio del sistema.

- Conexión a un host remoto.
- Acceso a determinados dominios.
- Transferencia de datos desde y hacia ciertos dominios.
- Acceso a URL, IP y puertos a través de varios protocolos de comunicación.
- Comprobación de los indicadores del entorno virtual.
- Comprobación de los indicadores de las herramientas de monitorización.
- Creación de instantáneas.
- Enlaces SSDT, IDT e IRP.
- Volcados de memoria para procesos sospechosos.
- Llamadas a funciones de la API de Windows.
- Inactividad durante un cierto período de tiempo para retrasar la ejecución.
- Creación de archivos con acciones que han de ejecutarse en determinados intervalos de tiempo.

Importante
Los informes HTML solo están disponibles en inglés, independientemente del idioma en que utilice GravityZone Control Center.

11.3. Reenvío de muestra

Desde la zona de tarjetas de envío, puede reenviar muestras ya detonadas a una instancia local de Sandbox Analyzer sin tener que cargarlas nuevamente. Puede hacer esto con las muestras enviadas previamente a la instancia local de Sandbox Analyzer desde cualquier sensor o método, de forma automática, manual o mediante API.

Para volver a enviar una muestra:

1. Haga clic en **Volver a enviar para analizar** en la tarjeta de envíos.
2. En la ventana de configuración, mantenga los ajustes de envío anteriores o cámbielos de la siguiente manera:
   a. En **Administración de imágenes**, seleccione la imagen de máquina virtual que desee usar para la detonación.
   b. En **Configuraciones de detonación**, configure los siguientes ajustes:
      i. **Límite de tiempo para la detonación de muestras (minutos)**. Asigne una cantidad fija de tiempo para completar el análisis de la muestra. El valor por defecto es 4 minutos, pero a veces el análisis puede tardar más tiempo. Al final del intervalo configurado, Sandbox Analyzer interrumpe el análisis y genera un informe basado en los datos recopilados hasta

ese momento. Si se interrumpe antes de completarse, el análisis podría arrojar resultados inexactos.

ii. **Número de repeticiones de ejecución permitidas**. En caso de errores inesperados, Sandbox Analyzer intenta detonar la muestra según se ha configurado hasta que finalice el análisis. El valor por defecto es 2. Eso significa que Sandbox Analyzer intentará detonar la muestra dos veces más en caso de error.

iii. **Filtrado previo**. Seleccione esta opción para excluir de la detonación las muestras ya analizadas.

iv. **Acceso a Internet durante la detonación**. Durante el análisis, algunas muestras requieren conectarse a Internet para poder completar el análisis. Para obtener los mejores resultados, se recomienda mantener está opción activada.

c. En **Perfil de detonación**, ajuste el nivel de complejidad del análisis de comportamiento, lo cual afecta al rendimiento de Sandbox Analyzer. Por ejemplo, si se fija en **Alto**, Sandbox Analyzer realizará, en el mismo intervalo, un análisis más preciso sobre menos muestras que si está en **Medio** o **Bajo**.

3. Haga clic en **Reenviar**.

Tras el reenvío, la página **Sandbox Analyzer** muestra una nueva tarjeta y la retención de datos de esa muestra se extiende consiguientemente.

Nota
La opción **Volver a enviar para analizar** está disponible para las muestras que sigan presentes en el datastore de Sandbox Analyzer. Asegúrese de que la retención de datos esté configurada en la página **Sandbox Analyzer > Sandbox Manager** de los ajustes de la política.

11.4. Eliminar tarjetas de envíos

Para eliminar una tarjeta de envío que ya no necesite:

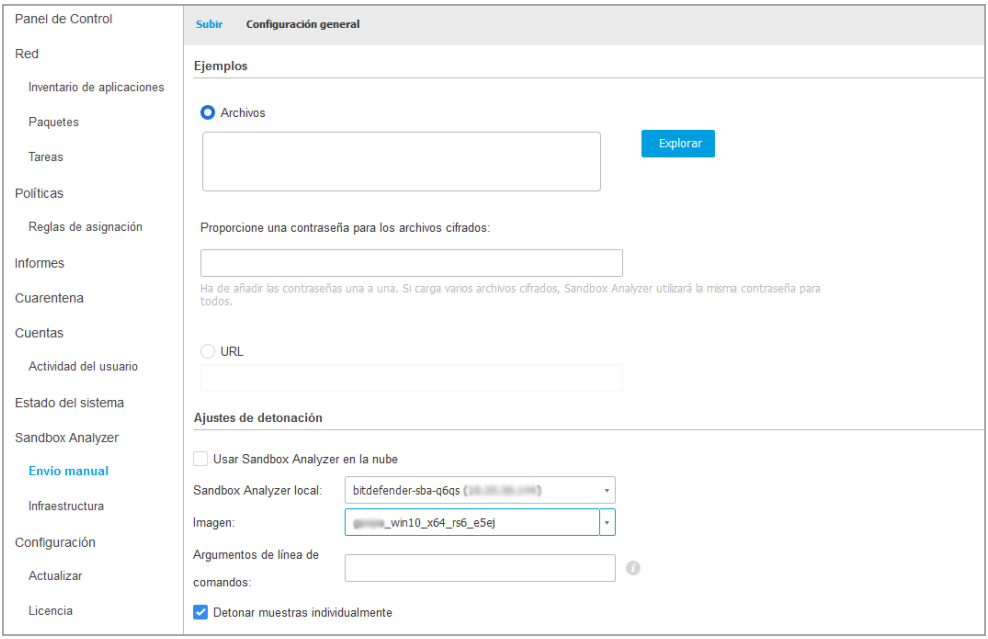
1. Acceda a la tarjeta de envío que desea eliminar.
2. Haga clic en la opción **Eliminar entrada** a la izquierda de la tarjeta.
3. Haga clic en **Sí** para confirmar la acción.

Nota
Siguiendo estos pasos, solo borrará la tarjeta de envío. La información sobre el envío seguirá disponible en el informe **Resultados de Sandbox Analyzer (en desuso)**. No obstante, este informe seguirá proporcionándose por tiempo limitado.

11.5. Envío manual

Desde **Sandbox Analyzer > Envío manual** puede enviar muestras de objetos sospechosos a Sandbox Analyzer para averiguar si son amenazas o archivos inofensivos. También puede acceder a la página de **Envío manual** haciendo clic en el botón **Enviar una muestra** de la parte superior derecha del área de filtrado en la página de Sandbox Analyzer.

Nota
El envío manual a Sandbox Analyzer es compatible con todos los navegadores requeridos por Control Center, excepto Internet Explorer 9. Para enviar objetos a Sandbox Analyzer, inicie sesión en Control Center con cualquier otro navegador compatible especificado en “Conectar a Control Center” (p. 20).



Sandbox Analyzer > Envío manual

Para enviar muestras a Sandbox Analyzer:

1. En la página **Cargar**, en **Muestras**, seleccione el tipo de objeto:
   a. **Archivos**. Haga clic en el botón **Examinar** para seleccionar los objetos que desea enviar para el análisis de comportamiento. En el caso de archivos protegidos con contraseña, puede definir una contraseña por sesión de carga en un campo a tal fin. Durante el proceso de análisis, Sandbox Analyzer aplica la contraseña especificada a todos los archivos enviados.
   b. **URL**. Rellene el campo correspondiente con cualquier URL que desee analizar. Puede enviar solo una URL por sesión.
2. En **Ajustes de detonación**, configure los parámetros de análisis para la sesión actual:
   - La instancia de Sandbox Analyzer que desee utilizar. Puede seleccionar la instancia en la nube o una instancia de Sandbox Analyzer instalada localmente.

Si elige utilizar una instancia local de Sandbox Analyzer, puede seleccionar varias máquinas virtuales a las que enviar simultáneamente la muestra.

- **Argumentos de línea de comandos**. Añada tantos argumentos de línea de comandos como desee, separados por espacios, para modificar el funcionamiento de ciertos programas, como los ejecutables. Los argumentos de la línea de comandos se aplican a todas las muestras enviadas durante el análisis.
- **Detonar muestras individualmente**. Marque la casilla de verificación para analizar los archivos del paquete uno por uno.

3. En **Perfil de detonación**, ajuste el nivel de complejidad del análisis de comportamiento, lo cual afecta al rendimiento de Sandbox Analyzer. Por ejemplo, si se fija en **Alto**, Sandbox Analyzer realizará, en el mismo intervalo, un análisis más preciso sobre menos muestras que si está en **Medio** o **Bajo**.
4. En la página **Ajustes generales**, puede establecer configuraciones aplicables a todos los envíos manuales, independientemente de la sesión:
   a. **Límite de tiempo para la detonación de muestras (minutos)**. Asigne una cantidad fija de tiempo para completar el análisis de la muestra. El valor por defecto es 4 minutos, pero a veces el análisis puede tardar más tiempo. Al final del intervalo configurado, Sandbox Analyzer interrumpe el análisis y genera un informe basado en los datos recopilados hasta ese momento. Si se interrumpe antes de completarse, el análisis podría arrojar resultados inexactos.
   b. **Número de repeticiones de ejecución permitidas**. En caso de errores inesperados, Sandbox Analyzer intenta detonar la muestra según se ha configurado hasta que finalice el análisis. El valor por defecto es 2. Eso significa que Sandbox Analyzer intentará detonar la muestra dos veces más en caso de error.
   c. **Filtrado previo**. Seleccione esta opción para excluir de la detonación las muestras ya analizadas.
   d. **Acceso a Internet durante la detonación**. Durante el análisis, algunas muestras requieren conectarse a Internet para poder completar el análisis. Para obtener los mejores resultados, se recomienda mantener está opción activada.
   e. Haga clic en **Guardar** para conservar los cambios.

5. Vuelva a la página **Cargar**.
6. Haga clic en **Enviar** Una barra de progreso indica el estado del envío.

   Después del envío, la página de **Sandbox Analyzer** muestra una nueva tarjeta. Una vez finalizado el análisis, la tarjeta proporciona el veredicto y los detalles correspondientes.

Nota
Para enviar muestras manualmente a Sandbox Analyzer debe tener privilegios de **administración de red**.

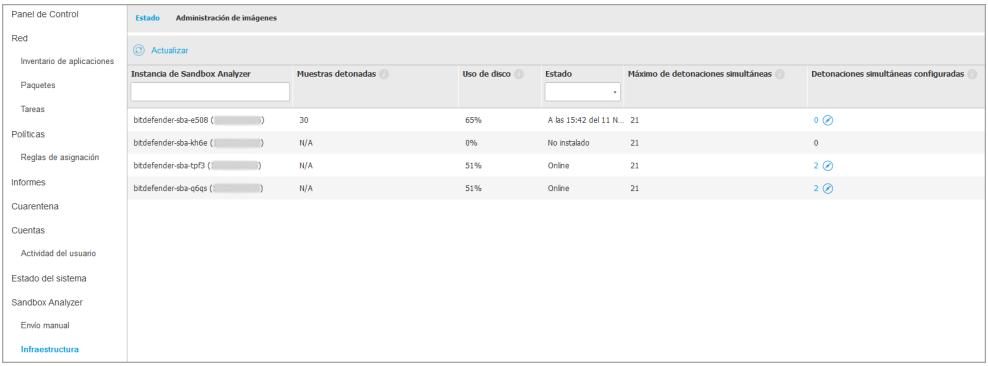
11.6. Infraestructura de administración de Sandbox Analyzer

En la sección **Sandbox Analyzer > Infraestructura**, puede realizar las siguientes acciones relacionadas con la instancia de Sandbox Analyzer instalada localmente:

- Comprobar el estado de la instancia de Sandbox Analyzer
- Configurar las detonaciones simultáneas
- Comprobar el estado de las imágenes de las máquinas virtuales
- Configurar y administrar las imágenes de las máquinas virtuales

11.6.1. Comprobación del estado de Sandbox Analyzer

Tras implementar y configurar el appliance virtual de Sandbox Analyzer en el hipervisor ESXi, puede obtener información sobre la instancia local de Sandbox Analyzer en la página **Estado**.



Sandbox Analyzer > Infraestructura > Estado

La tabla le proporciona la siguiente información:

- **Nombre de la instancia de Sandbox Analyzer**. Cada nombre corresponde a una instancia de Sandbox Analyzer instalada en un hipervisor ESXi. Puede instalar Sandbox Analyzer en varios hipervisores ESXi.
- **Muestras detonadas**. El valor indica el número de muestras analizadas desde que la instancia de Sandbox Analyzer obtuvo su licencia por primera vez.
- **Uso del disco**. El porcentaje indica la cantidad de espacio en disco consumido por Sandbox Analyzer en el datastore.
- **Estado**. En esta columna, verá si la instancia de Sandbox Analyzer está conectada, desconectada, si no está instalada, si la instalación está en curso o si la instalación ha fallado.
- **Máximo de detonaciones simultáneas**. El valor representa el número máximo de máquinas virtuales que Sandbox Analyzer puede crear para detonar muestras. Una máquina virtual no puede realizar varias detonaciones simultáneas. El número de máquinas virtuales viene dado por la cantidad de recursos de hardware disponibles en ESXi.
- **Detonaciones simultáneas configuradas**. Es el número real de máquinas virtuales creadas en función de la licencia disponible.
- **Usar proxy**. Haga clic en el conmutador de activar/desactivar para habilitar o inhabilitar la comunicación entre las instancias de GravityZone Control Center y Sandbox Analyzer a través de un servidor proxy. Para configurar un proxy,

vaya a **Configuración > Proxy** en el menú principal de Control Center. Si no se ha establecido ningún proxy, Control Center ignora esta opción.

Para obtener más información sobre la configuración proxy, consulte **Instalación de la protección > Instalación y configuración de GravityZone > Ajustes de configuración de Control Center > Proxy** en la Guía de instalación de GravityZone.

Nota
Control Center solo usa este proxy para comunicarse con instancias de Sandbox Analyzer On-Premises. Para comunicarse con la instancia en la nube de Sandbox Analyzer, Control Center usa el servidor proxy configurado en la página Sandbox Analyzer de los ajustes de la política.
Este proxy también es diferente del configurado en la página **General > Ajustes** de los ajustes de política, lo que garantiza la comunicación entre los endpoints y los componentes de GravityZone.

Puede buscar y filtrar columnas por estado y nombre de la instancia de Sandbox Analyzer. Utilice los botones de la esquina superior derecha de la tabla para actualizar la página, así como para mostrar y ocultar los filtros y columnas.

11.6.2. Configuración de detonaciones simultáneas

En la página **Estado**, puede configurar las detonaciones simultáneas, es decir, el número de máquinas virtuales que pueden ejecutar y detonar muestras simultáneamente en una instancia de Sandbox Analyzer. El número de detonaciones simultáneas depende de los recursos de hardware y de la distribución de slots de licencia en las diversas instancias de Sandbox Analyzer.

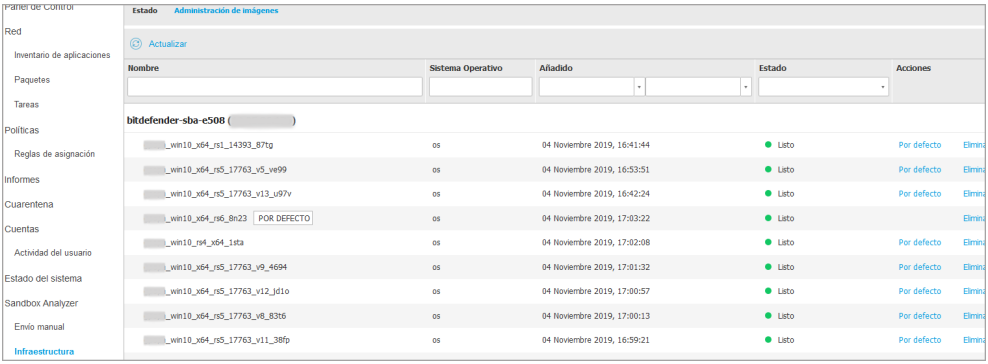
Para configurar las detonaciones simultáneas:

1. Haga clic en el número o en el icono **Editar** de la columna **Detonaciones simultáneas configuradas**.
2. En la nueva ventana, indique en el campo correspondiente el número de detonaciones simultáneas que desea asignar a la instancia de Sandbox Analyzer.
3. Haga clic en **Guardar**.

11.6.3. Comprobación del estado de las imágenes de las máquinas virtuales

Sandbox Analyzer utiliza imágenes de máquinas virtuales como entornos de detonación para realizar el análisis del comportamiento de las muestras enviadas.

Puede comprobar el estado de las máquinas virtuales en la página **Administración de imágenes**.



Sandbox Analyzer > Infraestructura > Administración de imágenes

La tabla le proporciona la siguiente información:

- **Nombre** de las imágenes de máquinas virtuales disponibles, como se indica en la consola del appliance de Sandbox Analyzer. Se agrupan varias imágenes de máquinas virtuales en la misma instancia de Sandbox Analyzer.
- **Sistema operativo**, como se indica en la consola del appliance de Sandbox Analyzer.
- La hora a la que se añadió la imagen de la máquina virtual.
- **Estado**. En esta columna, descubrirá si una imagen de máquina virtual es nueva y puede prepararse para la detonación, si está lista para la detonación o si el proceso de preparación ha fallado.
- **Acciones**. En esta columna, descubrirá qué puede hacer con las imágenes de las máquinas virtuales, según su estado: crear imágenes para la detonación, configurarlas como entornos de detonación por defecto o eliminarlas.

11.6.4. Configuración y administración de imágenes de máquinas virtuales

Creación de máquinas virtuales de detonación

Para detonar muestras usando la instancia local de Sandbox Analyzer, necesita crear máquinas virtuales dedicadas. La página **Administración de imágenes** le permite crear máquinas virtuales de detonación, siempre que haya añadido imágenes de máquinas virtuales en la consola del appliance de Sandbox Analyzer.

Nota
Para aprender a añadir imágenes de máquinas virtuales en la consola del appliance de Sandbox Analyzer, consulte el capítulo **Instalación del appliance virtual de Sandbox Analyzer** de la Guía de instalación de GravityZone.

Para crear máquinas virtuales de detonación, en la columna **Acciones**, haga clic en la opción **Crear imagen** para las imágenes de máquinas virtuales que tengan el estado: **nueva – requiere creación**. La creación de una máquina virtual requiere generalmente entre 15 y 30 minutos, dependiendo de su tamaño. Cuando finaliza su creación, el estado de las máquinas virtuales pasa a **Listo**.

Configuración de una máquina virtual por defecto

Una instancia de Sandbox Analyzer puede tener varias imágenes instaladas y configuradas como máquinas virtuales de detonación. En caso de envíos automáticos, Sandbox Analyzer empleará la primera imagen de máquina virtual creada para detonar las muestras.

Puede modificar este comportamiento configurando una imagen de máquina virtual por defecto. Para ello, haga clic en **Establecer por defecto** para la imagen de máquina virtual que prefiera.

Eliminación de máquinas virtuales

Para eliminar una imagen de máquina virtual de la página de **Administración de imágenes**, haga clic en **Eliminar** en la columna **Acciones**. En la ventana de confirmación, haga clic en **Eliminar imagen**.

12. 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
- Iniciar, finalizar, cancelar y detener procesos de solución de problemas en las máquinas afectadas
- Crear, editar, renombrar y eliminar cuentas de usuario
- Eliminar o mover endpoints entre grupos
- Crear, mover, renombrar y eliminar grupos
- Eliminar y restaurar archivos de la cuarentena
- Crear, editar y eliminar cuentas de usuario
- Crear, editar y eliminar reglas de permisos de acceso.
- Crear, editar, renombrar, asignar y eliminar políticas
- Editar los ajustes de autenticación para las cuentas de GravityZone.
- Crear, modificar, sincronizar y eliminar integraciones de Amazon EC2
- Crear, modificar, sincronizar y eliminar integraciones de Microsoft Azure
- Actualizar el appliance de GravityZone.

Para examinar los registros de actividad de usuarios, acceda a la página **Cuentas > Actividad del usuario** y escoja la vista de red que desee en el selector de vistas.

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.

13. USO DE HERRAMIENTAS

13.1. Inyección de herramientas personalizadas con HVI

Bitdefender HVI le libera de la carga de solucionar problemas, reunir datos forenses o ejecutar tareas de mantenimiento regulares en máquinas virtuales en su entorno Citrix, al permitirle inyectar sobre la marcha herramientas de terceros en los sistemas operativos guest. Estas operaciones se realizan a través de las API Direct Inspect (sin necesidad de conexión TCP/IP) y sin molestar a los usuarios finales. Para ello, las herramientas deben poder ejecutarse silenciosamente.

GravityZone le da 3 GB de espacio para mantener sus herramientas a salvo, desde donde podrá inyectarlas en los sistemas operativos guest.

Para cargar los kits de herramientas en GravityZone:

1. Descargue la versión más reciente de la herramienta en su equipo.
2. Comprima el kit en un archivo ZIP.
3. Acceda a GravityZone Control Center y haga clic en el menú **Herramientas** de la esquina inferior izquierda de la página. Se muestra la página del **Centro de administración de herramientas**.
4. Haga clic en el botón de carga correspondiente en la parte superior de la tabla, en función del sistema operativo de destino: **Cargar herramienta de Windows** o **Cargar herramienta de Linux**.
5. Si la herramienta es para Windows, también debe elegir en el menú desplegable la arquitectura de equipo aplicable.
6. Busque el archivo ZIP, selecciónelo y, a continuación, haga clic en **Abrir**.

   Para archivos grandes, es posible que tenga que esperar un par de minutos hasta que finalice la carga. Al terminar, la herramienta se añade en la tabla y la barra de progreso encima de esta actualiza la información referente al espacio disponible para cargas futuras.

Además del nombre de la herramienta, la tabla muestra otra información útil, como por ejemplo:

- El sistema operativo y la plataforma en la que se ejecuta la herramienta.
- Una breve descripción de la herramienta. Puede editar este campo en cualquier momento, si lo desea.

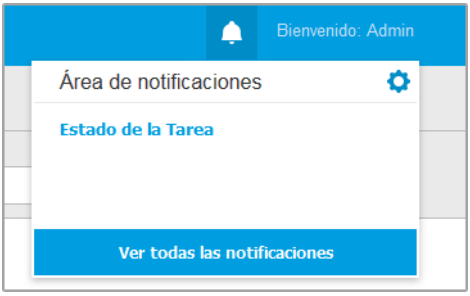
- El nombre del usuario que cargó la herramienta.
- Estado de la carga. Consulte este campo para asegurarse de que la herramienta se ha cargado correctamente.
- Fecha y hora de la carga.

A continuación, puede programar mediante políticas cuándo inyectar las herramientas, o inyectarlas en cualquier momento ejecutando tareas desde la página **Red**.

Cuando ya no utilice las herramientas, selecciónelas y, a continuación, haga clic en el botón **Eliminar** de la parte superior de la tabla para eliminarlas. Tendrá que confirmar esta acción haciendo clic en **Sí**.

14. 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**, ubicada en el lado derecho de Control Center.



Área de notificación

Cuando se detecten nuevos eventos en la red, el icono 11 de la esquina superior derecha de Control Center mostrará el número de nuevos eventos detectados. Haciendo clic en dicho icono se muestra el área de notificaciones que contiene la lista de eventos detectados.

14.1. 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 de malware según sus necesidades en la ventana **Opciones de notificación**. Para más información, diríjase a “Configurar las opciones de notificación” (p. 506).

Las amenazas detectadas por HyperDetect no se incluyen en esta notificación.

Disponibilidad de formato de Syslog: JSON, CEF

La licencia caduca

Esta notificación se envía 30 días, 7 días y un día antes de que caduque la licencia.

Debe tener privilegios de **administración de empresa** para ver esta notificación.

Disponibilidad de formato de Syslog: JSON, CEF

Se ha alcanzado el límite de utilización de licencias

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

Disponibilidad de formato de Syslog: JSON, CEF

Está a punto de alcanzarse el límite de licencia

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

Debe tener privilegios de **administración de empresa** para ver esta notificación.

Disponibilidad de formato de Syslog: JSON, CEF

Se ha alcanzado el límite de utilización de licencias de exchange

Esta notificación se activa cuando el número de buzones protegidos de sus servidores de Exchange alcanza el límite especificado en su clave de licencia.

Debe tener privilegios de **administración de empresa** para ver esta notificación.

Disponibilidad de formato de Syslog: JSON, CEF

Credenciales de usuario de Exchange no válidas

Esta notificación se envía cuando una tarea de análisis bajo demanda no se pudo iniciar en el servidor de Exchange objetivo debido a credenciales de usuario de Exchange no válidas.

Disponibilidad de formato de Syslog: JSON, CEF

Estado de actualización

Esta notificación se activa semanalmente si se encuentran versiones antiguas de productos en su red.

Disponibilidad de formato de Syslog: JSON, CEF

Actualización disponible

Esta notificación le informa de la disponibilidad de un nuevo GravityZone, un nuevo paquete o una nueva actualización de producto.

Disponibilidad de formato de Syslog: JSON, CEF

Conexión de Internet

Esta notificación se activa cuando los siguientes procesos detectan cambios en la conectividad a Internet:

- Validación de licencia.
- Obtención de una solicitud de firma de certificado de Apple.
- Comunicación con dispositivos móviles de Apple y Android.
- Acceso a la cuenta de MyBitdefender.

Disponibilidad de formato de Syslog: JSON, CEF

Conexión SMTP

Esta notificación se envía cada vez que Bitdefender GravityZone detecta cambios en cuanto a la conectividad del servidor de correo.

Disponibilidad de formato de Syslog: JSON, CEF

Usuarios de dispositivo móvil sin dirección de correo electrónico

Esta notificación se envía tras añadir dispositivos móviles a múltiples usuarios si no se ha especificado la dirección de correo electrónico para la cuenta de uno o varios usuarios seleccionados. Esta notificación tiene por objeto advertirle de que los usuarios que no tienen dirección de correo electrónico especificada no pueden inscribir los dispositivos móviles que se les asignen, dado que los detalles de activación se envían automáticamente por correo electrónico.

Para obtener más información sobre cómo añadir dispositivos móviles para múltiples usuarios, consulte la Guía de instalación de GravityZone.

Disponibilidad de formato de Syslog: JSON, CEF

Copia de Seguridad de la Base de datos

Esta notificación le informa sobre el estado de una copia de seguridad programada de una base de datos, ya sea con o sin éxito. Si la copia de seguridad de la base de datos ha fallado, el mensaje de notificación mostrará también la causa del error.

Para obtener más información acerca de la configuración de las copias de seguridad de bases de datos de GravityZone, consulte la Guía de instalación de GravityZone.

Disponibilidad de formato de Syslog: JSON, CEF

Malware de Exchange detectado

Esta notificación le informa cuando se detecta malware en un servidor de Exchange de su red.

Disponibilidad de formato de Syslog: JSON, CEF

Antiexploit avanzado

Esta notificación le informa de si el Antiexploit avanzado ha detectado un intento de exploit en su red.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Antimalware

Esta notificación le informa cuando se detecta malware en un endpoint de la red. Esta notificación se crea para cada detección de malware, con todos los detalles sobre el endpoint infectado (nombre, IP, agente instalado), el tipo de análisis, el malware detectado, la versión de firmas, el momento en que se detectó y el tipo de motor de análisis.

Disponibilidad de formato de Syslog: JSON, CEF

Integración sin sincronización

Esta notificación se envía cuando una integración de plataforma virtual existente no se ha podido sincronizar con GravityZone. En los ajustes de notificaciones, puede seleccionar las integraciones para las que desea recibir notificaciones cuando se produce un error de sincronización. Puede consultar más información sobre el estado de sincronización en los detalles de la notificación.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Antiphishing

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

Disponibilidad de formato de Syslog: JSON, CEF

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.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de ATC/IDS

Esta notificación se envía cada vez que se detecta y se bloquea una aplicación potencialmente peligrosa en un endpoint de la red. Hallará detalles sobre el tipo de aplicación, el nombre y la ruta, así como el ID y la ruta del proceso primario y la línea de comandos que inició el proceso, si fuera el caso.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Control de usuarios

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

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Protección de datos

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

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Módulos del producto

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

Disponibilidad de formato de Syslog: JSON, CEF

Evento de estado de Security Server

Este tipo de notificación proporciona información acerca de los cambios de estado de un determinado Security Server instalado en la red. Los cambios de estado del Security Server se refieren a los siguientes eventos: apagado/encendido, actualización del producto, actualización de los contenidos de seguridad y reinicio del sistema requerido.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Security Server sobrecargado

Esta notificación se envía cuando la carga de análisis en un Security Server de su red supera el umbral definido.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de Registro del producto

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

Disponibilidad de formato de Syslog: JSON, CEF

Auditoría de autenticación

Esta notificación le informa cuando se utiliza otra cuenta de GravityZone (excepto la suya propia) para iniciar sesión en Control Center desde un dispositivo no reconocido.

Disponibilidad de formato de Syslog: JSON, CEF

Inicio de sesión desde dispositivo nuevo

Esta notificación le informa de que se ha utilizado su cuenta de GravityZone para iniciar sesión en Control Center desde un dispositivo que no se había usado previamente a tal fin. La notificación se configura automáticamente para que sea visible tanto en Control Center como en el mensaje de correo electrónico y solo puede verla.

Disponibilidad de formato de Syslog: JSON, CEF

El certificado caduca

Esta notificación le informa de la caducidad de un certificado de seguridad. La notificación se envía treinta, siete y un día antes de la fecha de caducidad.

Disponibilidad de formato de Syslog: JSON, CEF

Actualización de GravityZone

La notificación se envía cuando se completa una actualización de GravityZone. Si se produce un error, la actualización se realizará de nuevo transcurridas 24 horas.

Disponibilidad de formato de Syslog: JSON, CEF

Estado de la Tarea

Esta notificación le informa cada vez que cambia el estado de una tarea o solo cuando termina una tarea, según sus preferencias.

Disponibilidad de formato de Syslog: JSON, CEF

Servidor de actualizaciones sin actualizar

Esta notificación se envía cuando un Servidor de actualizaciones de su red tiene contenidos de seguridad sin actualizar.

Disponibilidad de formato de Syslog: JSON, CEF

Evento de incidentes de red

Esta notificación se envía cada vez que el módulo Network Attack Defense detecta un intento de ataque en su red. Esta notificación también le informa de si el intento de ataque se realizó desde fuera de la red o desde un endpoint comprometido dentro de ella. Otros detalles incluyen datos sobre el endpoint,

la técnica de ataque, la IP del atacante y la medida adoptada por Network Attack Defense.

Disponibilidad de formato de Syslog: JSON, CEF

Se ha generado el informe personalizado

Esta notificación le informa de que se ha generado el informe basado en una consulta.

Disponibilidad de formato de Syslog: n/d

Violación de memoria detectada

Esta notificación le advierte cuando HVI detecta un ataque que viola la memoria de las máquinas virtuales protegidas en el entorno Citrix Xen. La notificación le proporciona datos importantes, como por ejemplo el nombre y la IP de la máquina infectada, la descripción del incidente, la fuente y el objetivo del ataque, la acción adoptada para eliminar la amenaza y el momento de la detección.

Se crean notificaciones para los siguientes incidentes:

- Intentos de utilizar un área de memoria de manera diferente a la prevista por el hipervisor mediante las tablas de página extendida (EPT).
- Intentos de los procesos de inyectar código en otros procesos.
- Intentos de cambiar las direcciones de procesos en las tablas de traducción.
- Intentos de cambiar los registros específicos del modelo (MSR).
- Intentos de cambiar los contenidos de determinados objetos de controlador o la tabla de descriptores de interrupción (IDT).
- Intentos de cargar determinados registros de control (CR) con valores no válidos.
- Intentos de cargar determinados registros de control extendidos (XCR) con valores no válidos.
- Intentos de cambiar las tablas de descriptores de interrupción o las tablas globales de descriptores.

Nota
La característica HVI puede estar disponible para su solución GravityZone con una clave de licencia independiente.

Disponibilidad de formato de Syslog: JSON, CEF

Nueva aplicación en el inventario de aplicaciones

Esta notificación le informa de cuándo el Control de aplicaciones ha detectado la instalación de una nueva aplicación en los endpoints supervisados.

Disponibilidad de formato de Syslog: JSON, CEF

Aplicación Bloqueada

Esta notificación le informa de cuándo el Control de aplicaciones ha bloqueado o habría bloqueado un proceso de una aplicación no autorizada, dependiendo de la configuración del módulo (modo de producción o de prueba).

Disponibilidad de formato de Syslog: JSON, CEF

Detección de Sandbox Analyzer

Esta notificación le avisa cada vez que Sandbox Analyzer detecta una nueva amenaza entre las muestras enviadas. Se le indican datos como el nombre de host o IP del endpoint, fecha y hora de la detección, tipo de amenaza, ruta de acceso, nombre, tamaño de los archivos y la acción de reparación adoptada para cada uno.

> **Nota**
> No recibirá notificaciones sobre las muestras analizadas que estén limpias. La información de todas las muestras enviadas está disponible en el informe **Resultados de Sandbox Analyzer (en desuso)** y en la sección **Sandbox Analyzer**, en el menú principal de Control Center.

Disponibilidad de formato de Syslog: JSON, CEF

Incidencia de ausencia de parche

Esta notificación se produce cuando a los endpoints de su red les faltan uno o más parches disponibles.

GravityZone envía automáticamente una notificación que contiene todos los resultados de las 24 horas anteriores a la fecha de notificación.

Puede ver qué endpoints se encuentran en esa situación haciendo clic en el botón **Ver informe** en los detalles de la notificación.

Por defecto, la notificación se refiere a los parches de seguridad pero también puede configurarla para que le informe sobre los ajenos a ella.

Disponibilidad de formato de Syslog: JSON, CEF

Detección de ransomware

Esta notificación le informa cuando GravityZone detecta un ataque de ransomware en su red. Se le proporciona información sobre el endpoint objetivo, el usuario que había iniciado sesión, el origen del ataque, la cantidad de archivos cifrados y la fecha y hora del ataque.

Cuando recibe la notificación, el ataque ya ha sido bloqueado.

El enlace presente en la notificación le dirigirá a la página **Actividad de ransomware**, donde puede ver la lista de archivos cifrados, y restaurarlos en caso necesario.

Disponibilidad de formato de Syslog: JSON, CEF

Antimalware de almacenamiento

Esta notificación se envía cuando se detecta malware en un dispositivo de almacenamiento compatible con ICAP. Esta notificación se crea para cada detección de malware, con todos los detalles sobre el dispositivo de almacenamiento infectado (nombre, IP, tipo), el malware detectado y el momento de la detección.

Disponibilidad de formato de Syslog: JSON, CEF

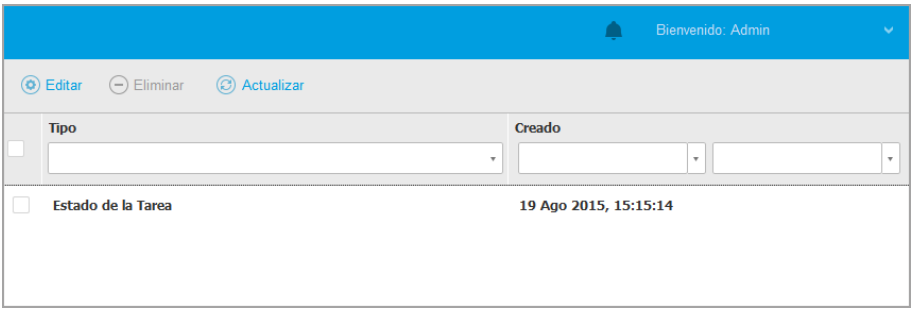
Dispositivos bloqueados

Esta notificación se activa cuando se conecta al endpoint un dispositivo bloqueado o con permisos de solo lectura. Si el mismo dispositivo se conecta varias veces en una hora, solo se envía una notificación durante este intervalo. Si el dispositivo se conecta nuevamente después de una hora, se remite una nueva notificación.

Disponibilidad de formato de Syslog: JSON, CEF

14.2. Ver notificaciones

Para ver las notificaciones, haga clic en el botón **Notificaciones** 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 tener varias páginas (por defecto solo se muestran 20 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.

14.3. Borrar notificaciones

Para borrar notificaciones:

1. Haga clic en el botón **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** de la zona superior de la tabla.

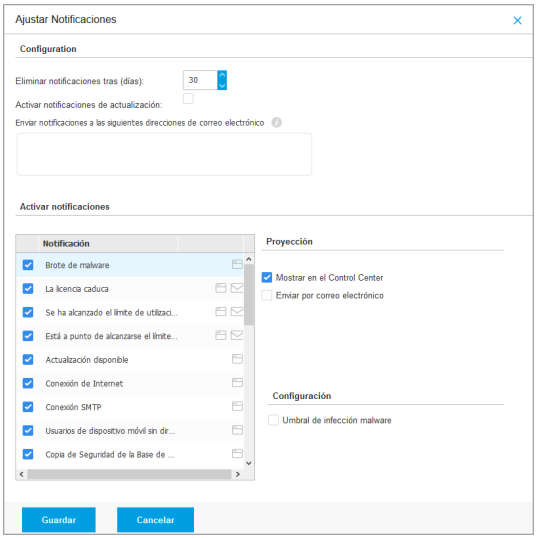
También puede configurar las notificaciones para que se borren automáticamente tras un cierto número de días. Para más información, diríjase a "Configurar las opciones de notificación" (p. 506).

14.4. 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 **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** en la zona superior 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:
   - Elimine automáticamente las notificaciones después de un cierto periodo de tiempo. Establezca el número que desee entre 0 y 365 en el campo **Eliminar notificaciones tras (días)**.
   - Marque la casilla de verificación **Activar notificaciones de actualización** si desea que el área de notificaciones se actualice automáticamente cada sesenta segundos.
   - Además, puede enviar las notificaciones por correo electrónico a determinados destinatarios. Escriba las direcciones de correo en el campo correspondiente y pulse la tecla `Intro` después de cada dirección.
4. En la sección **Activar notificaciones** puede elegir el tipo de notificaciones que desea recibir de GravityZone. 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. 496). Al seleccionar un tipo de notificación, puede configurar sus opciones concretas (cuando existan) en la zona de la derecha:

Proyección

- **Mostrar en Control Center** especifica que este tipo de eventos se muestra en Control Center, con la ayuda del botón **Notificaciones**.
- **Registrar en el servidor** especifica que este tipo de evento también se registra en el archivo `syslog`, en caso de que se haya configurado un syslog.

  Para obtener información sobre cómo configurar servidores syslog, consulte la Guía de instalación de GravityZone.
- **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.

Configuración

- **Usar umbral personalizado** permite definir un umbral a partir del cual se envía la notificación seleccionada para los eventos acontecidos.

  Por ejemplo, la Notificación de infección malware se envía por defecto 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, active la opción **Usar umbral personalizado** y, a continuación, introduzca el valor que desee en el campo **Umbral de infección malware**.

- En cuanto a la notificación de la **copia de seguridad de la base de datos**, puede elegir que se le notifique solo cuando haya fallado una copia de seguridad de la base de datos. Deje esta opción sin marcar si desea que se le notifiquen todos los eventos relacionados con la copia de seguridad de la base de datos.

- En **Evento de estado de Security Server** puede seleccionar los eventos de Security Server que activarán este tipo de notificación:

  - **Desactualizado** activa la notificación cada vez que se detecta en su red un Security Server sin actualizar.
  - **Apagado** activa la notificación cada vez que se ha apagado un Security Server en su red.
  - **Requiere reiniciar** activa la notificación cada vez que es necesario reiniciar un Security Server en su red.

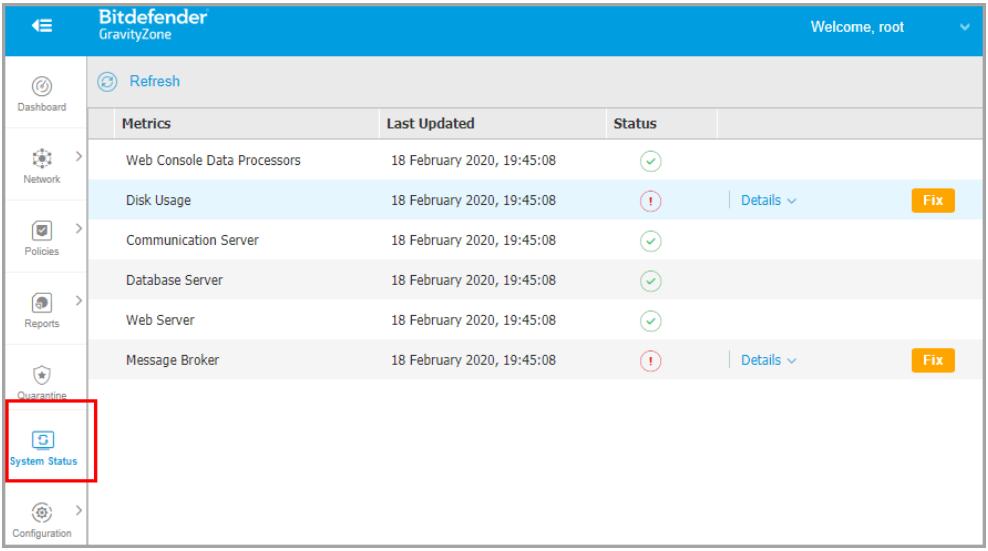
- Para **Estado de la tarea** puede seleccionar el tipo de estado que activará este tipo de notificación:

  - **Cualquier estado** activa la notificación cada vez que se ejecuta una tarea enviada desde Control Center con cualquier estado.
  - **Solo errores** activa la notificación cada vez que falla una tarea enviada desde Control Center.

5. Haga clic en **Guardar**.

15. ESTADO DEL SISTEMA

La página **Estado del sistema** muestra información del estado de salud de la implementación de GravityZone, lo que permite ver más fácilmente si algo va mal. La página proporciona métricas del sistema y su estado e indica cuándo se actualizaron por última vez, todo ello mostrado en forma de cuadrícula.



Página de Estado del sistema

La columna **Métricas** muestra todos los indicadores monitorizados por GravityZone Control Center. Para obtener más información sobre cada métrica y mensaje de estado, consulte "Procesadores de datos" (p. 533).

La columna **Última actualización** muestra la fecha y la hora de la última comprobación de estado de las métricas.

La columna **Estado** muestra el estado de cada métrica: **OK** u **Atención**. El **Estado** de las métricas se actualiza cada 15 minutos o cada vez que se hace clic en el botón **Actualizar**.

15.1. Estado OK

El estado OK indica que la métrica se comporta normalmente. En este caso, no se muestran detalles adicionales.

15.2. Estado de atención

El estado de atención indica que la métrica no está dentro de los parámetros normales.

En tal caso, debe investigar más para ver qué ha sucedido y solucionar los problemas actuales:

1. Haga clic en el botón **Detalles** para ampliar la información adicional relacionada con la métrica que vigila.

Detalles de métricas

- En **Appliance** puede hallar las direcciones IP de las máquinas afectadas
- En **Detalles** puede ver la información específica de cada métrica.

2. Haga clic en **Reparar** para reparar la métrica y GravityZone se encargará del resto.

Detalles de métricas

El estado de la métrica volverá a **OK** una vez que se haya reparado.

Nota
Para cualquier otro problema relacionado con las métricas, póngase en contacto con el servicio de soporte técnico empresarial.

15.3. Parámetros

La página **System Status** contiene información adicional sobre las siguientes métricas:

- Procesadores de datos de la consola web
- Uso de disco
- Servidor de comunicaciones
- Servidor de base de datos
- Servidor Web
- Agente de mensajes

Procesadores de datos de la consola web

Esta métrica monitoriza el estado de los procesadores de datos que se utilizan para compilar los datos mostrados en Control Center.

Mensaje de estado de atención	Detalles
`Procesadores que han fallado en este appliance: <lista de procesadores de datos> .`	Uno o varios procesadores de datos se han detenido.
`El appliance virtual está inactivo`	El appliance virtual que utiliza los servicios de la consola web está apagado.

Para ver una lista completa de los procesadores empleados por Control Center, consulte “Procesadores de datos” (p. 533).

Uso de disco

Esta métrica monitoriza la cantidad de espacio en disco utilizado por cada appliance virtual, cuánto queda y el espacio total en el disco. Si alguno de los discos se utiliza por encima del 80 %, la métrica muestra el estado de **Atención**.

Mensaje de estado de atención	Detalles
`Espacio usado en el disco (nombre del disco)?`	Uno o varios discos se utilizan por encima del 80 % de su capacidad máxima.
`El appliance virtual está inactivo`	El appliance virtual del que se informa está apagado.

Servidor de comunicaciones

Esta métrica monitoriza el enlace entre los agentes de seguridad instalados en sus endpoints y el Servidor de bases de datos.

Mensaje de estado de atención	Detalles
`El servicio está inactivo desde <marca de tiempo>`	El servicio ha dejado de funcionar.

Servidor de base de datos

Esta métrica monitoriza el estado de la base de datos de GravityZone.

Mensaje de estado de atención	Detalles
`El servicio está inactivo desde <marca de tiempo>`	El servicio ha dejado de ejecutarse en uno de los appliances.
`El appliance virtual está inactivo`	El appliance virtual que utiliza el Servidor de base de datos está apagado.

Servidor Web

Esta métrica monitoriza el estado del servidor web que aloja GravityZone Control Center.

Mensaje de estado de atención	Detalles
`El servicio está inactivo desde <marca de tiempo>`	El servidor ha dejado de ejecutarse en uno de los appliances.

Mensaje de estado de atención	Detalles
El appliance virtual está inactivo	El appliance virtual que utiliza este servidor está apagado.

Agente de mensajes

Esta métrica monitoriza el estado del servicio de agente de mensajes en appliances con roles de Consola web y de Servidor de comunicaciones.

Mensaje de estado de atención	Detalles
El servicio de agente de mensajes está inactivo en estos appliances	El servicio ha dejado de ejecutarse en uno de los appliances.
Ha fallado la conexión de red entre appliances	La conexión entre dos appliances se ha interrumpido.
El appliance virtual está inactivo	El appliance virtual que utiliza este servicio está apagado.

16. 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.

Nota
Puede encontrar información sobre los servicios y políticas de soporte que ofrecemos en nuestro Centro de Soporte técnico.

16.1. Centro de soporte de Bitdefender

El Centro de soporte de Bitdefender es el lugar al que acudir para obtener toda la asistencia técnica que necesite para su producto de 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.

La forma más sencilla de acceder a la documentación es desde la página **Ayuda y soporte** de Control Center. Haga clic en su nombre de usuario en la esquina superior derecha de la consola, seleccione **Ayuda y soporte** y, a continuación, elija el enlace de la guía en la que está interesado. La guía se abrirá en una nueva pestaña de su navegador.

También puede consultar y descargar la documentación en el Centro de soporte, en la sección **Documentación** disponible en las páginas de soporte de todos los productos.

16.2. Solicitar ayuda

Puede solicitar ayuda a través de nuestro Centro de soporte técnico online: Rellene el formulario de contacto y envíelo.

16.3. Usar la herramienta de soporte

La herramienta de soporte GravityZone 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.

16.3.1. Uso de la herramienta de soporte en sistemas operativos Windows

Ejecución de la aplicación de la herramienta de soporte

Para generar el registro en el equipo afectado, siga uno de estos métodos:

- Línea de comandos

  Para cualquier problema con BEST, instalado en el equipo.

- Incidencia de instalación

  En casos en los que BEST no esté instalado en el equipo y falle la instalación.

Método de línea de comandos

Mediante la línea de comandos puede recopilar registros directamente desde el equipo afectado. Este método es útil en situaciones en las que no se tiene acceso al GravityZone Control Center o en las que el equipo no se comunica con la consola.

1. Abra el símbolo del sistema con privilegios administrativos.
2. Diríjase a la carpeta de instalación del producto. La ruta por defecto es:

   `C:\Archivos de programa\Bitdefender\Endpoint Security`
3. Recopile y guarde los registros ejecutando este comando:

```
Product.Support.Tool.exe collect
```

Los registros se guardan por defecto en `C:\Windows\Temp`.

Como alternativa, si desea guardar el registro de la herramienta de soporte en una ubicación personalizada, use la ruta opcional:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Ejemplo:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Mientras se ejecuta el comando, podrá ver una barra de progreso en la pantalla. Tras finalizar el proceso, se muestra el nombre del archivo comprimido que contiene los registros y su ubicación.

Para enviar los registros al soporte empresarial de Bitdefender, acceda a `C:\Windows\Temp` o a la ubicación personalizada y busque el archivo comprimido `ST_[computername]_[currentdate]`. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

Incidencia de instalación

1. Para descargar la herramienta de soporte de BEST, haga clic aquí.
2. Ejecute como administrador el archivo ejecutable. Aparecerá una ventana.
3. Elija una ubicación para guardar el archivo comprimido con los registros.

   Mientras se recopilan los registros, podrá ver una barra de progreso en la pantalla. Tras finalizar el proceso, se muestra el nombre del archivo comprimido y su ubicación.

Para enviar los registros al soporte empresarial de Bitdefender, acceda a la ubicación seleccionada y busque el archivo comprimido `ST_[computername]_[currentdate]`. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

16.3.2. Uso de la herramienta de soporte en sistemas operativos Linux

En el caso de los sistemas operativos Linux, la herramienta de soporte va integrada con el agente de seguridad de Bitdefender.

Para recopilar información del sistema Linux mediante la herramienta de soporte, ejecute el siguiente comando:

```
# /opt/BitDefender/bin/bdconfigure
```

con las siguientes opciones disponibles:

- `--help` para obtener una lista con todos los comandos de la herramienta de soporte
- `enablelogs` para activar los registros del módulo de comunicaciones y del producto (todos los servicios se reiniciarán automáticamente)
- `enablelogs` para desactivar los registros del módulo de comunicación y del producto (todos los servicios se reiniciarán automáticamente)
- `deliverall` para crear:
  - Un archivo comprimido que contiene los registros de instalación, depositado en la carpeta `/var/log/BitDefender` con el siguiente formato: `bitdefender_nombreMáquina_hora.tar.gz`.

  Una vez creado el archivo comprimido:

  1. Se le preguntará si desea desactivar los registros. De ser necesario, los servicios se reiniciarán automáticamente.
  2. Se le preguntará si desea eliminar los registros.
- `deliverall -default` proporciona la misma información que en la opción anterior, pero se adoptarán las acciones por defecto para los registros, sin preguntar al usuario (los registros se desactivan y se eliminan).

También puede ejecutar el comando `/bdconfigure` directamente desde el paquete BEST (completo o downloader) sin tener el producto instalado.

Para informar de un problema de GravityZone que afecte a los sistemas Linux, siga los siguientes pasos, usando las opciones descritas anteriormente:

1. Active los registros del módulo de comunicaciones y del producto.
2. Trate de reproducir el problema.
3. Desactive los registros.
4. Cree el archivo comprimido con los registros.

5. Abra un ticket de soporte de correo electrónico mediante el formulario disponible en la página **Ayuda y soporte** de Control Center, con una descripción del problema y adjuntando el archivo comprimido de los registros.

La herramienta de soporte para Linux ofrece la siguiente información:

- Las carpetas `etc`, `var/log`, `/var/crash` (si existe) y `var/epag` de `/opt/BitDefender`, que contienen los ajustes y registros de Bitdefender
- El archivo `/var/log/BitDefender/bdinstall.log`, que contiene la información sobre la instalación
- El archivo `Network.txt`, que contiene los ajustes de red y la información de conectividad de la máquina
- El archivo `product.txt`, que incluye el contenido de todos los archivos `update.txt` de `/opt/BitDefender/var/lib/scan` y una lista recursiva completa de todos los archivos de `/opt/BitDefender`.
- El archivo `system.txt`, que contiene información general del sistema (versiones del kernel y de la distribución, RAM disponible y espacio libre en el disco duro)
- El archivo `users.txt`, que contiene información sobre el usuario
- Otra información referente al producto en relación con el sistema, como por ejemplo las conexiones externas de los procesos y el uso de la CPU
- Registros del sistema.

16.3.3. Uso de la herramienta de soporte en sistemas operativos Mac

Para enviar una solicitud al equipo de soporte técnico de Bitdefender, ha de proporcionar lo siguiente:

- Una descripción detallada del problema que se ha encontrado.
- Una captura de pantalla (si procede) del mensaje de error exacto que aparece.
- El registro de la herramienta de soporte.

Para obtener información del sistema Mac mediante la herramienta de soporte:

1. Descargue el archivo ZIP que contiene la herramienta de soporte.
2. Extraiga el archivo **BDProfiler.tool** del archivo comprimido.

3. Abra una ventana de Terminal.
4. Acceda a la ubicación del archivo **BDProfiler.tool**.

   Por ejemplo:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Dote al archivo de permisos de ejecución:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Ejecute la herramienta.

   Por ejemplo:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Pulse `Y` e introduzca la contraseña cuando se le pida que proporcione la contraseña del administrador.

   Espere un par de minutos a que la herramienta acabe de generar el registro. Hallará el archivo comprimido resultante (**Bitdefenderprofile_output.zip**) en su escritorio.

16.4. Información de contacto

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 18 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.

16.4.1. Direcciones

Departamento de ventas: enterprisesales@bitdefender.com
Centro de soporte:http://www.bitdefender.com/support/business.html
Documentación: gravityzone-docs@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.com

16.4.2. Distribuidor Local

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área, tanto a nivel comercial como en otras áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite http://www.bitdefender.es/partners.
2. Ir a **Localizador de Partner**.
3. La información de contacto de los distribuidores locales de Bitdefender debería mostrarse automáticamente. Si esto no sucede, seleccione el país en el que reside para ver la información.
4. Si no encuentra un distribuidor Bitdefender en su país, no dude en contactar con nosotros por correo en enterprisesales@bitdefender.com.

16.4.3. 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

Bitdefender

49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Teléfono: +33 (0)1 47 35 72 73
Correo: b2b@bitdefender.fr
Página web: http://www.bitdefender.fr
Centro de soporte: http://www.bitdefender.fr/support/business.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
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Tel (oficina&comercial): +49 (0) 2304 94 51 60
Teléfono (soporte técnico): +49 (0) 2304 99 93 004
Comercial: firmenkunden@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) 203 695 3415
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
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
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
Centro de soporte: http://www.bitdefender.com/support/business.html

A. Apéndices

A.1. Tipos de archivo compatibles

Los motores de análisis antimalware incluidos en las soluciones de seguridad de Bitdefender pueden analizar todos los tipos de archivo que puedan contener amenazas. La lista siguiente incluye los tipos de archivo que se analizan más comúnmente.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

```
xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo
```

A.2. Tipos y estados de los objetos de red

A.2.1. Tipos de objetos de red

Cada tipo de objeto disponible en la página **Red** está representado por un icono determinado.

En la tabla que se muestra a continuación hallará el icono y la descripción de todos los tipos de objeto disponibles.

icono	Tipo
	Grupo de red
	Equipo
	Equipo de relay
	Equipo de Exchange Server
	Equipo de relay de Exchange Server
	Máquina virtual
	Máquina virtual de relay
	Imagen maestra
	Máquina virtual de Exchange Server
	Máquina virtual de relay de Exchange Server
	Máquina virtual con vShield
	Máquina virtual relay con vShield
	Inventario Nutanix
	Nutanix Prism
	Cluster Nutanix
	Inventario VMware
	VMware vCenter
	Datacenter VMware

icono	Tipo
	Pool de recursos VMware
	Cluster VMware
	Inventario Citrix
	XenServer
	Pool Xen
	Inventario de Amazon EC2
	Integración de Amazon EC2
	Región de Amazon EC2/Microsoft Azure
	Zona de disponibilidad de Amazon EC2/Microsoft Azure
	Inventario de Microsoft Azure
	Integración de Microsoft Azure
	Security Server
	Security Server con vShield
	Host sin Security Server
	Host con Security Server
	VMware vApp
	Usuario de dispositivo móvil
	Dispositivo Móvil

A.2.2. Estados de objetos de red

Cada objeto de red puede tener diferentes estados en lo que respecta a su estado de administración, problemas de seguridad, conectividad, etc. En la tabla que se muestra a continuación hallará todos los iconos de estado disponibles y su descripción.

Nota
La tabla siguiente contiene algunos ejemplos de estado genéricos. Se pueden aplicar los mismos estados, por separado o combinados, a todos los tipos de objetos de red, como por ejemplo grupos de red, equipos, etc.

icono	Estado
	Host sin Servidor de seguridad, Desconectado
	Máquina virtual, Offline, No administrada
	Máquina virtual, Online, No administrada
	Máquina virtual, Online, Administrada
	Máquina virtual, Online, Administrada, Con problemas
	Máquina virtual, reinicio pendiente
	Máquina virtual, Suspendida
	Máquina virtual, Eliminada

A.3. 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; iso; 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; ps1; 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.4. Tipos de archivo de filtrado de adjuntos

El módulo de Control de contenidos ofrecido por Security for Exchange puede filtrar archivos adjuntos de correo electrónico según el tipo de archivo. Los tipos disponibles en Control Center incluyen las siguientes extensiones de archivo:

Archivos ejecutables

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Imágenes

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archivos

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Hojas de cálculo

fm3; ods; wk1; wk3; wks; xls; xlsx

Presentaciones

odp; pps; ppt; pptx

Documentos

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Variables del 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:

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

`%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`.

`%USERPROFILE%`

La ruta a la carpeta de perfil del usuario. Ruta típica:

`C:\Users\{username}`

En macOS, la carpeta del perfil del usuario corresponde a la carpeta Inicio. Use `$HOME` o ~ cuando configure exclusiones.

A.6. Herramientas del Control de aplicaciones

Para establecer las reglas del Control de aplicaciones en función del hash del ejecutable o de la huella digital del certificado, debe descargar las siguientes herramientas:

- **Fingerprint**, para obtener el valor personalizado del hash.
- **Thumbprint**, para obtener el valor personalizado de la huella digital del certificado.

Fingerprint

Haga clic aquí para descargar el ejecutable de Fingerprint , o acceda a http://download.bitdefender.com/business/tools/ApplicationControl/

Para obtener el hash de la aplicación:

1. Abra la ventana del **Símbolo del sistema**.
2. Acceda a la ubicación de la herramienta Fingerprint. Por ejemplo:

```
cd/users/fingerprint.exe
```

3. Para mostrar el valor hash de una aplicación, ejecute el siguiente comando:

```
fingerprint <application_full_path>
```

4. Vuelva a Control Center y configure la regla basada en el valor que obtuvo. Para obtener más información, consulte “Control de aplicaciones” (p. 344).

Thumbprint

Haga clic aquí para descargar el ejecutable de Thumbprint, o acceda a http://download.bitdefender.com/business/tools/ApplicationControl/

Para obtener la huella digital del certificado:

1. Ejecute el **Símbolo del sistema** como administrador.
2. Acceda a la ubicación de la herramienta Thumbprint. Por ejemplo:

```
cd/users/thumbprint.exe
```

3. Para mostrar la huella digital del certificado, ejecute el siguiente comando:

```
thumbprint <application_full_path>
```

4. Vuelva a Control Center y configure la regla basada en el valor que obtuvo. Para obtener más información, consulte "Control de aplicaciones" (p. 344).

A.7. Objetos Sandbox Analyzer

A.7.1. Tipos de archivo y extensiones admitidas para el envío manual

Las siguientes extensiones de archivo se admiten y pueden detonarse manualmente en Sandbox Analyzer:

Lotes, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (comprimido), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, archivos MZ/PE (ejecutable), PDF, PEF (ejecutable), PIF (ejecutable), RTF, SCR, URL (binario), VBE, VBS, WSF, WSH, WSH-VBS y XHTML.

Sandbox Analyzer es capaz de detectar los tipos de archivo antes mencionados también si se incluyen en archivos de los siguientes tipos: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, archivo comprimido

LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolumen), ZOO y XZ.

A.7.2. Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos

El prefiltrado de contenidos determinará un tipo de archivo en particular atendiendo tanto al contenido del objeto como a su extensión. Eso significa que un ejecutable que tenga la extensión `.tmp` será reconocido como una aplicación y, si parece sospechoso, se enviará a Sandbox Analyzer.

- Aplicaciones: archivos que tienen el formato PE32, incluyendo, entre otras, las extensiones `exe, dll y com`.
- Aplicaciones: archivos que tienen el formato de documento, incluyendo, entre otras, las extensiones `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf y pdf`.
- Scripts: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse y vbe`.
- Archivos comprimidos: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace y r00`.
- Correos electrónicos (guardados en el sistema de archivos): `eml y tnef`.

A.7.3. Exclusiones predeterminadas del envío automático

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png y txt`.

A.7.4. Aplicaciones recomendadas para las máquinas virtuales de detonación

Sandbox Analyzer On-Premises requiere que se instalen ciertas aplicaciones en las máquinas virtuales de detonación para que abran las muestras enviadas.

Aplicaciones	Tipos archivo
Suite Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx

Aplicaciones	Tipos archivo
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Windows por defecto	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Procesadores de datos

Nombre	Detalles
Reenviador de solicitudes de procesador	Reenvía solicitudes de procesador en entornos distribuidos
Integrador de hipervisión de VMware	Sincroniza el inventario de VMware y otra información con GravityZone
Integrador del hipervisor de Citrix	Sincroniza el inventario de Xen y otra información con GravityZone
Integrador genérico de virtualización	Sincroniza el inventario de Nutanix, Amazon EC2 y Azure con GravityZone
Integrador de NTSA	Sincroniza el estado de integración de Network Traffic Security Analytics (NTSA) y envía actualizaciones de licencia al appliance NTSA
Sincronizador del inventario de equipos de Active Directory	Sincroniza el inventario de equipos de Active Directory con GravityZone

Nombre	Detalles
Sincronizador del inventario de grupos de Active Directory	Sincroniza el inventario de grupos de Active Directory con GravityZone
Sincronizador de la importación de usuarios de Active Directory	Sincroniza las cuentas de usuario de Active Directory con GravityZone (se emplea para vincular cuentas de AD con cuentas de GravityZone)
Sincronizador del inventario de usuarios de Active Directory	Sincroniza el inventario de usuarios de Active Directory con GravityZone
Procesador de correo electrónico	Pone en cola los correos electrónicos para su envío desde GravityZone
Procesador de informes	Procesa informes y portlets
Implementador del agente de seguridad de Windows	Implementa el agente de seguridad de Bitdefender en dispositivos Windows
Implementador del Servidor de seguridad	Implementa Security Virtual Appliances
Administrador de licencias	Administra licencias de endpoints instalados
Procesador de notificaciones push para dispositivos móviles	Envía notificaciones push a dispositivos móviles protegidos
Implementador del agente de seguridad de Linux y macOS	Implementa el agente de Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE) en dispositivos Linux y macOS
Actualizador de productos y kits de endpoints	Descarga y publica kits de endpoint de Bitdefender y actualizaciones de productos
Actualizador de GravityZone	Actualiza automáticamente GravityZone cuando se configura. Actualiza la versión de los appliances virtuales de GravityZone
Limpiador de paquetes	Elimina los archivos de paquete sin uso
Procesador de problemas de seguridad	Procesa problemas de seguridad para los elementos de la sección Red
Procesador de copias de seguridad	Realiza copias de seguridad de la base de datos de GravityZone

Nombre	Detalles
Procesador de notificaciones	Envía notificaciones a los usuarios
Procesador de eventos del sistema	Gestiona eventos desde la infraestructura (Control de aplicaciones, Sandbox Analyzer, Serenity y SVA) o integraciones (Exchange, Nutanix y NSX)
Implementador del paquete suplementario HVI	Gestiona la instalación, actualización y eliminación del paquete suplementario HVI para hosts XEN
Procesador de tareas de reinicio HVI	Gestiona tareas de reinicio en hosts HVI
Procesador de estado de alimentación y de estado de conexión	Calcula el estado de alimentación y de conectividad de equipos y máquinas virtuales
Procesador de limpieza de máquinas sin conexión	Elimina de la red las máquinas sin conexión
Ejecutor de tareas en segundo plano	Maneja y ejecuta tareas y procesos en segundo plano

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.

Archivos sospechosos y tráfico de red

Los archivos sospechosos son los que tienen una reputación dudosa. Esta clasificación se otorga en función de muchos factores, entre los cuales se cuentan la existencia de la firma digital, el número de ocurrencias en las redes informáticas, el empaquetador utilizado, etc. El tráfico de red se considera sospechoso cuando se desvía del patrón. Por ejemplo, una fuente no fiable,

peticiones de conexión a puertos inusuales, aumento del uso de ancho de banda, tiempos de conexión aleatorios, etc.

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.

Ataques personalizados

Ataques informáticos que persiguen principalmente beneficios económicos o minar la reputación. El objetivo puede ser un individuo, una empresa, un software o un sistema que se ha estudiado concienzudamente antes de que el ataque tenga lugar. Estos ataques se desarrollan durante un largo período de tiempo y por etapas, aprovechando uno o más puntos de infiltración. Apenas se notan; la mayoría de las veces solo cuando el daño ya está hecho.

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.

Bootkit

Un bootkit es un programa malicioso que tiene la capacidad de infectar el registro de arranque maestro (MBR), el registro de arranque de volumen (VBR) o el sector de arranque. El bootkit permanece activo incluso después de un reinicio del sistema.

Capas de protección

GravityZone proporciona protección a través de una serie de módulos y roles, denominados colectivamente capas de protección, que se dividen en protección para endpoints (EPP) o protección central, así como varios complementos. La protección para endpoints incluye Antimalware, Advanced Threat Control, Antiexploit avanzado, Cortafuego, Control de contenido, Control de dispositivos,

Network Attack Defense, Usuario avanzado y Relay. Los complementos incluyen capas de protección como Security for Exchange y Sandbox Analyzer.

Para obtener más información sobre las capas de protección disponibles con su solución GravityZone, consulte “Capas de protección de GravityZone” (p. 2).

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.

Downloader de Windows

Es el nombre genérico que reciben los programas que tienen una funcionalidad primaria de descarga de contenidos con fines no deseados o maliciosos.

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).

Exploit

Un exploit se refiere generalmente a cualquier método utilizado para obtener acceso no autorizado a equipos, o una vulnerabilidad en la seguridad de un sistema que lo expone a un ataque.

Explorador

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web.

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.

Grayware

Una clase de aplicaciones de software entre el software legítimo y el malware. A pesar de que no son tan dañinas como el malware que afecta a la integridad del sistema, su comportamiento sigue siendo inquietante, y conduce a situaciones no deseadas como el robo de datos y el uso no autorizado o la publicidad no deseada. Las aplicaciones de grayware más comunes son el spyware y el adware.

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).

Ladrón de contraseñas

Un ladrón de contraseñas recopila datos que pueden ser nombres de cuentas y contraseñas asociadas a ellos. Estas credenciales robadas se utilizan con fines maliciosos, como por ejemplo apoderarse de las cuentas.

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 endpoint 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.

Ransomware

Un malware que le impide acceder a su equipo o bloquea su acceso a los archivos y aplicaciones. El ransomware le exigirá que pague una cantidad determinada (pago de un rescate) a cambio de una clave de descifrado que le permita recuperar el acceso a su equipo o a sus archivos.

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.

Tormentas de análisis antimalware

Un uso intensivo de recursos del sistema que tiene lugar cuando el software antivirus analiza simultáneamente múltiples máquinas virtuales en un solo host físico.

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.