

Bitdefender®

GravityZone

GUÍA DEL ADMINISTRADOR

Bitdefender GravityZone Guía del Administrador

fecha de publicación 2021.02.01

Copyright© 2021 Bitdefender

Advertencia legal

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

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

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

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

Tabla de contenidos

Prólogo	viii
1. Convenciones utilizadas en esta guía	viii
1. Acerca de GravityZone	1
2. Capas de protección de GravityZone	2
2.1. Antimalware	2
2.2. Control avanzado de amenazas	4
2.3. HyperDetect	4
2.4. Antiexploit avanzado	4
2.5. Cortafuego	4
2.6. Control de Contenido	5
2.7. Network Attack Defense	5
2.8. Administración de parches	5
2.9. Control de dispositivos	6
2.10. Cifrado completo del disco duro	6
2.11. Security for Exchange	6
2.12. Sandbox Analyzer	7
2.13. Detección y respuesta para endpoints (EDR)	7
2.14. Análisis de riesgos en los endpoints (ERA)	8
2.15. Email Security	8
2.16. Security for Storage	8
2.17. Disponibilidad de capas de protección de GravityZone	9
3. Architecture GravityZone	10
3.1. Consola web (GravityZone Control Center)	10
3.2. Security Server	10
3.3. Agentes de seguridad	10
3.3.1. Bitdefender Endpoint Security Tools	11
3.3.2. Endpoint Security for Mac	13
3.4. Arquitectura de Sandbox Analyzer	14
3.5. Arquitectura EDR	16
4. Iniciando	17
4.1. Conectar a Control Center	17
4.2. Control Center en resumen	18
4.2.1. Descripción general de Control Center	19
4.2.2. Datos de tablas	21
4.2.3. Barras de herramientas de acción	22
4.2.4. Menú Contextual	23
4.3. Gestionar su cuenta	23
4.4. Cambiar la Contraseña de Inicio de Sesión	26
4.5. Administración de su empresa	27
4.5.1. Información y ajustes de licencia	27
4.5.2. Ajustes de autenticación	29
5. Cuentas de usuario	33

5.1. Roles de usuario	34
5.2. Privilegios de usuario	35
5.3. Gestión de cuentas de usuario	36
5.3.1. Administrar cuentas de usuario individualmente	36
5.4. Gestión de los métodos de autenticación de usuario	38
5.5. Restablecer las contraseñas de inicio de sesión	39
5.6. Administración de la autenticación en dos fases	39
6. Administración de endpoints	42
6.1. Comprobación del estado del endpoint	44
6.1.1. Estado de administración	44
6.1.2. Estado de conexión	44
6.1.3. Estado de seguridad	46
6.2. Ver información de los endpoints	47
6.2.1. Comprobación de la página Red	47
6.2.2. Comprobación de la ventana Información	48
6.3. Organizar los endpoints en grupos	62
6.4. Clasificación, filtrado y búsqueda de endpoints	63
6.4.1. Clasificación de endpoints	64
6.4.2. Filtrado de endpoints	64
6.4.3. Búsqueda de endpoints	66
6.5. Inventario de parches	67
6.5.1. Consulta de la información de parches	68
6.5.2. Búsqueda y filtrado de parches	69
6.5.3. Ignorar parches	70
6.5.4. Instalación de parches	71
6.5.5. Desinstalación de parches	72
6.5.6. Crear estadísticas de parches	75
6.6. Ejecución de tareas	75
6.6.1.	76
6.6.2. Analizar en busca de indicadores de compromiso	86
6.6.3. Análisis de riesgos	90
6.6.4. Tareas de parches	91
6.6.5. Análisis de Exchange	93
6.6.6. Instalar	98
6.6.7. Migrar cliente	103
6.6.8. Desinstalar cliente	103
6.6.9. Actualizar cliente	104
6.6.10. Reconfigurar cliente	104
6.6.11. Reparar cliente	106
6.6.12. Reiniciar máquina	107
6.6.13. Descubrimiento de red	108
6.6.14. Actualizar Security Server	108
6.7.	109
6.7.1. Integración con Active Directory	109
6.8. Crear informes rápidos	112
6.9. Asignando Políticas	112
6.10.	114
6.10.1. Uso del Gestor de recuperación con volúmenes cifrados	114

6.11. Eliminación de endpoints del inventario de red	115
6.12. Ver y administrar tareas	116
6.12.1. Comprobar el estado de la tarea	116
6.12.2. Ver los informes de tareas	118
6.12.3. Reinicio de tareas	119
6.12.4. Detención de tareas de análisis de Exchange	119
6.12.5. Eliminar Tareas	119
6.13. Configuración de los ajustes de red	120
6.13.1. Ajustes del inventario de red	120
6.13.2. Limpieza de máquinas sin conexión	121
6.14. Administrador de Credenciales	123
6.14.1. Añadir credenciales al Gestor de credenciales	123
6.14.2. Eliminación de credenciales del Gestor de credenciales	124
7. Políticas de Seguridad	125
7.1. Administrando las Políticas	126
7.1.1. Crear políticas	126
7.1.2. Asignando Políticas	127
7.1.3. Modificar los ajustes de políticas	135
7.1.4. Renombrando Políticas	135
7.1.5. Eliminando Políticas	136
7.2. Políticas de equipos y máquinas virtuales	136
7.2.1. General	137
7.2.2. Antimalware	152
7.2.3. Sandbox Analyzer	192
7.2.4. Cortafuego	196
7.2.5. Protección de red	211
7.2.6. Administración de parches	226
7.2.7. Control de dispositivos	229
7.2.8. Relay	235
7.2.9. Protección de Exchange	237
7.2.10. Cifrado	269
7.2.11. Protección de almacenamiento	274
7.2.12. Sensor de incidentes	278
7.2.13. Administración del riesgo	279
8. Panel de monitorización	281
8.1. Panel de Control	281
8.1.1. Actualización de los datos del portlet	283
8.1.2. Editar los ajustes de portlets	283
8.1.3. Añadir un nuevo portlet	283
8.1.4. Eliminar un Portlet	284
8.1.5. Organizar portlets	284
8.2. Resumen ejecutivo	284
9. Investigar incidentes	289
9.1. La página de incidentes	289
9.1.1. La cuadrícula de filtros	291
9.1.2. Ver la lista de eventos de seguridad	295

9.1.3. Investigación de incidentes extendidos	299
9.1.4. Investigación de incidentes de endpoints	312
9.2. Incluir archivos en lista de bloqueo	359
9.3. Buscar eventos de seguridad	361
9.3.1. El lenguaje de consulta	362
9.3.2. Ejecutar consultas	364
9.3.3. Búsquedas favoritas	366
9.3.4. Consultas predefinidas	367
9.4. Reglas personalizadas	368
9.4.1. Detecciones	368
9.4.2. Exclusiones	375
10. Administración de riesgos en endpoints	382
10.1. El panel de control de Administración de riesgos	383
10.2. Riesgos de seguridad	391
11. Usar informes	409
11.1. Tipos de informes	409
11.1.1. Informes de equipos y máquinas virtuales	410
11.1.2. Informes de servidores de Exchange	421
11.2. Creando Informes	425
11.3. Ver y administrar informes programados	427
11.3.1. Visualizando los Informes	428
11.3.2. Editar informes programados	429
11.3.3. Eliminar informes programados	431
11.4. Adopción de medidas en base a informes	431
11.5. Guardar Informes	432
11.5.1. Exportando los Informes	432
11.5.2. Descarga de informes	432
11.6. Enviar informes por correo	433
11.7. Imprimiendo los Informes	433
12. Cuarentena	434
12.1. Exploración de la cuarentena	434
12.2. Cuarentena de equipos y máquinas virtuales	435
12.2.1. Visualización de la información de la cuarentena	435
12.2.2. Administración de los archivos en cuarentena	435
12.3. Cuarentena de servidores de Exchange	438
12.3.1. Visualización de la información de la cuarentena	438
12.3.2. Objeto en cuarentena	440
13. Uso de Sandbox Analyzer	445
13.1. Filtrar tarjetas de envíos	445
13.2. Consulta de los detalles del análisis	447
13.3. Eliminar tarjetas de envíos	449
13.4. Envío manual	449
14. Registro de actividad del usuario	453
15. Uso de herramientas	455

16. Notificaciones	456
16.1. Tipo de notificaciones	456
16.2. Ver notificaciones	462
16.3. Borrar notificaciones	463
16.4. Configurar las opciones de notificación	463
17. Obtener Ayuda	466
17.1. Centro de soporte de Bitdefender	466
17.2. Solicitar ayuda	467
17.3. Usar la herramienta de soporte	467
17.3.1. Uso de la herramienta de soporte en sistemas operativos Windows	468
17.3.2. Uso de la herramienta de soporte en sistemas operativos Linux	469
17.3.3. Uso de la herramienta de soporte en sistemas operativos Mac	471
17.4. Información de contacto	472
17.4.1. Direcciones	472
17.4.2. Distribuidor Local	473
17.4.3. Oficinas de Bitdefender	473
A. Apéndices	476
A.1. Tipos de archivo compatibles	476
A.2. Tipos y estados de los objetos de red	477
A.2.1. Tipos de objetos de red	477
A.2.2. Estados de objetos de red	477
A.3. Tipos de archivos de aplicación	478
A.4. Tipos de archivo de filtrado de adjuntos	479
A.5. Variables del sistema	480
A.6. Objetos Sandbox Analyzer	481
A.6.1. Tipos de archivo y extensiones admitidas para el envío manual	481
A.6.2. Tipos de archivos admitidos por el prefiltrado de contenidos para los envíos automáticos	481
A.6.3. Exclusiones predeterminadas del envío automático	482
A.7. Recopilación de datos sobre riesgos humanos	482
Glosario	486

Prólogo

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 recomendable 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, 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, inclusión de aplicaciones en la lista negra 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
- Sandbox Analyzer
- Detección y respuesta para endpoints (EDR)
- Análisis de riesgos en los endpoints (ERA)
- Email Security

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 obfuscado, 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.

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

i 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. 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, analizar su comportamiento e informar de cualquier cambio sutil en el sistema que pueda indicar malas intenciones.

Sandbox Analyzer envía automáticamente los archivos sospechosos desde los endpoints administrados, aunque no los detecten los servicios antimalware basados en firmas. La heurística dedicada que incorpora el módulo antimalware on-access de Bitdefender Endpoint Security Tools desencadena el proceso de envío.

El servicio Sandbox Analyzer puede evitar que se ejecuten amenazas desconocidas en el endpoint. Funciona en modo de monitorización o bloqueo, permitiendo o denegando el acceso al archivo sospechoso hasta que se recibe un veredicto. Sandbox Analyzer resuelve automáticamente las amenazas detectadas de acuerdo con las acciones de reparación definidas en la política de seguridad de los sistemas afectados.

Además, Sandbox Analyzer le permite enviar manualmente muestras directamente desde Control Center, para que pueda decidir qué más hacer con ellos.

2.13. Detección y respuesta para endpoints (EDR)

La detección y respuesta en los endpoints es un componente de correlación de eventos, capaz de identificar amenazas avanzadas o ataques en curso. Como parte de nuestra plataforma de protección de endpoints completa e integrada, la EDR aporta inteligencia en los dispositivos para toda la red de su empresa. Esta solución viene a apoyar el esfuerzo de los equipos de respuesta ante incidentes en su afán de investigar y responder a las amenazas avanzadas.

A través de Bitdefender Endpoint Security Tools, puede activar en los endpoints administrados un módulo de protección llamado Sensor EDR, con el fin de recopilar datos del hardware y de los sistemas operativos. Siguiendo un marco cliente-servidor, los metadatos se recopilan y procesan en ambos lados.

Este componente aporta información detallada sobre los incidentes detectados y un mapa interactivo de incidentes, así como acciones de reparación e integración con Sandbox Analyzer y HyperDetect.

2.14. Análisis de riesgos en los endpoints (ERA)

El análisis de riesgos en los endpoints (ERA, por sus siglas en inglés) identifica, evalúa y repara las debilidades de los endpoints de Windows a través del análisis de riesgos para la seguridad (bajo demanda o según programación mediante política) teniendo en cuenta un gran número de indicadores de riesgo. Una vez que haya analizado su red buscando ciertos indicadores de riesgo, obtendrá una visión de conjunto del estado de su red en cuanto al riesgo mediante el panel de control de **Administración de riesgos**, disponible en el menú principal. Podrá resolver ciertos riesgos de seguridad automáticamente desde GravityZone Control Center y ver las recomendaciones para mitigar la exposición de los endpoints.

2.15. Email Security

Con Email Security puede controlar la entrega de correo electrónico, filtrar mensajes y aplicar políticas en toda la empresa para detener las amenazas de correo electrónico selectivas y sofisticadas, incluidas las de compromiso del correo electrónico empresarial y el fraude del CEO. Email Security requiere aprovisionamiento de cuentas para acceder a la consola. Para más información, consulte la [Guía de usuario de Bitdefender Email Security](#).

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 cumplen 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. 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 solución de GravityZone incluye los siguientes componentes:

- [Consola Web Control Center](#)
- [Security Server](#)
- [Agentes de seguridad](#)

3.1. Consola web (GravityZone Control Center)

Las soluciones de seguridad de Bitdefender se gestionan en GravityZone desde un único punto de administración, la consola Web Control Center, que facilita el acceso y la administración de la estrategia general de seguridad, las amenazas a la seguridad general, y el control sobre todos los módulos de seguridad que protegen a los equipos de escritorio virtuales o físicos y servidores e instancias de Amazon. Equipado con la Arquitectura Gravity, Control Center es capaz de abordar las necesidades de incluso las organizaciones más grandes.

Control Center, una interfaz basada en Web, se integra con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a las estaciones de trabajo y servidores no administrados.

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.

El Security Server debe instalarse en uno o varios hosts con el fin de adaptarse al número de máquinas virtuales protegidas.

3.3. 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](#)

3.3.1. 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
- Sandbox Analyzer
- Detección y respuesta para endpoints (EDR)
- Análisis de riesgos en los endpoints (ERA)

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.
Esta funcionalidad es esencial para la implementación del agente de seguridad en un entorno de GravityZone en la nube.
- 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 faltan 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.

3.3.2. 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. Arquitectura de Sandbox Analyzer

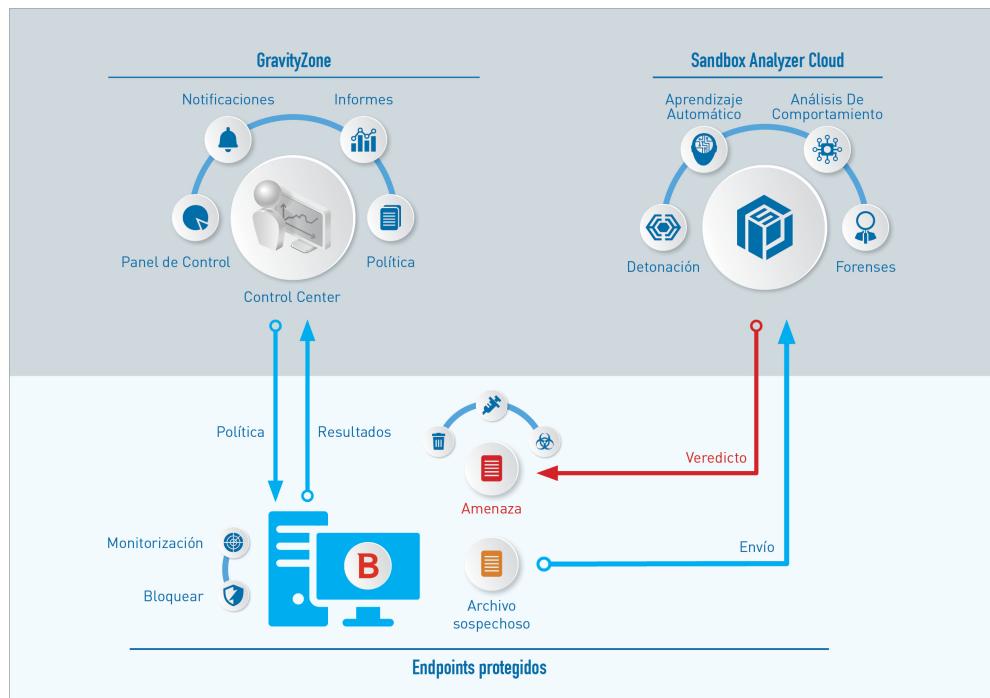
Bitdefender Sandbox Analyzer proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender.

Sandbox Analyzer contiene los siguientes componentes:

- **Portal de Sandbox Analyzer.** Este componente es un servidor de comunicaciones alojado que se utiliza para gestionar las solicitudes entre los endpoints y el clúster de Sandbox Analyzer de Bitdefender.
- **Clúster de Sandbox Analyzer.** Este componente es 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.



Arquitectura de Sandbox Analyzer

Una vez que se activa el servicio Sandbox Analyzer desde Control Center en los endpoints:

1. El agente de seguridad de Bitdefender comienza a enviar los archivos sospechosos que coinciden con las reglas de protección establecidas en la política.
2. Tras analizarse los archivos, se devuelve una respuesta al portal y al endpoint.
3. Si se considera que un archivo es peligroso, se le notifica al usuario y se realiza una acción correctiva.

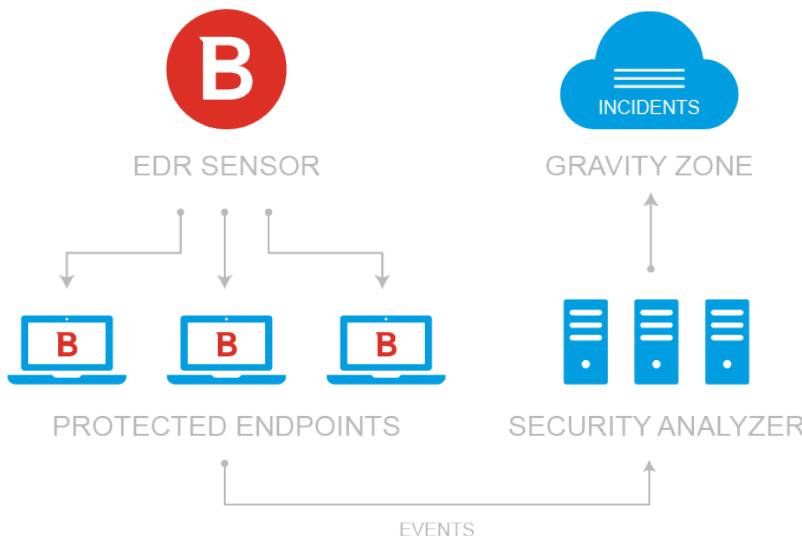
Los resultados del análisis se conservan vinculados al valor hash del archivo en la base de datos de Sandbox Analyzer. Cuando se envía un archivo analizado previamente desde un endpoint diferente, se devuelve inmediatamente una respuesta, puesto que los resultados ya están disponibles en la base de datos.

3.5. Arquitectura EDR

Para identificar las amenazas avanzadas y los ataques en curso, la **EDR** requiere datos del hardware y del sistema operativo. Algunos de los datos en bruto se procesan localmente, mientras que los algoritmos de aprendizaje automático de análisis de seguridad realizan tareas más complejas.

La EDR consta de dos componentes principales:

- El sensor de incidentes, que recopila, procesa e informa sobre los datos de comportamiento de aplicaciones y endpoints.
- Security Analytics, un componente de back-end que forma parte del conjunto de tecnologías de Bitdefender utilizadas para interpretar los metadatos recopilados por el Sensor de incidentes.



Flujo de EDR desde el endpoint al Control Center

4. INICIANDO

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. Abra su navegador Web.
2. Acceda a la siguiente dirección: <https://gravityzone.bitdefender.com>
3. Si usa **credenciales de GravityZone**:
 - a. Escriba la dirección de correo electrónico de su cuenta y haga clic en **Siguiente**.
 - b. Escriba la contraseña de su cuenta y haga clic en **Siguiente**.
 - c. Introduzca el código de seis dígitos de la aplicación de autenticación como parte de la autenticación en dos fases.
 - d. Haga clic en **Continuar** para iniciar sesión.
- Si usa el **inicio de sesión único**:
 - a. Cuando inicie sesión por primera vez, escriba la dirección de correo electrónico de su cuenta y haga clic en **Siguiente**.
GravityZone le redirigirá a la página de autenticación de su proveedor de identidad.
 - b. Autentíquese con el proveedor de identidad.

- c. El proveedor de identidad le redirigirá de nuevo a GravityZone e iniciará sesión automáticamente en Control Center.

La próxima vez, iniciará sesión en Control Center solo con su dirección de correo electrónico.

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

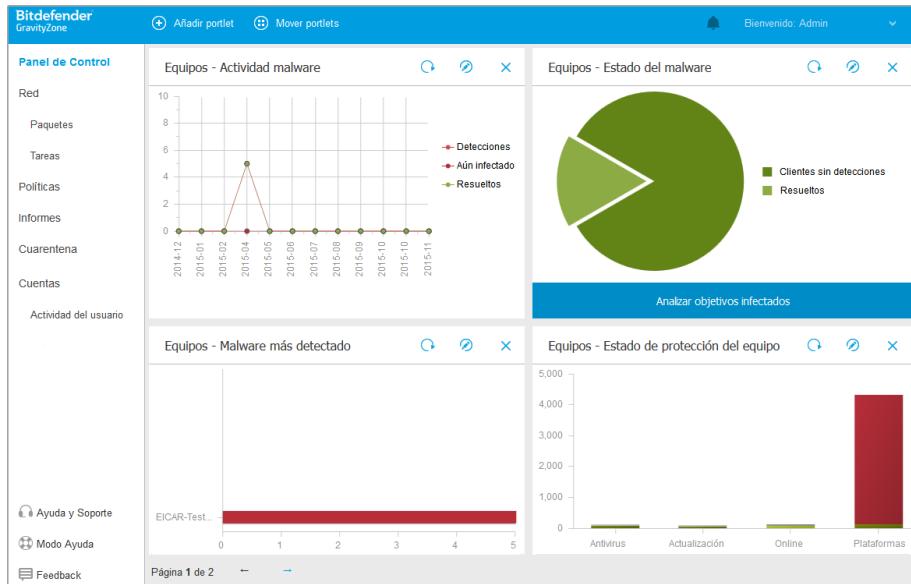


Nota

- 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.
- Si su cuenta utiliza el inicio de sesión único pero GravityZone le solicita una contraseña, póngase en contacto con su administrador para que le ayude. Mientras tanto, inicie sesión con su contraseña anterior o utilice el enlace de recuperación de contraseña para recibir una nueva.

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

Utilice el botón Ver Menú de la esquina superior izquierda para contraer a la vista de íconos, 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.

Incidentes

Ver y gestionar incidentes de seguridad en toda la red de la empresa.

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 del inventario de red de Control Center, incluyendo las reglas programadas para la limpieza automática de máquinas virtuales sin uso.



Nota

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

En la esquina inferior izquierda de Control Center, la sección **Herramientas** le permite utilizar más recursos de GravityZone, como el envío manual de archivos a Sandbox Analyzer.

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

- **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 ícono **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 ícono **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.

Reportes			
Acción	Nombre del informe	Tipo	Recurrencia
Añadir Descargar Eliminar Actualizar	<input type="checkbox"/> <input type="text"/>		
	<input type="checkbox"/> Informe de Actividad de Malware	Actividad de malware	Semanalmente 19 Sep 2015 - 11:00

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

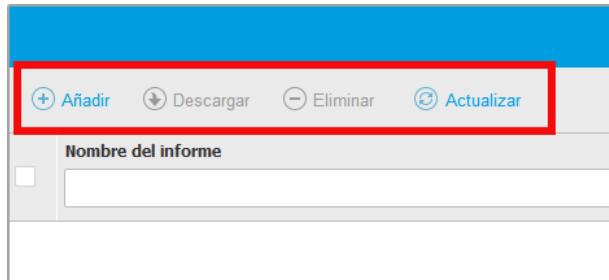
Para asegurarse de que la consola muestra la información más reciente, haga clic en el botón  **Actualizar** de la parte superior de la tabla.

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:

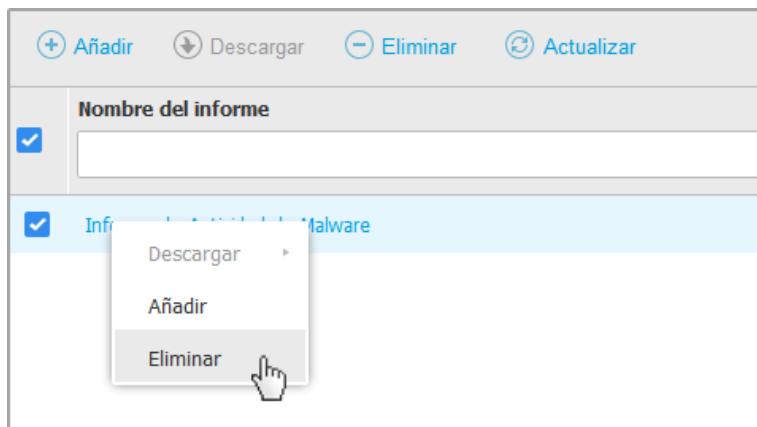
-  Crear un nuevo informe.
-  Descargar un informe programado.
-  Eliminar un informe programado.



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

4.3. 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**.
 - **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.

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.

4.5. Administración de su empresa

Como usuario con privilegios de **administración de empresa**, puede comprobar o cambiar los detalles de su empresa y los ajustes de la licencia, así como administrar los ajustes de autenticación, como la autenticación en dos fases y el inicio de sesión único.

4.5.1. Información y ajustes de licencia

Para consultar o cambiar la información de su empresa y los ajustes de la licencia:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.
2. En **Detalles de la empresa**, introduzca la información de su empresa, como por ejemplo el nombre de la empresa, la dirección y el teléfono.

Puede cambiar el logotipo que aparece en Control Center y también en los informes de su empresa y en las notificaciones de correo electrónico como se indica a continuación:

- Haga clic en **Cambiar** para buscar el logotipo en su equipo. El formato de archivo de imagen debe ser .png o .jpg y el tamaño de la imagen ha de ser 200x30 píxeles.
 - Haga clic en **Predeterminada** para borrar la imagen y restaurar la proporcionada por Bitdefender.
3. Por defecto, su empresa puede ser administrada por las cuentas de partner de otras empresas que puedan tener a la suya en su Bitdefender Control Center. Puede bloquear el acceso de estas empresas a su red deshabilitando la opción **Dejar que su partner le ayude con la administración de la seguridad de esta empresa**. Como resultado de ello, su red no será visible en la Control Center de otras empresas, pero podrán administrar su suscripción.
 4. Puede consultar y modificar los detalles de su licencia en la sección **Licencia** e introducir una clave de complemento.
 - Para añadir una nueva clave de licencia:

- a. En el **menú Tipo**, seleccione un tipo de suscripción de **licencia**.
 - b. Introduzca la licencia en el campo **Clave de licencia**.
 - c. Haga clic en el botón **Comprobar** y espere a que Control Center recupere la información acerca de la clave de licencia introducida.
- Para verificar los detalles de su clave de licencia, consulte la información que se muestra debajo de la clave de licencia:
 - **Fecha de caducidad:** la fecha hasta la cual se puede utilizar la clave de licencia.
 - **Utilizado:** el número de puestos utilizados de la cantidad total de puestos de la clave de licencia. Un puesto de licencia se utiliza cuando se ha instalado el cliente de Bitdefender en un endpoint de la red bajo su administración.
 - **Total:** el número total de puestos disponibles en su clave de licencia o suscripción.

Además, si tiene una suscripción mensual, puede generar el informe de **Uso de licencia mensual** para el mes en curso. Para más información, diríjase a [Uso de licencia mensual](#).

- Para introducir una clave de complemento:
 - Rellene la clave en el campo **Clave de complemento**.
 - Haga clic en el botón **Añadir** y espere a que GravityZone compruebe la clave de complemento. Si es válida, Control Center obtiene la siguiente información sobre el complemento: el tipo, la clave y la opción para eliminarla.



Nota

El campo de la **Clave de complemento** no aparece si tiene una licencia de prueba o mensual.

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

Para cambiar su proveedor de servicios administrados:

- a. Haga clic en el botón **Cambiar**.
- b. Introduzca el ID de empresa del partner en el campo **ID del partner**.

**Nota**

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

- c. Haga clic en **Guardar**.

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

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

4.5.2. Ajustes de autenticación

GravityZone ofrece opciones adicionales para proteger la autenticación de usuarios en el Control Center, como por ejemplo:

- Autenticación en dos fases
- Caducidad de la contraseña
- Bloqueo de cuenta
- Inicio de sesión único

Como administrador de la empresa, puede habilitar fácilmente estas medidas adicionales de seguridad de inicio de sesión para toda su empresa:

1. Acceda a la página **Configuración > Ajustes de autenticación**.

2. Seleccione o configure las opciones que precisa habilitar.

En las siguientes secciones puede encontrar más información sobre cada opción.

3. Haga clic en **Guardar** para aplicarlos.

Impponer la autenticación en dos fases

La autenticación en dos fases certifica que la persona que intenta iniciar sesión en Control Center es realmente el usuario que dice ser. La autenticación en dos fases solicita un código de autenticación además de las credenciales de Control Center en cada inicio de sesión. GravityZone usa la aplicación Google Authenticator para el código de autenticación en dos fases.

En GravityZone, la imposición de la autenticación en dos fases viene habilitada por defecto para toda la empresa. Esto significa que todos los usuarios de GravityZone deben configurar y usar la autenticación en dos fases en sus cuentas.

Desmarcar esta opción desactivará la imposición de la autenticación en dos fases. Necesitará confirmar esta acción. Como resultado de ello, los usuarios seguirán teniendo habilitada la autenticación en dos fases, pero podrán inhabilitarla desde los ajustes de su cuenta.

Nota

- Puede ver el estado de la autenticación en dos fases de una cuentas de usuario en la página **Cuentas**.
- Si un usuario con la autenticación en dos fases activada no pudiese iniciar sesión en GravityZone (debido a que tenga un nuevo dispositivo o a que haya perdido la clave secreta de Google Authenticator), podrá restablecer la activación de su autenticación en dos fases desde los ajustes de su cuenta en la página **Cuentas**. Para obtener más información, consulte "[Administración de la autenticación en dos fases](#)" (p. 39).

Fijar en noventa días la antigüedad máxima de la contraseña

Esta opción habilita la política de caducidad de la contraseña. Los usuarios deben cambiar sus contraseñas antes de que alcancen la antigüedad especificada. De lo contrario, ya no podrán iniciar sesión en GravityZone.

Bloquear cuentas tras cinco intentos de inicio de sesión con contraseñas no válidas

Esta opción limita el número de contraseñas no válidas consecutivas para evitar ataques. Cuando el contador alcanza el umbral, la cuenta se bloquea y el usuario debe restablecer su contraseña.

La política se aplica a las cuentas creadas en GravityZone.

Configurar el inicio de sesión único con SAML

GravityZone admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios como una alternativa sencilla y segura al inicio de sesión tradicional con nombre de usuario y contraseña.

Este método requiere la integración con proveedores de identidad (IdP) externos mediante SAML 2.0, como AD FS, Okta y Azure AD, que autentican a los usuarios de GravityZone y les brindan acceso a Control Center.

El SSO de GravityZone funciona de la siguiente manera:

1. Los usuarios introducen sus direcciones de correo electrónico en la página de inicio de sesión de GravityZone.
2. GravityZone crea una solicitud SAML y reenvía la solicitud y los usuarios al proveedor de identidad.
3. Los usuarios deben autenticarse con el proveedor de identidad.
4. Despues de la autenticación, el proveedor de identidad envía una respuesta a GravityZone en forma de documento XML firmado con un certificado X.509. Además, el proveedor de identidad redirige a los usuarios a GravityZone.
5. GravityZone recupera la respuesta, la valida con la huella digital del certificado y permite a los usuarios iniciar sesión en Control Center sin ninguna otra interacción por su parte.

Los usuarios siguen iniciando sesión automáticamente en Control Center mientras tengan una sesión activa con el proveedor de identidad.

Para habilitar el SSO, debe hacer lo siguiente:

1. Configure el proveedor de identidad para usar GravityZone como proveedor de servicio. Para más información sobre los proveedores de identidad compatibles y los detalles de la configuración, consulte [este artículo de la base de conocimientos](#).
2. Habilite el SSO para su empresa:
 - a. En **Configurar el inicio de sesión único con SAML**, introduzca la URL de metadatos del proveedor de identidad en el campo correspondiente y haga clic en **Guardar**.
 - b. Haga clic en **Guardar**.
3. Configure los usuarios de su empresa para que se autentiquen con su proveedor de identidad. Para obtener información, consulte [“Gestión de los métodos de autenticación de usuario” \(p. 38\)](#).



Importante

Como administrador de GravityZone, puede configurar el inicio de sesión único para los usuarios de su empresa, pero no para su propia cuenta, por motivos de seguridad.

Para inhabilitar el inicio de sesión único para su empresa:

1. Elimine la URL de metadatos del proveedor de identidad.
2. Haga clic en **Guardar** y confirme la acción.

Tras inhabilitar el inicio de sesión único para su empresa, los usuarios pasarán automáticamente a iniciar sesión con las credenciales de GravityZone. Los usuarios pueden obtener nuevas contraseñas haciendo clic en el enlace **¿Olvidó su contraseña?** de la página de inicio de sesión de Control Center y siguiendo las instrucciones.

Al volver a habilitar el SSO para su empresa, los usuarios seguirán iniciando sesión en Control Center con las credenciales de GravityZone. Debe configurar manualmente todas las cuentas para que usen nuevamente el SSO.

5. CUENTAS DE USUARIO

Puede configurar y administrar GravityZone desde Control Center mediante la cuenta que recibió tras suscribirse al servicio.

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

- Para permitir a otros empleados de la empresa acceder a Control Center, puede crear cuentas de usuario internas. Puede asignar cuentas de usuario con diferentes roles, según su nivel de acceso en la empresa.
- Para cada cuenta de usuario, puede personalizar el acceso a las características de 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.

Panel de Control	Añadir Eliminar Actualizar		
	Nombre completo	Correo	Rol
Red	<input type="checkbox"/> reporter	reporter@company.com	Informador
Paquetes	<input type="checkbox"/> administrator	admin@company.com	Administrador de red
Tareas			
Políticas			
Informes			
Cuarentena			
Cuentas			
Actividad del usuario			

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.
- Dirección de correo electrónico de la cuenta (usada para iniciar sesión en Control Center). 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).

- El estado de la autenticación en dos fases, que permite comprobar rápidamente si el usuario la ha activado.
- Método de autenticación, que indica si el usuario inicia sesión con credenciales de GravityZone o con un proveedor de identidad para inicio de sesión único (SSO).

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** - Adecuado para administradores de empresas cliente que hayan adquirido una licencia de GravityZone a un partner. Un administrador de empresa administra la licencia, el perfil de la empresa y toda su implementación de GravityZone, permitiendo un control de máximo nivel sobre todos los ajustes de seguridad (a no ser que sea anulado por la cuenta partner principal en caso de un proveedor de servicios de seguridad). Los administradores de empresa pueden compartir o delegar sus responsabilidades operativas 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. 35).

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

Antes de crear una cuenta de usuario, asegúrese de tener a mano la dirección de correo electrónico necesaria. Esta dirección es obligatoria para crear la cuenta de usuario de GravityZone. Los usuarios reciben su información de inicio de sesión en GravityZone en la dirección de correo electrónico suministrada.

5.3.1. Administrar cuentas de usuario individualmente

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

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:
 - **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.
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.
 - **Método de autenticación**. Este ajuste está disponible para cuentas de una empresa que tenga habilitado el inicio de sesión único. Elija la cuenta para el menú para iniciar sesión utilizando las credenciales de GravityZone o un proveedor de identidad. Para más información sobre los métodos de

autenticación disponibles, consulte “[Gestión de los métodos de autenticación de usuario](#)” (p. 38).

- **Rol.** Seleccione el rol del usuario. Para más información sobre los roles de usuarios, consulte “[Roles de usuario](#)” (p. 34).
 - **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. 35).
 - **Seleccionar objetivos.** Seleccione los grupos de red a los que tendrá acceso el usuario.
5. Haga clic en **Guardar** para añadir el usuario. La nueva cuenta se mostrará en la lista de cuentas de usuario.



Nota

La contraseña de cada cuenta de usuario se genera automáticamente una vez que se crea la cuenta, y se envía a la dirección de correo electrónico del usuario junto con la restante información de la misma.

Puede cambiar la contraseña una vez creada la cuenta. Haga clic en el nombre de cuenta en la página de **Cuentas** para modificar su contraseña. Una vez modificada la contraseña, se le notificará inmediatamente al usuario por correo electrónico.

Los usuarios pueden cambiar su contraseña de inicio de sesión desde Control Center, accediendo a la página **Mi cuenta**.

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.

5.4. Gestión de los métodos de autenticación de usuario

Al crear o editar una cuenta de usuario en una empresa con el inicio de sesión único (SSO) habilitado, puede configurar cómo iniciar sesión en Control Center.

En la sección **Ajustes y privilegios**, dispone de las siguientes opciones:

- **Iniciar sesión con las credenciales de GravityZone.** Seleccione esta opción para que esta cuenta inicie sesión en Control Center con un nombre de usuario y contraseña.
- **Iniciar sesión con su proveedor de identidad.** Seleccione esta opción para que esta cuenta utilice el inicio de sesión único (SSO).

Puede configurar el método de autenticación de las cuentas de usuario de GravityZone una por una.

GravityZone admite diferentes métodos de autenticación para usuarios de la misma empresa. Por lo tanto, unas cuentas pueden iniciar sesión con su nombre de usuario y contraseña mientras que otras pueden autenticarse con un proveedor de identidad.

Para obtener información sobre cómo habilitar el SSO para su empresa, consulte "["Configurar el inicio de sesión único con SAML" \(p. 30\)](#)".



Importante

- Como administrador de GravityZone, puede configurar el inicio de sesión único para los usuarios de su empresa, pero no para su propia cuenta, por motivos de seguridad.
- Para el SSO, los usuarios deben tener las mismas direcciones de correo electrónico en GravityZone que en el proveedor de identidad. Las direcciones de correo electrónico distinguen entre mayúsculas y minúsculas para el SSO en GravityZone. Por ejemplo, **nombreusuario@empresa.dominio** es distinto de **NombreUsuario@empresa.dominio** y de **NOMBREUSUARIO@empresa.dominio**.
- Bitdefender trabaja con dos instancias en la nube de GravityZone. En algunos casos, puede que los usuarios tengan que elegir una instancia durante el primer inicio de sesión.

Para consultar los cambios relativos al inicio de sesión único de los usuarios de GravityZone, acceda a la página **Cuentas > Actividad del usuario** y filtre los registros de actividades por Área > Ajustes de autenticación.

5.5. 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.

5.6. 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 de su empresa. Para más información, diríjase a ["Administración de su empresa" \(p. 27\)](#).



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. 23)

6. ADMINISTRACIÓN DE ENDPOINTS

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

La página Red

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

Todos los endpoints eliminados se almacenan en la carpeta **Eliminados**. Para obtener más información, consulte “[“Eliminación de endpoints del inventario de red” \(p. 115\)](#).



Nota

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

2. El panel derecho muestra el contenido del grupo que ha seleccionado en el árbol de directorios. Este panel consiste en una cuadricular, 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 ícono junto a su nombre. 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 ícono 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 ícono de los objetos de red y sus estados disponibles, consulte “[Tipos y estados de los objetos de red](#)” (p. 477).

- 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 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.

Desde la página **Red** puede administrar también los paquetes de instalación y las [tareas](#) para sus endpoints.

Nota

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

Para consultar los endpoints de su cuenta, acceda a la página **Red** y seleccione el grupo de red deseado en el panel izquierdo.

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 endpoint que se muestran en la tabla:

1. Haga clic en el botón **III 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 endpoints de la siguiente manera:

- [Comprobar el estado del endpoint.](#)
- [Ver la información de los endpoints.](#)
- [Organizar los equipos en grupos.](#)
- [Ordenar, filtrar y buscar.](#)

- Administrar parches
- Ejecutar tareas.
- Definir la integración con Active Directory
- Crear informes rápidos
- Asignar políticas
- Eliminar endpoints del inventario de red.

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.

6.1. Comprobación del estado del endpoint

Los endpoints están representados en la página de red mediante los iconos correspondientes a su tipo y estado.

Consulte “[Tipos y estados de los objetos de red](#)” (p. 477) 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](#)

6.1.1. Estado de administración

Los endpoints pueden tener los siguientes estados de administración:

- **Administrados** - Endpoints 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** - Endpoints detectados en los que no se ha instalado aún el agente de seguridad.
- **Eliminados** - Endpoints que ha eliminado de Control Center. Para más información, diríjase a “[Eliminación de endpoints del inventario de red](#)” (p. 115).

6.1.2. Estado de conexión

El estado de conectividad se refiere a todas las máquinas virtuales y solo a los equipos administrados. Los endpoints administrados pueden ser:

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

Un endpoint se considera offline si su agente de seguridad permanece inactivo durante más de 5 minutos. Posibles razones por las cuales los endpoints aparecen offline:

- El endpoint está apagado, en suspensión o hibernando.

Nota

Los endpoints aparecen online incluso cuando están bloqueados o cuando el usuario ha finalizado la sesión.

- El agente de seguridad carece de conexión con Bitdefender Control Center o con el Endpoint Security Relay asignado:
 - El endpoint puede estar desconectado 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.
 - El endpoint 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 endpoints 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 endpoint 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.

- El agente de seguridad se ha desinstalado manualmente del endpoint mientras el endpoint carecía de conexión con Bitdefender Control Center o con el Endpoint Security Relay asignado. Normalmente, cuando el agente de seguridad de un equipo se desinstala manualmente, se le notifica a Control Center y el endpoint se marca como no administrado.
- Puede que el agente de seguridad no esté funcionando adecuadamente.

Para averiguar cuánto tiempo han estado inactivos los endpoints:

1. Muestre solo los endpoints 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 por última vez** para organizar los endpoints por periodo de inactividad.

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

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

Nota

Se recomienda [actualizar](#) la tabla de red de vez en cuando para actualizar la información de los endpoints con los últimos cambios.

6.1.3. Estado de seguridad

El estado de seguridad se refiere únicamente a los endpoints administrados. Los iconos de estado muestran un símbolo de advertencia que le permite identificar los endpoints con problemas de seguridad:

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

Un endpoint 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:
 - 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 endpoint con problemas de seguridad, haga clic en su nombre para mostrar la ventana **Información**. Puede identificar los problemas de seguridad mediante el ícono !. Asegúrese de revisar la información de seguridad de todas las [pestañas de la página de información](#). Muestre la información sobre herramientas del ícono 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. Ver información de los endpoints

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

- [Comprobación de la página Red](#)
- [Comprobación de la ventana Información](#)

6.2.1. Comprobación de la página Red

Para conocer más detalles sobre un endpoint, 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 **III Columnas** de la esquina superior derecha del panel.

1. Diríjase a la página **Red**.
2. Seleccione el grupo que desee del panel de la izquierda.
Todos los endpoints del grupo seleccionado se muestran en la tabla del panel derecho.
3. Puede identificar fácilmente el estado del endpoint consultando el ícono correspondiente. Para información detallada, diríjase a “[Comprobación del estado del endpoint](#)” (p. 44).
4. Consulte la información mostrada en las columnas para cada endpoint.
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 períodos 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.

6.2.2. 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 endpoint, 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 endpoints](#)” (p. 63).

- 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.
- Para endpoints con **rol de integrador de Active Directory**: el nombre de dominio y la última fecha y hora de sincronización.

Información

X

General Protección Política Informes

Equipo		Capas de protección	
Nombre:	CC-WIN7X32	Endpoint:	Activo
FQDN:	cc-win7x32.newdomain.loc		
IP:	10.10.14.199		
SO:	Windows 7 Professional		
Etiqueta:	<input type="text"/>		
Infraestructura:	Grupos personalizados		
Grupo:	Custom Groups		
Estado:	Online		
Última sinc.:	Online		

Guardar **Cerrar**

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. 46).
- 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. 425).
- 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 ["" \(p. 114\)](#).
- Información sobre el análisis de seguridad, como parte de la EDR:
 - La información específica del agente indica lo siguiente:
 - Proveedor de eventos: BEST informa al componente de análisis de seguridad sobre el comportamiento de las aplicaciones y los endpoints.
 - Estado de la comunicación: BEST se conecta con el análisis de seguridad.
 - Última actualización de estado: el estado más reciente.
 - Información general sobre el estado de activación del Sensor de incidentes.
- 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.

Información

General Protección Política Informes

Protección de endpoint Vulnerable !

B Agente

- Tipo: BEST
- Versión del producto: 6.2.4.649
- Última actualización del producto: 21 Octubre 2015 09:33:15
- Versión de firmas: 7.63005 !
- Actualización de las últimas firmas: 21 Octubre 2015 09:33:15
- Motor de análisis principal: Análisis local
- Motor de análisis de reserva: Ninguno

Resumen

- Módulos**
 - Antimalware: Activado
 - Usuario con Permisos: Desactivado
 - Control avanzado de amenazas: Activado
- Informes (hoy)**
 - Estado de malware: > No hay Detecciones Visualización
 - Actividad de malware: > Sin actividad Visualización

Guardar **Cerrar**

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.

The screenshot shows the 'Information' window with the 'Policy' tab selected. It includes sections for 'Resumen' (Summary) and 'Políticas aplicables' (Applicable Policies). The 'Resumen' section shows the active policy is 'Default Policy', it's a 'Dispositivo' (Device) type, and it's 'Heredado de Máquinas virtuales' (Inherited from Virtual Machines). The 'Políticas aplicables' section lists two policies: 'PolicyComplianceReport_1j6' (Applied, Location: RuleForPolicyComplianceReport..., Type: Device) and 'Default policy' (Applied, Type: Device). The bottom of the window has buttons for 'Guardar' (Save) and 'Cerrar' (Close).

Ventana Información - pestaña Política

Para obtener más información con respecto a las políticas, consulte "["Modificar los ajustes de políticas"](#) (p. 135)

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.

Nombre del endpoint	IP	Etiqueta
TA_SVE_W7_192.168.2.26	10.17.47.208	
TA_SVE_W7_192.168.2.27	10.17.46.77	
TA_SVE_UBUNTUX64_192.168.2.142	10.17.44.162	

Primera Página ← Página 1 de 1 → Última página 20 3 elementos

Guardar Cerrar

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.

< Back AST-TB-W7X66-2						
General	Protection	Policy	Connected Endpoints	Repository details	Scan Logs	Troubleshooting
Bitdefender Endpoint Security Tools						
BEST (Windows)						
Product version (stored locally)						
Slow ring:	6.6.18.265					
Fast ring:	6.6.19.273					
Product version (Bitdefender repository)						
Slow ring:	N/A					
Fast ring:	N/A					
Last update time:	26 June 2020 18:4...					
Last check time:	N/A					
Security Content						
FULL ENGINES (Local Scan)			LIGHT ENGINES (Hybrid Scan)			
Signatures stored locally			Signatures stored locally			
x86:	7.84969	x86:	7.84969	N/A		
x64:	N/A	x64:	N/A	7.84969		
Signatures in Bitdefender repository			Signatures in Bitdefender repository			
x86:	7.84969	x86:	7.84969	N/A		
x64:	N/A	x64:	N/A	7.84969		
Last update time:	29 June 2020 14:5...	Last update time:	29 June 2020 14:5...			
Last check time:	29 June 2020 16:0...	Last check time:	29 June 2020 16:0...			
Status:	● Up to date	Status:	● Up to date			

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.

Información

General Protección Política **Informes**

Registros de análisis disponibles

Se muestran registros de análisis para: Endpoint Protection

Tipo	Creado
Quick Scan	25 Octubre 2017, 14:06:15
Full Scan	05 Septiembre 2017, 16:16:02

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 máquinas Windows, Linux, macOS y Servidor de seguridad multiplataforma.

Atrás | DESKTOP-30507PT

General Protección Política Informes **Resolución de Problemas** Actualizar

Recopilar registros

Gather logs and general information necessary for troubleshooting.

Recopilar registros

Sesión de depuración

Activate advanced logging to gather specific Bitdefender logs while reproducing the issue.

Comenzar sesión

Última Actividad

Nombre de la actividad	Comenzada el	Finalizada el	Estado	Acciones
Sesión de depuración	26 Marzo 2020, 10:55:31	26 Marzo 2020, 17:02:29	Finalizado	Reiniciar
Recopilar registros	23 Marzo 2020, 11:17:47	23 Marzo 2020, 11:18:02	Detenido	Reiniciar

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.
 - **Bitdefender Cloud**: el archivo de registros se guarda en una ubicación de almacenamiento de Bitdefender Cloud, donde el servicio de soporte técnico empresarial puede acceder a los archivos.

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, ruta a la ubicación compartida e ID del caso) según la ubicación seleccionada.
4. Haga clic en el botón **Recopilar registros**.

Nota

Si elige **Bitdefender Cloud** como opción de almacenamiento, tenga en cuenta lo siguiente:

- El archivo de registros se guarda con nombres idénticos tanto en **Bitdefender Cloud** como en la máquina objetivo. Haga clic en el evento de solución de problemas para ver el nombre del archivo en la ventana de detalles.
- Después de cargar el archivo, proporcione al servicio de soporte técnico empresarial de Bitdefender la información necesaria (nombre de la máquina objetivo y nombre del archivo) en el caso abierto. Abra un nuevo caso si no existiese uno.

● **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)	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– Mensajes de error aparecidos durante las actualizaciones de contenidos de seguridad o del producto
Control de contenido (análisis de tráfico y control de usuarios)	<ul style="list-style-type: none">– No se carga el sitio web– Los elementos de la página web no se muestran correctamente
Conectividad de Cloud Services	<ul style="list-style-type: none">– El endpoint carece de conectividad con los servicios de Bitdefender Cloud
Problemas generales del producto (registro con mucho texto)	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">- 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- El endpoint no se puede conectar a la consola GravityZone.
Problemas generales del producto (registro con mucho texto)	<ul style="list-style-type: none">- 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)	<p>Cualquier comportamiento inesperado del Servidor de seguridad, que incluye:</p> <ul style="list-style-type: none">- 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	<p>Cualquier comportamiento inesperado observado de la consola de GravityZone:</p> <ul style="list-style-type: none">- 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

Tipo de incidencia	Caso de uso
	<p>Nota</p> <p>Utilice este método por recomendación del servicio de soporte técnico empresarial de Bitdefender.</p>

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.
- **Bitdefender Cloud**: el archivo de registros se guarda en una ubicación de almacenamiento de Bitdefender Cloud, donde el servicio de soporte técnico empresarial puede acceder a los archivos.

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, ruta a la ubicación compartida e ID del caso) 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 cuadricula.

6.3. Organizar los endpoints en grupos

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

Puede administrar grupos de endpoints en el panel de la izquierda de la página **Red**, en la carpeta **Equipos y grupos**.

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

Nota

- Un grupo puede contener tanto endpoints como otros grupos.
- Cuando se selecciona un grupo en el panel izquierdo, puede ver todos los endpoints excepto los ubicados en sus subgrupos. Para ver todos los endpoints 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 la carpeta **Equipos y grupos** en el panel de la izquierda.
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**.

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 endpoints

Puede mover entidades a **Equipos y grupos** 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. 125).

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**.

6.4. Clasificación, filtrado y búsqueda de endpoints

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 endpoint específico o elegir ver únicamente los endpoints administrados.

6.4.1. Clasificación de endpoints

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

	Nombre	SO	IP	Última sinc.
<input type="checkbox"/>	<input type="text"/> 🔍	<input type="text"/> 🔍	<input type="text"/> 🔍	<input type="text"/>

Ordenar equipos

6.4.2. Filtrado de endpoints

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 deseé 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).

Tipo	Seguridad	Política	Profundidad
Filtrar por			
<input type="checkbox"/> Equipos			
<input type="checkbox"/> Máquinas virtuales			
<input type="checkbox"/> Grupos / Carpetas			
Profundidad: dentro de las carpetas seleccionadas			
Guardar	Cancelar	Restablecer	

Endpoints - Filtrar por tipo

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

Tipo	Seguridad	Política	Profundidad
Centralizada	Incidencias de Seguridad		
<input type="checkbox"/> Administrados (puntos finales)	<input type="checkbox"/> Con problemas de seguridad		
<input type="checkbox"/> Administrados (Servidores de Exchange)	<input type="checkbox"/> Sin problemas de seguridad		
<input type="checkbox"/> Administrados (Relays)			
<input type="checkbox"/> Servidores de seguridad			
<input type="checkbox"/> No administrado			
Profundidad: dentro de las carpetas seleccionadas			
Guardar		Cancelar	Restablecer

Endpoints - Filtrar por seguridad

- **Política.** Seleccione la plantilla de política según la cual quiere filtrar los endpoints, 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.

Tipo	Seguridad	Política	Profundidad
Plantilla:	<input type="text"/>		
	<input type="checkbox"/> Modificado por Usuario avanzado		
Tipo:	<input type="checkbox"/> Directo <input type="checkbox"/> Heredados		
Estado:	<input type="checkbox"/> Activo <input type="checkbox"/> Aplicado <input type="checkbox"/> Pendiente		
Profundidad: dentro de las carpetas seleccionadas			
Guardar		Cancelar	Restablecer

Endpoints - Filtrar por política

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



Endpoints - 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 **Q 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 endpoints por el criterio seleccionado. El filtro permanece activo en la página **Red** hasta que cierra la sesión o restablece el filtro.

6.4.3. Búsqueda de endpoints

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 endpoint que está buscando en el campo **IP**. Solo aparecerá en la tabla el endpoint coincidente.

Vacie el cuadro de búsqueda para mostrar la lista completa de endpoints.

	Nombre	SO	IP	Última sinc.
<input type="checkbox"/>	SRV	 		
<input type="checkbox"/>	 2003SRV	Windows Server 2003		N/A

Buscar endpoints

6.5. 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.

Red	Buscar productos...	Ignorar parches	Instalar	Desinstalar	Estadísticas de parches	Comprobar	Extralibre
Inventario de parches	 						
Paquetes	 Microsoft						
Tareas	 VMware						
Políticas							
Reglas de asignación							

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

6.5.1. 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.
- **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 **III 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.

6.5.2. 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.

6.5.3. 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 deseé 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 deseé 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. 75)
- 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.

6.5.4. 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 ícono 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. 107).
- 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. 143).

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. 92).
- 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.

6.5.5. 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 deseé 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 ícono 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. 107).

- 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. 143).

- 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 deseé.



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.

6.5.6. 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.

6.6. Ejecución de tareas

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

Esto es lo que puede hacer:

- “[Analizar](#)” (p. 76)
- “[Analizar en busca de indicadores de compromiso](#)” (p. 86)
- “[Análisis de riesgos](#)” (p. 90)
- “[Tareas de parches](#)” (p. 91)
- “[Análisis de Exchange](#)” (p. 93)
- “[Instalar](#)” (p. 98)

- “Desinstalar cliente” (p. 103)
- “Actualizar cliente” (p. 104)
- “Reconfigurar cliente” (p. 104)
- “Reparar cliente” (p. 106)
- “Reiniciar máquina” (p. 107)
- “Descubrimiento de red” (p. 108)
- “Actualizar Security Server” (p. 108)

Puede elegir crear tareas individuales para cada endpoint o para grupos de endpoints. Por ejemplo, puede instalar de forma remota el agente de seguridad en un grupo de endpoints no administrados. En un momento posterior, puede crear una tarea de análisis para un determinado endpoint del mismo grupo.

Solo puede ejecutar tareas compatibles para cada endpoint. Por ejemplo, si selecciona un endpoint no administrado, solo puede elegir instalar el agente de seguridad; todas las demás tareas aparecen desactivadas.

Para un grupo, la tarea seleccionada se creará únicamente para endpoints compatibles. Si ninguno de los endpoints 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 endpoints conectados. Si un endpoint no está conectado, la tarea se ejecutará tan pronto como vuelva a estarlo.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte [Ver y administrar tareas](#).

Analizar

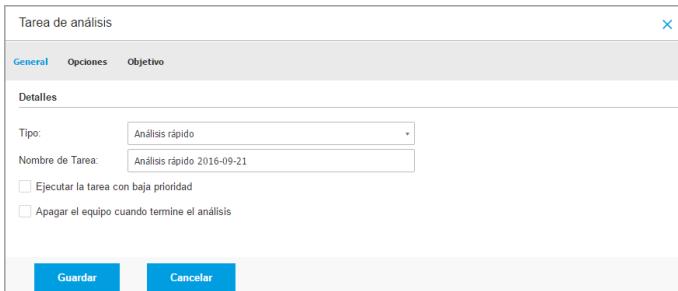
Para ejecutar de forma remota una tarea de análisis en uno o varios endpoints:

1. Diríjase a la página **Red**.
2. 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.
3. Marque las casillas de verificación correspondientes a los endpoints que quiera analizar.
4. Haga clic en el botón  **Tareas** de la zona superior de la tabla y seleccione **Analizar**.

Aparecerá una nueva ventana de configuración.

5. Configure las opciones de análisis:

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



Tarea de análisis - 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 endpoint.
- 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 - 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

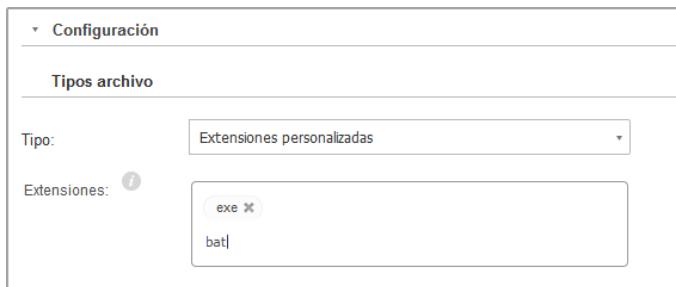
Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a “[Tipos de archivos de aplicación](#)” (p. 478).

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 - 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 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 endpoint.

- **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 deseé 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 endpoints 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. 480).
- 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.

Archivo	Rutas específicas	Acción
Tipos de excepciones	Archivos y carpetas a analizar	

Tarea de análisis - 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. 182).

6. 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 obtener más información, consulte [Ver y administrar tareas](#).



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. 163).

6.6.2. Analizar en busca de indicadores de compromiso

En cualquier momento, puede ejecutar análisis bajo demanda en busca de indicadores de compromiso (IoC) en los endpoints seleccionados, de la siguiente manera:

1. Diríjase a la página **Red**.
2. Examine los contenedores y seleccione los endpoints que desea analizar.
3. Haga clic en el botón **Tareas** y seleccione **Analizar en busca de indicadores de compromiso**.

Aparecerá una página de configuración, donde deberá seleccionar los indicadores que se tendrán en cuenta para el análisis de indicador de compromiso.

The screenshot shows the Bitdefender GravityZone interface. On the left, there's a vertical navigation menu with icons for Dashboard, Incidents, Network (selected), Risk Management, Policies, Reports, and Quarantine. The main content area has a header 'Scan devices for IOCs'. It shows 'Selected devices: EWP01-10RS6X64' and a 'Scan name:' field containing 'ScanIOCs-2020.02.28'. Below this is a section titled 'Indicators of Compromise' with a note: 'Select the indicators you want the devices to be scanned for'. A red box highlights a group of buttons: MD5, SHA1, SHA256, SHA512, File names, Process names, Registry Values, and Registry Keys. To the right of this group is a yellow exclamation mark icon with the text 'At least one indicator should be selected.'

Configurar la tarea de análisis en busca de indicadores de compromiso (IoC)

Nota

Debe seleccionar al menos un tipo de indicador de compromiso para crear una tarea válida.

4. Seleccione uno o más tipos de IoC que desee tener en cuenta para el análisis y escriba el nombre del IoC conocido en el campo recién añadido.

This screenshot shows the 'Add Indicators of Compromise' configuration page. It has a section titled 'Indicators of Compromise' with the instruction 'Select the indicators you want the devices to be scanned for'. Below this are buttons for MD5, SHA1, SHA256, SHA512, File names, Process names, Registry Values, and Registry Keys. The 'Process names' button is highlighted with a blue border and a cursor is hovering over it. To the right, there's a 'Process names:' field containing 'svchost.exe' with a red box around it, and a delete 'X' button and a save 'disk' icon. At the bottom right of the page is a large red 'X' button.

Añadir indicadores de compromiso

Puede seleccionar entre los siguientes tipos:

- MD5
- SHA1
- SHA256
- SHA512
- Nombres de archivo
- Nombres de procesos
- Valores del registro
- Claves del registro

Nota

El contenido añadido en cada campo debe ser válido. De no ser así, se le presentará una señal de advertencia y un mensaje.

5. Haga clic en **Guardar** para crear y ejecutar la tarea **Analizar en busca de indicadores de compromiso**. Aparecerá un mensaje de confirmación.

Puede consultar el progreso de la tarea en la página **Red/Tareas**.

Name	Task type	Status	Start period	Reports
<input type="checkbox"/>				
<input checked="" type="checkbox"/> Scan for IOC 2020-03-02	Scan for IOC	Finished (1 / 1)	02 March 2020, 15:33:53	
<input type="checkbox"/>	Scan for IOC	Finished (1 / 1)	02 March 2020, 15:30:48	

Progreso de la tarea

6. Una vez que la tarea haya finalizado correctamente, puede hacer clic en el botón  **Informes** para leer el informe generado y determinar el impacto del indicador de compromiso analizado.

Las extensiones de archivo válidas para los indicadores de compromiso añadidos a la tarea incluyen las siguientes: exe, dll, com, scr, jar, msi, msc, bat, ps1, vbs, vbe, js, jse, wsf, wsh, psc1, lnk, doc, docx, docm, xls, xlsx, xlsm, ppt,

pptx, pptm, eml, rtf, pdf, html, ppsx, pps, ppsm, pot, potx, potm, ocx, sys, fnr, fne y pif.

La tarea **Analizar en busca de indicadores de compromiso** analizará las siguientes ubicaciones:

- %Windows%\System32\Drivers
- %Windows%\System32\WindowsPowerShell\v1.0
- %Windows%\system32\config\systemprofile\AppData
- %Windows%\System32\Tasks
- %Windows%\System32\wbem
- %Windows%\SysWOW64\WindowsPowerShell\v1.0
- %Windows%\SysWOW64\config\systemprofile\AppData
- %Windows%\SysWOW64\sysprep
- %Windows%\Scripts
- %Windows%\System
- %Windows%\Web
- %Users%



Importante

Las tareas de **Analizar en busca de indicadores de compromiso** no se ejecutarán, o fallarán, en los endpoints en las siguientes situaciones:

- El endpoint no tiene un sistema operativo Windows.
- La licencia del agente de Bitdefender del endpoint no es válida.
- El módulo de **EDR** no está instalado en el cliente BEST presente en los endpoints objetivo.
- Actualmente hay en cola más de cien tareas de **Analizar en busca de indicadores de compromiso**.
- El usuario ha introducido datos no válidos en la página de configuración de la tarea de **Analizar en busca de indicadores de compromiso**.

6.6.3. Análisis de riesgos

En cualquier momento, puede ejecutar tareas de análisis de riesgos bajo demanda en los endpoints que elija de la siguiente manera:

1. Diríjase a la página **Red**.
2. Examine los contenedores del panel izquierdo y seleccione los endpoints que desea analizar.
3. Haga clic en el botón  **Tareas** y seleccione **Análisis de riesgos**.

Aparecerá un mensaje que le solicitará que confirme la ejecución de la tarea de análisis de riesgos.

Nota

La tarea de análisis de riesgos se ejecutará con todos los indicadores de riesgo activados por defecto.

4. Una vez que la tarea haya finalizado satisfactoriamente, puede acceder a la pestaña **Configuraciones erróneas** de la página **Riesgos de seguridad**, analizarlos y elegir qué indicadores ignorar, en caso necesario.

La puntuación general de riesgo de la empresa se recalculará en función de los indicadores de riesgo ignorados.

Nota

Para ver la lista completa de indicadores y su descripción, consulte [este artículo de la base de conocimientos](#).

Importante

Las tareas de **Análisis de riesgos** no se ejecutarán, o fallarán, en los endpoints en las siguientes situaciones:

- El endpoint no tiene un sistema operativo Windows.
- La licencia del agente de Bitdefender del endpoint no es válida.
- La política aplicada al endpoint tiene el módulo de Administración de riesgos desactivado.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte [Ver y administrar tareas](#).

6.6.4. 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. 67).

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. 226).

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 “[Ejecución de tareas](#)” (p. 75).

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. 226).
- 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. 71).
- 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.

6.6.5. 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. 246).

Para analizar una base de datos de servidor de Exchange:

1. Diríjase a la página **Red**.
2. 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.

3. Marque la casilla de verificación del servidor de Exchange cuya base de datos quiera analizar.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y elija **Análisis de Exchange**. Aparecerá una nueva ventana de configuración.
5. 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 deseé 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. 478).

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**.

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

7. Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte [Ver y administrar tareas](#).

6.6.6. Instalar

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

Una vez que haya instalado un agente de relay, éste detectará automáticamente los endpoints no protegidos de la misma red.

La protección de Bitdefender puede instalarse en endpoints 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. 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**.

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

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

Usuario	Contraseña	Descripción	Acción
admin	*****		

Instalación de Bitdefender Endpoint Security Tools desde el menú Tareas

6. 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.

7. Si quiere que los endpoints objetivo se reinicien automáticamente para completar la instalación, seleccione **Reiniciar automáticamente (si es necesario)**.
8. 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.

9. 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.

10. En la sección **Implementador**, configure el relay al que se conectarán los endpoints objetivo para instalar y actualizar el cliente:

- **Importante**

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

Implementador			
Implementador:	Endpoint Security Relay		
Nombre	IP	Nombre/IP del servidor per...	Etiqueta
CO_SUPA	192.168.0.183		N/A
FC-WIN7-X64-01	192.168.3.80		N/A

Primeras Página ← Página 0 de 0 → Última página 20 0 elementos

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 con anterioridad para su cuenta y también el paquete de instalación por defecto disponible con Control Center.

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.

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.

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
- epupdatestable.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](#).

6.6.7. 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. 425).

6.6.8. Desinstalar cliente

Para desinstalar de forma remota la protección de Bitdefender:

1. Diríjase a la página [Red](#).
2. 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.
3. Marque las casillas de verificación de los endpoints de los que desee desinstalar el agente de seguridad de Bitdefender.
4. Haga clic en el botón [Tareas](#) de la zona superior de la tabla y seleccione [Desinstalar el cliente](#).
5. Se muestra una ventana de configuración que le permite optar por conservar los elementos en la cuarentena de la máquina cliente.
6. Haga clic en [Guardar](#) para crear la tarea. Aparecerá un mensaje de confirmación. Puede ver y administrar las tareas en la página [Red > Tareas](#). Para obtener más información, consulte [Ver y administrar tareas](#).

**Nota**

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

6.6.9. 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. 46).

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. 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.
3. Marque las casillas de verificación de los endpoints donde quiera realizar la actualización del cliente.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar**. Aparecerá una nueva ventana de configuración.
5. Puede optar por actualizar solo el producto, solo los contenidos de seguridad o ambos.
6. Haga clic en **Actualizar** para ejecutar la tarea. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte [Ver y administrar tareas](#).

6.6.10. 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 endpoints:

1. Diríjase a la página **Red**.
2. 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.
3. Marque las casillas de verificación de los endpoints a los que deseé cambiar los ajustes de instalación.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Reconfigurar el cliente**.
5. 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.
6. 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](#).

7. 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.

8. 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**.

9. 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.

10. 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](#).

6.6.11. 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.

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

1. Diríjase a la página **Red**.

- 2.
- 3.
4. Haga clic en el botón  **Tareas** de la zona superior de la tabla y seleccione **Reparar cliente**. Aparecerá una ventana de configuración.
5. 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.

6.6.12. Reiniciar máquina

Puede elegir reiniciar de forma remota los endpoints administrados.

**Nota**

Consulte la página [Red > Tareas](#) antes de reiniciar determinados endpoints. Las tareas creadas previamente pueden estar todavía en proceso en los endpoints objetivo.

1. Diríjase a la página [Red](#).
2. 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.
3. Marque las casillas de verificación correspondientes a los endpoints que quiera reiniciar.
4. Haga clic en el botón  **Tareas** de la zona superior de la tabla y seleccione **Reiniciar máquina**.
5. Seleccione la opción reiniciar programación:
 - Seleccione **Reiniciar ahora** para reiniciar los endpoints inmediatamente.
 - Seleccione **Reiniciar el** y use los campos inferiores para programar el reinicio en la fecha y hora deseadas.
6. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página [Red > Tareas](#). Para obtener más información, consulte [Ver y administrar tareas](#).

6.6.13. Descubrimiento de red

Los agentes de seguridad con **rol de relay** realizan automáticamente la detección de redes cada hora. No obstante, puede ejecutar manualmente la tarea de detección de redes desde Control Center en cualquier momento, partiendo de cualquier máquina protegida por Bitdefender Endpoint Security Tools.

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

1. Diríjase a la página **Red**.
2. 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.
3. Marque la casilla de verificación correspondiente al endpoint de relay con el que quiere llevar a cabo la detección de redes.
4. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Detección de redes**.
5. Aparecerá un mensaje de confirmación. Haga clic en **Sí**.

Puede ver y administrar las tareas en la página **Red > Tareas**. Para obtener más información, consulte [Ver y administrar tareas](#).

6.6.14. Actualizar Security Server

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

1. Diríjase a la página **Red**.
2. 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**.
3. Haga clic en el botón **Tareas** de la zona superior de la tabla y seleccione **Actualizar Security Server**.
4. 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 obtener más información, consulte [Ver y administrar tareas](#).

6.7.1. Integración con Active Directory

La integración permite a GravityZone importar el inventario del equipo desde Active Directory local y desde Active Directory alojado en Microsoft Azure. De esta forma, puede implementar y administrar fácilmente la protección en los endpoints de Active Directory. La integración se realiza a través de un endpoint administrado denominado integrador de Active Directory.

Para administrar la integración de Active Directory, puede hacer lo siguiente:

- [Configurar el integrador de Active Directory](#)
- [Eliminar el integrador de Active Directory](#)
- [Eliminar la integración](#)

Configurar el integrador de Active Directory

Puede definir varios integradores de Active Directory para el mismo dominio, y también para cada dominio disponible.

Requisitos

El integrador de Active Directory debe cumplir las siguientes condiciones:

- Ejecutar el sistema operativo Windows.
- Estar unido a Active Directory.
- Estar protegido por Bitdefender Endpoint Security Tools.
- Estar siempre conectado. De lo contrario, puede afectar a la sincronización con Active Directory.



Importante

Se recomienda que los endpoints unidos a Active Directory tengan la política asignada directamente. Todos los endpoints detectados en un dominio de Active Directory se moverán de su carpeta original a la de Active Directory. En este caso, si estos endpoints tienen una política heredada, se les asignará la establecida por defecto.

Configuración del integrador de Active Directory

Puede definir varios integradores de Active Directory para el mismo dominio, y también para cada dominio disponible.

Para configurar un endpoint como integrador de Active Directory:

1. Diríjase a la página **Red**.
2. Desplácese por el inventario de red hasta el grupo donde esté su endpoint y selecciónelo.

Nota

Si desea definir varios integradores, debe seleccionar un endpoint cada vez.

3. Haga clic en el botón  **Integraciones** de la zona superior de la tabla y seleccione **Establecer como integrador de Active Directory**.
4. Confirme esta acción haciendo clic en **Sí**.

Se percibirá del nuevo ícono  del endpoint, que indica que es un integrador de Active Directory. En un par de minutos, podrá ver el árbol de **Active Directory** junto a **Equipos y grupos**. En redes grandes con Active Directory, la sincronización puede tardar mucho tiempo en completarse. Los endpoints unidos en el mismo dominio que el integrador de Active Directory se trasladarán desde los **Equipos y grupos** al contenedor de Active Directory.

Sincronizar con Active Directory

GravityZone se sincroniza automáticamente con Active Directory cada hora.

GravityZone no puede sincronizar con un dominio de Active Directory si se producen las siguientes situaciones:

- Se han eliminado todos los roles de integrador de Active Directory.
- Se ha perdido la conexión entre los integradores de Active Directory y GravityZone durante al menos dos horas.
- Ninguno de los integradores de Active Directory del mismo dominio puede comunicarse con el controlador de dominio.

En cualquiera de estos casos, se comunicará un problema de Active Directory en el **área de notificaciones**. Para más información, diríjase a “[Notificaciones](#)” (p. 456).

Eliminar el integrador de Active Directory

Para eliminar el rol de integrador de Active Directory de un endpoint:

1. Diríjase a la página **Red**.
2. Desplácese por el inventario de red hasta el grupo donde esté el integrador de Active Directory y selecciónelo.

Nota

Si desea eliminar varios integradores, debe seleccionar un endpoint cada vez.

3. Haga clic en el botón **Integraciones** de la zona superior de la tabla y seleccione **Eliminar integrador de Active Directory**.
4. Aparecerá un mensaje de confirmación.
 - Si no hay otro endpoint con el rol de integrador de Active Directory en el mismo dominio, el mensaje de confirmación también le advertirá de que el dominio actual dejará de sincronizarse con GravityZone.
 - Si el endpoint está desconectado, el rol de integrador de Active Directory se eliminará una vez que se active.

Puede comprobar si se ha eliminado algún integrador de Active Directory de su red administrada en la sección **Actividad del usuario**, filtrando los registros de usuario con los siguientes criterios:

- **Área:** Active Directory
- **Acción:** Integrador de AD eliminado

Para más información, diríjase a “[Registro de actividad del usuario](#)” (p. 453).

Eliminar la integración de Active Directory

Puede eliminar uno o varios dominios de la carpeta de Active Directory de la siguiente manera:

1. Diríjase a la página **Red**.
2. En el árbol de **Red** del panel izquierdo, seleccione la carpeta **Active Directory**.
3. Vaya al panel derecho y seleccione la carpeta del dominio que desea eliminar.
4. Haga clic en el botón **Integraciones** de la zona superior de la tabla y seleccione **Eliminar integración de Active Directory**.

5. Aparecerá un mensaje de confirmación. Una opción disponible con este mensaje le permite elegir si desea eliminar o no los endpoints no administrados del inventario de red. Cuidado: esta opción está activada por defecto. Haga clic en **Confirmar** para continuar.
6. Todos los endpoints del dominio seleccionado se situarán en la carpeta **Equipo y grupos** (o en sus grupos originales) y se eliminará el rol del integrador de Active Directory de los endpoints asignados de este dominio.

6.8. Crear informes rápidos

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

1. Diríjase a la página **Red**.
2. Seleccione el grupo que desee del panel de la izquierda. Todos los endpoints del grupo seleccionado se muestran en la tabla del panel de la derecha. Opcionalmente, puede filtrar los contenidos del grupo seleccionado solo por los endpoints administrados.
3. Marque las casillas de verificación correspondientes a los equipos que desea incluir en el informe.
4. 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. 410](#)).

5. Configure las opciones del informe. Para más información, diríjase a “[Creando Informes](#)” ([p. 425](#)).
6. Haga clic en **Generar**. El informe se mostrará inmediatamente.

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

6.9. Asignando Políticas

Puede administrar los ajustes de seguridad en los endpoints mediante [políticas](#). En la página **Red** puede consultar, modificar y asignar políticas para cada endpoint o grupo de endpoints.



Nota

Los ajustes de seguridad solo están disponibles para los endpoints administrados. Para ver y administrar los ajustes de seguridad con mayor facilidad, puede [filtrar](#) el inventario de red para que aparezcan solo los endpoints administrados.

Para ver la política asignada a un endpoint concreto:

1. Diríjase a la página [Red](#).
2. Seleccione el grupo que desee del panel de la izquierda. Todos los endpoints del grupo seleccionado se muestran en la tabla del panel de la derecha.
3. Haga clic en el nombre del endpoint administrado que le interese. Aparecerá una ventana de información.
4. En la sección **Seguridad** de la pestaña **General**, haga clic en el nombre de la política actual para consultar sus ajustes.
5. Puede cambiar los ajustes de seguridad según sus necesidades, siempre y cuando el propietario de la política haya permitido que otros usuarios realicen cambios en dicha política. Tenga en cuenta que cualquier cambio que realice afectará a todos los endpoints que tengan la misma política asignada.

Para obtener más información sobre la modificación de los ajustes de políticas, consulte “[Políticas de equipos y máquinas virtuales](#)” (p. 136).

Para asignar una política a un equipo o grupo:

1. Diríjase a la página [Red](#).
2. Seleccione el grupo que desee del panel de la izquierda. Todos los endpoints del grupo seleccionado se muestran en la tabla del panel de la derecha.
3. Marque la casilla de verificación del endpoint o grupo que desee. Puede seleccionar uno o varios objetos del mismo tipo solamente desde el mismo nivel.
4. Haga clic en el botón [Asignar política](#) de la zona superior de la tabla.
5. Haga los ajustes necesarios en la ventana **Asignación de política**. Para más información, diríjase a “[Asignando Políticas](#)” (p. 127).

6.10.1. 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 llenar 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. 269).

6.11. 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 deseé 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. En el panel de la izquierda, seleccione el grupo de red que le interese.

Nota

Solo puede eliminar los endpoints mostrados en **Equipos y grupos**, que se detectan fuera de cualquier infraestructura de red integrada.

3. En el panel de la derecha, marque la casilla de verificación del endpoint que deseé eliminar.
4. 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.
5. El endpoint se moverá a la carpeta **Eliminados**.

En cualquier momento, puede mover endpoints de la carpeta **Eliminados** a **Equipos y grupos** 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.

6.12. 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](#)

6.12.1. 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.

Tareas					
		Nombre	Tipo de tarea	Estado	Reasignar cliente
					Informes
<input type="checkbox"/>	<input type="checkbox"/>	Análisis rápido 2015-08-28	Analizar	Pendiente (0 / 1)	28 Ago 2015, 15:34:18

La página Tareas

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

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

El estado de la tarea principal puede ser:

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

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

Diríjase a la subtarea que le interese y haga clic en el enlace disponible en la columna **Estado** para abrir la ventana **Estado**. Puede ver la lista de objetos de red asignada con la tarea principal y el estado correspondiente a la subtarea. El estado de las subtareas puede ser:

- **En curso**, cuando la subtarea todavía está en ejecución.
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.
- **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.

The screenshot shows a 'Task Status' window with the following details:

Computer Name	Status
SRV2012	Pending

Below the table, there is a 'Details' section containing the text: 'Created on: 21 Oct 2015, 14:55:06'. At the bottom left is a 'Close' button.

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.

6.12.2. Ver los informes de tareas

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

1. Diríjase a la página **Red > Tareas**.
2. Marque la casilla de verificación correspondiente a la tarea de análisis que le interese.
3. Haga clic en el botón correspondiente de la columna **Informes**. Espere hasta que se muestre el informe. Para más información, diríjase a “[Usar informes](#)” (p. 409).

6.12.3. Reinicio de tareas

Por diversas razones, las tareas de instalación, desinstalación o actualización del cliente quizás 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. Marque las casillas de verificación correspondientes a las tareas fallidas.
3. 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.

6.12.4. 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. Haga clic en la columna **Estado** para abrir la ventana **Estado de la tarea**.
3. Marque la casilla de verificación correspondiente a las subtareas pendientes o en ejecución que deseé detener.
4. 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.

6.12.5. 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. Marque la casilla de verificación correspondiente a la tarea que deseé eliminar.
3. 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 cualesquier subtareas pendientes. En tal caso, no podrá deshacerse ninguna subtarea finalizada.

6.13. 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](#)

6.13.1. 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**.

6.13.2. 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.

The screenshot shows the Bitdefender GravityZone interface with the 'Configuration' section selected in the sidebar. The main area is titled 'Offline machines cleanup' with the sub-instruction 'Configure rules to automatically delete unused virtual machines from the Network Inventory and clear their license seats.' Below this is a table for managing cleanup rules:

Rule name	Offline for	Machines name	Location	Deleted(last 24h)	State
Rule 3	66 days	[redacted]	Custom Groups	0 machines	<input checked="" type="checkbox"/>
Rule 4	78 days	[redacted]	Custom Groups	0 machines	<input type="checkbox"/>

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 comutador 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**.

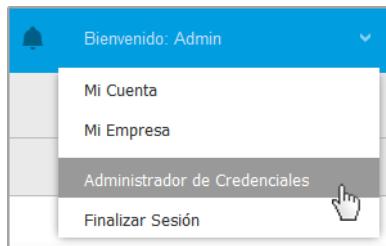
Para eliminar una o más reglas:

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.

6.14. Administrador de Credenciales

El Gestor de credenciales le ayuda a definir las credenciales necesarias 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

6.14.1. Añadir credenciales al Gestor de credenciales

Con el Gestor de credenciales 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:

A screenshot of the "Administrador de Credenciales" interface. On the left is a sidebar with "Panel de Control", "Red", "Paquetes", "Tareas", "Políticas", "Reglas de asignación", and "Informes". The main area has tabs for "Sistema Operativo" and "Credenciales". Under "Credenciales", there is a table with columns: "Nombre de Usuario", "Contraseña", "Descripción", and "Acción". There are three rows: 1. "administrator" with password "*****" and description "Windows7-User1". 2. "administrator" with password "*****" and description "Windows8-User1". 3. "admin" with password "*****" and description "Windows7-User2". Each row has a delete icon in the "Acción" column.

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.

6.14.2. Eliminación de credenciales del Gestor de credenciales

Para eliminar credenciales obsoletas del Gestor de credenciales:

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

7. POLÍTICAS DE SEGURIDAD

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

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 en todo momento o solo en determinadas condiciones, en función de la ubicación del endpoint. 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**.

Nombre de política	Creado por	Modificado el	Empresa
Política predeterminada (predeterminado)	root@bitdefender.com		

La página Políticas

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

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

Para personalizar los datos de la política que se muestran en la tabla:

1. Haga clic en el botón **III 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.

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. 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.
3. Configure los ajustes de la política. Para información detallada, diríjase a “[Políticas de equipos y máquinas virtuales](#)” (p. 136).
 4. Haga clic en **Guardar** para crear la política y volver a la lista de políticas.

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.

Puede asignar políticas 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**.

Asignación de políticas de dispositivos

En GravityZone, puede asignar políticas de varias maneras:

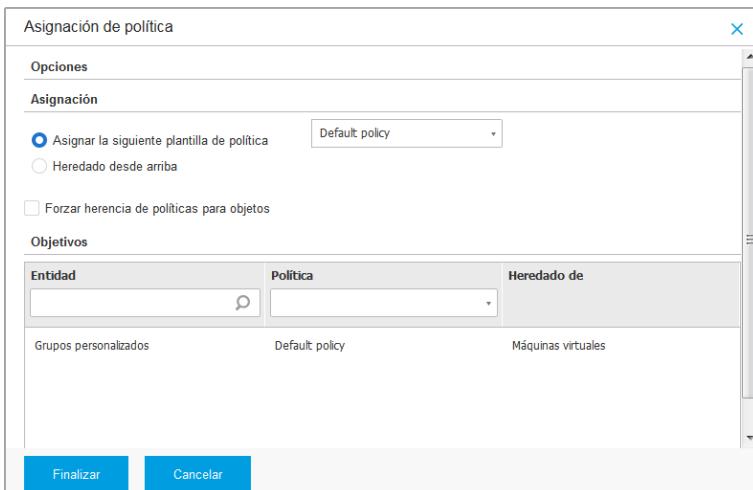
-
- Asignar la política del grupo primario mediante la herencia.
- Forzar la herencia de políticas al objetivo.

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.
3. 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

4. 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.

5. De aparecer una advertencia, haga clic en el enlace **Excluir estos objetivos** para continuar.
6. 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.
7. 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.
8. 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:

Asignación de políticas basadas en reglas

La página **Políticas > Reglas de asignación** le permite definir las reglas de asignación de políticas para un lugar específico. Por ejemplo, puede aplicar reglas de cortafuego más restrictivas cuando los usuarios se conecten a Internet desde fuera de la empresa, o definir diferentes frecuencias de tareas bajo demanda en tales casos.

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**
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	Direcciones IP específicas en una red o subred.
IP	Para subredes, utilice el formato CIDR.

Tipo	Valor
	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	<p>Dirección IP del servidor WINS</p> <p>Importante Esta opción no se aplica en sistemas Linux y Mac.</p>
Dirección del servidor DNS	Dirección IP del servidor DNS
Sufijo DNS de conexión DHCP	<p>Nombre del DNS sin el nombre de host para una conexión DHCP determinada</p> <p>Por ejemplo: central.empres.biz</p>
El endpoint puede resolver el host	<p>Nombre del host.</p> <p>Por ejemplo: serv.empres.biz</p>
Tipo de red	<p>Inalámbrica/Ethernet</p> <p>Al elegir una red inalámbrica, también puede añadir el SSID de esta.</p> <p>Importante Esta opción no se aplica en sistemas Linux y Mac.</p>
Nombre del host	<p>Nombre del host</p> <p>Por ejemplo: cmp.bitdefender.com</p> <p>Importante También puede usar comodines. El asterisco (*) sustituye cero o más caracteres y el signo de interrogación (?) sustituye exactamente un carácter. Ejemplos: *.bitdefender.com</p>

Tipo	Valor
	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		
X		
Ubicaciones		
IP/Prefijo de red		+
Tipo	Valor	Acciones
IP/Prefijo de red	10.10.0.0/16;192.168.0.0/24	X
Dirección de la puerta de enlace	10.10.0.1;192.168.0.1	X

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. 131).
- 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.

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. Encuentre la política que está buscando en la lista y haga clic en su nombre para editarla.
3. Configure las opciones de la política según sea necesario. Para información detallada, diríjase a “[Políticas de equipos y máquinas virtuales](#)” (p. 136).
4. Haga clic en **Guardar**.

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

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. Haga clic en el nombre de la política. Esto abrirá la página de políticas.
3. Introduzca el nombre de la nueva política.
4. 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 eliminar una política:

1. Diríjase a la página **Políticas**.
2. Marque la casilla de verificación de la política que desea eliminar.
3. 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. Haga clic en el nombre de la política. Esto abrirá la página de configuración de políticas.
3. Configure las opciones de la política según sea necesario. Los ajustes se organizan en las siguientes secciones:
 - General
 - Antimalware
 - Sandbox Analyzer
 - Cortafuego
 - Protección de red
 - Administración de parches
 - Control de dispositivos
 - Relay
 - Protección de Exchange
 - Cifrado
 - Protección de almacenamiento
 - Sensor de incidentes
 - Administración del riesgo

Navegue por las secciones mediante el menú de la izquierda de la página.

4. Haga clic en **Guardar** para guardar los cambios y aplicarlos a los equipos objetivo. Para abandonar la página de política sin guardar los cambios, haga clic en **Cancelar**.



Nota

Para saber cómo utilizar las políticas, diríjase a “[Administrando las Políticas](#)” (p. 126).

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.

The screenshot shows the Bitdefender GravityZone web interface. On the left, there's a sidebar with links like 'Panel de Control', 'Red', 'Paquetes', 'Tareas', 'Políticas' (which is highlighted in blue), 'Informes', and 'Cuaarentena'. Below that is another section with 'Antimalware'. The main content area has a title 'Detalles de política'. It shows the policy name 'Política predeterminada (158)', a checkbox for 'Permitir a otros usuarios cambiar esta política' which is unchecked, and a history section with 'Creado por: Admin' and 'Creado el: N/A'.

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 ícono **B** 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.

The screenshot shows the Bitdefender GravityZone interface with the following configuration:

- General** tab selected.
- Activar Modo Oculto** checkbox is unchecked.
- Detalles** section:
 - Mostrar ícono en el área de notificación** checkbox is checked.
 - Mostrar ventanas emergentes de notificación** and **Mostrar ventanas emergentes de alerta** checkboxes are unchecked.
- Notificaciones**, **Configuración**, **Comunicación**, **Actualizar**, **Antimalware**, **Cortafueg.**, **Control Contenido**, **Control de dispositivos**, and **Relay** sections are collapsed.
- Alertas de estado** tab selected under **Configuración**.
- Personalizado: ajustes de notificación definidos por el administrador** is selected.
- Activar todo**, **- Personalizado** (selected), and **- Desactivar todo** radio buttons are available.
- Información del soporte técnico** link is present.
- Página web:** <http://www.bitdefender.com/support/business.html>

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 ícono en el área de notificación**, **Mostrar ventanas emergentes de notificación** y **Mostrar ventanas emergentes de alerta** 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 ícono en el área de notificación.** Seleccione esta opción para mostrar el ícono de Bitdefender **B** en el área de notificación (también conocida como bandeja del sistema). El ícono 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.

Por ejemplo, después de marcar las casillas de verificación asociadas a Sandbox Analyzer, Bitdefender Endpoint Security Tools informa al usuario cuando se envía un archivo para analizar su comportamiento.

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 ícono **B** 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 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 ícono 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 llenar 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 ícono **B** 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.

i 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 se enviará información personal.

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 agentes de relay disponibles en la red objetivo, puede asignar a los equipos seleccionados uno o varios endpoints de relay mediante políticas.

Para asignar endpoints de relay a equipos objetivo:

1. En la tabla de **Asignación de comunicación de endpoint**, haga clic en el campo **Nombre**. Se muestra la lista de endpoints de relay detectados en su red.
2. Seleccione una entidad.

Prioridad	IP	Nombre personalizado/IP	Acciones
	ECS 192.168.3.71	BDVM-PC-TEO	
		WIN-AKORN6RFLJC	

Políticas - Ajustes de comunicación

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

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 GravityZone Control Center (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:

- **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.

Prioridad	Servidor	Proxy	Acción
1	Servidores de Relay		▼ ▲ X
2	update.cloud.2d585.cdn.bitdefender.net:80		□ ▼ ▲ X

Use Bitdefender Servers as fallback location

Políticas - 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).
 - Para tener más control sobre cuándo cambiar la configuración y actualizar el proceso de ensayos, puede configurar el agente BEST en sus máquinas

Linux para ejecutar actualizaciones del módulo del kernel de EDR a través de la **Actualización del producto**.

Cuando la casilla de verificación **Actualización del producto** está marcada:

- Si marca la casilla de verificación **Actualizar los módulos EDR de Linux mediante la actualización del producto**, GravityZone actualizará las versiones del kernel a través de la **Actualización del producto**.
- Si deja esta opción inhabilitada, las versiones del kernel se actualizarán a través de la **Actualización de contenidos de seguridad**.

Nota

Si marca la casilla de verificación **Actualizar los módulos EDR de Linux mediante la actualización del producto** pero inhabilita la opción **Actualización del producto**, no se actualizarán los módulos de EDR de Linux.

- **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 <http://upgrade.bitdefender.com>. 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](#).

- **update.cloud.2d585.cdn.bitdefender.net.** Esta es la ubicación de actualización por defecto de Bitdefender, desde donde Bitdefender facilita las actualizaciones. Esta ubicación de actualización debe ser siempre la última opción de la lista.
- 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.

7.2.2. 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 en ejecución: Protege proactivamente contra amenazas y detecta y bloquea automáticamente ataques sin archivos en la fase previa a la ejecución.
- 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

The screenshot shows the Bitdefender GravityZone web interface. The left sidebar has a tree view with nodes like 'Panel de Control', 'Red', 'Páginas', 'Tareas', 'Políticas', 'Reglas de asignación', 'Informes', 'Cuarentena', 'Cuentas', 'Actividad del usuario', 'Configuración', 'Actualizar', and 'Licencia'. The 'Políticas' node is expanded, showing 'General', 'Antivirus', 'On-access', 'Bajo demanda', 'Configuración', 'Control de dispositivos', and 'Rápida'. The 'On-access' node is selected and expanded, showing 'Analisis en tiempo real' and 'Configuración'. The 'Analisis en tiempo real' section contains a radio button group for 'Normal - Seguridad estándar, uso bajo de recursos' (selected), 'Agresivo', 'Tolerante', and 'Personalizado'. A note says: 'Esta opción es deseada para proporcionar el equilibrio óptimo entre seguridad y rendimiento. - Protege mediante análisis frente a cualquier tipo de malware. - Todos los archivos accedidos desde unidades locales y archivos de aplicación de unidades de red (excepto archivos comprimidos y de riesgo casi nulo).'. The 'Configuración' section contains a radio button group for 'Control avanzado de amenazas': 'Normal - Recomendado para la mayoría de los sistemas' (selected), 'Agresivo', 'Tolerante', and 'Vacuna contra el ransomware'. A note says: 'Esta opción establece el índice de detección de Bitdefender Advanced Threat Control a medio, mostrando alertas que podrían incluir algunos falsos positivos (aplicaciones limpias detectadas como malintencionadas)'.

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. 478).

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 un 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 deseé 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:

- [Detección de amenazas basada en la nube](#)
- [Control avanzado de amenazas](#)
- [Protección contra ataques sin archivos](#)
- [Mitigación de ransomware](#)

The screenshot shows the 'En ejecución' (Execution) section of the Bitdefender GravityZone configuration interface. On the left, there's a sidebar with navigation links: General, Antimalware, On-Access, En ejecución (selected), Bajo demanda, Hyper Detect, Antexploit avanzado, Configuración, and Servidores de seguridad. The main panel has two sections: 'Control avanzado de amenazas' and 'Protección contra ataques sin archivos'. Under 'Control avanzado de amenazas', there's a dropdown menu set to 'Desinfectar' (Scan and clean). It includes three radio button options: '- Agresivo' (Aggressive), which is selected; '- Normal' (Normal); and '- Tolerante' (Tolerant). A note next to the radio buttons says: 'Normal - Recomendado para la mayoría de sistemas' (Normal - Recommended for most systems) and 'Esta opción establece el índice de detección de Bitdefender Advanced Threat Control a medio, mostrando alertas que podrían indicar amenazas detectadas como malintencionadas.' (This option sets the Bitdefender Advanced Threat Control detection index to medium, displaying alerts that may indicate detected malicious threats). Under 'Protección contra ataques sin archivos', there's a note: 'Cuando se activa, esta opción permite que GravityZone detecte y bloquee automáticamente ataques sin archivos en la fase previa a su ejecución.' (When activated, this option allows GravityZone to detect and block automatically fileless attacks in the pre-execution phase).

Políticas - Ajustes en ejecución

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 puntuá 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

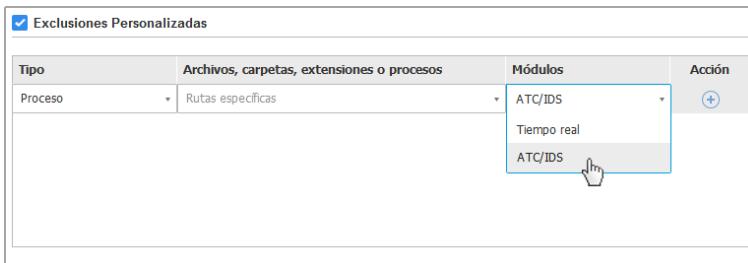
Si desactiva Advanced Threat Control, los equipos serán vulnerables al malware desconocido.

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 - Exclusión de procesos ATC/IDS

Protección contra ataques sin archivos

Nota

Este módulo está disponible para:

- Windows para estaciones de trabajo

- Windows para servidores

La Protección contra ataques sin archivos detecta y bloquea el malware sin archivos en la fase previa a la ejecución, incluyendo la finalización de PowerShell cuando ejecute una línea de comandos maliciosa, el bloqueo de tráfico malicioso, el análisis del búfer de memoria antes de la inserción de código y el bloqueo del proceso de inserción de código.

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. 456).

- 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. 182).

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.

Nombre de Tarea	Tipo de tarea	Repetir cada	Primera ejecución
Mi tarea	Análisis rápido	1 semana(s)	09/24/2015 15:21

Políticas - 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:

The screenshot shows the 'Editar tarea' (Edit Task) dialog box with the 'General' tab selected. The 'Detalles' section contains fields for 'Nombre de Tarea:' (Task Name: Mi tarea), a checkbox for 'Ejecutar la tarea con baja prioridad' (Run task with low priority) which is checked, and another for 'Apagar el equipo cuando termine el análisis' (Turn off the computer when analysis is finished) which is unchecked. The 'Programador' section includes a date and time picker set to '09/22/2016 11:12', a recurrence option where 'Programar la tarea para ejecutarse una vez cada:' (Schedule task to run once every) is selected with '1 dia(s)' (1 day), and a weekly repeat checkbox for 'Dom Lun Mar Mié Jue Vie Sáb' (Sunday through Saturday) which is unchecked. There are also checkboxes for 'Si se pasa el momento de ejecución programado, ejecutar la tarea lo antes posible' (If scheduled execution time passes, run task as soon as possible) and 'Omitir si el próximo análisis programado está previsto que comience en menos de' (Skip if the next scheduled analysis is expected to start in less than) followed by a dropdown menu for 'dia(s)' (days). At the bottom are 'Guardar' (Save) and 'Cancelar' (Cancel) buttons.

Políticas - 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 deseé.
- **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 - 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.

i 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. 478).

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.

i 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.

i 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

Mueve 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. 182).

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 límite (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. 177).

- **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. 178).

- **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. 178).

Puede expandir o contraer cada sección haciendo clic en su encabezado. De esta manera, llegará rápidamente a los ajustes que deseé 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.

Técnica	Descripción
	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. 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

Técnica	Descripción
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
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.

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.

Tipo	Archivos, carpetas, extensiones o procesos	Módulos	Acción
Proceso	Rutas específicas	Tiempo real	(+) Add

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 carpetas:

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](#)

Prioridad	Servidor de seguridad	IP	Nombre/IP del servidor personalizado	Acciones
<input type="checkbox"/> Conectarse en primer lugar al Servidor de seguridad instalado en el mismo host físico, si está disponible, cualquiera que sea la prioridad asignada.				
<input type="checkbox"/> Limitar el número de análisis bajo demanda simultáneos <input type="button" value="Bajo"/>				
<input type="checkbox"/> Usar SSL				
Comunicación entre los Servidores de seguridad y GravityZone				
<input checked="" type="radio"/> Mantener los ajustes de la instalación				
<input type="radio"/> Utilizar el proxy definido en la sección General				

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.

Para obtener más información sobre los puertos, consulte el artículo de la base de conocimientos [Puertos de comunicación de GravityZone](#).

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.

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:

- **Límite el número de análisis bajo demanda simultáneos.**

La ejecución de múltiples tareas de análisis bajo demanda en máquinas virtuales que comparten 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: $N = a \times \text{MAX}(b; vCPUs - 1)$, donde:

- $N = \text{límite máximo de tareas de análisis}$
- $a = \text{coeficiente multiplicador, con los siguientes valores: 1 - para Bajo; 2 - para Medio; 4 - para Alto}$
- $\text{MAX}(b ; vCPU - 1) = \text{una función que devuelve el número máximo de slots de análisis disponibles en el Security Server.}$
- $b = \text{el número por defecto de slots de análisis bajo demanda, que actualmente se establece en cuatro.}$
- $vCPUs = \text{número de CPUs virtuales asignadas al Security Server}$

Por ejemplo:

Para un Security Server con 12 CPU y un límite Alto de análisis simultáneos, tenemos un límite de:

$N = 4 \times \text{MAX}(4 ; 12-1) = 4 \times 11 = 44$ 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.

- **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.

7.2.3. 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 los ajustes de Sandbox Analyzer para el envío automático a través de Bitdefender Endpoint Security Tools. Para obtener información sobre el envío manual, consulte "["Envío manual"](#) (p. 449).

Sensor de endpoints

Bitdefender Endpoint Security Tools puede actuar como un sensor de alimentación de Sandbox Analyzer desde los endpoints de Windows.

Equipos y máquinas virtuales ▾

General	+ <input checked="" type="checkbox"/> Envío automático de muestras desde endpoints administrados
Antimalware	+ Habilité el sensor de endpoints integrado para enviar muestras que contengan objetos sospechosos a Sandbox Analyzer para un análisis en profundidad del comportamiento.
Sandbox Analyzer	-
Sensor de endpoints	
Cortafuegos.	+ <input checked="" type="radio"/> Monitización
Control Contenido	+ <input type="radio"/> Bloquear
Control de aplicaciones	
Control de dispositivos	+ Acción por defecto: Solo informar
Relay	+ Acción de reserva: Cuarentena
...	

Políticas > Sandbox Analyzer > Sensor de endpoints

Configure los ajustes de Sandbox Analyzer para el envío automático:

1. **Configuración de la Conexión.** El sensor de endpoints está configurado para enviar muestras a una instancia por defecto de Sandbox Analyzer alojada por Bitdefender, dependiendo de la región.

- **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 llenar 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” \(p. 152\)](#).
- 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:

i 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 prefiltro de contenidos para los envíos automáticos](#)" (p. 481).

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.

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. 235).

Nota

Un proxy configurado en los ajustes de conexión de Sandbox Analyzer anulará cualquier endpoint con rol de relay.

7.2.4. 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. 199).



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.

The screenshot shows the 'General' tab under the 'Cortafueg.' (Firewall) section. It includes options like 'Bloquear análisis de puertos' (Block port analysis), 'Permitir Conexión Compartida a Internet (ICS)', 'Monitorizar conexiones Wi-Fi', 'Registrar nivel de detalle' (Register detail level) set to 'Bajo' (Low), and 'Sistema de detección de intrusiones (IDS)' (IDS detection system). Below these, there are three radio button options for 'Control Contenido': '- Agresivo' (Aggressive), which is selected and described as 'Normal - Recomendado para la mayoría de sistemas' (Normal - Recommended for most systems); '- Normal', described as 'Bloquea inyecciones dll, instalación de controladores malware. Protege los archivos Bitdefender de ser alterados por aplicaciones de terceros no autorizadas. Generará un número moderado de alertas.' (Blocks DLL injections, installs malware drivers. Protects Bitdefender files from being altered by unauthorized third-party applications. Generates a moderate number of alerts.); and '- Tolerante' (Tolerant).

- **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 legítima 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](#)

Nombre	Tipo	Identificación	MAC	IP	Acción

Tipo	Tipo de red	Visibilidad de la red
Con cable	Hogar / Oficina	Desactivado
Wireless	Público	Desactivado
Virtual	De Confianza	Desactivado

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 delimita 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 añadirla 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](#).

The screenshot shows the Bitdefender GravityZone interface with the 'Reglas' (Rules) section selected. On the left, there's a sidebar with various modules: General, Antimalware, Sandbox Analyzer, Cortafuego (selected), General, Configuración, Reglas (selected), Protección de red, and Control de aplicaciones. The main panel has two tabs: 'Configuración' and 'Reglas'. Under 'Configuración', the 'Nivel de protección' is set to 'Juego de reglas, archivos conocidos y permitir'. Under 'Reglas', several checkboxes are checked: 'Crear reglas agresivas', 'Crear reglas para aplicaciones bloqueadas por IDS', 'Monitorizar cambios de procesos', and 'Ignorar los procesos firmados'. Below these tabs is a toolbar with buttons for 'Añadir', 'Arriba', 'Abajo', 'Exportar', 'Importar', and 'Eliminar'. At the bottom, there are columns for 'Priori...', 'Nombre', 'Tipo de regla', 'Red', 'Protocolo', and 'Permisos'.

Políticas - 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, introduzcalo 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**.
- Si 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 deseé 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
<code>ruleType</code>	Tipo de regla: 1 para la Regla de aplicación 2 para la Regla de conexión
<code>tipo</code>	El valor de este campo es opcional.
<code>details.name</code>	Nombre de la regla

Campo	Nombre y valor
details.applicationPath	Ruta de aplicación (sólo para reglas basadas en aplicaciones)
details.commandLine	Línea de comando (sólo para reglas basadas en aplicaciones)
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

Campo	Nombre y valor
settings.localAddress.ipMask	La Dirección local se establece en IP o IP/máscara
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.

7.2.5. 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](#)

General	<input checked="" type="checkbox"/> Protección de red Al inhabilitar este módulo, inhabilitará todas sus características y no podrá modificar ningún ajuste. Configuración general <input type="checkbox"/> Analizar SSL <input type="checkbox"/> Mostrar la barra de herramientas del navegador (antiguo) <input checked="" type="checkbox"/> Asesor de búsquedas del navegador (antiguo) <input type="checkbox"/> Exclusiones globales <table border="1"><thead><tr><th>Tipo</th><th>Entidad excluida</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Tipo	Entidad excluida		
Tipo	Entidad excluida				
Antimalware					
Sandbox Analyzer					
Cortafuegos					
Protección de red					
General					
Control Contenido					
Protección Web					
Ataques de red					
Administración de parches					
Control de dispositivos					

Políticas - Protección de 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 ícono 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.** Excluya 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 caracteres 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
<code>www.ejemplo*</code>	Cualquier URL que comience por <code>www.ejemplo</code> (sin importar la extensión del dominio).

Sintaxis:	Aplicación de excepciones
	La exclusión no se aplicará a los subdominios del sitio Web especificado, como por ejemplo subdominio.ejemplo.com.
*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**

The screenshot shows the Bitdefender GravityZone interface. On the left, there's a sidebar with various security modules: General, Antimalware, Sandbox Analyzer, Cortafuegos, Protección de red (selected), Control Contenido (selected), Protección Web, Ataques de red, Administración de parches, and Control de dispositivos. The main panel has a title bar 'Control de acceso Web' and 'Configuración'. It contains three sections: 'Permitir' (Allow), 'Bloquear' (Block), and 'Programar' (Schedule). Below these are sections for 'Lista negra de aplicaciones' (Blacklist) and 'Ruta de la aplicación' (Application path). At the bottom right, there's a 'Permisos' (Permissions) section. A toolbar at the top of the main panel includes icons for 'Añadir' (Add), 'Eliminar' (Delete), and 'Actualizar' (Update).

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 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 períodos 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 períodos. 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 períodos 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 períodos. 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 deseé proteger.
 - d. Introduzca los datos que deseé 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](#)

<input checked="" type="radio"/> General	<input checked="" type="checkbox"/> Antiphishing
<input checked="" type="radio"/> Antimalware	<input checked="" type="checkbox"/> Protección contra fraude
<input checked="" type="radio"/> Sandbox Analyzer	<input checked="" type="checkbox"/> Protección contra phishing
<input checked="" type="radio"/> Cortafuegos.	<input checked="" type="checkbox"/> Análisis del tráfico web
<input checked="" type="radio"/> Protección de red	<input checked="" type="checkbox"/> Tráfico Web (HTTP)
General	<input type="checkbox"/> Correos electrónicos entrantes (POP3) ⓘ
Control Contenido	<input type="checkbox"/> Correos electrónicos salientes (SMTP) ⓘ
Protección Web	

Políticas - Protección de 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 no 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.

The screenshot shows the Bitdefender GravityZone interface. On the left, there's a sidebar with various security modules: General, Antimalware, Sandbox Analyzer, Cortafuegos, Protección de red (selected), General, Control Contenido, Protección Web, Ataques de red, and Administración de parches. The main panel is titled 'Network Attack Defense' with a sub-section 'Técnicas de ataque'. It lists five attack techniques with dropdown menus: 'Acceso inicial' (Bloquear), 'Acceso a credenciales' (Bloquear), 'Detección' (Bloquear), 'Movimiento lateral' (Bloquear), and 'Crimeware' (Bloquear). A blue button at the bottom says 'Restablecer la configuración por defecto'.

Políticas - Protección de red - Ataques de red

Para configurar Network Attack Defense:

1. Marque la casilla de verificación **Network Attack Defense** para activar el módulo.
2. Marque 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.

7.2.6. 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](#)

7.2.7. 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

Tipo de dispositivo	Windows	macOS
Windows Portable	x	x
Puertos COM/LPT	x	Compatible LPT a puertos serie
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 deseé:

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 deseé para cada componente.

Por ejemplo, para Almacenamiento externo, puede bloquear solamente USB y permitir que se utilicen todos los demás puertos.

Almacenamiento externo Regla

Permisos: *	Personal
Descripción: *	External Storage
Permisos personalizados	
Firewire:	Permitido
Plug & Play ISA:	Permitido
PCI:	Permitido
PCMCIA:	Permitido
SCSI:	Permitido
Tarjeta SD:	Permitido
USB:	Permitido
Other	Permitido

Guardar **Cancelar**

Políticas - 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 - Control de dispositivos - Exclusiones

7.2.8. 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.

- La ubicación de actualización por defecto para los agentes de relay es <http://upgrade.bitdefender.com>. Puede especificar otras ubicaciones de actualización introduciendo la IP o el nombre de host local de una o varias máquinas de relay 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.

7.2.9. 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.

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.

Configuración

- **Eliminar archivos en cuarentena de más de (días).** Por defecto, los archivos de más de 15 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 cumplen 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 deseé 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 deseé 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 deseé 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 **Especifico** 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 **Especifico** 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. 478).

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 deseé 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:
Carpetas públicas	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 desea 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. 478).

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 a cabo 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 antispyware 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" \(p. 254\)](#)".
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 deseé 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 **Especifico** 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 **Especifico** 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. 251).



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. 256)

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 cumplen 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:

- Parte 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 deseé 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. 258).

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 0
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. 258).

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. 479).
- 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**.

7.2.10. 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.

The screenshot shows the Bitdefender GravityZone Control Center interface. On the left, there's a sidebar with various modules: General, Antimalware, Cortafuegos, Protección de red, Control de aplicaciones, Control de dispositivos, Relay, and Cifrado. The Cifrado module is currently selected and expanded. Inside the Cifrado section, there are two main configuration sections: 'Gestión de cifrado' and 'Exclusiones'. The 'Gestión de cifrado' section contains a checked checkbox for enabling encryption management. Below it, there are two radio button options: 'Descifrar' (selected) and 'Cifrar'. Under 'Cifrar', there's a note about requiring a password at startup if a TPM module is present. The 'Exclusiones' section has a checked checkbox and a table with columns for 'Tipo', 'Elementos excluidos', and 'Acción'. At the bottom, there are navigation links for 'Primera Página', 'Página', '0 de 0', 'Última página', and a page size selector set to '20'. A note indicates '0 elementos'.

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" \(p. 271\)](#).

- **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. 114).

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** .

7.2.11. 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.

The screenshot shows the Bitdefender GravityZone interface under the 'Equipos y máquinas virtuales' tab. On the left, a sidebar lists various policy categories: General, Antivirus, Sandbox Analyzer, Firewall, Content Control, Patch Management, Application Control, Device Protection, Relay, Cifrado, and Protección de almacenamiento. The 'Protección de almacenamiento' category is selected. The main pane displays configuration for 'Análisis en tiempo real'. It includes fields for 'Nombre del servicio:' (bdicap) and 'Puerto:' (1394). Below this is the 'Configuración de Análisis de Archivos' section, which contains a checkbox for 'Analizar archivo comprimido' and sliders for 'Tamaño de archivo máximo (MB)' (set to 3) and 'Profundidad de archivo máxima (niveles)' (set to 2). The 'Control de congestión' section contains two radio button options: 'Ignorar automáticamente las nuevas conexiones en dispositivos de almacenamiento si el Servidor de seguridad está sobrecargado' (selected) and 'Número máximo de conexiones en dispositivos de almacenamiento' (set to 300). At the bottom, the 'Acciones del Análisis' section shows a dropdown menu set to 'Acceso denegado'.

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.

Equipo y máquinas virtuales

Exclusiones

Estas exclusiones se aplican a los Servidores de seguridad cuando se utilizan como servicio de análisis para dispositivos de almacenamiento.

Exportar Importar

Tipo	Ruta	Descripción	Acción
Hash		Altado descripto	<input type="button" value="+"/>

Página 0 de 0 Última página 20 0 elementos

Políticas - Protección de almacenamiento - ICAP

7.2.12. Sensor de incidentes

El sensor de incidentes monitoriza continuamente las actividades del endpoint, como los procesos en ejecución, las conexiones de red, los cambios en el registro y el comportamiento de los usuarios. Estos metadatos se recopilan, se comunican y procesan mediante algoritmos de Machine Learning y tecnologías de prevención que detectan actividades sospechosas en el sistema y generan incidentes.

Marque la casilla Sensor de incidentes para habilitar este módulo.

Incidents Sensor

Continuously monitors endpoint activity such as running processes, network connections, registry metadata is being collected, reported and processed by machine learning algorithms and prevent suspicious activity on the system, and generate Incidents.

Sensor de incidentes

7.2.13. Administración del riesgo



Nota

Este módulo está disponible para:

- Windows para estaciones de trabajo
- Windows para servidores

El módulo de Análisis de riesgos en los endpoints le ayuda a identificar y reparar gran cantidad de riesgos de la red y del sistema operativo a nivel de endpoints mediante tareas de análisis de riesgos que pueden configurarse en la política para que se ejecuten recurrentemente en los endpoints objetivo.

Puede elegir entre una larga lista de indicadores de riesgo para analizar sus endpoints y determinar si son vulnerables. Para obtener más información sobre los indicadores de riesgo de GravityZone, consulte [este artículo de la base de conocimientos](#).

Para configurar el Análisis de riesgos en los endpoints (ERA, por sus siglas en inglés):

- Marque la casilla para habilitar las características de **Administración de riesgos** y empiece a configurar políticas que definan cómo ejecutar la tarea de **Análisis de riesgos**.
- **Programador:** Defina el programa de análisis de riesgos para los endpoints objetivo:
 1. Especifique la fecha y hora de inicio para el análisis de riesgos programado.
 2. Elija el tipo de recurrencia del análisis:
 - Periódicamente, según un número concreto de horas, días o semanas.
 - Según el día de la semana.



Importante

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.

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).

3. 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 deseé.

Las tareas de análisis de riesgos se ejecutarán con todos los indicadores de riesgo activados por defecto.

Después de que una tarea de análisis de riesgos haya finalizado satisfactoriamente, puede acceder a la pestaña [Configuraciones erróneas](#) de la página [Riesgos de seguridad](#), analizarlos y elegir qué indicadores ignorar, en caso necesario.

La puntuación general de riesgo de la empresa se recalculará en función de los indicadores de riesgo ignorados.



Nota

Para ver la lista completa de indicadores de riesgo y su descripción, consulte [este artículo de la base de conocimientos](#).

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.

La sección de monitorización de GravityZone consta de lo siguiente:

- [Panel de Control](#)
- [Resumen ejecutivo](#)

8.1. Panel de Control

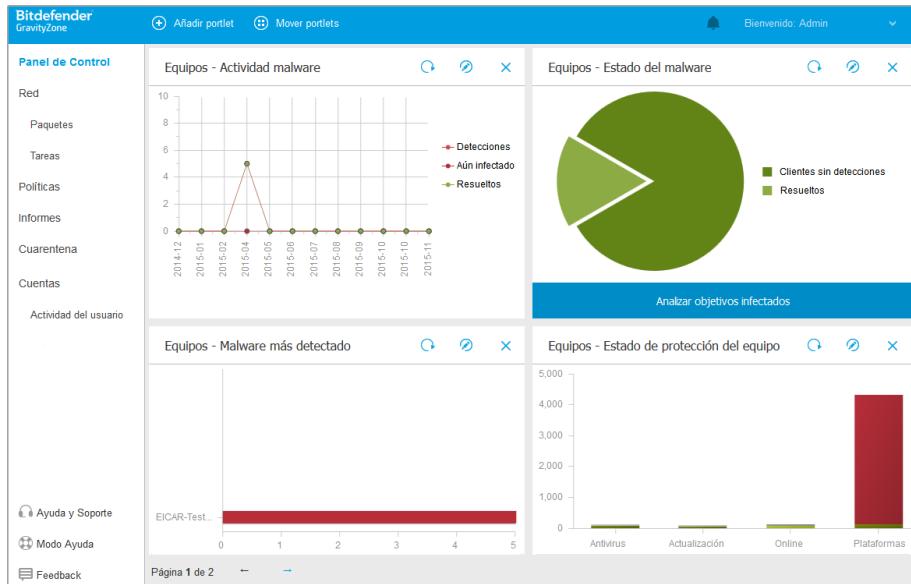
El panel de control Control Center es una visualización personalizable que proporciona un resumen de seguridad rápido de todos los endpoints protegidos y del estado de la red.

Se compone de dos secciones:

- Barra de estado de la red del panel de control
- Portlets del panel de control

La barra de estado de red del panel de control le informa de la cantidad de incidentes abiertos o en curso, recursos (endpoints) amenazados y amenazas detectadas en su red. Use esta información para conocer los elementos de red pendientes de resolver. Haga clic en [Ver](#) para acceder a la página de **Incidentes**. Para más información, diríjase a “[Investigar incidentes](#)” (p. 289).

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 ícono **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 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. 409).

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.



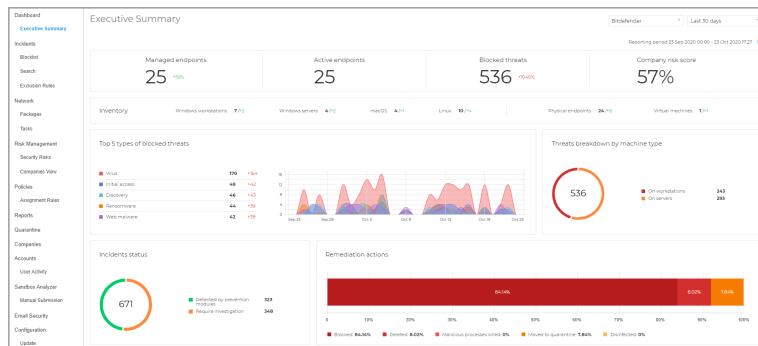
Nota

Solo puede mover los portlets en las posiciones ya ocupadas.

8.2. Resumen ejecutivo

El **Resumen ejecutivo** presenta un conciso resumen de la seguridad de todos los endpoints protegidos en su red y está especialmente diseñado para ayudarle a monitorizar, analizar y proporcionar datos fáciles de interpretar a la dirección ejecutiva.

Se compone principalmente de widgets y mejora la visibilidad al ofrecer información sobre los módulos de los endpoints, las detecciones y las medidas adoptadas, los tipos y técnicas de las amenazas, y la puntuación de riesgo de su empresa, entre otras cosas.



Resumen ejecutivo



Importante

- Todas las estadísticas proporcionadas se basan en datos recopilados después de habilitar la característica. No se incluyen eventos anteriores.

Las secciones iniciales ubicadas en la parte superior de la página son las siguientes:

Endpoints administrados

Esta sección presenta todas las máquinas de su red que tienen el agente de seguridad instalado.

Endpoints activos

Esta sección le informa de todos los endpoints que estaban conectados durante el período seleccionado o que lo estaban en el momento de generarse el informe.

Amenazas bloqueadas

Esta sección informa del número total de amenazas bloqueadas que se han identificado en sus endpoints.

Inventario

Esta sección proporciona información sobre los tipos de endpoints y sus sistemas operativos.

Puntuación de riesgo de empresa

En esta sección, puede hallar información sobre el nivel de riesgo de su empresa.

En la esquina superior derecha de la página, puede escribir el nombre de una empresa o seleccionar la empresa que desee en el menú desplegable. Tenga en cuenta que el resumen proporciona estadísticas de una sola empresa cada vez, y no de toda la estructura del árbol.

También puede seleccionar un intervalo de tiempo respecto al momento actual:

- **Últimas 24 horas**
- **Últimos 7 días**
- **Últimos 30 días**

Nota

- Todos los datos presentados se correlacionan directamente con el período y la empresa seleccionados.
- Para asegurarse de que la consola muestra la información más reciente, use el botón **Actualizar** de la parte superior derecha de la página.

Dependiendo del intervalo seleccionado, puede observar una diferencia (delta) mostrada como porcentaje en algunas secciones.

Los valores delta indican las diferencias en su red que se produjeron entre dos períodos dados:

- El período anterior al intervalo seleccionado con el mismo número de días u horas.
- El intervalo seleccionado.

Por ejemplo, en la imagen siguiente, el número total de amenazas bloqueadas en su red ha disminuido un **6 %** durante los **últimos treinta días**. Este porcentaje se obtuvo comparando los valores de justo los treinta días anteriores al intervalo seleccionado con los valores de los últimos treinta días.

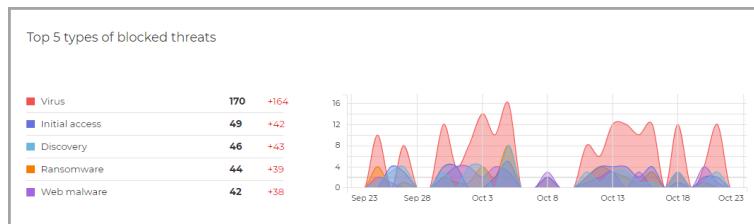


Resumen ejecutivo: delta

Los principales widgets del resumen son los siguientes:

Los cinco tipos principales de amenazas bloqueadas

El widget ofrece información sobre los tipos de amenazas más frecuentes en función del número de detecciones en sus endpoints. La columna de la izquierda muestra los tipos de amenazas y, correlacionados en la columna de la derecha, puede ver el número de detecciones para cada tipo, así como los valores delta.



Resumen ejecutivo: los cinco tipos principales de amenazas bloqueadas

Desglose de amenazas por tipo de máquina

Este widget presenta los tipos de endpoints, estaciones de trabajo y servidores, así como el número de detecciones que se ha producido en cada uno.

Estado de incidentes

Este widget detalla los incidentes de seguridad en toda la red de la empresa.

Las categorías de incidentes son las siguientes:

- **Detectados por módulos de prevención:** eventos de seguridad identificados como amenazas por los módulos de prevención de GravityZone.
- **Requiere investigación:** incidentes sospechosos que requieren investigación, sobre los cuales aún no se ha adoptado ninguna medida.

Acciones de reparación

Esta sección describe las acciones que se llevaron a cabo en relación con los elementos bloqueados en función de los ajustes de la política aplicada.

Estado de los módulos de endpoint

Proporciona una visión de conjunto de la cobertura de los módulos de protección en sus endpoints. El gráfico indica los módulos y si están habilitados, inhabilitados o sin instalar en sus endpoints.

Puntuación de riesgo de empresa

Este widget proporciona información sobre el nivel de riesgo al que está expuesta su organización debido a configuraciones erróneas del sistema, vulnerabilidades conocidas de las aplicaciones instaladas actualmente y riesgos potenciales causados por el comportamiento y actividad de los usuarios.

Detecciones basadas en reglas de políticas

Esta sección detalla el número de detecciones y sus tipos en función de las reglas que el administrador haya personalizado en la política.

Los tipos de detección incluyen los siguientes:

- **Dispositivos bloqueados:** el número de detecciones según las reglas del Control de dispositivos.
- **Conexiones bloqueadas:** el número de detecciones según las reglas del Cortafuego.
- **Aplicaciones bloqueadas:** el número de detecciones según las reglas de la Lista negra de aplicaciones.
- **Sitios web bloqueados:** el número de detecciones según las reglas del Control de acceso web.

Páginas Web bloqueadas

Este widget presenta el número de detecciones organizadas por tipos de amenazas e identificadas en sus endpoints por la **Protección de red**.

Técnicas de ataque a la red bloqueadas

Esta sección proporciona información sobre las técnicas de ataque bloqueadas descubiertas en su red.

9. INVESTIGAR INCIDENTES

La sección **Incidentes** le ayuda a filtrar, investigar y adoptar medidas sobre todos los eventos de seguridad detectados por el Sensor de incidentes durante un intervalo de tiempo determinado.

La sección de **Incidentes** contiene las siguientes páginas:

- **Incidentes**: permite ver e investigar eventos de seguridad.
- **Lista de bloqueo**: administra los archivos bloqueados involucrados en eventos de seguridad.
- **Búsqueda**: proporciona opciones para consultar la base de datos de eventos de seguridad.

9.1. La página de incidentes

Use la página **Incidentes** para filtrar y administrar los eventos de seguridad.

Extended Incidents		Endpoint Incidents		Detected Threats			
Change Status							
ID	Date	Status	Confidence Score	Endpoint	Alerts	Attack type	
<input type="checkbox"/> #763	Updated at 04:54 on 5 Sep	Open	● 99	LEV-EDRS	155	Malware +1	
<input type="checkbox"/> #755	Created at 13:35 on 20 Aug	Open	● 40	LEV-EDRS	27	Ransomware	
<input type="checkbox"/> #746	Created at 13:58 on 19 Aug	Open	● 40	LEV-EDRS	26	Ransomware	
<input type="checkbox"/> #739	Created at 16:59 on 31 Jul	Open	● 90	LEV-EDRS	35	Ransomware +2	
<input type="checkbox"/> #737	Created at 16:57 on 31 Jul	Open	● 90	LEV-EDRS	35	Ransomware +2	
<input type="checkbox"/> #735	Created at 16:45 on 28 Jul	Open	● 90	LEV-EDRS	35	Ransomware +2	

Descripción general de la página de incidentes

Nota

La disponibilidad de estas pestañas puede variar según la licencia incluida en su plan actual.

Esta página contiene las siguientes áreas:

1. Una barra con pestañas que incluye diferentes tipos de incidentes:

- **Incidentes extendidos:** muestra los incidentes de toda la red detectados en su entorno por diversos sensores (EDR y NTSA), los cuales pueden poner en riesgo a su organización.
 - **Incidentes de endpoints:** muestra todos los incidentes sospechosos detectados a nivel de endpoints que requieren investigación y sobre los que aún no se ha adoptado ninguna medida.
 - **Amenazas detectadas:** muestra todos los eventos de seguridad identificados como amenazas por los módulos de prevención de GravityZone. Estos incidentes se detectan a nivel de endpoints y se actúa sobre ellos con medidas predefinidas en las políticas de seguridad aplicadas a su entorno.
2. Opciones de filtrado para personalizar su cuadrícula:
- Haga clic en el botón  **Mostrar/Ocultar columnas** para añadir o eliminar columnas de filtro.
La página se actualizará automáticamente y cargará las tarjetas de eventos de seguridad con información que coincide con las columnas añadidas.
 - Haga clic en el botón  **Mostrar/Ocultar filtros** para mostrar u ocultar la barra de filtros.
 - Haga clic en el botón  **Borrar filtros** para quitar todos los filtros.
3. La cuadrícula de Incidentes muestra una lista de eventos de seguridad en función de los filtros aplicados.



Nota

Esta característica ya no es compatible con Internet Explorer.

La barra de Información general

La barra de **Información general** indica los incidentes abiertos, las alertas principales y los dispositivos afectados, entre otros datos relevantes, para darle una idea de la situación general de las amenazas a las que se enfrenta su entorno.

OPEN INCIDENTS	TOP ALERTS	TOP TECHNIQUES	TOP AFFECTED DEVICES
High 3	ATC.Malicious 3	Modify Registry 3	LEV-ENDPOINT2 3
Medium 0	CertUtil Process 2	PowerShell 3	
Low 0	PowerShell Command 2	Command-Line Interface 3	

La barra de Información general

Nota

La disponibilidad y el contenido de la barra de **Información general** pueden variar según la licencia incluida en su plan actual.

Filtrar incidentes desde la barra de información general

Puede filtrar la lista de incidentes seleccionando valores en la barra de Información general:

- Si hace clic en un valor de la sección **INCIDENTES ABIERTOS**, solo se mostrarán los incidentes con el nivel de gravedad seleccionado.
- Si hace clic en un valor de la sección **ALERTAS PRINCIPALES**, se llenará el campo de búsqueda con el nombre de la alerta y se mostrarán solo los incidentes donde se detectó esa alerta.
- Si hace clic en un valor de la sección **TÉCNICAS PRINCIPALES**, se llenará el campo de búsqueda con el nombre de la técnica y se mostrarán solo los incidentes donde se detectó esa técnica.
- Si hace clic en un valor de la sección **DISPOSITIVOS MÁS AFECTADOS**, se mostrarán solo los incidentes que afecten al dispositivo seleccionado.

9.1.1. La cuadrícula de filtros

La página **Incidentes** le permite elegir qué incidentes mostrar al personalizar la cuadrícula de filtros.

The screenshot shows a search bar at the top with a magnifying glass icon and a placeholder 'Search for filenames, IP addresses, hostnames ...'. Below it is a table header with columns: Score, Date, Status, ID, Endpoint, Attack type, Alerts, and a column with icons for more actions. Under 'Score', there's a dropdown menu set to '100-30' with a 'Select...' button. Under 'Status', there are 'Open' and 'Search...' buttons. Under 'Endpoint', there are 'Search...' and 'Choose...' buttons. The 'Alerts' column has a red box around its header and a red X icon at the bottom right. Below the table, there's a row of details: a checkbox, a progress bar at 90%, the text 'Created at 12:57', an 'Open' button, the number '3', the endpoint 'LEV-ENDPOINT2', the attack type 'Other', and the alert count '20'.

La cuadrícula de filtros

- Haga clic en el botón **Mostrar/Ocultar columnas** para añadir o eliminar columnas de filtro.
La página se actualizará automáticamente y cargará las tarjetas de eventos de seguridad con información que coincide con las columnas añadidas.
- Haga clic en el botón **Mostrar/Ocultar filtros** para mostrar u ocultar la barra de filtros.
- Haga clic en el botón **Borrar filtros** para quitar todos los filtros.

La siguiente tabla le informa de las opciones de filtrado disponibles:

Opción de filtrado	Detalles
Puntuación	<p>La puntuación de confianza es un número de 100 a 10 que indica la peligrosidad potencial de un evento de seguridad. Cuanto más alta sea la puntuación, más probable será que el evento sea peligroso. Aporta contexto en base a los indicadores de ataque y las técnicas ATT&CK, si procede.</p> <p>Para filtrar por la puntuación de confianza, desplace la barra deslizante hasta los valores escogidos. También puede usar los campos numéricos debajo de la barra deslizante. Haga clic en OK para confirmar la selección de puntuación.</p>
Fecha	<p>Para filtrar por fecha:</p> <ol style="list-style-type: none"> 1. Haga clic en el ícono del calendario o el campo Fecha para abrir la página de configuración de fecha. 2. Seleccione el marco de tiempo en que sucedió el incidente:

Opción de filtrado	Detalles
	<ul style="list-style-type: none">Haga clic en las pestañas Desde y Hasta para seleccionar las fechas que definen el intervalo de tiempo. <p>Nota</p> <p>Puede especificar la hora exacta para las fechas de inicio y finalización utilizando los campos de horas y minutos debajo del calendario.</p> <ul style="list-style-type: none">También puede seleccionar un período predeterminado respecto al momento actual (los últimos siete días; para obtener espacio adicional para el almacenamiento de eventos, debe ponerse en contacto con su representante de ventas para actualizar su solución con un complemento de retención de datos de 30, 90 o 180 días). <ol style="list-style-type: none">Haga clic en Aceptar para aplicar el filtro.
Estado	Filtre los incidentes por su estado actual marcando una o varias de las opciones de estado disponibles en el menú desplegable Estado : <ul style="list-style-type: none">Abierto: para los eventos de seguridad que no han sido investigados.Investigando: Para los eventos de seguridad en proceso de investigación.Falso positivo: para eventos de seguridad etiquetados como falsa alarma.Cerrado: Para los eventos de seguridad cuya investigación haya finalizado.
ID	Reduzca la lista de incidentes buscando un ID de evento de seguridad concreto.
Impacto en la organización	Esta categoría muestra la cantidad de endpoints y servidores afectados.

Opción de filtrado	Detalles
Última fase de la cadena de ataque	Puede filtrar los incidentes seleccionando una fase concreta de la cadena de ataque.
Endpoint	Reduzca la lista de incidentes buscando un nombre de endpoint concreto de la red que administra.
Tipo de ataque	El tipo de ataque es una lista dinámica de los tipos más comunes, que cambia según los indicadores de ataque que se encuentran en los eventos de seguridad incluidos en la lista.
Alertas	La columna Alertas muestra el número de alertas desencadenadas por cada incidente.
SO del endpoint	Esta opción filtra los eventos de seguridad según el sistema operativo de los endpoints involucrados.



Nota

Las opciones de filtrado pueden variar según el tipo de clave de licencia incluida en su plan actual.

Para buscar más elementos que no estén visibles en la cuadrícula de filtro, seleccione una de las opciones de búsqueda en el menú desplegable **Buscar**:

- **Nombre de la alerta:** de 3 a 1000 caracteres como máximo.
- **Técnica ATT&CK:** 100 caracteres como máximo.
- **IP del endpoint:** 45 caracteres como máximo.
- **MD5:** 32 caracteres como máximo.
- **SHA256:** 64 caracteres como máximo.
- **Nombre del nodo:** 360 caracteres como máximo.
- **Nombre de usuario:** 1000 caracteres como máximo.

La página se actualizará automáticamente y cargará solo las tarjetas de eventos de seguridad correspondientes al elemento que se busca. Para una búsqueda más detallada, puede crear consultas de búsqueda en la [página de búsqueda](#).

9.1.2. Ver la lista de eventos de seguridad

La página **Incidentes** muestra una lista de eventos de seguridad que coinciden con los filtros seleccionados.

Por defecto, se muestran veinte eventos por página, agrupados por fecha. La página se actualiza automáticamente a intervalos regulares, conforme EDR va aportando nuevos eventos.

Importante

Todos los eventos de seguridad con más de noventa días de antigüedad se eliminan automáticamente de todas las secciones de incidentes, así como del repositorio de eventos de seguridad.

Para navegar a través de la página, use las teclas de flecha, la rueda del ratón o haga clic en la barra de desplazamiento. Cambie la cantidad de eventos mostrados en la parte inferior de la página. Puede llegar hasta cien eventos por página.

Cada entrada de un evento de seguridad se muestra en un formato de tarjeta enriquecido, que proporciona una visión general de cada incidente, con información basada en los filtros seleccionados.

Nota

Compruebe el color del borde izquierdo para evaluar rápidamente el nivel de confianza (bajo, medio o alto).



Tarjeta de evento de seguridad

- Si hace clic en el botón **Ver gráfico** correspondiente de una tarjeta de evento de seguridad, se [abrirá en una nueva página](#), donde puede analizar detalladamente el incidente y adoptar las medidas oportunas.
- Si hace clic en una tarjeta de evento de seguridad, se abrirá un panel lateral de vista rápida con información sobre el incidente seleccionado.

The screenshot shows the 'INCIDENT DETAILS' section of the Bitdefender GravityZone interface. It displays the following information:

- INCIDENT DETAILS**
 - Incident ID: #1
 - Status: Open
 - Created On: 16 Jan 2020, 13:27:05
 - Last Updated on: 16 Jan 2020, 13:27:05
 - Endpoint: LEV-ENDPOINT2
 - Artifacts Involved: 45
- DETECTION**
 - Confidence Score: 90
 - Incident Trigger: user.exe(PID:3584)
 - ScriptFileWrittenByPowershell**
 - A suspicious script was written by powershell.exe or another process with powershell.exe as parent which could indicate lateral movement.
 - Detected By: EDR
 - Detected on: 16 Jan 2020, 13:26
 - Severity: Low
- ATTACK INFO**
 - Attack Type: Other

At the bottom, there are two buttons: **View Graph** and **View Events**. A blue arrow points from the 'Attack Info' section down to both buttons.

Vista rápida de los detalles del incidente

- Haga clic en el botón **Ver gráfico** para acceder a la visualización gráfica del incidente.
- Haga clic en el botón **Ver eventos** para acceder a la línea de tiempo del incidente.
- Si marca la casilla de verificación de cualquier tarjeta de evento de seguridad, se activará el botón **Cambiar estado**, que le permite cambiar el estado actual del incidente.



Cambio del estado de los eventos de seguridad

El estado de la investigación le ayuda a realizar un seguimiento de los incidentes que ya se han investigado y marcado como cerrados o falsos positivos, de los incidentes que se están investigando actualmente y de los incidentes abiertos o nuevos que aún no se han analizado.

Puede cambiar el estado de uno o varios eventos de seguridad a la vez:

1. Marque las casillas de las tarjetas de eventos de seguridad que cambiarán de estado.

Score	Date
100-30	Select...
All	Created at 06:01 on 21 Feb
All from page	Created at 06:01 on 21 Feb
50	Created at 06:01 on 21 Feb
90	Created at 13:30 on 19 Feb
50	Created at 13:30 on 19 Feb

Selección de tarjetas de eventos de seguridad

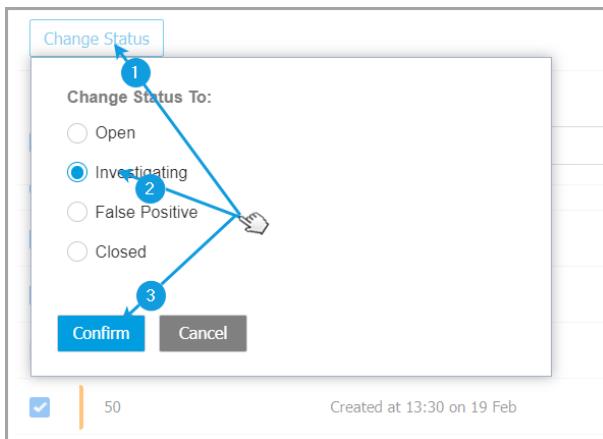
Puede seleccionarlas individualmente o utilizando las opciones de selección en bloque del menú desplegable.



Nota

También puede navegar por varias páginas de eventos de seguridad mientras conserva su selección.

2. Haga clic en el botón **Cambiar estado** y seleccione las opciones que desee:



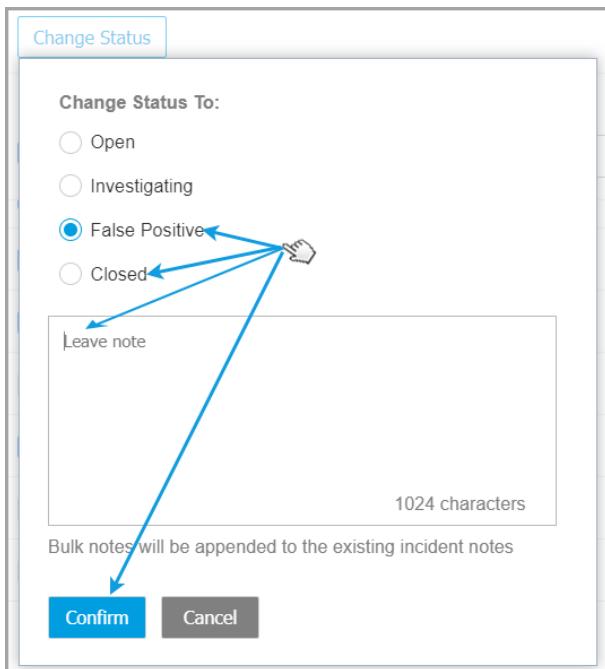
Cambio del estado del evento de seguridad

- **Abierto:** Cuando el evento de seguridad no se está investigando todavía.
- **Investigando-** cuando haya empezado a investigar el evento.
- **Falso positivo:** cuando analizó el evento y lo identificó como un falso positivo.
- **Cerrado-** cuando haya terminado de investigar.



Nota

Al cambiar el estado de los eventos a **Falso positivo** o **Cerrado**, se abrirá un cuadro donde puede dejar una nota sobre los motivos para cambiar el estado del evento, para una consulta posterior.



Dejar una nota para eventos cerrados y falsos positivos



Nota

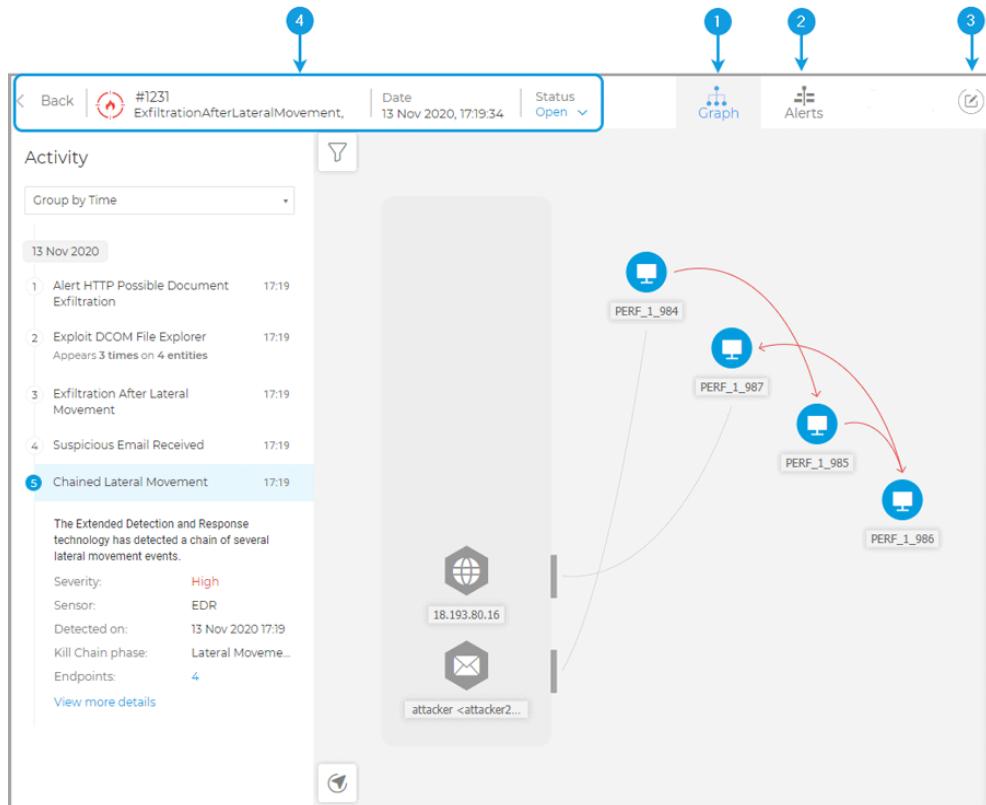
La nota se añadirá a las ya existentes en los incidentes filtrados.

3. Haga clic en **Confirmar** para aplicar la opción de estado seleccionada.

9.1.3. Investigación de incidentes extendidos

En la pestaña **Incidentes extendidos**, identifique el evento de seguridad que deseé analizar y haga clic en el botón **Ver gráfico** para mostrarlo en una nueva página.

Cada incidente extendido tiene una página específica que muestra los eventos correlacionados que se han producido en su entorno, lo que ofrece una perspectiva de toda la red en relación con cada aspecto de un posible ataque por fases.



1. Pestaña Gráfico

El **Gráfico** muestra una representación gráfica animada del incidente extendido que se está investigando y desglosa la secuencia de eventos correlacionados que se han producido en su entorno a lo largo de la línea de tiempo de **Actividad**.

2. Pestaña Alertas

La pestaña **Alertas** muestra la secuencia de alertas que se han desplegado para desencadenar el incidente extendido que está investigando. Muestra la correlación entre los eventos detectados por las tecnologías de GravityZone, como EDR, Network Attack Defense, Detección de anomalías, Antiexploit

avanzado, Interfaz de análisis antimalware de Windows (AMSI) y Análisis del tráfico de red (NTSA).

3. Portapapeles de notas

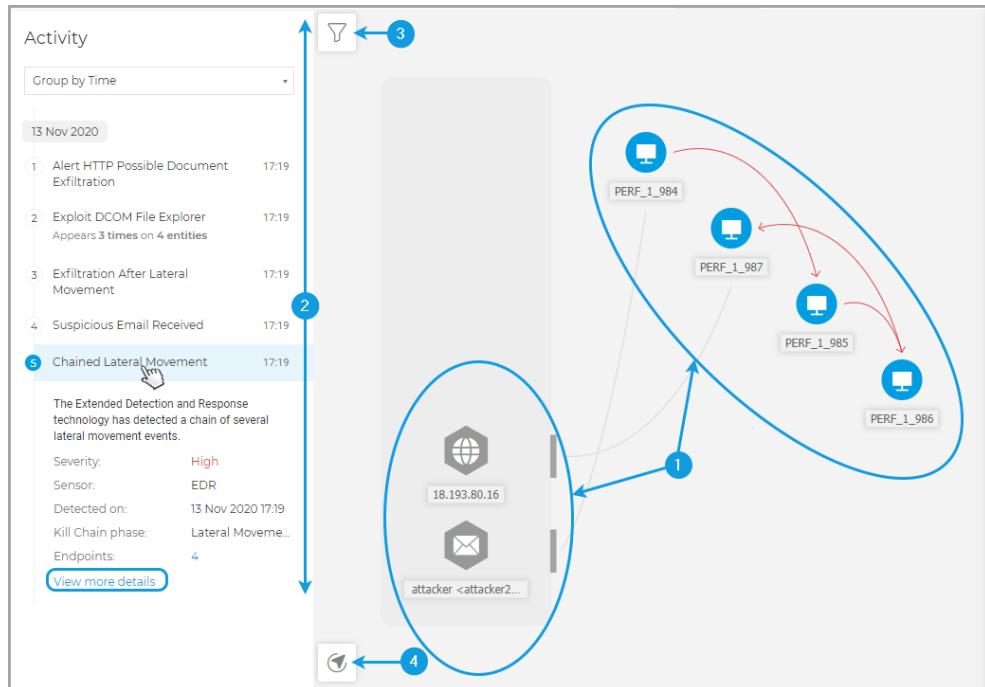
Al hacer clic en el botón **Notas** se abre un portapapeles donde puede añadir notas sobre el incidente actual, que podrá leer cuando vuelva a visitar el incidente más adelante.

4. Barra de estado

La barra de estado ofrece información sobre el ID y nombre del incidente, la fecha y hora en que se generó y el estado actual. Al hacer clic en el botón **Atrás**, volverá a la página principal de **Incidentes**.

Gráfico

El **Gráfico** muestra una representación gráfica animada del incidente extendido que se está investigando y proporciona una línea de tiempo detallada de actividades con la secuencia de eventos correlacionados causados por agentes externos que se han producido en su entorno, en múltiples endpoints y en dispositivos de red.



La pestaña Gráfico

El **Gráfico** incluye las siguientes áreas:

1. Visualización gráfica de incidentes
2. Panel de Actividad
3. Leyenda
4. Navegador

La visualización gráfica de un incidente extendido

Incluye nodos que representan todos los elementos implicados en el ataque, divididos en dos categorías:

- Elementos externos en el lado izquierdo del gráfico.
Tipos disponibles:

- Atacador
 - Correo
 - Dominio/Conexión (IP, Dominio, Controlador de dominio, URL, Dominio del algoritmo de generación de dominio (DGA) y TOR)
 - Almacenamiento en la nube
 - Unidad externa
 - Servidores externos (mando y control)
- Elementos internos de su entorno en el lado derecho del gráfico.
- Tipos disponibles:
- Endpoints (portátiles y equipos de escritorio)
 - Usuarios
 - Dispositivos móviles
 - Servidores (servidor de uso compartido de archivos, controlador de AD, servidor DNS y servidor de correo electrónico)
 - Impresora
 - Router
 - IoT

Comportamiento gráfico

- En el estado de Información general, son visibles todas las conexiones entre los nodos, pero no se resalta ninguna dirección de ataque.
- Para ver la evolución del ataque, acceda al **panel Actividad** y pase por cada fase. Las alertas del panel Actividad deben agruparse por tiempo para reflejar el orden de los eventos.
- Siempre se agruparán tres o más nodos del mismo tipo en grupos de nodos. Al hacer clic en un grupo, se expandirá un panel lateral que muestra todas las entidades disponibles en este grupo.
- A continuación, puede acceder a cada elemento de la lista y se abrirá un panel de información individual para poder profundizar en la investigación. Al cerrar el panel, volverá a la lista de entidades agrupadas.

- Al hacer clic, cada nodo abre su propio panel de información lateral.

 **Nota**

En el caso de los nodos del **Atacante**, no se muestra ningún panel lateral ni información adicional, ya que a menudo se desconoce su identidad.

En la mayoría de los tipos de nodos, el panel lateral incluye las siguientes secciones:

- Alertas: muestra todas las alertas que afectan a este elemento.
- Reparación: muestra acciones y recomendaciones para mitigar los efectos del ataque. Actualmente, la única acción que puede realizar es **Aislar el host**, disponible en los nodos de Endpoint y Servidor.
- Detalles: muestra información específica de cada nodo, como su nombre, tipo de entidad, IP, etc.

El panel de Actividad

Incluye todas las alertas detectadas y correlacionadas en el incidente extendido que está investigando.

Activity

Group by Time ▾

13 Nov 2020

- 1 Alert HTTP Possible Document Exfiltration 17:19
- 2 Exploit DCOM File Explorer 17:19
Appears 3 times on 4 entities
- 3 Exfiltration After Lateral Movement 17:19
- 4 Suspicious Email Received 17:19
- 5 Chained Lateral Movement 17:19

The Extended Detection and Response technology has detected a chain of several lateral movement events.

Severity: **High**

Sensor: EDR

Detected on: 13 Nov 2020 17:19

Kill Chain phase: Lateral Moveme...

Endpoints: 4

[View more details](#)

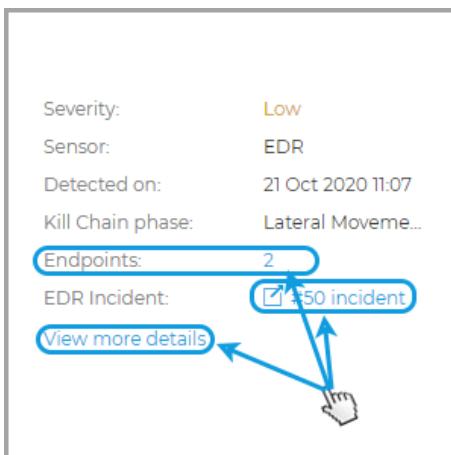
El panel de Actividad

Desde el menú desplegable, puede agrupar las alertas por tiempo o por su posición en la cadena de ataque.

1. Para ver la evolución del ataque, agrupe las alertas por tiempo y pase por cada una.

La animación del gráfico mostrará cómo se ha desplegado el ataque en su entorno, realizando movimientos laterales para saltar de una entidad a otra, filtrando datos, etc.

2. Al hacer clic, se expande cada alerta en la línea de tiempo para mostrar su nombre, una descripción de lo que ha sucedido e información como la gravedad de la alerta, el sensor que realizó la detección, la fecha y hora, la posición en la cadena de ataque, los endpoints afectados y la IP.

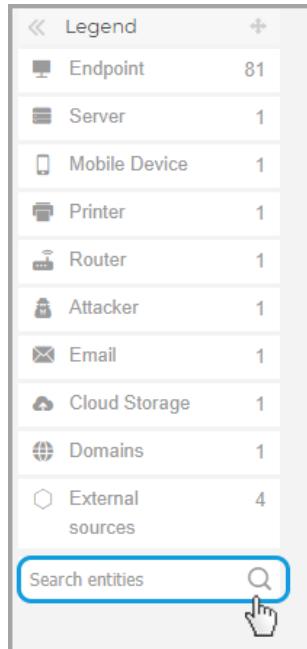


Información de la alerta expandida en la línea de tiempo del incidente

- Si se ha detectado la misma alerta en varios endpoints, puede investigarlos más a fondo expandiendo un panel lateral que muestra una lista de ellos.
- Si la alerta también forma parte de un incidente de endpoint, puede investigarla más detalladamente abriéndola en una nueva pestaña del navegador.
- Si desea ver información adicional sobre esta alerta, haga clic en **Ver más detalles** para expandir su panel de detalles.

Leyenda

La **Leyenda** muestra los tipos de elementos correlacionados en el incidente extendido que está analizando. Puede buscar nombres o extensiones de archivo de componentes de incidentes en el campo de búsqueda y los resultados se mostrarán en el panel lateral.



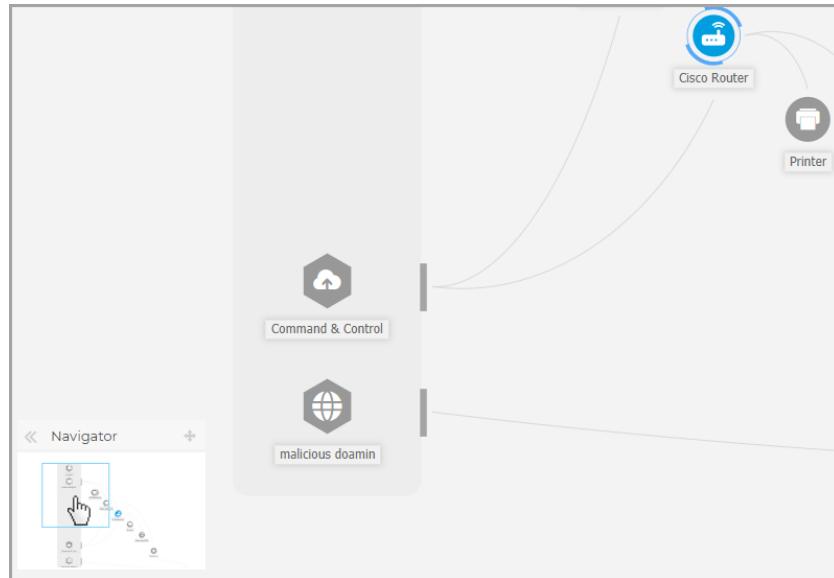
Leyenda

Navegador

Navegación le permite moverse rápidamente por el gráfico de incidentes y explorar todos los elementos mostrados utilizando el minimapa y los diferentes niveles de visualización.

Haga clic y mantenga pulsado el icono  **Arrastrar** para situar el panel de Navegación flotante en cualquier lugar del gráfico de incidentes.

La **Navegación** está contraída por defecto. Al expandirla, el menú mostrará la versión en miniatura de todo el mapa de incidentes y botones de acción para ajustar el nivel de visualización.



Navegador

Alertas

Use la pestaña **Alertas** para ver cómo se desarrolló la secuencia de alertas que desencadenó el incidente extendido que está investigando actualmente. Esta ventana muestra las alertas correlacionadas detectadas por las tecnologías de GravityZone, como EDR, Network Attack Defense, Detección de anomalías,

Antiexploit avanzado, Interfaz de análisis antimalware de Windows (AMSI) y Análisis del tráfico de red (NTSA).

Todas las alertas se describen detalladamente, incluyendo la técnica ATT&CK utilizada, su posición en la cadena de ataque y cómo afecta a su entorno.

The screenshot shows a list of alerts from a SpearPhishing incident. The interface includes a header with the incident ID (#1790), date (13 Nov 2020, 12:10:47), status (Open), and navigation links for Graph and Alerts. A search bar allows filtering by alert name. The main table lists five alerts, each with details like Alert name, Sensor (EDR), Kill Chain phase (Execution or Exfiltration), and Alert description. The alerts are categorized by timestamp (2:10:45) and type (Activities). The descriptions mention various ATT&CK Techniques such as Command-Line Interface, PowerShell, and Automated Exfiltration.

2:10:45 Activities	Alert name	Sensor	Kill Chain phase	Alert description
	Exploit DCOM File Explorer	EDR	Execution	Network Attack Defense has
	ATT&CK Techniques: Execution -Command-Line Interface			
	Exploit DCOM File Explorer	EDR	Execution	Network Attack Defense has
	ATT&CK Techniques: Execution -Command-Line Interface			
	Alert HTTP Possible Document Exfiltration	EDR	Execution	Network Attack Defense has
	ATT&CK Techniques: Execution -Command-Line Interface, PowerShell			
	Exploit DCOM File Explorer	EDR	Execution	Network Attack Defense has
	ATT&CK Techniques: Execution -Command-Line Interface			
	Exfiltration After Lateral Movement	EDR	Exfiltration	The Extended Detection and
	ATT&CK Techniques: Exfiltration -Automated Exfiltration			

Pestaña Alertas

Puede filtrar estas alertas mediante las siguientes opciones:

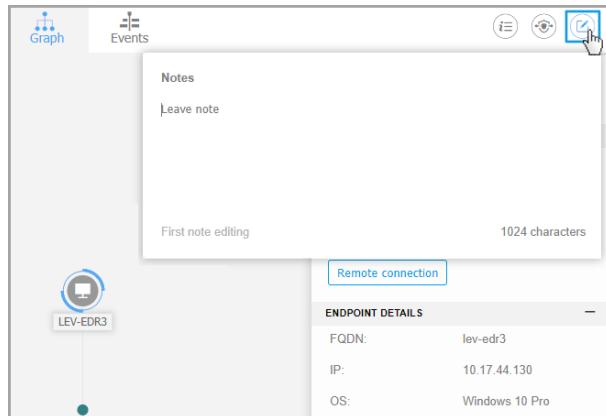
- Utilice el menú desplegable **Todos los sensores** para habilitar las alertas de todos los sensores o solo de uno de ellos.
Opciones disponibles:
 - EDR
 - NTSA
- Utilice el menú desplegable **Todas las fases de la cadena de ataque** para habilitar las alertas que son parte de una determinada fase en la cadena de ataque, desde todas las fases de ella.

Opciones disponibles:

- Acceso inicial
 - Ejecución
 - Persistencia
 - Escalamiento de privilegios
 - Elusión de defensas
 - Acceso a credenciales
 - Detección
 - Movimiento lateral
 - Colección
 - Mando y control
 - Filtración
 - Impacto
- Utilice el campo **Buscar** para localizar alertas por nombre o extensión de archivo.

Notas

La sección **Notas** le permite añadir una nota para realizar un seguimiento de cambios recientes y facilitar el cambio de propiedad de los incidentes.



Portapapeles de notas

1. Para añadir una nota al evento actual, haga clic en el botón **Notas** y se mostrará una nueva ventana.
2. Introduzca su mensaje en esta ventana (de 2048 caracteres como máximo).

Barra de Estado

La barra de estado proporciona etiquetas de eventos de seguridad que pueden ayudarle a detectar información clave sobre el incidente extendido que está analizando.



Barra de Estado

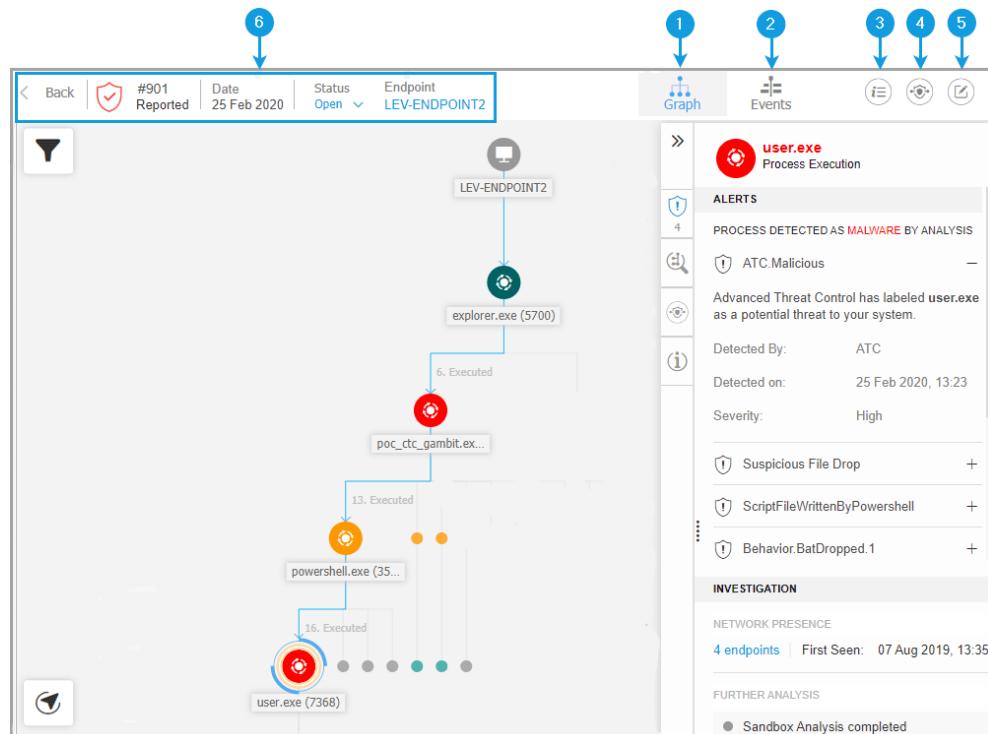
1. ID del incidente: el número de identificación y el nombre del incidente que se está investigando.
2. Momento de la detección: La fecha y hora en que se desencadenó el incidente.
3. Estado del incidente: El estado actual del incidente.

Al hacer clic en el botón **Atrás**, volverá a la página principal de **Incidentes**.

9.1.4. Investigación de incidentes de endpoints

En la página **Incidentes**, identifique el evento de seguridad que deseé analizar y haga clic en el botón  **Ver gráfico** para mostrarlo en una nueva página.

Cada incidente de seguridad tiene una página dedicada que contiene información detallada sobre la secuencia de eventos (se muestran en el gráfico como nodos de eventos de seguridad vinculados) que condujo a desencadenar el incidente y ofrece opciones para adoptar acciones de reparación.



1. Pestaña Gráfico

El gráfico muestra el incidente de seguridad y sus elementos, destacando la ruta crítica del incidente y los detalles del nodo que desencadenó el incidente en el panel **Detalles de nodos**.

2. Pestaña Eventos

La pestaña Eventos muestra eventos y alertas del sistema detectables y filtrables, así como sus descripciones correspondientes.

3. Panel de Información de incidentes

Este panel contiene secciones contraíbles con datos como ID del incidente, estado actual, momento en el que se creó y se actualizó por última vez, número de rastros involucrados, nombre del desencadenador e información del ataque.

4. Panel de Reparación

Este panel incluye secciones contraíbles con medidas adoptadas automáticamente por GravityZone y los pasos recomendados que puede dar para mitigar el incidente.

5. Portapapeles de notas

Al hacer clic en el botón **Notas** se abre un portapapeles donde puede añadir notas sobre el incidente actual, que podrá leer cuando vuelva a visitar el incidente más adelante.

6. Barra de estado del incidente

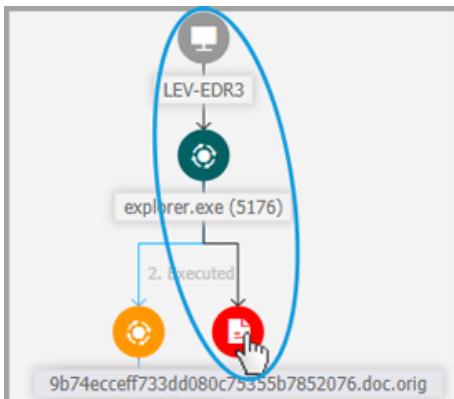
La barra de estado ofrece información sobre el ID del incidente, la fecha y hora en que se generó, el estado, el desencadenante del incidente y el endpoint al que afecta. Al hacer clic en el botón **Atrás**, volverá a la página principal de **Incidentes**.

Nodos de los eventos de seguridad

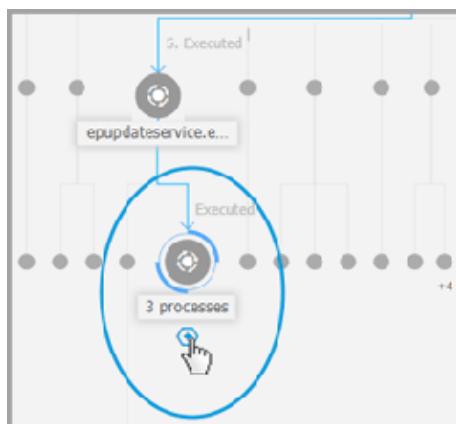
Esto es lo que necesita saber sobre los nodos de los eventos de seguridad:

- Cada nodo representa un elemento concreto involucrado en el incidente investigado.
- Todos los nodos que constituyen la ruta crítica se muestran detalladamente por defecto cuando abre el incidente, mientras que los otros elementos se atenúan, para evitar saturar la vista.

- Al pasar el ratón sobre un nodo que no forma parte de la ruta crítica, se resaltará y mostrará la ruta hasta el punto de origen, sin romper la [ruta crítica](#).



- Cuando tres o más nodos de evento del mismo tipo de acción se generen a partir de un nodo primario, se agrupan en un nodo de clúster expandible.



- Solo se ocultarán en el gráfico de incidentes los nodos sin elementos secundarios cuando se contraiga el nodo del clúster.

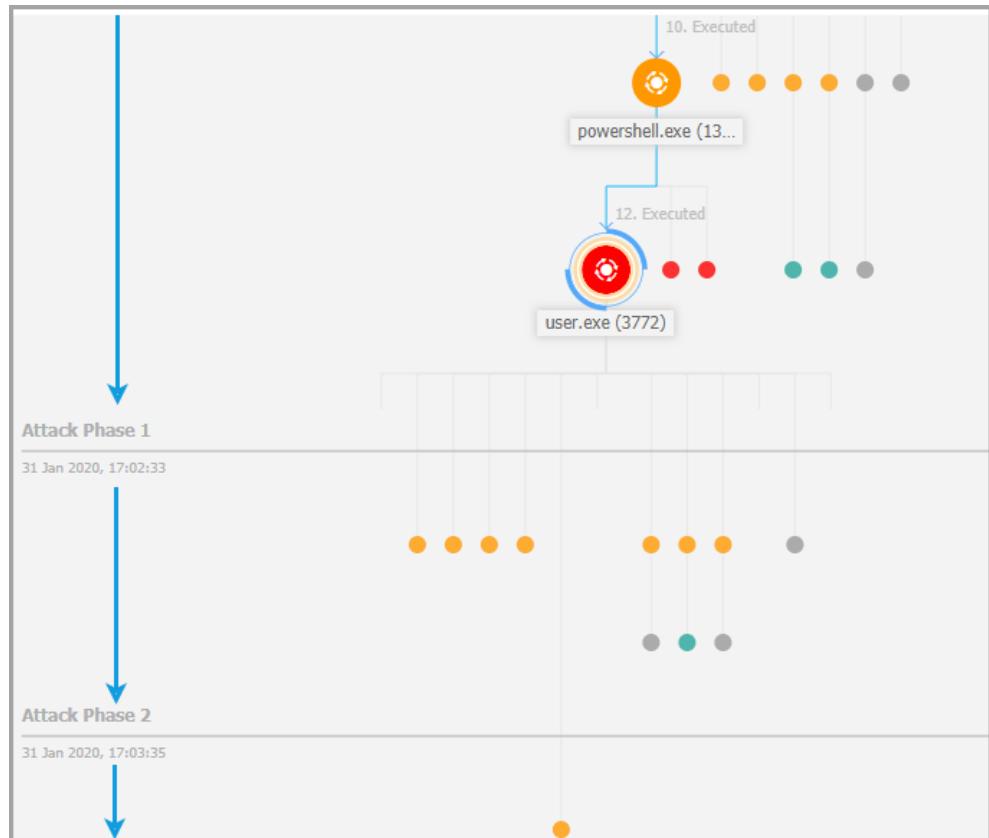
- Los nodos donde se ha detectado actividad sospechosa no se añadirán al nodo del clúster.
- Al hacer clic en un nodo, se mostrará la siguiente información:
 - Se resaltarán en azul la ruta al nodo endpoint junto con los demás elementos involucrados.
 - Un panel lateral, con secciones expandibles que proporcionan información detallada del nodo seleccionado, alerta en caso de que se desencadenen detecciones, con acciones disponibles y recomendaciones. Consulte "[Detalles de nodos](#)" (p. 326) para obtener más información.
- Los nodos están vinculados por líneas con punta de flecha que indican la línea de actuación que se siguió en el endpoint durante el incidente. Cada línea está etiquetada con el nombre de la acción y su número cronológico.

Se pueden representar como nodos los siguientes elementos de un incidente:

Tipo de nodo	Descripción
Endpoint	Muestra la información del endpoint y el estado de administración de parches.
Dominio	Muestra información sobre el host de dominio y sus endpoints.
Proceso	Muestra información sobre la función del proceso en el incidente actual, información de archivo, datos de ejecución de procesos, presencia en la red y opciones para una investigación adicional.
Archivo	Muestra información sobre la función del archivo en el incidente actual, información del archivo, presencia en la red y opciones para una investigación adicional.
Registro	Muestra información del registro y del proceso primario.

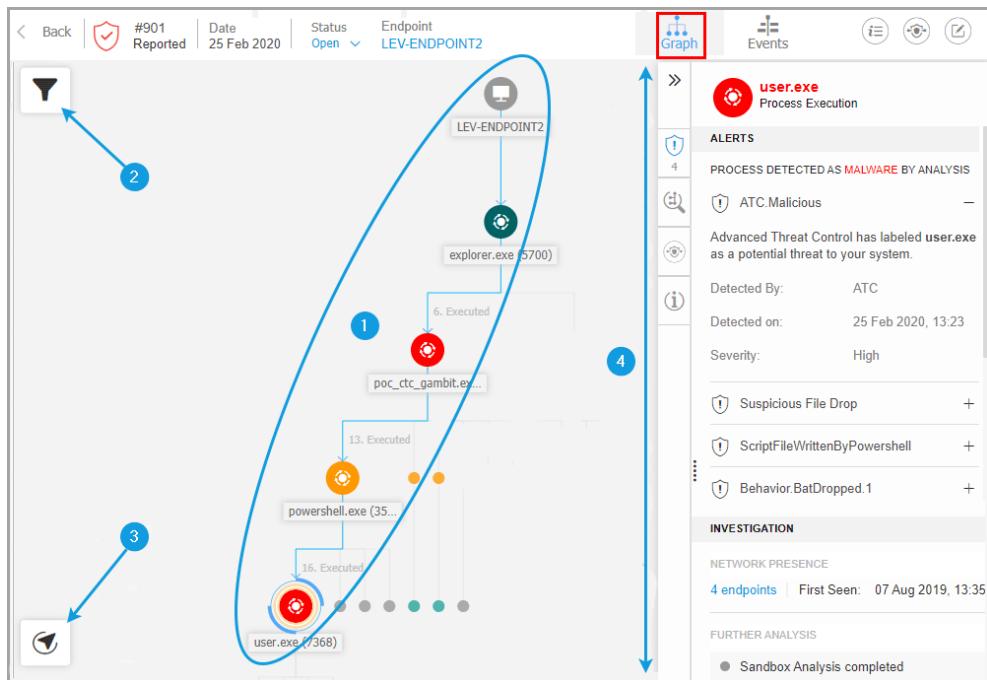
Gráfico

El **gráfico** proporciona una representación gráfica interactiva del incidente investigado y su contexto, en el que se destaca la secuencia de elementos directamente involucrados en su activación, conocida como **ruta crítica** del incidente, así como todos los demás elementos involucrados, que se atenúan por defecto. En caso de incidentes complejos que evolucionan con el tiempo, el gráfico muestra cada una de las etapas del ataque.



Ataque por etapas

El gráfico incluye opciones de filtrado que permiten la personalización del gráfico de incidentes para mejorar la visualización, características para navegar por el mapa de incidentes y paneles de detalles con más información sobre cada elemento.



La pestaña Gráfico

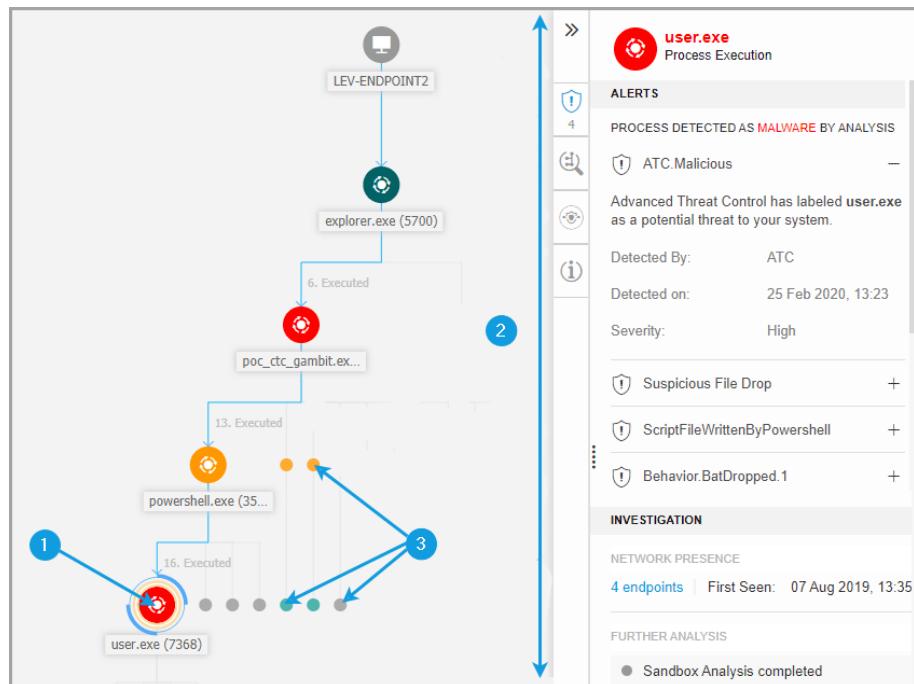
1. Ruta crítica
2. Menú Filtros
3. Menú Navegación
4. Panel de Detalles de nodos

Ruta crítica

La **ruta crítica** es la secuencia de eventos de seguridad vinculados que han conducido a activar una alerta, desde el punto de entrada en la red hasta el nodo del evento que desencadenó el incidente. La ruta crítica del incidente se resalta por defecto en el gráfico, junto con todos sus nodos de eventos que la componen, mientras que los demás elementos aparecen minimizados.

El nodo desencadenante destaca claramente del resto de los elementos en el gráfico, al estar rodeado de características adicionales que lo resaltan (dos círculos

naranjas), y por defecto se muestra un panel de información relacionada junto con el gráfico del incidente, que proporciona información detallada sobre el nodo desencadenante.



Ruta crítica

1. Nodo desencadenante
2. Panel de detalles de nodos con información agrupada por categorías y secciones contraíbles
3. Nodos atenuados indirectamente involucrados en el incidente

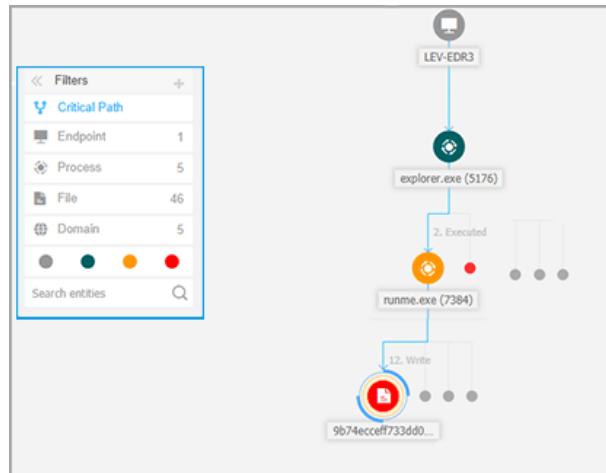
Nota

Al hacer clic en cualquier otro elemento que no sea el nodo desencadenante, se romperá la ruta crítica y se resaltarán la ruta hasta el origen, desde el nodo seleccionado al principio hasta el del endpoint.

Filtros

El menú **Filtros** brinda mejores posibilidades de filtrado, lo que permite la manipulación completa del gráfico del incidente, al resaltar los elementos según su tipo o relevancia, o al ocultarlos para hacer que el incidente sea más compacto y fácil de analizar.

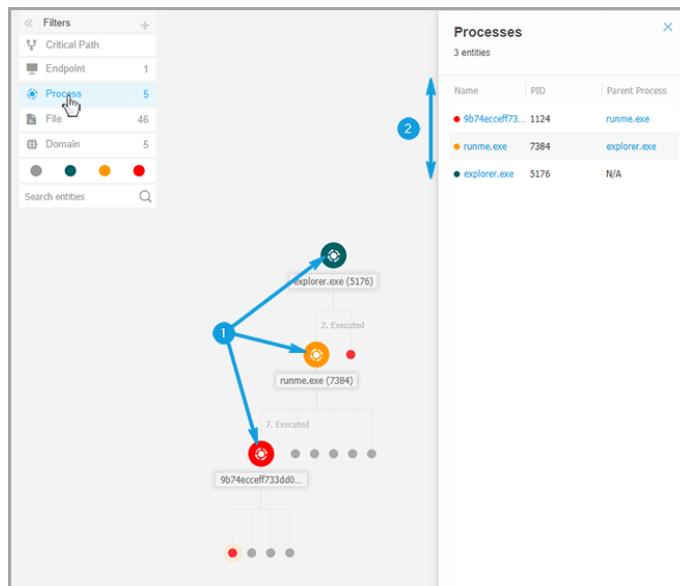
Haga clic y mantenga pulsado el icono  **Arrastrar** para situar el panel de Filtros flotante en cualquier lugar del gráfico de incidentes.



Filtros de gráficos de incidentes

Al seleccionar un filtro de tipo elemento:

1. El gráfico del incidente se aleja y resalta todos los elementos del tipo seleccionado, mientras que los elementos de tipos diferentes se atenúan.
2. Abre instantáneamente un panel con la lista de todos los elementos resaltados.



Nota

Al seleccionar un elemento de la lista que se muestra, se resaltarán en el gráfico del incidente y se abrirá un panel con información relativa a ese elemento.
Solo se puede aplicar simultáneamente un filtro.

Las opciones de filtrado incluyen:

- **Ruta crítica:** Destaca la ruta crítica del incidente de compromiso.
- **Endpoint:** Destaca los endpoints afectados por el incidente.
- **Proceso:** Destaca todos los nodos de tipo proceso involucrados en el incidente.
- **Archivo:** Destaca todos los nodos de tipo archivo involucrados en el incidente.
- **Dominio:** Destaca todos los nodos de tipo dominio involucrados en el incidente.
- **Registro:** Destaca todos los nodos de tipo registro involucrados en el incidente.

- **Relevancia del elemento:** También puede filtrar los elementos según su importancia en el incidente.
 - ⚪ **Nodo neutral:** Elementos sin impacto directo en el incidente de seguridad.
 - ⬤ **Nodo importante:** Elementos con función relevante en el incidente de seguridad.
 - ⬧ **Nodo origen:** Punto de entrada del ataque a la red.
 - ⬨ **Nodo sospechoso:** Elementos con comportamiento sospechoso directamente involucrados en el incidente de seguridad.
 - ⬭ **Nodo malicioso:** Elementos que han causado daños a su red.

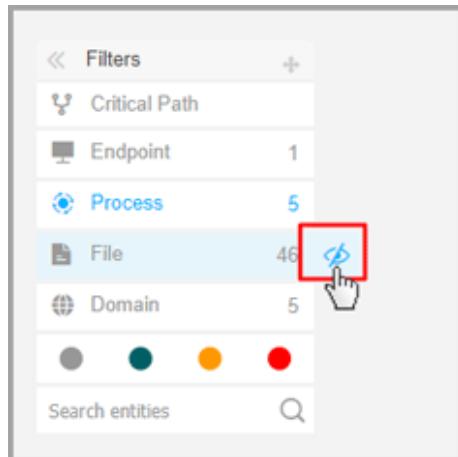
Nota

Al pasar el ratón sobre cualquiera de los filtros de color, se muestra cuántos elementos con la misma relevancia hay involucrados en el incidente.

- **Buscar entidades:** Puede buscar nombres o extensiones de archivo de componentes de incidentes en el campo de búsqueda y los resultados se mostrarán en el panel lateral.

Si no se seleccionan filtros, el gráfico de incidentes se restablece a su estado por defecto, con los endpoints, el origen y los elementos desencadenantes resaltados, mientras que los otros elementos se atenúan.

También puede ocultar ciertos elementos del gráfico de incidentes haciendo clic en el botón **Mostrar/Ocultar** que aparece al poner el ratón sobre los filtros de tipo archivo, dominio y registro.



Al ocultar un tipo de elemento, se vuelve a dibujar el gráfico de incidentes eliminando todos los elementos correspondientes, aunque no estén ampliados, a excepción del nodo desencadenante y los nodos con elementos secundarios.

Navegador

Navegación le permite moverse rápidamente por el gráfico de incidentes y explorar todos los elementos mostrados utilizando el minimapa y los diferentes niveles de visualización.

Haga clic y mantenga pulsado el ícono **Arrastrar** para situar el panel de Navegación flotante en cualquier lugar del gráfico de incidentes.

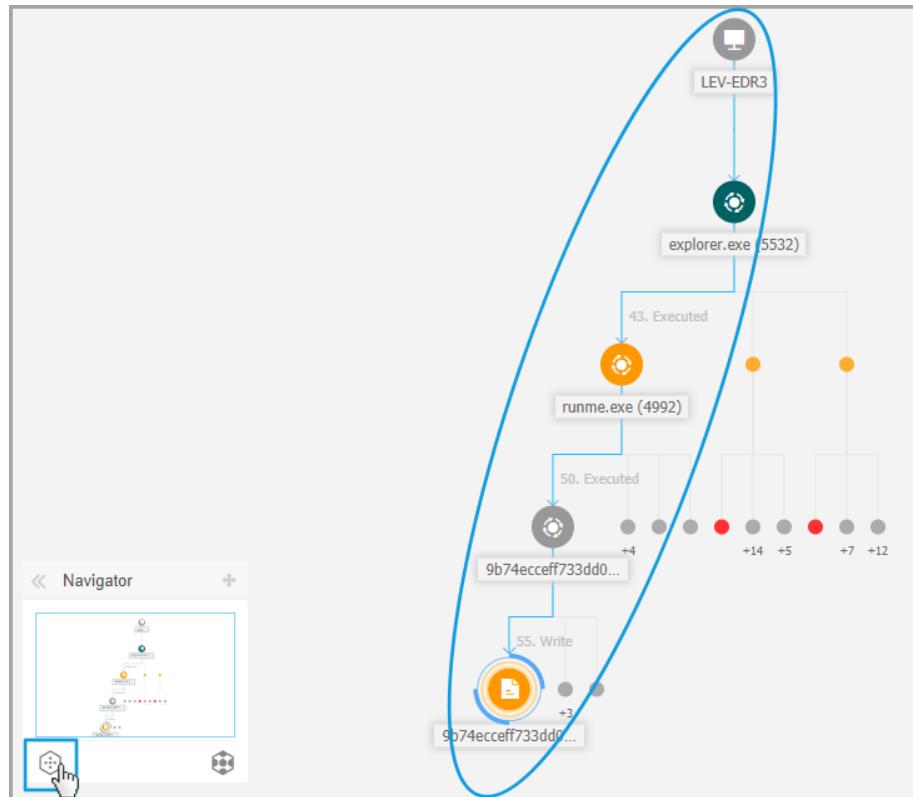
La **Navegación** está contraída por defecto. Al expandirla, el menú mostrará la versión en miniatura de todo el mapa de incidentes y botones de acción para ajustar el nivel de visualización.



Navegador

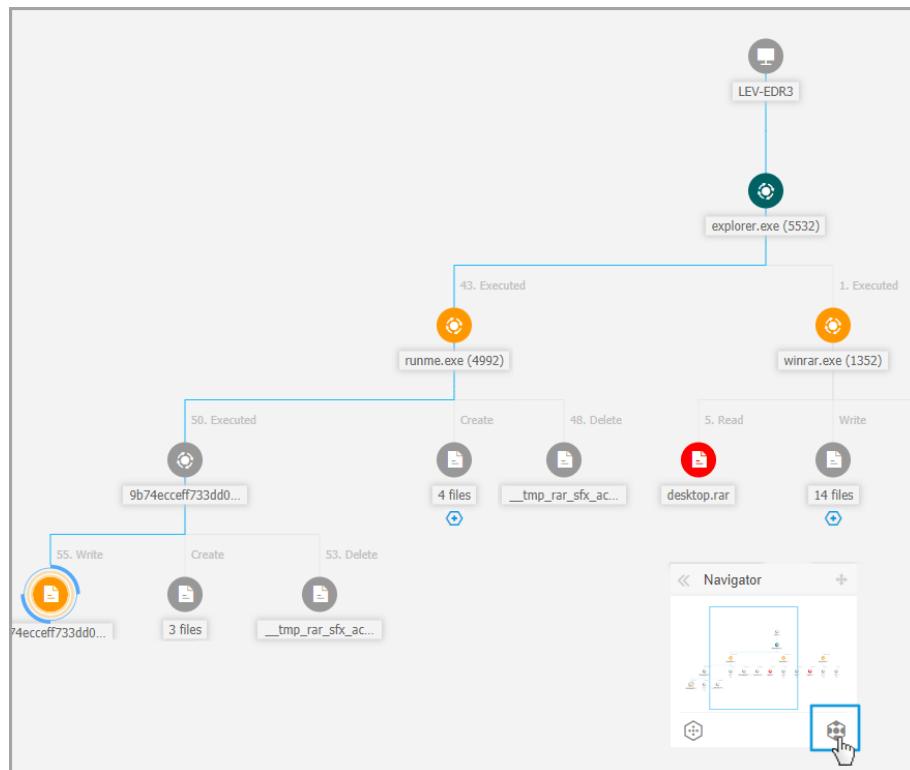
El menú **Navegación** proporciona dos botones de acción para ajustar la visualización del gráfico de incidentes: **Menos detalles** y **Más detalles**.

Al hacer clic en el botón **Menos detalles**, el gráfico se restablece a su estado por defecto, con lo que resalta solo la ruta crítica del incidente.



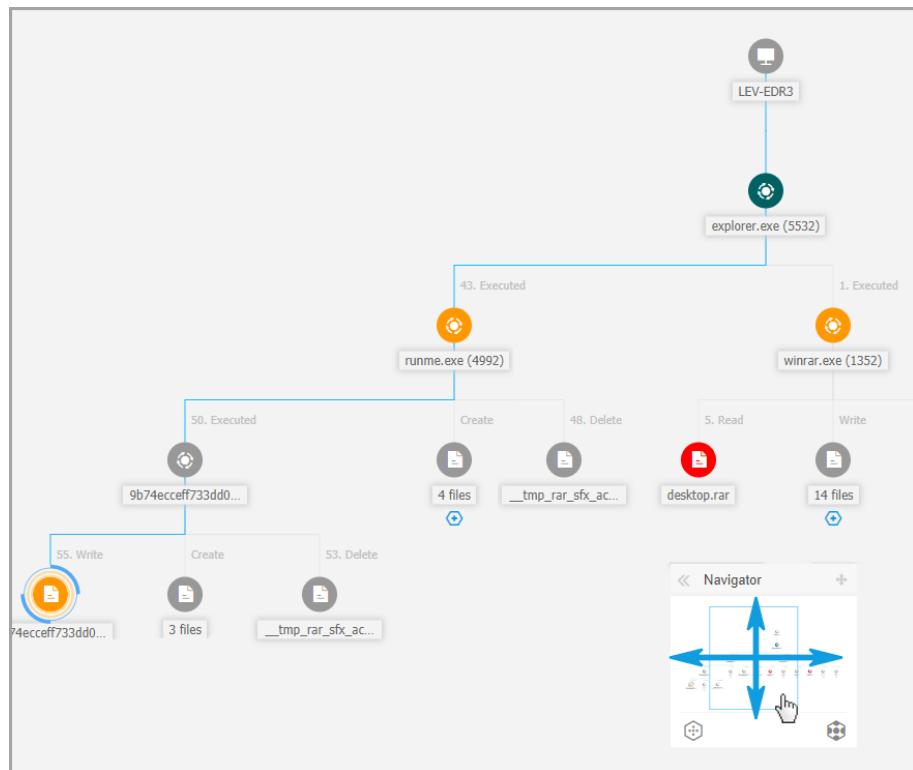
Visualización general

Al hacer clic en el botón **Más detalles**, se expanden todos los elementos del gráfico de incidentes y se resaltan todos los nodo y grupos de nodos.



Visualización ampliada

Cuando se amplía la visualización del incidente y se resaltan todos los elementos, el gráfico a menudo se expande más allá de los límites de la pantalla. En tal caso, mantenga pulsado y arrastre el selector de mapa del minimapa de navegación para deslizarse fácilmente hasta el área deseada del mapa de incidentes o, simplemente, arrastre el área del gráfico en la dirección deseada.

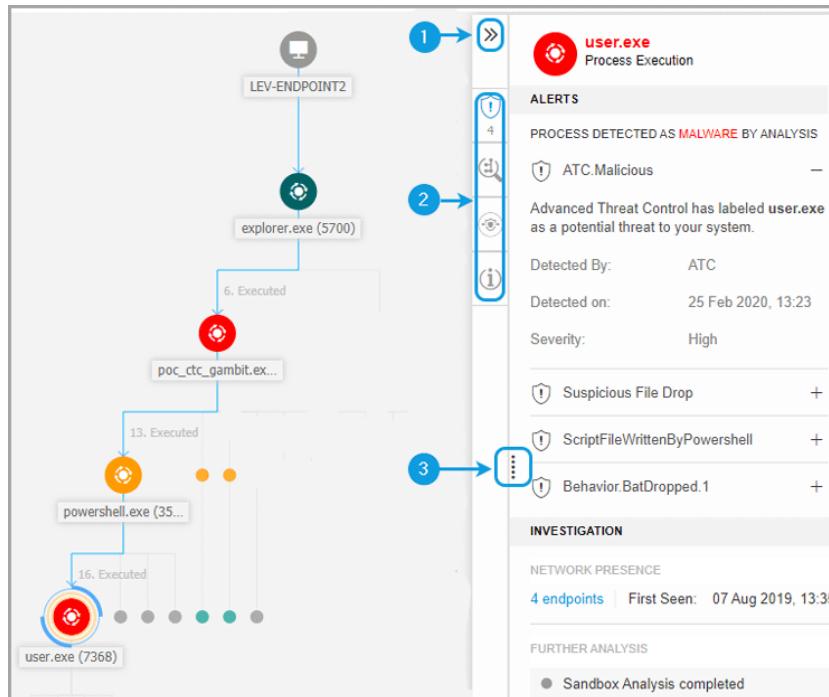


Selector de minimapa

Detalles de nodos

El panel **Detalles de nodos** incluye secciones con información detallada del nodo seleccionado, incluyendo las medidas preventivas o de reparación que puede adoptar para mitigar el incidente, información sobre el tipo de detección y alertas detectadas en el nodo, presencia en la red, información de ejecución del proceso, recomendaciones adicionales para administrar el evento de seguridad o acciones para una investigación adicional del elemento.

Para ver esta información y adoptar acciones dentro del panel, seleccione un nodo dentro del mapa de eventos de seguridad.



Panel de Detalles de nodos

1. Puede contraer o expandir el panel **Detalles de nodos** haciendo clic en el botón **Contraer**.

2. Puede navegar fácilmente por la información que se muestra en el panel **Detalles de nodos** haciendo clic en los iconos de cada una de las cuatro categorías principales:

- **ALERTAS**

Esta sección muestra una o varias detecciones desencadenadas en el nodo seleccionado, incluyendo detalles sobre la tecnología de Bitdefender que incluyó el elemento en el incidente, el motivo que desencadenó la detección, el nombre de la detección y la fecha en que se detectó.

- **INVESTIGACIÓN**

Esta sección muestra el momento de la detección inicial y todos los endpoints donde se detectó este elemento.

- **REPARACIÓN**

Esta sección muestra las acciones realizadas automáticamente por GravityZone y las medidas que puede adoptar de inmediato para mitigar la amenaza, así como recomendaciones detalladas para cada alerta detectada en el nodo seleccionado, con el fin de ayudarle a mitigar el incidente y aumentar el nivel de seguridad de su entorno.

- **INFORMACIÓN**

Esta sección muestra información general sobre cada archivo e información concreta según el tipo de nodo seleccionado.

3. Puede arrastrar el panel **Detalles de nodos** hacia el centro de la pantalla para revisar fácilmente su contenido.

The screenshot shows the Bitdefender GravityZone interface with the 'Node Details' panel expanded. On the left, there's a sidebar with a tree view of nodes, including '648', '8. Executed (6192)', '9. Executed (.exe (33...))', and '10. Executed'. The main area displays detailed information for a selected node:

- Behavior.Ransomware.5**: A warning icon indicates a ransomware threat. The description states: "The transactions.db.ryk file with common ransomware extension has been written, to encrypt user data and perpetually block access to it unless ransom is paid." Details include:
 - Detected By: EDR
 - Detected on: 26 Feb 2020, 15:58
 - Severity: Medium
- Behavior.Ransomware.2**: Another ransomware threat entry.
- Document Read**: A threat entry.

INVESTIGATION section:

- NETWORK PRESENCE: 1 endpoint | First Seen: 26 Feb 2020, 15:58

FURTHER ANALYSIS section:

- Add to Sandbox | VirusTotal | Google

REMEDIATION section:

ACTIONS TAKEN section (partially visible):

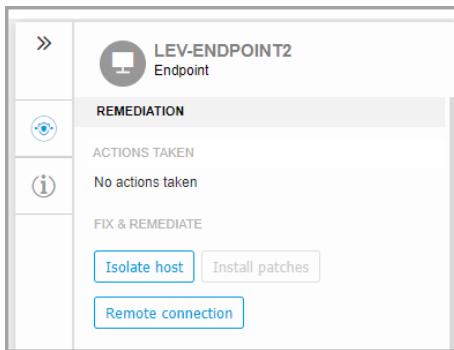
Panel expandido

Panel de detalles para nodos de endpoints

El panel **Detalles de nodos** para endpoints incluye dos categorías:

- **REPARACIÓN**

Muestra información sobre las medidas adoptadas automáticamente por GravityZone para mitigar las amenazas y las acciones que se pueden acometer:



- **Aislamiento de host:** Use esta solución de reparación para aislar el endpoint de la red.
- **Instalar parches:** Use esta acción para instalar un parche de seguridad en el endpoint objetivo. Esta opción es visible solo con el módulo Administración de parches, un complemento disponible con una clave de licencia independiente. Consulte [Instalación de parches](#) para obtener más información.
- **Conexión remota:** Use esta acción para establecer una conexión remota con el endpoint involucrado en el incidente actual y ejecutar una serie de comandos personalizados de shell directamente en su sistema operativo para mitigar la amenaza al instante o recopilar datos para su investigación adicional.

Al hacer clic en este botón, se mostrará la ventana [Conexión remota](#).

- **INFORMACIÓN DEL DISPOSITIVO**

Muestra información general sobre el endpoint afectado, como el nombre del endpoint, la dirección IP, el sistema operativo, el grupo correspondiente, el estado, las políticas activas y un enlace que abre una nueva ventana donde se muestran todos los detalles del endpoint.

The screenshot shows a detailed view of an endpoint named 'LEV-ENDPOINT2'. The interface includes a sidebar with navigation icons (Back, Home, Device Info, Endpoint Details, Patch Management, Reports, Help) and a main content area.

DEVICE INFO

FQDN:	lev-endpoint2
IP:	10.17.44.116
OS:	Windows 10 Pro
Infrastructure:	Computers and Groups
Group:	Custom Groups
State:	Online
Last seen:	Online
Active Policy:	forSandbox

[View full endpoint details](#)

PATCH INFORMATION

ⓘ Patch Management license not available

Last Checked:	Never
Patch status:	Unknown C

[View endpoint patch status report](#)

También proporciona información como la cantidad de parches instalados, los parches fallidos o cualquier parche que falte, ya sea de seguridad o no. Además, puede generar un informe de estado de parches en el endpoint. Esta sección se suministra bajo demanda para el endpoint escogido.

Puede llevar a cabo las siguientes acciones dentro del panel:

- Ver información de parches para el endpoint objetivo. Para ver la información de parches, haga clic en **Actualizar** dentro de la sección.
- Ver informe de estado de parches para el endpoint seleccionado. Para generar este informe, haga clic en **Ver informe de estado de parches del endpoint**.

Panel de detalles para nodos de procesos

El panel **Detalles de nodos** para nodos de procesos incluye dos categorías:

- **ALERTAS**

Muestra una o varias detecciones desencadenadas en el nodo seleccionado, incluyendo detalles sobre la tecnología de Bitdefender que incluyó esta entidad en el incidente, el motivo que desencadenó la detección, el nombre de la detección y la fecha en que se detectó. La descripción de cada alerta sigue los últimos estándares de MITRE.

»

acro32.exe
Process Execution

ALERTS

PROCESS DETECTED AS MALWARE BY ANALYSIS

! Gen:Illusion.Slingshot.PowerShell.10.2010 —
100

HyperDetect has detected unwanted activity in your system, caused by this file.

Detected By: Hyper detect

Detection Level: Normal

Detected on: 26 Feb 2020, 15:58

Severity: High

! Behavior.Ransomware.5 +

! Behavior.Ransomware.2 +

! Document Read +

- **INVESTIGACIÓN**

Muestra el momento de la detección inicial y todos los endpoints donde se detectó este elemento.

The screenshot shows a process execution investigation for 'acro32.exe'. The main panel displays the file name and its status as 'Process Execution'. Below this is the 'INVESTIGATION' section, which includes 'NETWORK PRESENCE' information showing 1 endpoint and the first seen date as 26 Feb 2020, 15:58. At the bottom of the main panel are links for 'Add to Sandbox', 'VirusTotal', and 'Google'. To the left of the main panel is a sidebar with several icons: a double arrow (top), a shield with a checkmark (second), a magnifying glass (third), and an info circle (fourth).

Para ver esta lista, haga clic en el número que se muestra en el campo de **endpoints** y aparecerá una nueva ventana.

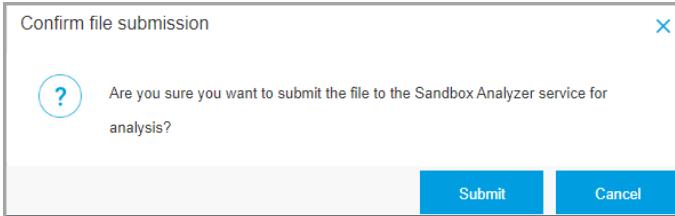
The screenshot shows a search results window titled 'Endpoints'. It displays a single result for a file named '9b74ecceff733dd080c75355b7852076.doc.orig' found on the endpoint 'LEV-EDR3'. The result includes the file name, path ('c:\users\admin\desktop\9b74ec...'), and the first seen date ('28 August 2019, 13:31:38'). Below the table are navigation controls for pages (First Page, Previous Page, Next Page, Last Page) and items (1 item). A blue 'OK' button is located at the bottom right of the window.

Esta sección también proporciona un análisis externo a través de los componentes internos y las soluciones de terceros.

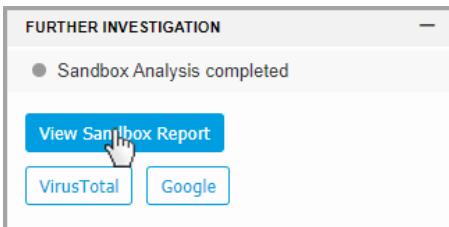
Dispone de las siguientes opciones:

- **Añadir a Sandbox:** Use esta acción para generar un informe de Sandbox Analyzer.

Al elegir **Añadir a Sandbox** se muestra una pantalla para confirmar el envío del archivo.



Tras la confirmación, será dirigido automáticamente a la pantalla de envío. Cuando finalice el análisis, haga clic en el botón **Ver informe de Sandbox** para abrir el informe completo.



- **VirusTotal:** Use esta acción para enviar un archivo al exterior para su análisis.
- **Google:** Use esta acción para buscar el valor hash de un archivo.
- **REPARACIÓN**
Muestra información sobre las medidas adoptadas automáticamente por GravityZone para mitigar las amenazas y las acciones que se pueden acometer:

The screenshot shows the Bitdefender GravityZone interface for investigating an incident. On the left, there's a sidebar with icons for shield (4), magnifying glass, eye, and information. The main panel displays the following details:

- Process:** acro32.exe (red shield icon)
- Category:** Process Execution
- REMEDIATION:** No actions taken.
- ACTIONS TAKEN:** Kill or Quarantine file.
- FIX & REMEDIATE:** Add file to Blocklist or Add file as exception.
- PREVENT:** Add file to Blocklist or Add file as exception.
- RECOMMENDED STEPS:** We recommend you take the following steps to mitigate this incident:
 1. Make sure all the endpoints in your network are protected and update the security solution on all of them
 2. Perform a network-wide full-system scan.
 3. Check whether all operating systems in the network are up-to-date with the latest security[Show more](#)
- Behavior:** Ransomware.5

- **Detener:** Use esta acción para detener la ejecución de un proceso. Esta acción crea una tarea de detención o terminación de proceso visible en la barra de ejecución de procesos. Los procesos System32 y de Bitdefender quedan excluidos de esta acción.
- **Poner archivo en cuarentena:** Use esta acción para almacenar el elemento en cuestión y evitar que ejecute su carga útil. Esta acción requiere la instalación del módulo de Cortafuego en el endpoint objetivo.
- **Añadir archivo a la lista de bloqueo:** Administre los elementos bloqueados en la sección [Lista de bloqueo](#).
- **Añadir archivo como excepción:** Use esta opción para excluir una actividad legítima de una política específica. Cuando escoge esta acción, una ventana de configuración le solicita que seleccione la política en la que quiere añadir la excepción. Administre la exclusión en la página [Políticas > Antimalware > Ajustes](#).

- **Añadir como exclusión EDR:** Use esta opción para crear una regla personalizada que ya no tratará el proceso como una detección de EDR sospechosa o maliciosa.
 1. Cuando pulsa el botón **Añadir como exclusión EDR**, aparece una nueva ventana que le solicita que confirme la acción o la cancele.
 2. Tras confirmar la acción, GravityZone le notifica que la nueva regla está disponible en la cuadrícula de [Reglas de exclusión](#). Observe que los nombres de todas las reglas creadas desde el gráfico de incidentes comienzan con el número de incidente.



Nota

Cuando acceda a los detalles de la regla para editarla, notará que todos los criterios para esta regla se llenaron automáticamente y se añadió un criterio de solo lectura con el nombre de la alerta.



Importante

Añadir como exclusión EDR solo está disponible para:

- Alertas activadas por la tecnología EDR
- Nodos generados por otro proceso
- Nodos sospechosos y maliciosos

Si el proceso excluido forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión dejarán de generarse en la cuadrícula de incidentes. Los eventos consistentes seguirán estando disponibles para su visualización y análisis en la página [Búsqueda](#).

Si el proceso excluido no forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión seguirán generándose en la cuadrícula de incidentes, pero ya no considerarán este proceso como sospechoso o malicioso.

Esta sección también proporciona recomendaciones detalladas para cada alerta detectada en el nodo seleccionado con el fin de ayudarle a mitigar el incidente y aumentar el nivel de seguridad de su entorno.

● INFORMACIÓN DEL PROCESO

Muestra detalles sobre el nodo de proceso seleccionado, incluyendo el nombre del proceso, la línea de comandos ejecutada, el usuario, el tiempo de ejecución, el origen y la ruta del archivo, el valor hash o la firma digital.

The screenshot shows a process details window for 'acro32.exe' (ID: 7668). The left sidebar has icons for Home, Alerts (4), Threats, and Details (selected). The main area is divided into sections: PROCESS INFO, PROCESS EXECUTION DETAILS, FILE INFO, and a bottom section with three dots. PROCESS EXECUTION DETAILS includes fields for Process Name, Command Line, User, and Execution Time. FILE INFO includes Hash, Digitally Signed, Size, and Path.

PROCESS INFO	
Process Name:	acro32.exe (ID:7668)
Command Line:	N/A
User:	WIN10X64-PC\Jack
Execution Time:	26 Feb 2020, 15:58

FILE INFO	
Hash:	SHA256 MD5
Digitally Signed:	No
Size:	105.5 KB
Path:	c:\users\jack\appdata...

Puede copiar el valor hash en el portapapeles haciendo clic en los algoritmos de hash disponibles en el campo **Hash** y, a continuación, en **Copiar en el portapapeles**, y usarlo para añadir un valor hash del archivo a la **Lista de bloqueo**. Para obtener más información, consulte **Incluir archivos en lista de bloqueo**.

Panel de detalles para nodos de archivos

El panel **Detalles de nodos** para nodos de archivos incluye dos categorías:

- **ALERTAS**

Muestra una o varias detecciones desencadenadas en el nodo seleccionado, incluyendo detalles sobre la tecnología de Bitdefender que incluyó esta entidad en el incidente, el motivo que desencadenó la detección, el nombre de la detección y la fecha en que se detectó. La descripción de cada alerta sigue los últimos estándares de MITRE.

The screenshot shows a file analysis interface. On the left is a vertical toolbar with icons for navigation, alerts, network presence, further analysis, and help. The main area displays the following information:

- cv.docm** File
- ALERTS**
 - FILE DETECTED AS **MALWARE** BY ANALYSIS
 - Proton.VB.Vexillum.1.419.3000001
 - HyperDetect has detected unwanted activity in your system, caused by this file.
- Detected By:** Hyper detect
- Detection Level:** Aggressive
- Detected on:** 26 Feb 2020, 15:58
- Severity:** High

• INVESTIGACIÓN

Muestra el momento de la detección inicial y todos los endpoints donde se detectó este elemento.

The screenshot shows the investigation details for the same file. The vertical toolbar on the left is identical to the previous screenshot. The main area displays:

- cv.docm** File
- INVESTIGATION**
 - NETWORK PRESENCE
 - 1 endpoints | First Seen: 26 Feb 2020, 15:58
- FURTHER ANALYSIS**
 - Add to Sandbox | VirusTotal | Google

Para ver esta lista, haga clic en el número que se muestra en el campo de **endpoints** y aparecerá una nueva ventana.

The screenshot shows a search results page for a specific file. At the top, there's a search bar with the file name '9b74ecceff733dd080c75355b7852076.doc.orig'. Below the search bar, there are four filter fields: 'Endpoint' (with a search icon), 'File Name' (with a search icon), 'Path' (with a search icon), and 'First Seen' (with a dropdown menu). The main table displays one item: 'LEV-EDR3' with file name '9b74ecceff733dd080c75355b78...' and path 'c:\users\admin\desktop\9b74ec...'. The 'First Seen' column shows '28 August 2019, 13:31:38'. Below the table, there are navigation buttons: 'First Page', '← Page 1 of 1 → Last Page', '20', and a dropdown menu. On the right side of the table, there's a '1 items' indicator and a large blue 'OK' button.

Esta sección también proporciona un análisis externo a través de los componentes internos y las soluciones de terceros.

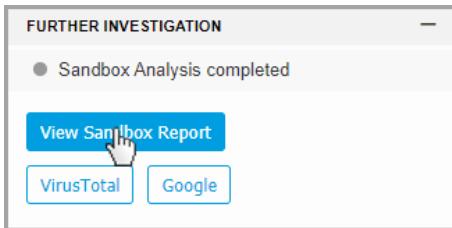
Dispone de las siguientes opciones:

- **Añadir a Sandbox:** Use esta acción para generar un informe de Sandbox Analyzer.

Al elegir **Añadir a Sandbox** se muestra una pantalla para confirmar el envío del archivo.

The confirmation dialog box has a title 'Confirm file submission' and a close button 'X'. It contains a question: 'Are you sure you want to submit the file to the Sandbox Analyzer service for analysis?' with a blue circular icon containing a question mark. At the bottom, there are two buttons: 'Submit' (blue) and 'Cancel' (white).

Tras la confirmación, será dirigido automáticamente a la pantalla de envío. Cuando finalice el análisis, haga clic en el botón **Ver informe de Sandbox** para abrir el informe completo.



- **VirusTotal:** Use esta acción para enviar un archivo al exterior para su análisis.
- **Google:** Use esta acción para buscar el valor hash de un archivo.

- **REPARACIÓN**

Muestra información sobre las medidas adoptadas automáticamente por GravityZone para mitigar las amenazas y las acciones que se pueden acometer:

The screenshot shows a file remediation interface for a document named 'cv.docm'. On the left, there's a sidebar with icons for navigation, protection level (1), search, and prevent. The main area displays the file name 'cv.docm' with a red 'File' status indicator. Below it, under 'REMEDIALION', is a shield icon with the number '1'. Under 'ACTIONS TAKEN', it says 'No actions taken'. Under 'FIX & REMEDIATE', there's a button labeled 'Quarantine file' which is highlighted with a blue border. Under 'PREVENT', there are two buttons: 'Add file to Blocklist' and 'Add file as exception'. A section titled 'RECOMMENDED STEPS' contains a list of three steps to mitigate the incident, followed by a 'Show more' link.

- **Poner archivo en cuarentena:** Use esta acción para almacenar el elemento en cuestión y evitar que ejecute su carga útil. Esta acción requiere la instalación del módulo de Cortafuego en el endpoint objetivo.
- **Añadir archivo a la lista de bloqueo:** Administre los elementos bloqueados en la sección [Lista de bloqueo](#).
- **Añadir archivo como excepción:** Use esta opción para excluir una actividad legítima de una política específica. Cuando escoge esta acción, una ventana de configuración le solicita que seleccione la política en la que quiere añadir la excepción. Administre la exclusión en la página **Políticas > Antimalware > Ajustes**.
- **Añadir como exclusión EDR:** Use esta opción para crear una regla personalizada que ya no tratará el archivo como una detección de EDR sospechosa o maliciosa.
 1. Cuando pulsa el botón **Añadir como exclusión EDR**, aparece una nueva ventana que le solicita que confirme la acción o la cancele.

- Tras confirmar la acción, GravityZone le notifica que la nueva regla está disponible en la cuadrícula de [Reglas de exclusión](#). Observe que los nombres de todas las reglas creadas desde el gráfico de incidentes comienzan con el número de incidente.



Nota

Cuando acceda a los detalles de la regla para editarla, notará que todos los criterios para esta regla se llenaron automáticamente y se añadió un criterio de solo lectura con el nombre de la alerta.



Importante

Añadir como exclusión EDR solo está disponible para:

- Alertas activadas por la tecnología EDR
- Nodos generados por otro proceso
- Nodos sospechosos y maliciosos

Si el archivo excluido forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión dejarán de generarse en la cuadrícula de incidentes. Los eventos consistentes seguirán estando disponibles para su visualización y análisis en la página [Búsqueda](#).

Si el archivo excluido no forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión seguirán generándose en la cuadrícula de incidentes, pero ya no considerarán este proceso como sospechoso o malicioso.

Esta sección también proporciona recomendaciones detalladas para cada alerta detectada en el nodo seleccionado con el fin de ayudarle a mitigar el incidente y aumentar el nivel de seguridad de su entorno.

• INFORMACIÓN DEL ARCHIVO

Muestra detalles sobre el nodo de archivo seleccionado, incluyendo el origen y la ruta del archivo, el valor hash o la firma digital.

The screenshot shows a file analysis interface. On the left is a vertical toolbar with icons for navigation, file type, file info, alerts, investigation, and help. The main panel displays the file name "cv.docm" with a "File" icon. Below it is a "FILE INFO" section containing the following data:

Hash:	SHA256 MD5
Digitally Signed:	No
Size:	32.9 KB
Path:	c:\users\jack\appdata...

Puede copiar el valor hash en el portapapeles haciendo clic en los algoritmos de hash disponibles en el campo **Hash** y, a continuación, en **Copiar en el portapapeles**, y usarlo para añadir un valor hash del archivo a la **Lista de bloqueo**. Para obtener más información, consulte [Incluir archivos en lista de bloqueo](#).

Panel de detalles para nodos de dominios

El panel **Detalles de nodos** para nodos de dominios incluye dos categorías:

- **ALERTAS**

Muestra la gravedad del dominio marcado por la tecnología de Bitdefender que incluyó a esta entidad en el incidente, el motivo que desencadenó la detección y la fecha en que se detectó.

The screenshot shows a node details interface. On the left is a vertical toolbar with icons for navigation, file type, file info, alerts, investigation, and help. The main panel displays the host name "amtso.security-features-check.c..." with a "Requested Host" icon. Below it is an "ALERTS" section containing the following data:

DOMAIN MARKED AS INVOLVED	
Detected By:	Security analytics
Reason:	Resource download
Detected on:	14 Feb 2020, 14:33

- **INVESTIGACIÓN**

Muestra el momento de la detección inicial y todos los endpoints donde se detectó este elemento.

The screenshot shows a window titled 'amtso.security-features-check.c...' under the 'Requested Host' section. On the left, there's a sidebar with icons for 'INVESTIGATION' (selected), 'NETWORK ACTIVITY', and a magnifying glass icon for '6 endpoints'. Below the main title, it says 'Requested Host' and 'First Seen: 28 Aug 2019, 16:30'.

Para ver esta lista, haga clic en el número que se muestra en el campo de **endpoints** y aparecerá una nueva ventana.

This screenshot shows a modal window titled 'Endpoints' with one item listed. The item details are: File Name: 9b74ecceff733dd080c75355b7852076.doc.orig, Endpoint: LEV-EDR3, File Name: 9b74ecceff733dd080c75355b78..., Path: c:\users\admin\desktop\9b74ec..., First Seen: 28 August 2019, 13:31:38. At the bottom, there are buttons for 'First Page', 'Page 1 of 1', 'Last Page', '20', 'OK', and '1 items'.

● REPARACIÓN

Muestra información sobre las medidas adoptadas automáticamente por GravityZone para mitigar las amenazas y las acciones que se pueden acometer:

The screenshot shows a remediation screen for a host named 'amtso.security-features-check.c...'. The interface includes a sidebar with icons for 'REMEDIALION' (shield), 'ACTIONS TAKEN' (magnifying glass), 'PREVENT' (eye), and 'Add URL as exception' (information). The main area displays the host name and its status as a 'Requested Host'.

- **Añadir URL como excepción:** Use esta opción para excluir una actividad legítima de una política específica. Cuando escoge esta acción, una ventana de configuración le solicita que seleccione la política en la que quiere añadir la excepción. Administre la exclusión en la página **Políticas > Antimalware > Ajustes**.
- **Añadir como exclusión EDR:** Use esta opción para crear una regla personalizada que ya no tratará el dominio como una detección de EDR sospechosa o maliciosa.
 1. Cuando pulsa el botón **Añadir como exclusión EDR**, aparece una nueva ventana que le solicita que confirme la acción o la cancele.
 2. Tras confirmar la acción, GravityZone le notifica que la nueva regla está disponible en la cuadrícula de **Reglas de exclusión**. Observe que los nombres de todas las reglas creadas desde el gráfico de incidentes comienzan con el número de incidente.

Nota

Cuando acceda a los detalles de la regla para editarla, notará que todos los criterios para esta regla se llenaron automáticamente y se añadió un criterio de solo lectura con el nombre de la alerta.

Importante

Añadir como exclusión EDR solo está disponible para:

- Alertas activadas por la tecnología EDR
- Nodos generados por otro proceso
- Nodos sospechosos y maliciosos

Si el dominio excluido forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión dejarán de generarse en la cuadrícula de incidentes. Los eventos consistentes seguirán estando disponibles para su visualización y análisis en la página [Búsqueda](#).

Si el dominio excluido no forma parte de la ruta crítica del incidente, los incidentes futuros que coincidan con este criterio de exclusión seguirán generándose en la cuadrícula de incidentes, pero ya no considerarán este proceso como sospechoso o malicioso.

- **INFORMACIÓN DEL DOMINIO**

Muestra detalles sobre el nodo de dominio seleccionado, incluyendo la URL solicitada, el puerto utilizado, el método de solicitud, el tipo de secuencia, el nombre del archivo extraído y la aplicación de origen.

amtso.security-features-check.c...
Requested Host

DOMAIN INFO

COMMUNICATION DETAILS

Requested URL:	http://amtso.security-features-check.c...
Remote Port:	80
Request Method:	GET
Stream Type:	application/x-msdos-program
Extracted File Name:	N/A
Source Application:	c:\users\admin\desktop\amtso...

Panel de detalles para nodos de registro

El panel **Detalles de nodos** para nodos de registro incluye dos categorías:

- **ALERTAS**

Muestra la gravedad del registro marcado por la tecnología de Bitdefender que incluyó a esta entidad en el incidente, el motivo que desencadenó la detección, la fecha en que se detectó y el tipo de registro.

»	 POC-To-Delete Registry
 0	ALERTS
	REGISTRY DETECTED AS IMPORTANT BY ANALYSIS
 0	Detected By: Security analytics
 0	Reason: Registry write
	Detected on: 14 Feb 2020, 14:33
	Registry Type: Startup or Autorun

- **REPARACIÓN**

Muestra información sobre las medidas adoptadas automáticamente por GravityZone.

»	 POC-To-Delete Registry
 0	REMEDIATION
 0	ACTIONS TAKEN
	No actions taken

La sección **REPARACIÓN** para los nodos de registro no proporciona ninguna opción de acción del usuario.

- **INFORMACIÓN DEL REGISTRO**

Muestra detalles sobre el nodo de registro seleccionado, incluyendo la clave del registro, el valor y los datos.

The screenshot shows a software interface for investigating incidents. On the left is a vertical toolbar with icons for back (double arrow), shield (protect), and information (i). The main area has a title bar 'POC-To-Delete Registry'. Below it is a 'REGISTRY INFO' section with three entries: 'Registry Key: hku\software\micros...', 'Registry Value: POC-To-Delete', and 'Registry Data: C:\Users\admin\Desktop...'. The background features a futuristic, glowing blue and white design.

Puede hacer clic en la clave y valor del registro para copiarlos en el portapapeles con el fin de analizarlos posteriormente.

Eventos

Use la pestaña **Eventos** para ver cómo se desarrolló la secuencia de eventos que desencadenó el incidente investigado actualmente. Esta ventana muestra, correlacionados, los eventos y alertas del sistema detectados por tecnologías de GravityZone como EDR, Network Attack Defense, Detección de anomalías, Antiexploit avanzado y la interfaz de análisis antimalware de Windows (AMSI, por sus siglas en inglés).

Cada evento complejo tiene una descripción detallada que explica qué se detectó y qué podría suceder si el rastro se utilizase con fines maliciosos, de acuerdo con las últimas técnicas y tácticas de MITRE.

The screenshot shows the Bitdefender GravityZone interface with the 'Events' tab selected. The top navigation bar includes 'Back', a status indicator (#549 Blocked), date (16 Oct 2019), status dropdown (Open), incident trigger (9b74ecceff733dd0...), endpoint (LEV-EDR3), and a 'Graph' button. Below the navigation is a filter bar with 'All', 'Alerts', and 'System events' (highlighted with a blue box and arrow 1). The main area displays a list of system events:

Date	Event name	Event description
16 Oct 2019, 08:43:17 LEV-EDR3 10.17.44.130	Process Create	A process has been created.
16 Oct 2019, 08:43:17 LEV-EDR3 10.17.44.130	ScreenCaptureModuleLoaded	A process has dynamically loaded dwmapi.dll module capable of screen capturing. ATT&CK Techniques: Collection -Screen Capture
16 Oct 2019, 08:43:17 LEV-EDR3 10.17.44.130	File Rename	A file has been renamed.
16 Oct 2019, 08:43:17 LEV-EDR3 10.17.44.130	File Rename	A file has been renamed.

Each event row has a 'More Details' link. At the bottom, there are navigation controls for 'First Page', 'Page', '1 of 1', 'Last Page', '100 items', and '96 item'.

Pestaña Eventos

1. Use las opciones de filtrado para mostrar o bien todos los eventos, o bien solo eventos del sistema o eventos complejos (alertas).
2. Haga clic en el botón **Más detalles** para expandir cada evento y tener acceso a información adicional.

Event name: Event description:
ScreenCaptureModuleLoaded A process has dynamically loaded dwmapi.dll module capable of screen capturing.

ATT&CK Techniques: Collection –Screen Capture [Hide Details ^](#)

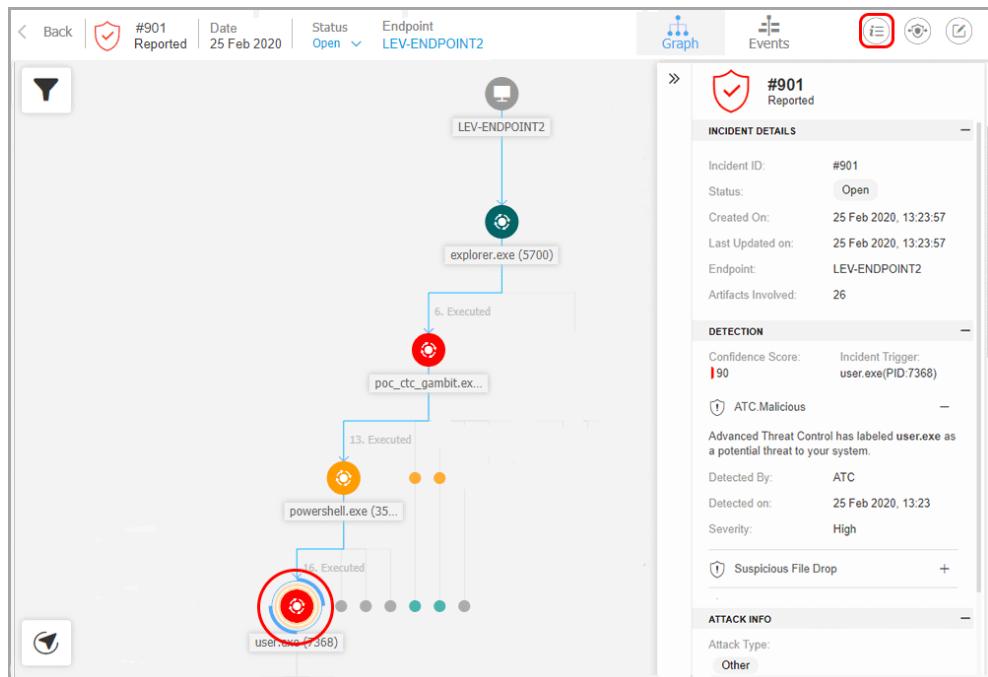
 Process  File  Network  Registry Other

Pid: 2420
Process Path: c:\users\administrator\Desktop\9b74ecceff733dd080c75355b7852076.1.exe
Command Line: <unknown>
Parent Pid: 4992
Loaded Module: c:\windows\syswow64\dwmapi.dll

Información de incidentes

Este panel contiene secciones contraíbles con datos como ID del incidente, estado actual, fecha y hora en que se creó y en que se actualizó por última vez, número de rastros involucrados, nombre y descripción del desencadenante e información del ataque.

Desde esta sección puede acceder al incidente extendido que incluye este incidente de endpoint, de ser el caso.

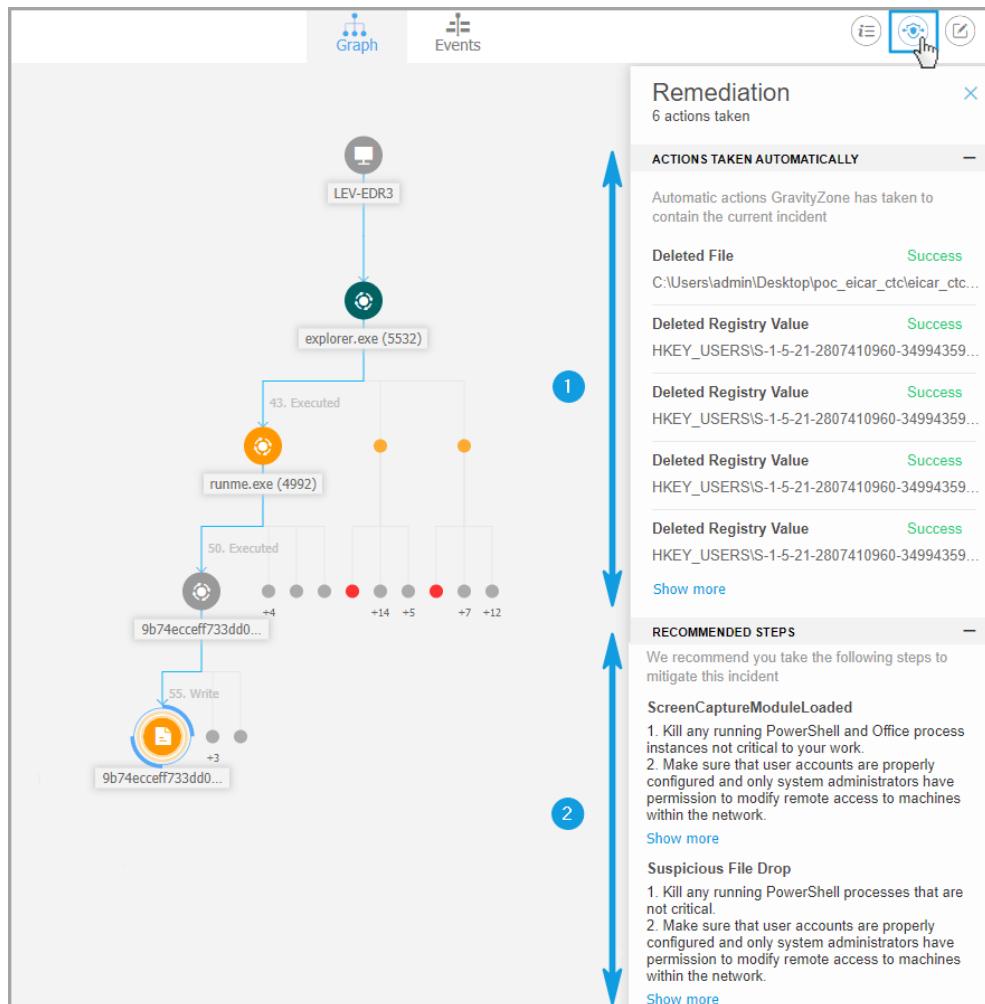


Panel de Información de incidentes

El panel también incluye las alertas detectadas en el elemento que desencadenó el incidente.

Reparación

El panel **Reparación** le proporciona información muy útil sobre qué medidas correctivas adoptó automáticamente GravityZone, en el caso de ataques bloqueados por tecnologías como Advanced Threat Control (ATC), HyperDetect y Antimalware, así como los pasos recomendados que puede dar para mitigar el incidente y aumentar el nivel de seguridad de su sistema.



Panel de Reparación

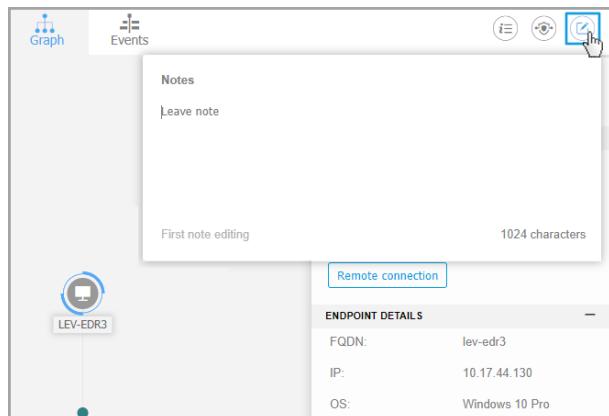
- Medidas adoptadas automáticamente por GravityZone.
- Recomendaciones para mitigar aún más el incidente y aumentar la seguridad.

Nota

Los pasos recomendados corresponden a las alertas detectadas en el nodo que desencadenó el incidente investigado.

Notas

La sección **Notas** le permite añadir una nota para realizar un seguimiento de cambios recientes y facilitar el cambio de propiedad de los incidentes.

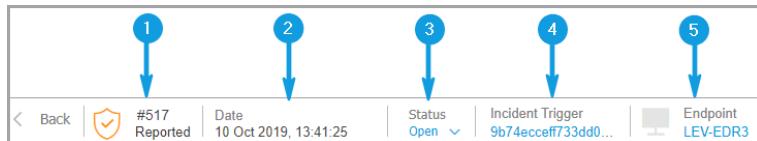


Portapapeles de notas

1. Para añadir una nota al evento actual, haga clic en el botón **Notas** y se mostrará una nueva ventana.
2. Introduzca su mensaje en esta ventana (de 2048 caracteres como máximo).

Barra de estado del incidente

La barra de estado del incidente proporciona etiquetas de eventos de seguridad que pueden ayudarle a detectar información clave sobre los endpoints de la red involucrados.



Barra de estado del incidente

1. ID del incidente: El número de identificación del incidente bajo investigación y si el incidente está bloqueado o solo se informa de él.

Nota

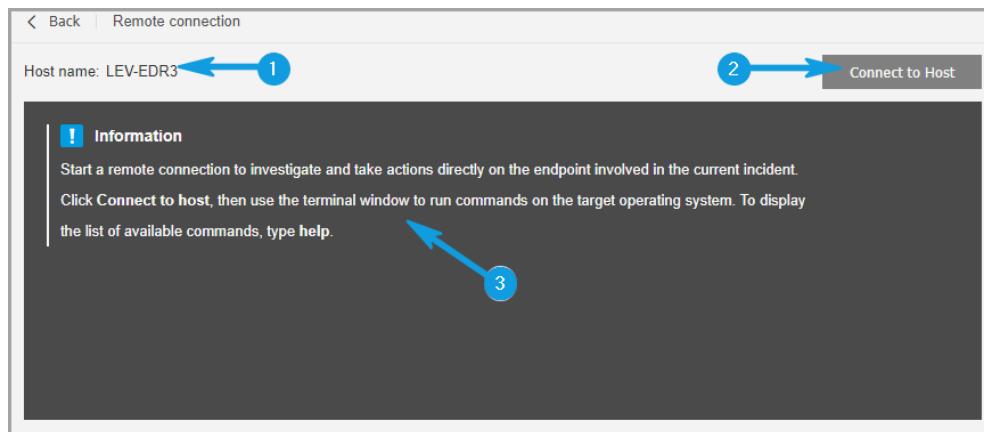
Esta etiqueta también muestra si XDR ha correlacionado el incidente con un ataque en toda la red. Haga clic en el enlace para abrir el incidente extendido en una nueva pestaña del navegador, con el fin de investigarlo más a fondo.

2. Momento de la detección: La fecha y hora en que se desencadenó el incidente.
3. Estado del incidente: El estado actual del incidente.
4. Desencadenante del incidente: El nombre del elemento que generó el incidente.
5. Endpoint: El nombre del endpoint objetivo.

Al hacer clic en el botón **Atrás**, volverá a la página principal de **Incidentes**.

Conexión remota

Use esta pestaña para establecer una conexión remota con el endpoint involucrado en el incidente actual y ejecutar una serie de comandos personalizados de shell directamente en su sistema operativo para anular la amenaza al instante o recopilar datos para su investigación adicional.



Pestaña Conexión remota

La pestaña **Conexión remota** contiene los siguientes elementos:

1. El nombre del endpoint involucrado en el evento de seguridad actual
2. El botón que controla la conexión remota (conectar/desconectar)
3. La ventana de terminal

Requisitos previos de la sesión de terminal

- La versión del agente de Bitdefender instalada en el endpoint debe ser compatible con la conexión remota.
- El endpoint debe estar encendido y online.
- El endpoint debe tener el sistema operativo Windows.
- GravityZone debe poder comunicarse con el endpoint.
- Su cuenta de GravityZone debe tener permisos de administración para el endpoint objetivo.

Creación de una conexión remota

La conexión remota funciona de la siguiente manera:

1. Comience la sesión en vivo haciendo clic en el botón **Conectar a host**.
El estado de la conexión se mostrará junto al nombre del endpoint.

Si falla la conexión, aparecerá un mensaje de error en la ventana de terminal.

Nota

Puede abrir un máximo de cinco sesiones de terminal con el mismo endpoint simultáneamente.

- Una vez conectado, el terminal muestra la lista de comandos disponibles y su descripción. Escriba el comando que desee en la ventana de terminal seguido de `Intro`.

Para obtener más información sobre un comando, escriba `help` seguido del nombre del comando (por ejemplo, `help ps`).

- El terminal muestra la salida devuelta por el comando cuando este se ejecuta correctamente.

Si el endpoint no consigue finalizar la ejecución del comando, este se descartará.

El historial de comandos se registra en la ventana de terminal. No obstante, puede ver los comandos escritos anteriormente pulsando las teclas de flecha.

- Para finalizar la conexión, haga clic en el botón **Finalizar sesión**.

La sesión de terminal caduca automáticamente tras cinco minutos de inactividad.

Salir de la pestaña **Conexión remota** mientras está conectado a un endpoint también finaliza la sesión de terminal.

Comandos de la sesión de terminal

Los comandos de la sesión de terminal de EDR son comandos de shell personalizados, independientes de la plataforma, que utilizan una sintaxis genérica. Más adelante puede ver la lista de comandos disponibles que puede utilizar en los endpoints a través de una sesión de terminal:

- `ps`
 - **Descripción:** Muestra información sobre los procesos actuales en ejecución en el endpoint objetivo, como el ID del proceso (PID), el nombre, la ruta o el uso de memoria.
 - **Sintaxis:** `ps`
 - **Alias:** `tasklist`

- Parámetros: -

● kill

- **Descripción:** Finaliza una aplicación o un proceso en ejecución en el endpoint objetivo por su PID (ID de proceso). Utilice el comando `ps/tasklist` para obtener el PID.
- **Sintaxis:** `kill [PID]`
- **Alias:** -
- **Parámetros:** `[PID]`: el ID de un proceso en el endpoint objetivo.

● ls (dir)

- **Descripción:** Muestra información sobre todos los archivos y carpetas del directorio especificado, como el nombre, tipo, tamaño y fecha de modificación. Permite comodines para especificar la ruta. Por ejemplo:
`C:\Users\admin\Desktop\s*` se refiere a todos los contenidos de la carpeta de Desktop que comienzan por "s"
`C:\Users\publ??` se refiere a todos los contenidos de la ruta especificada, cualesquiera que sean sus dos últimas letras.
- **Sintaxis:** `ls [ruta]`
- **Alias:** `dir`
- **Parámetros:** `[Path]` - la ruta a un archivo o carpeta en el endpoint objetivo.

● rm (del, delete)

- **Descripción:** Elimina archivos y carpetas de la ruta especificada en el endpoint objetivo.
 - **Sintaxis:** `rm [ruta]`
 - **Alias:** `del/delete`
 - **Parámetros:** `[Path]` - la ruta a un archivo o carpeta en el endpoint objetivo.
- reg query
- **Descripción:** Devuelve toda la información (nombre, tipo y valor) de la ruta de la clave de registro especificada.

- **Sintaxis:** reg query [rutaclave] [/k] [nombreclave] [/v] [nombrevalor]
- **Alias:** -
- **Parámetros:**
 - rutaclave: devuelve toda la información de las claves de registro de la ruta especificada.
 - /k [nombreclave]: filtra los resultados de las claves de registro por determinado nombre de clave. También puede usar comodines (*, ?) para filtrar un abanico más amplio de nombres.
 - /v [nombrevalor]: filtra los valores de registro por determinado nombre de valor. También puede usar comodines (*, ?) en el nombre de valor para filtrar un abanico más amplio de nombres.
- reg add
 - **Descripción:** Añade una nueva clave o valor de registro. Sobrescribe un valor de registro, si ya existía. Para sobrescribir la información del registro, debe especificar todos los parámetros definidos.
 - **Sintaxis:** reg add [nombreclave] [/v] [nombrevalor] [/t] [tipodatos] [/d] [datos]
 - **Alias:** -
 - **Parámetros:**
 - [nombreclave] : el nombre de la clave de registro.
 - /v [nombrevalor]: el nombre del valor de registro. También requiere añadir al menos el parámetro /d [datos].
 - /t [tipodatos]: el tipo de datos del valor de registro. Puede añadir uno de los siguientes tipos de datos:
REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY,
REG_DWORD_LITTLE_ENDIAN, REG_LINK,
REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ
Si no se especifica, se asigna el tipo REG_SZ por defecto.

Cuando se establece el tipo en `REG_BINARY`, los datos de registro se interpretan como valores hexadecimales.

- `reg delete`

- **Descripción:** Elimina una clave de registro o sus valores..

- **Sintaxis:**

- ```
reg delete [nombreclave] [/v] [nombrevalor]
```

- ```
reg delete [nombreclave] [/va]
```

- **Alias:** -

- **Parámetros:**

- `[nombreclave]` : elimina la clave de registro y todos sus valores.

- `/v [nombrevalor]`: elimina el valor de registro especificado.

- `/va`: elimina todos los valores de la clave de registro especificada.

- `cd`

- **Descripción:** Cambia el directorio de trabajo a la ruta especificada. Este comando requiere, como parámetro, la ruta a una unidad o carpeta desde el endpoint objetivo.

- **Sintaxis:** `cd [ruta]`

- **Alias:** -

- **Parámetros:** `[Path]` - la ruta a un archivo o carpeta en el endpoint objetivo.

- `ayuda`

- **Descripción:** Sin especificar un parámetro, la ayuda muestra todos los comandos disponibles con una breve descripción. Al acceder a la ayuda seguida de un parámetro, se muestra la sintaxis completa de ese comando, una breve descripción y un ejemplo de uso.

- **Sintaxis:** `help [comando]`

- **Alias:** -

- **Parámetros:** nombre del comando (por ejemplo, `cd`, `kill`, `ls`, `ps`)

- `clear (cls)`

- **Descripción:** Borra la ventana de terminal y muestra el símbolo del sistema en la carpeta de trabajo actual.
- **Sintaxis:** clear
- **Alias:** cls
- **Parámetros:** -

9.2. Incluir archivos en lista de bloqueo

En la página **Lista de bloqueo** puede ver y administrar los elementos por sus valores hash. Vea los registros de actividad en el [registro de actividad del usuario](#).

Type	File Hash	Source Type	Source Info	File Name
MD5	77e864a0d175cbd380c7185b2f9026c	Incident	#6	user.exe
SHA256	c893b6baef3610e9812317f4411ea6df29afb718cf22d583a...	Incident	#6	user.exe

Página de lista de bloqueo

En una tabla de datos, puede ver la siguiente información sobre cada elemento:

- **Tipo de fichero:**
 - MD5
 - SHA256
- **Valor hash del archivo**
- **Tipo de fuente:**
 - Incidente
 - Importar
 - Manual

- Información de fuente
- Archivo
- Empresa

Añada valores hash a la lista de bloqueo existente:

1. Copie el valor hash de la [Información del archivo](#).
2. Elija entre **MD5** o **SHA256** y pegue el valor en el cuadro que aparece a continuación.
3. Añada una nota en caso necesario.

3. Haga clic en **Guardar**.

Add Hashes

Manually add the hash to Blocklist

Note:

Paste Hash: MD5 SHA256

Select Target

- BIT
+ Company 1
+ Company 2

Selected Groups

Save Cancel

Ventana Añadir valor hash

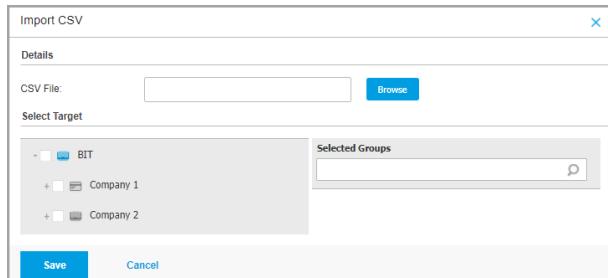


Importante

El **Sensor de incidentes** evitara que cualquier binario cuyo valor hash se haya añadido a la lista de bloqueo inicie un proceso.

Importe registros hash a la lista de bloqueo existente. Para importar un archivo CSV:

1. Haga clic en **Importar CSV**.
2. Busque su archivo CSV y haga clic en **Guardar**.



Ventana Importar CSV

También puede importar archivos CSV locales desde su dispositivo a la página **Lista de bloqueo**, pero primero debe asegurarse de que su CSV sea válido.

Para crear un archivo CSV válido que poder importar, debe llenar las tres primeras columnas con los siguientes datos:

1. La primera columna del CSV debe contener el tipo de hash: `md5` o `sha256`.
2. La segunda columna debe contener los valores hash hexadecimales correspondientes.
3. La tercera columna puede contener información textual opcional relacionada con la columna **Información de origen** de la página **Lista de bloqueo**.



Nota

La información correspondiente a las otras columnas de la página **Lista de bloqueo** se llenará automáticamente al [importar el archivo CSV](#).

9.3. Buscar eventos de seguridad

La página **Buscar** le permite recorrer eventos pasados en función de un criterio complejo.

Descripción general de la página de búsqueda

Para ver los eventos que le interesan, debe crear consultas usando el lenguaje de consulta disponible en GravityZone.

La página **Búsqueda** proporciona las siguientes opciones:

- Una barra de búsqueda para introducir **consultas** que muestra la lista de términos por categorías cuando se hace clic en ella, así como un asistente de autocompletar.
- Guardar las búsquedas favoritas para su uso posterior.
-
- Una sección de **Puesta en marcha** con un enlace a la [ayuda sobre la sintaxis del lenguaje de consulta](#).
- **Consultas predefinidas**, diseñadas para búsquedas de eventos de seguridad particularmente útiles.

9.3.1. El lenguaje de consulta

El lenguaje de consulta le ofrece el vocabulario (campos y operadores) y la sintaxis con la que puede crear consultas. Estas se describen a continuación.

Haga clic en el enlace **Ayuda sobre sintaxis** y seleccione la pestaña **Lenguaje de consulta** para ver su contenido.

Campos

El campo de consulta es el mismo que el campo en la base de datos de GravityZone. Los campos representan entidades como rutas de archivo, hashes de archivo o nombres de dominio.

Cualquier campo puede tener uno o más valores que representan el estado del campo en un momento determinado. Los valores pueden incluir distintos tipos de datos, dependiendo del significado del campo.

Operadores

Los operadores le permiten crear relaciones entre campos para crear un criterio de búsqueda. Puede usar los siguientes operadores:

Operador	Ejemplo	Descripción
:	fieldCategory.option: value1	Compara el valor del campo de consulta con valores del mismo campo en la base de datos.

Operador	Ejemplo	Descripción
" "	fieldCategory.option: "value1 value2"	Las cadenas incluidas entre comillas se tratan en conjunto como una sola frase.
()	fieldCategory1.option: value1 AND (fieldCategory2.option: value2 OR fieldCategory3.option: value3)	Términos de consulta agrupados
AND	fieldCategory1.option: value1 AND fieldCategory2.option: value2	Devuelve resultados que coinciden con todas sus condiciones de consulta.
o	fieldCategory1.option: value1 OR fieldCategory2.option: value2	Devuelve resultados que coinciden con alguna de sus condiciones de consulta.
AND NOT	fieldCategory1.option: value1 AND NOT fieldCategory2.option: value2	Este operador es útil en consultas complejas y devuelve resultados que no coinciden con el término especificado, a excepción de las demás condiciones.
existe _exists_ :	fieldCategory.option	Devuelve resultados que contienen el campo especificado.
-	fieldCategory.option: -value	Use el signo menos (-) cuando deba excluirse el valor de los resultados.
?	fieldCategory.option: ???_file.path	Use un signo de interrogación (?) para sustituir a un solo carácter en su valor del campo.
*	fieldCategory.option: file.*	Use un asterisco (*) para sustituir cualquier valor de campo.

Sintaxis de consulta

Una consulta es una condición lógica o una serie de condiciones limitada por operadores, que ofrece como resultado los eventos de la base de datos EDR.

Todas las condiciones deben referirse a campos. Algunas condiciones requieren que proporcione un valor, pero otras no. Por ejemplo, no necesita un valor cuando solo consulta si el campo existe en la información del evento.

El nivel de las consultas puede variar de simples a complejas. Las consultas complejas pueden tener consultas anidadas (consultas dentro de consultas).

Una sintaxis de campo válida consiste en la categoría de campo seguida de una de las opciones de la sección **Lenguaje de consulta** y su valor correspondiente: fieldCategory.option: value.

Por ejemplo, file.path: "%system32%\com\svchost.exe" es una consulta bastante simple que busca todos los eventos que incluyen %system32%\com\svchost.exe y consiste en:

- Una categoría de campo obligatoria y una opción correspondiente (separadas por un punto): file.path
- Un operador: los dos puntos (:)- para comprar los valores del campo
- El valor que se busca: %system32%\com\svchost.exe
- Comillas (" "), porque el valor contiene caracteres especiales como <\> y <.>

9.3.2. Ejecutar consultas

Para ejecutar una consulta:

1. Escriba la cadena de la consulta en el campo.

Al hacer clic en el campo **Buscar**, se mostrará la lista de términos de búsqueda agrupados por categorías. Seleccione el término que deseé para empezar a crear su consulta.

A medida que escribe, Control Center le ayuda con las sugerencias de autocompletar. Utilice las teclas de las flechas para seleccionar una opción recomendada y a continuación pulse la tecla **Intro** para añadirla a la consulta.

Si necesita más ayuda, haga clic en el enlace **Ayuda sobre sintaxis**.

Nota

Puede usar consultas anidadas para realizar búsquedas complejas.

2. Para filtrar los eventos dentro de un intervalo temporal, haga clic en el campo de hora.

Importante

El intervalo por defecto para la retención de datos de eventos es de siete días. Si desea aumentar su capacidad, debe ponerse en contacto con su representante de ventas para actualizar su solución con un complemento de **retención de datos** de 30, 90 o 180 días).

Tiene varias opciones para definir el período de búsqueda:

- Solo la fecha específica.
Seleccione una fecha en la pestaña **Desde** del calendario.
- Un intervalo de tiempo exacto.
 - a. Seleccione la fecha de inicio en la pestaña **Desde** del calendario.
 - b. Seleccione la fecha de finalización en la pestaña **Hasta**.
- Un último periodo de tiempo desde las opciones disponibles.
- Haga clic en **Aceptar**.

3. Haga clic en **Buscar** o pulse **Intro**.

Bajo su consulta puede ver los eventos que coinciden con el criterio de búsqueda, junto a información del evento.

Importante

Cuando ejecuta la consulta `detections.detection_type` en el campo **Buscar**, Control Center le requiere que la complete con un valor entero de 1 a 15 (es decir, `detections.detection_type:1`).

Los valores que introduzca corresponderán a un cierto tipo de detección, tal como se indica a continuación:

- a. `detections.detection_type:1` - Detección de Advanced Threat Control
- b. `detections.detection_type:2` - Detección de motores estáticos antimalware

- c. detections.detection_type:3 - Detección de HyperDetect
- d. detections.detection_type:4 - Notificación de evento sospechoso de Advanced Threat Control
- e. detections.detection_type:5 - Detección de tipos de ataque de los que informa HyperDetect
- f. detections.detection_type:6 - Detección antimalware del analizador de línea de comandos
- g. detections.detection_type:7 - Detección de correlación de tecnologías cruzadas
- h. detections.detection_name:8 - Detección de Network Attack Defense
- i. detections.detection_type:9 - Detección de tipos de ataque de los que no informa HyperDetect
- j. detections.detection_type:10 - Detección de análisis dinámico contenido con Sandbox Analyzer
- k. detections.detection_type:11 - Detección de análisis de registro de búfer de memoria
- l. detections.detection_type:12 - Detección de URL
- m. detections.detection_type:13 - Detección de Antiexploit avanzado
- n. detections.detection_type:14 - Detección de análisis del comportamiento del usuario
- o. detections.detection_type:15 - Detección de la interfaz de análisis antimalware
- p. detections.detection_type:16 - Detección de correlación entre tecnologías basada en Machine Learning.

Control Center puede mostrar hasta 10 000 eventos. Si los resultados de la consulta contienen más de 10 000 eventos, se mostrará un mensaje en la pantalla. En este caso necesitará ajustar su búsqueda.

9.3.3. Búsquedas favoritas

Dado que la mayoría de las consultas son largas, es complicado crearlas o incluso recordarlas. En lugar de guardarlas en un campo y copiarlas y pegarlas en GravityZone, puede guardarlas directamente en GravityZone para tenerlas a mano.

Para guardar su consulta:

1. Introduzca la cadena en el campo **Buscar**.
2. Haga clic en el ícono  a la derecha del campo **Buscar**.
3. Cuando se le pida asignar un nombre a la consulta, escriba el nombre que desee dar a su consulta.
4. Haga clic en **Añadir**.

Haga clic en el enlace **Búsquedas favoritas** bajo el campo **Consulta** para ver sus consultas guardadas.

Más adelante, dispondrá de tres opciones:

- Ejecutar la consulta.
- Editar el nombre de la consulta.
- Eliminar la consulta.

Ejecutar una consulta guardada:

1. Haga clic en el enlace **Búsquedas favoritas**.
2. Seleccione su consulta preferida.

La cadena guardada se añadirá al campo **Buscar**.

Nota

De ser necesario, modifique la cadena de la consulta. Además, puede guardar la nueva consulta de búsqueda en sus Búsquedas favoritas.

3. Use los filtros empresa y calendario para restringir la búsqueda.
4. Haga clic en **Buscar**.

Cuando su lista de consultas necesite ajustes, sitúe el cursor del ratón sobre la consulta guardada para mostrar las opciones en línea.

- Haga clic en el ícono  **Editar** para cambiar de nombre la consulta.
- Haga clic en el ícono  **Eliminar** si ya no necesita la consulta.

9.3.4. Consultas predefinidas

La página **Buscar** proporciona algunos ejemplos de búsquedas con consultas complejas, específicas para investigaciones de eventos de seguridad.

Las consultas predefinidas se agrupan por categorías de investigación de seguridad.

Para iniciar una consulta predefinida:

- Haga clic en el ícono  junto a la descripción de la consulta predefinida.
- La frase de la consulta aparecerá automáticamente en la barra **Buscar**. Rellene los datos concretos para los términos de la consulta.
- Haga clic en el botón **Buscar** para ejecutar la consulta.

Nota

Puede volver en cualquier momento a las opciones de **Puesta en marcha** desde la página **Buscar** haciendo clic en el enlace **Puesta en marcha** en la parte superior derecha de la página.

9.4. Reglas personalizadas

La página **Reglas personalizadas** le proporciona el marco para crear y administrar reglas personalizadas con el fin de incluir o excluir de los incidentes desencadenantes comportamientos concretos.

Esta característica de EDR incluye dos categorías principales:

- [Detecciones](#)
- [Exclusiones](#)

9.4.1. Detecciones

La pestaña **Detecciones** le proporciona el marco para crear y administrar reglas de detección personalizadas, marcar determinado comportamiento de su entorno como una detección válida y generar los incidentes correspondientes en la página de [Incidentes](#).

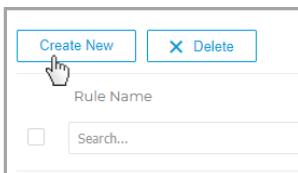
Rule Name	Last Modified	Status	Tag
net1	15 November 2020, 11:04	Active	net
netbots	15 November 2020, 11:03	Active	bot

Pestaña de detecciones

1. Haga clic en el botón **Crear nuevo** para crear una nueva regla de detección personalizada. Para más información, consulte la sección [Crear reglas de detección personalizadas](#).
2. Use estos botones de acción para personalizar su cuadrícula:
 - Haga clic en el botón **Mostrar/Ocultar columnas** para añadir o eliminar columnas de filtro.
La página se actualizará automáticamente y cargará las tarjetas con información que coincide con las columnas añadidas.
Siempre puede restablecer las columnas de filtro con el botón **Restablecer** del menú desplegable **Mostrar/Ocultar columnas**.
 - Haga clic en el botón **Mostrar/Ocultar filtros** para mostrar u ocultar la barra de filtros.
 - Haga clic en el botón **Actualizar** para actualizar la lista.
3. Marque la casilla de verificación general o las casillas individuales de las reglas para seleccionarlas y haga clic en **Eliminar** para eliminarlas de la lista.
4. Haga clic en una regla de la lista para expandir su panel de detalles, ver los detalles de la regla y actualizarla o eliminarla si fuera necesario. Para más información, consulte el [Panel de detalles de reglas de detección](#).

Crear reglas de detección personalizadas

Para crear una regla de detección personalizada, haga clic en el botón **Crear nuevo**.



Crear una nueva regla de detección

Le conducirá a la página **Crear regla de detección**, en la ventana **Definición de la regla**, donde puede comenzar a editar la regla:

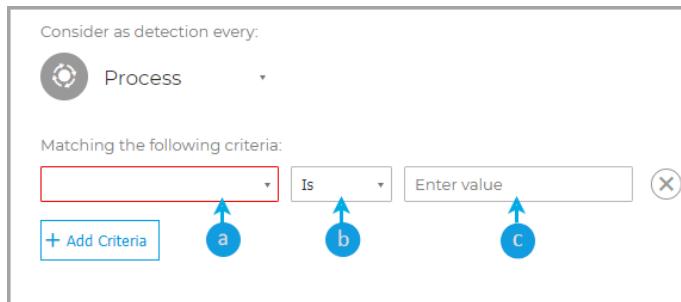
1. Seleccione qué tipo de elemento desea incluir en la regla de exclusión.

A screenshot of a 'Create Detection Rule' window. On the left, there's a section titled 'Rule definition' with a description: 'Define rules to mark a specific behavior as a valid detection. Avoid creating generic rules, to prevent overloading your security team's backlog with false-positive incidents.' On the right, there's a dropdown menu labeled 'Consider as detection every:' with 'Process' selected. Below it is a list of options: 'Process' (selected), 'File', 'Connection', and 'Registry'. A cursor is hovering over the 'File' option.

Puede elegir entre:

- Proceso
- Archivo
- Conexión

- Registro
2. Cada tipo de elemento tiene criterios de coincidencia específicos que puede elegir en el menú desplegable:



- a. Seleccione una de las opciones de criterios disponibles.
- b. Seleccione el tipo de relación entre los criterios de coincidencia y su valor:
 - **Es:** Incluirá todos los incidentes con elementos que coincidan con el valor exacto introducido en el campo de valor.
 - **Contiene:** Incluirá todos los incidentes con elementos que contengan el valor introducido en el campo de valor (por ejemplo, caracteres comodín, extensiones de archivo, etc.).



Importante

El uso de caracteres comodín al crear una regla de detección aumenta el riesgo de hacerla demasiado genérica, lo que incrementa las probabilidades de saturar sus tareas pendientes con incidentes que son falsos positivos.

- **Es uno de:** Incluirá todos los incidentes con elementos que coincidan con uno de los valores introducidos en el campo de valor (se aplica el operador **O** entre los valores introducidos).
- c. Introduzca el valor específico para cada criterio.



Nota

Al introducir varios valores para un criterio (cuando se usa la condición **Es uno de**), debe pulsar **Intro** después de cada valor para completar la acción.

3. Utilice **Añadir criterios** para añadir un nuevo criterio a la regla.

Nota

La regla desencadenará incidentes que incluyan todos los criterios definidos (se aplica el operador **Y** entre los diversos criterios añadidos).

4. Una vez que se hayan definido todos los criterios, haga clic en **Paso siguiente**. Le conducirá a la sección **Ajustes de reglas**, donde debe llenar los detalles de la regla.

Create Detection Rule

① Rule definition

Define rules to mark a specific behavior as a valid detection. Avoid creating generic rules, to prevent overloading your security team's backlog with false-positive incidents.

② Rule settings

Specify rule details and what should happen when this behavior is identified.

Rule Name: * Enter...

Rule Details: Enter...

Tag:

Status: * Active

Rule Outcome

Generate an alert with the following severity: *

The generated alerts will be displayed in the [Incident](#) page. You can also browse all the alerts in the [Search](#) page.

High
Low
Medium
High

5. Asigne un nombre a la nueva regla en el campo **Nombre de la regla**. Este campo es obligatorio.
6. Añada una breve descripción de la regla en el área de texto **Detalles de la regla**.
7. Añada etiquetas específicas a esta regla en el campo **Etiqueta**, para facilitar la agrupación y administración de las reglas.

8. Establezca el estado de la regla en Activa o Inactiva en el menú desplegable **Estado**.
9. Mediante el menú desplegable, establezca la gravedad de las alertas desencadenadas por esta regla en baja, media o alta.
10. Haga clic en **Crear regla** para completar la creación de la regla de exclusión personalizada.

La nueva regla está disponible en la pestaña **Detecciones**.

Panel de detalles de reglas de detección

El panel **Detalles de reglas** incluye información detallada de la regla seleccionada, incluida la fecha de creación y quién la creó, la fecha en que se actualizó por última vez y el estado e ID único, así como un enlace a la lista de eventos que coinciden con los criterios de la regla. También incluye una descripción de la regla, etiquetas asociadas, criterios de coincidencia incluidos y el resultado de la regla.

The screenshot shows a detailed view of a detection rule named 'emotet'. At the top right are navigation icons: a downward arrow, an upward arrow, and a blue 'X'. Below the title 'emotet' are several metadata fields:

- Created by: vagrant
- Created on: 15 November 2020, 13:52
- Last Updated: 15 November 2020, 13:52
- Results: [View Incidents](#)
- Rule ID: 5fb1168c25a3ff315511f212
- Rule Status: Active

A 'DETAILS' section follows, containing the rule name 'emotet' and a tag 'emo' highlighted with a light blue box.

The 'IN CASE THIS HAPPENS' section describes a process matching criteria: 'Name is: emotet.exe'.

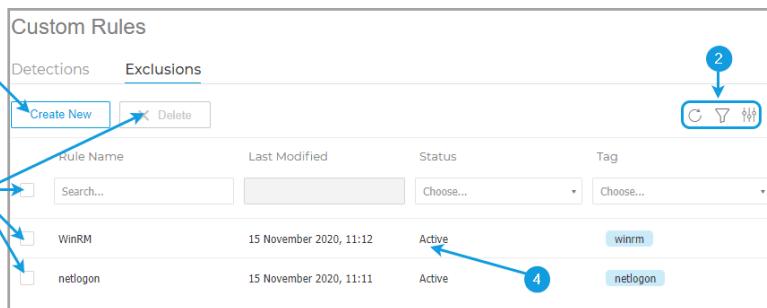
The 'DO THE FOLLOWING' section contains the instruction: 'Generate an alert with **High** severity and display it in an incident.' Below this are two buttons: 'Edit' and 'Delete', with a cursor pointing at the 'Edit' button.

Panel de Detalles de reglas

- Haga clic en **Editar** para acceder a la ventana **Crear regla de detección**, donde puede actualizar la definición de la regla.
- Haga clic en **Eliminar** para eliminar la regla de exclusión de la lista.

9.4.2. Exclusiones

La pestaña **Exclusiones** le proporciona el marco para crear y administrar reglas de exclusión personalizadas, con el fin de excluir los incidentes que considere irrelevantes para su organización, que de otra manera destacaría la EDR normalmente en la página [Incidentes](#).



Pestaña exclusiones

1. Haga clic en el botón **Crear nuevo** para crear una nueva regla de exclusión personalizada. Para más información, consulte la sección [Crear reglas de exclusión personalizadas](#).

Como alternativa, siempre puede crear una regla directamente desde el gráfico de incidentes, seleccionando un nodo objetivo y añadiéndolo como exclusión desde su panel lateral de detalles. Para más información, consulte [Añadir como exclusión EDR](#).

2. Use estos botones de acción para personalizar su cuadrícula:

- Haga clic en el botón **Mostrar/Ocultar columnas** para añadir o eliminar columnas de filtro.

La página se actualizará automáticamente y cargará las tarjetas con información que coincide con las columnas añadidas.

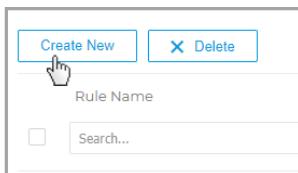
Siempre puede restablecer las columnas de filtro con el botón **Restablecer** del menú desplegable **Mostrar/Ocultar columnas**.

- Haga clic en el botón **Mostrar/Ocultar filtros** para mostrar u ocultar la barra de filtros.
- Haga clic en el botón **Actualizar** para actualizar la lista.

3. Marque la casilla de verificación general o las casillas individuales de las reglas para seleccionarlas y haga clic en **Eliminar** para eliminarlas de la lista.
4. Haga clic en una regla de la lista para expandir su panel de detalles, ver los detalles de la regla y actualizarla o eliminarla si fuera necesario. Para más información, consulte el [Panel de detalles de reglas de exclusión](#).

Crear reglas de exclusión personalizadas

Para crear una regla de exclusión personalizada, haga clic en el botón **Crear nuevo** de la pestaña **Exclusiones**.

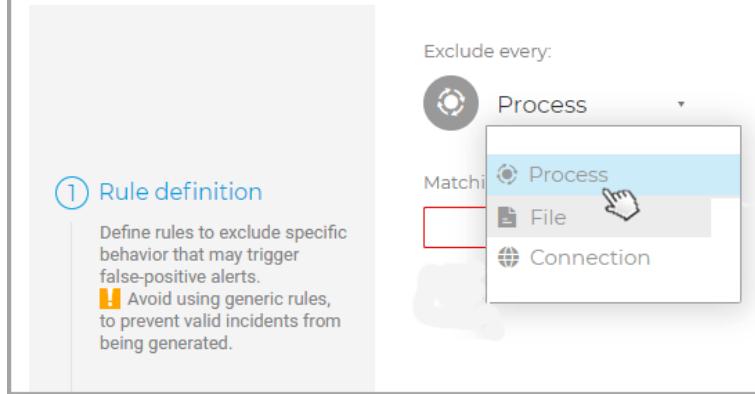


Crea una nueva regla de exclusión

Le conducirá a la página **Crear regla de exclusión**, en la sección **Definición de la regla**, donde puede comenzar a editar la regla:

1. Seleccione qué tipo de elemento desea incluir en la regla de exclusión.

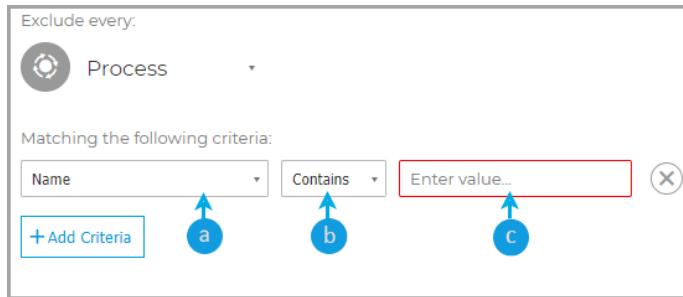
Create Exclusion Rule



Puede elegir entre:

- Proceso
- Archivo
- Conexión

2. Cada tipo de elemento tiene criterios de coincidencia específicos que puede elegir en el menú desplegable:



- Seleccione una de las opciones de criterios disponibles.
- Seleccione el tipo de relación entre los criterios de coincidencia y su valor:
 - Es:** Excluirá todos los incidentes con elementos que coincidan con el valor exacto introducido en el campo de valor.
 - Contiene:** Excluirá todos los incidentes con elementos que contengan el valor introducido en el campo de valor (por ejemplo, caracteres comodín, extensiones de archivo, etc.).



Importante

El uso de caracteres comodín al crear una regla de exclusión aumenta el riesgo de hacerla demasiado genérica, con la posibilidad de ignorar las amenazas reales y dejar a su empresa más vulnerable.

- Es uno de:** Excluirá todos los incidentes con elementos que coincidan con uno de los valores introducidos en el campo de valor (se aplica el operador **O** entre los valores introducidos).
- Introduzca el valor específico para cada criterio.



Nota

Al introducir varios valores para un criterio (cuando se usa la condición **Es uno de**), debe pulsar **Intro** después de cada valor para completar la acción.

- Utilice **Añadir criterios** para añadir un nuevo criterio a la regla.



Nota

La regla excluirá los incidentes que incluyen todos los criterios definidos (se aplica el operador **Y** entre los diversos criterios añadidos).

- Una vez que se hayan definido todos los criterios, haga clic en **Paso siguiente**. Le conducirá a la sección **Ajustes de reglas**, donde debe llenar los detalles de la regla.

The screenshot shows the 'Rule definition' configuration page. On the left, there are two sections: 'Rule definition' and 'Rule Settings'. The 'Rule definition' section contains fields for 'Rule Name' (with placeholder 'Enter...'), 'Rule Details' (with placeholder 'Enter...'), 'Tags' (with placeholder 'Enter...'), and 'Status' (set to 'Active'). The 'Rule Settings' section contains a note about saving events and stopping incident generation, along with a note about alert behavior and incident tracking.

① Rule definition	Rule Name: *	Enter...
	Rule Details:	Enter...
	Tags:	Enter...
	Status: *	Active
② Rule Settings	Rule Outcome	
	Save all events, but stop generating incidents This behavior will no longer be treated as a suspicious/malicious EDR detection. In case this alert becomes trigger for future incidents, they will no longer be generated in the Incidents page. You can still see the events in the Search page.	

- Asigne un nombre a la nueva regla en el campo **Nombre de la regla**. Este campo es obligatorio.
- Añada una breve descripción de la regla en el área de texto **Detalles de la regla**.
- Añada etiquetas específicas a esta regla en el campo **Etiqueta**, para facilitar la agrupación y administración de las reglas.
- Establezca el estado de la regla en Activa o Inactiva en el menú desplegable **Estado**.
- Haga clic en **Crear regla** para completar la creación de la regla de exclusión personalizada.

La nueva regla está disponible en la página **Reglas de exclusión**.

Panel de detalles de reglas de exclusión

El panel **Detalles de reglas** incluye información detallada de la regla seleccionada, incluida la fecha de creación y quién la creó, la fecha en que se actualizó por última vez y el estado e ID único, así como un enlace a la lista de eventos que coinciden con los criterios de la regla. También incluye una descripción de la regla, etiquetas asociadas, criterios de coincidencia incluidos y el resultado de la regla.

Exclude net and net1

Created By: dcirneala@bitdefender.com

Created On: 26 June 2020, 23:40

Last Updated: 26 June 2020, 23:40

Results: [View events](#)

Rule ID: 5ef65d255a687e095e0f1a33

Rule Status: Active

DETAILS

Exclude incidents that include net and net1

net

IN CASE THIS HAPPENS

A process matching the following criteria:

Name is one of: net1.exe OR net.exe

DO THE FOLLOWING

Save all events, but stop generating incidents

[Edit](#) [Delete](#)

Panel de Detalles de reglas

- Haga clic en **Editar** para acceder a la página **Crear regla de exclusión**, donde puede actualizar la definición de la regla.
- Haga clic en **Eliminar** para eliminar la regla de exclusión de la lista.

10. ADMINISTRACIÓN DE RIESGOS EN ENDPOINTS

El análisis de riesgos en los endpoints (ERA) le ayuda a evaluar y endurecer las configuraciones de seguridad de sus endpoints atendiendo a las recomendaciones del sector para minimizar la superficie de ataque.

Importante

! El módulo de Análisis de riesgos en endpoints solo está disponible para sistemas operativos compatibles de servidor y equipos de escritorio Windows.

El ERA recopila y analiza datos a través de tareas de análisis de riesgos ejecutadas en dispositivos seleccionados de su red.

Para ello, primero debe asegurarse de que el módulo ERA esté activado desde la política aplicada a los dispositivos seleccionados:

1. Diríjase a la página **Políticas**.
2. Haga clic en el botón **Añadir** y configure los ajustes de **General**.
3. Desplácese y seleccione la política de **Administración de riesgos**.
4. Marque la casilla de verificación para habilitar las características de **Administración de riesgos** y empiece a configurar políticas que definan cómo ejecutar la tarea de **Análisis de riesgos**.

Nota

i Para obtener más información sobre los indicadores de riesgo de GravityZone, consulte [este artículo de la base de conocimientos](#).

Para obtener más información sobre vulnerabilidades de aplicaciones conocidas, consulte el sitio web [Detalles de CVE](#).

Siga estos pasos para ejecutar tareas de análisis de riesgos y evaluar los resultados:

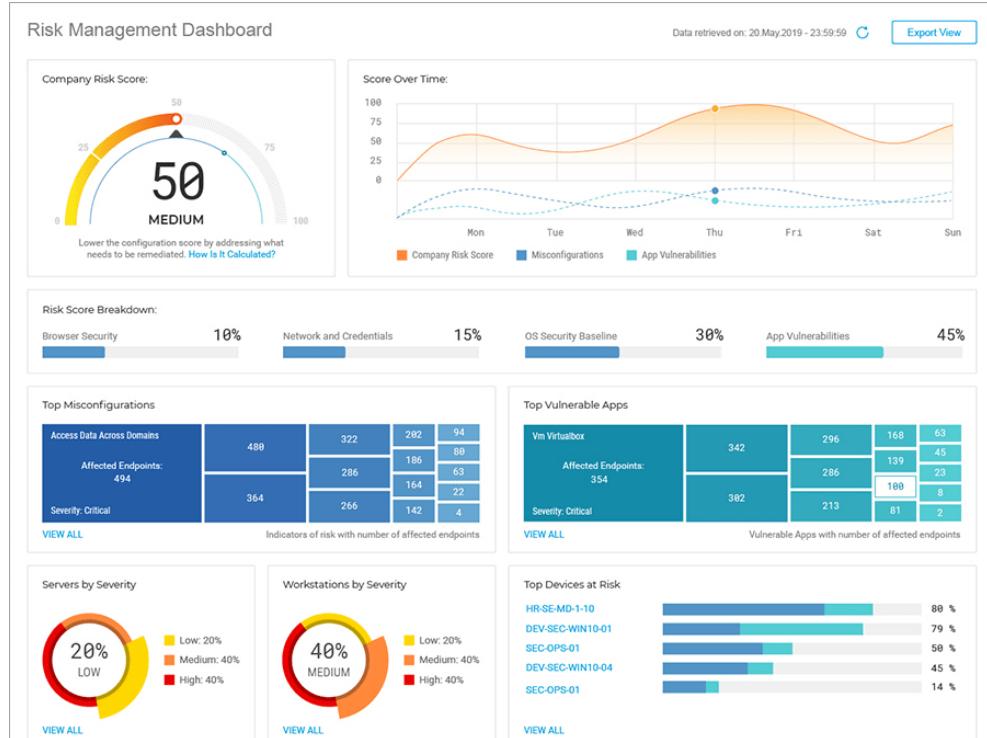
1. Puede ejecutar tareas de análisis de riesgos en endpoints de dos maneras:
 - a. Bajo demanda- seleccionando los endpoints de la página **Red** y enviando una tarea de **Análisis de riesgos** desde el menú **Tareas**.
 - b. Programada; configurando una tarea de análisis de riesgos desde la política que se ejecuta automáticamente en los endpoints objetivo dentro de un intervalo definido.

Después de que el análisis de riesgos haya finalizado correctamente, GravityZone calcula una puntuación de riesgo para cada endpoint..

2. Acceda al panel de control de **Administración de riesgos** para obtener la siguiente información:
 - La puntuación de riesgo de la empresa y la evolución de la puntuación
 - Puntuaciones de riesgo y estadísticas desglosadas en configuraciones erróneas, aplicaciones vulnerables, riesgos humanos y dispositivos afectados
 - La descripción de cada indicador de riesgo y las acciones correctivas recomendadas
3. Acceda a la página **Riesgos de seguridad** para analizar y mitigar las configuraciones erróneas descubiertas, las vulnerabilidades de las aplicaciones y los riesgos potenciales derivados del comportamiento de los usuarios.

10.1. El panel de control de Administración de riesgos

La página **Administración de riesgos** proporciona una descripción general de la seguridad de su red e información de evaluación de riesgos.



Panel de control de Administración de riesgos

1. Puntuación de riesgo de empresa
2. Puntuación a lo largo del tiempo
3. Principales configuraciones erróneas
4. Principales aplicaciones vulnerables
5. Principales riesgos humanos
6. Servidores según gravedad
7. Estaciones de trabajo según gravedad
8. Principales dispositivos en riesgo
9. Principales usuarios según su comportamiento respecto a la seguridad

Los datos mostrados en esta página se organizan en varios widgets:

Puntuación de riesgo de empresa

La puntuación general de riesgo muestra el nivel de riesgo al que está expuesta su organización debido a configuraciones erróneas del sistema, vulnerabilidades conocidas de las aplicaciones instaladas actualmente y riesgos potenciales causados por el comportamiento de los usuarios. La puntuación se ajusta dinámicamente mediante el modificador de salud del sector, que calcula el riesgo causado por las vulnerabilidades de las aplicaciones específicas de su sector de las que se aprovechan los atacantes.

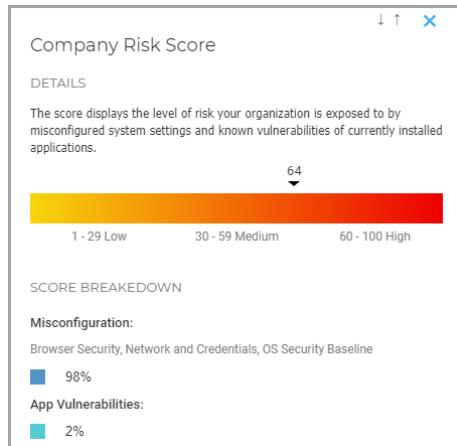
La puntuación representa la media de las tres principales categorías de riesgo

Configuraciones erróneas, Vulnerabilidades de aplicaciones y Riesgos humanos.



Widget de puntuación de riesgo de empresa

Haga clic en el widget y se abrirá un panel de detalles donde podrá ver la información de cómo se calcula el riesgo general y se desglosa en subcategorías.



Panel de detalles de puntuación de riesgo de empresa

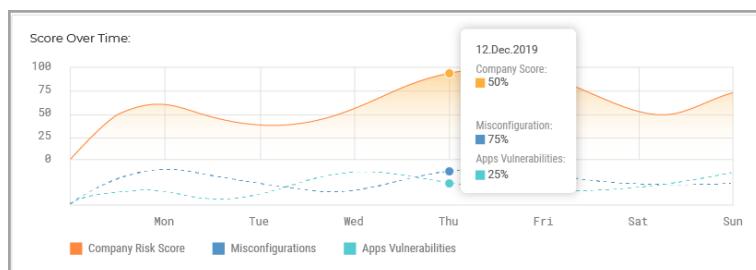


Nota

Ejecutar un [Análisis de riesgos](#) bajo demanda en un nuevo dispositivo objetivo influirá en la puntuación general. Los resultados se conservarán durante noventa días o hasta el próximo análisis.

Puntuación a lo largo del tiempo

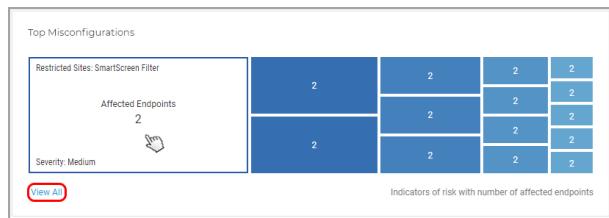
Este widget es un histograma que muestra la evolución semanal del número de dispositivos afectados detectados como vulnerables tras el análisis de riesgos. Los datos del histograma representan el número de dispositivos afectados por indicadores de riesgo durante los últimos siete días, hasta las 12 a. m. (hora del servidor) del día en curso.



Widget de puntuación a lo largo del tiempo

Principales configuraciones erróneas

Este widget muestra los quince principales resultados para los indicadores que activaron una alerta de riesgo después de analizar los dispositivos, ordenados según el número de dispositivos afectados. Cada tarjeta representa un indicador que generó una alerta de riesgo para al menos un dispositivo.



Widget de principales configuraciones erróneas

Cada tarjeta muestra los siguientes elementos:

- El nombre del indicador.
- El número de dispositivos detectados como vulnerables para este indicador.
- La gravedad de la configuración errónea.

Si hace clic en el widget del indicador individual, se abrirá el indicador de riesgo seleccionado en la pestaña [Configuraciones erróneas](#) de la página **Riesgos de seguridad**, donde puede adoptar las medidas apropiadas para mitigar este riesgo.

Si hace clic en el botón **Ver todo**, verá la lista completa de configuraciones erróneas descubiertas en la pestaña [Configuraciones erróneas](#) de la página **Riesgos de seguridad**.



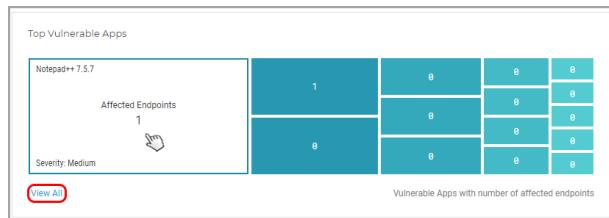
Nota

Para obtener más información sobre las configuraciones erróneas, consulte [este artículo de la base de conocimientos](#).

Principales aplicaciones vulnerables

Este widget muestra los quince principales resultados para las vulnerabilidades de aplicaciones conocidas que activaron una alerta de riesgo después de analizar los dispositivos, ordenados según el número de dispositivos afectados. Cada tarjeta

representa una aplicación vulnerable que generó una alerta de riesgo para al menos un dispositivo.



Widget de principales aplicaciones vulnerables

Cada tarjeta muestra los siguientes elementos:

- El nombre de la aplicación.
- El número de dispositivos que esta aplicación hace vulnerables.
- La gravedad de la aplicación vulnerable.

Si hace clic en el widget de la aplicación individual, se abrirá la vulnerabilidad seleccionada en la pestaña [Vulnerabilidades de aplicaciones](#) de la página **Riesgos de seguridad**, donde puede adoptar las medidas apropiadas para mitigar este riesgo.

Si hace clic en el botón **Ver todo**, verá la lista completa de vulnerabilidades de aplicaciones descubiertas en la pestaña [Vulnerabilidades de aplicaciones](#) de la página **Riesgos de seguridad**.

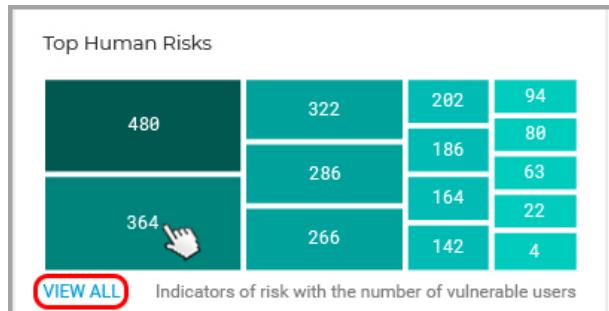


Nota

Puede obtener más información sobre vulnerabilidades de aplicaciones conocidas en el sitio web [Detalles de CVE](#).

Principales riesgos humanos

Este widget muestra los quince resultados principales de los riesgos potenciales causados por el comportamiento involuntario o imprudente de los usuarios activos en su red, ordenados por el número de usuarios vulnerables. Cada tarjeta representa un riesgo de origen humano causado por al menos un usuario.



Widget de principales riesgos humanos

Cada tarjeta muestra los siguientes elementos:

- El nombre del riesgo humano.
- La cantidad de usuarios cuyo comportamiento imprudente o involuntario puede poner en riesgo a su organización.
- La gravedad del riesgo humano.

Si hace clic en el widget de riesgo humano individual, se abrirá el riesgo seleccionado en la pestaña [Riesgos humanos](#) de la página [Riesgos de seguridad](#), donde podrá verlo y analizarlo con mayor detalle.

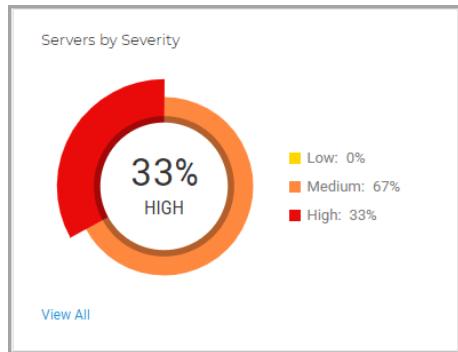
Si hace clic en el botón **Ver todo**, verá la lista completa de todos los riesgos humanos generados por la actividad de los usuarios en la pestaña [Riesgos humanos](#) de la página [Riesgos de seguridad](#).

Nota

Esta nueva función de ERA (análisis de riesgos en los endpoints) está disponible de forma preliminar, y le permite ver solo los riesgos humanos e ignorarlos si son irrelevantes para su entorno. En un futuro próximo se añadirán funciones mejoradas.

Servidores según gravedad

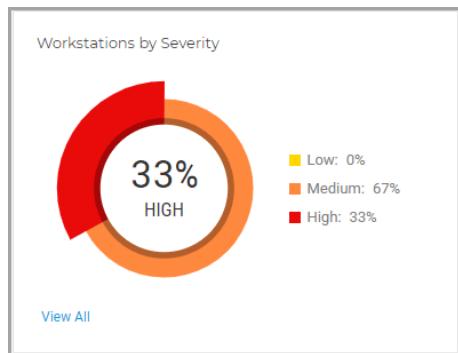
Este widget muestra la gravedad de los riesgos que amenazan a los servidores de su entorno. El impacto de las configuraciones erróneas descubiertas y las vulnerabilidades de aplicaciones se muestran como porcentajes.



Widget de servidores según gravedad

Estaciones de trabajo según gravedad

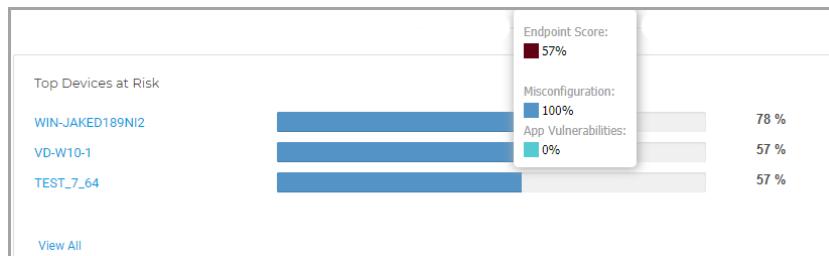
Este widget muestra la gravedad de los riesgos que amenazan a las estaciones de trabajo de su entorno. El impacto de las configuraciones erróneas descubiertas y las vulnerabilidades de aplicaciones se muestran como porcentajes.



Widget de estaciones de trabajo según gravedad

Principales dispositivos en riesgo

Este widget muestra los servidores y estaciones de trabajo más vulnerables de su entorno, según la puntuación general calculada después de analizar en busca de configuraciones erróneas y vulnerabilidades.

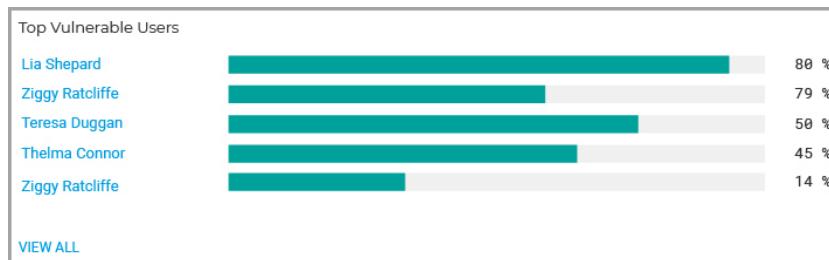


Widget de principales dispositivos en riesgo

Si hace clic en el botón **Ver todo**, verá la lista completa de dispositivos expuestos a amenazas potenciales en la pestaña **Dispositivos** de la página **Riesgos de seguridad**.

Principales usuarios vulnerables

Este widget muestra los usuarios más vulnerables de su entorno, según la puntuación general calculada después de analizar su comportamiento y actividad.



Widget de principales usuarios vulnerables

Si hace clic en el botón **Ver todo**, verá la lista completa de usuarios que pueden estar exponiendo a su organización a amenazas potenciales debido a su comportamiento, en la pestaña **Usuarios** de la página **Riesgos de seguridad**.

10.2. Riesgos de seguridad

Esta página muestra todos los riesgos, dispositivos afectados y usuarios vulnerables descubiertos en su entorno después de ejecutar una tarea de **Análisis de riesgos**.

The screenshot shows the 'Security Risks' section of the Bitdefender GravityZone interface. At the top, there's a search bar with the text 'hydra-is'. Below it, three tabs are visible: 'Misconfigurations' (which is selected and highlighted with a blue border), 'App Vulnerabilities', and 'Devices'. A large blue arrow labeled '1' points from the top right towards the search bar. A smaller blue arrow labeled '2' points down to the 'Misconfigurations' tab. Another small blue arrow labeled '3' points down to the filter icons on the right side of the table.

Misconfigurations	Severity	Mitigation Type	Status
<input type="checkbox"/> Search...	Choose...	Choose...	Choose...
<input checked="" type="checkbox"/> Drive redirection	Medium (50%)	Manual	Active
<input checked="" type="checkbox"/> WinRM Service	Low (10%)	Manual	Active
<input checked="" type="checkbox"/> Write removable drives with BitLocker	Medium (30%)	Automatic	Active
<input type="checkbox"/> WinRM Client Digest Authentication	Medium (50%)	Automatic	Active
<input type="checkbox"/> Windows Ink Workspace	Medium (30%)	Automatic	Active

La página de riesgos de seguridad

Los indicadores de riesgo se muestran en una cuadrícula totalmente personalizable con detalladas opciones de filtrado:

1. Seleccione la empresa que administre cuyos riesgos desee analizar y mitigar.
2. Seleccione qué categoría investigar:
 - [Configuraciones erróneas](#)
 - [Vulnerabilidades de aplicaciones](#)
 - [Riesgos humanos](#)
 - [Dispositivos](#)
 - [Usuarios](#)
3. Use estos botones de acción para personalizar su cuadrícula:

- Haga clic en el botón  Mostrar/Ocultar columnas para añadir o eliminar columnas de filtro.

La página se actualizará automáticamente y cargará las tarjetas de indicadores de riesgo con información que coincida con las columnas añadidas.

Siempre puede restablecer las columnas de filtro con el botón Restablecer del menú desplegable Mostrar/Ocultar columnas.

- Haga clic en el botón  Mostrar/Ocultar filtros para mostrar u ocultar la barra de filtros.
- Haga clic en el botón  Actualizar para actualizar la lista.

Todas las entradas de indicadores se muestran en un formato de tarjeta enriquecido, que proporciona una visión general de cada indicador de riesgo con información basada en los filtros seleccionados.

Configuraciones erróneas

La pestaña **Configuraciones erróneas** muestra por defecto todos los indicadores de riesgo de GravityZone. Proporciona información detallada de su gravedad, número de dispositivos afectados, tipo de configuración errónea, tipo de mitigación (manual o automática) y estado (activo o ignorado).

Para resolver varias configuraciones erróneas a la vez:

1. Marque la casilla de verificación principal o las casillas individuales de los indicadores de riesgo para seleccionarlos.

Misconfigurations	Severity
<input type="checkbox"/> Search...	Choose...
Auto logon	Low (25%)
Telnet Server Service	Low (10%)
UAC insecure	Medium (30%)
<input type="checkbox"/> SMB Shared Everyone Read	Low (20%)

Resolver varios riesgos en la pestaña Configuraciones erróneas

2. Haga clic en el botón **Resolver riesgos**.
Aparece una nueva ventana donde debe confirmar la acción o cancelarla.
3. Se crea una nueva tarea para aplicar la configuración recomendada en todos los dispositivos afectados.



Nota

Puede comprobar el progreso de la tarea en la página **Red > Tareas**.

Si el indicador de riesgo solo puede mitigarse manualmente, debe acceder usted mismo a los dispositivos afectados y aplicar la configuración recomendada.

Para cambiar el estado de las configuraciones erróneas:

1. Marque la casilla de verificación principal o las casillas individuales de los indicadores de riesgo para seleccionarlos de cara al cambio de estado.

Misconfigurations	Severity
<input type="checkbox"/> Drive redirection	Medium (50%)
<input checked="" type="checkbox"/> WinRM Service	Low (10%)
<input checked="" type="checkbox"/> Write removable drives with BitLocker	Medium (30%)
<input type="checkbox"/> WinRM Client Digest Authentication	Medium (50%)

Cambiar el estado de varios riesgos en la pestaña Configuraciones erróneas

2. Haga clic en el botón **Ignorar/Restaurar riesgos** para cambiar el estado de **Activo** a **Ignorado** o viceversa.



Nota

La acción **Ignorar riesgos** se aplica a todos los dispositivos seleccionados e influye en la puntuación general de riesgo de la empresa al realizar un nuevo análisis de riesgos. Le recomendamos encarecidamente que evalúe cómo pueden afectar los indicadores de riesgo ignorados a la seguridad de su organización.

Puede personalizar la información que se muestra en las tarjetas y filtrar las configuraciones erróneas mediante estas opciones:

Opción de filtrado	Detalles
Error de configuración	Esta columna incluye un menú desplegable en el que puede buscar y que le permite filtrar la lista de indicadores por nombre.
Gravedad	Esta columna le permite filtrar la lista de indicadores por el nivel de gravedad de cada indicador de riesgo. Puede seleccionar entre Bajo, Medio y Alto.

Opción de filtrado	Detalles
Dispositivos afectados	Esta columna muestra el número de servidores y estaciones de trabajo que pueden estar expuestos a amenazas por un indicador de riesgo concreto.
Tipo	Esta columna le permite filtrar la lista de indicadores de riesgo por su tipo: <ul style="list-style-type: none">● Seguridad del navegador● Red y credenciales● Seguridad de SO
Tipo de mitigación	Esta columna le permite filtrar la lista de indicadores de riesgo que se pueden mitigar de forma manual o automática.
Estado	Esta columna le permite filtrar la lista de indicadores de riesgo por su estado: Activo o Ignorado.

Haga clic en la configuración errónea que deseé analizar para expandir su panel lateral concreto.

The screenshot shows a detailed configuration panel for a security zone policy. At the top, it says "Security Zones add / delete sites". Below that, there are three sections: "Severity" (Medium (30%)), "Affected Devices" (4), and "Type" (Browser Security). A large blue arrow on the left side points downwards through three numbered sections: 1. "DETAILS", 2. "MITIGATIONS / NETWORK ACTIONS", and 3. "Fix Risk".

1 Severity Medium (30%)
Affected Devices 4
Type Browser Security

2 DETAILS
Verifies the local group policy "Security Zones: Do not allow users to add/delete sites", located in "Computer Configuration > Administrative Templates > Windows Components > Internet Explorer". Prevents users from adding or removing sites from security zones. A security zone is a group of websites with the same security level. If you enable this policy, the site management settings for security zones are disabled. (To see the site management settings for security zones, in the Internet Options dialog box, click the Security tab, and then click the Sites button.)

3 MITIGATIONS / NETWORK ACTIONS
We recommend setting this policy on "Enabled".

Fix Risk

Panel de detalles para configuraciones erróneas

Cada panel contiene lo siguiente:

1. Una sección de información con el nombre del indicador de riesgo, su nivel de gravedad, el número de dispositivos afectados y el tipo.
2. Una sección **Detalles** que describe detalladamente la configuración y sus pautas.
3. Una sección **Mitigaciones** que incluye recomendaciones que minimizan el riesgo en los dispositivos afectados, así como sobre las acciones disponibles:
 - a. Haga clic en el botón **Resolver riesgo** para configurar correctamente este ajuste.
Aparece una nueva ventana donde debe confirmar la acción o cancelarla.
 - b. Se crea una nueva tarea para aplicar la configuración recomendada en todos los dispositivos afectados.



Nota

Puede comprobar el progreso de la tarea en la página **Red > Tareas**.

Si el indicador de riesgo solo puede mitigarse manualmente, debe acceder usted mismo a los dispositivos afectados y aplicar la configuración recomendada.

- c. El botón **Ignorar riesgo** cambia el estado del riesgo seleccionado de **Activo** a **Ignorado**.



Nota

Puede volver a cambiarlo al estado activo en cualquier momento que desee, haciendo clic en el botón **Restaurar riesgo**.

- d. El botón **Ver dispositivos** le conduce a la pestaña **Dispositivos** para ver todos los dispositivos a los que está afectando actualmente este indicador de riesgo.

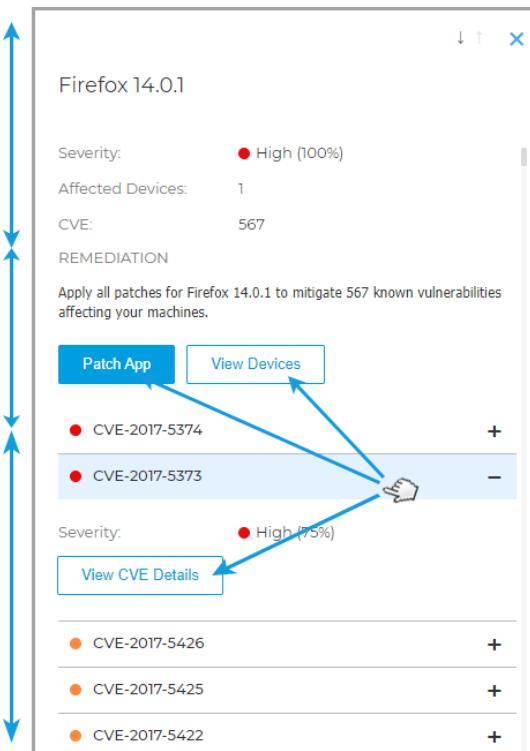
Vulnerabilidades de aplicaciones

La pestaña **Vulnerabilidades de aplicaciones** muestra todas las aplicaciones vulnerables descubiertas en los dispositivos de su entorno durante el análisis. Proporciona información detallada de su nivel de gravedad, el número de CVE conocidos por aplicación y el número de dispositivos afectados.

Puede personalizar la información que se muestra en las tarjetas y filtrar las aplicaciones vulnerables mediante estas opciones:

Opción de filtrado	Detalles
Aplicaciones	Esta columna incluye un menú desplegable en el que puede buscar y que le permite filtrar la lista de aplicaciones vulnerables por nombre.
Gravedad	Esta columna le permite filtrar la lista de aplicaciones vulnerables por el nivel de gravedad de cada aplicación. Puede seleccionar entre Bajo, Medio y Alto.
CVE	Esta columna muestra el número de vulnerabilidades o riesgos comunes (CVE) para las aplicaciones instaladas actualmente en su entorno.
Dispositivos afectados	Esta columna muestra el número de servidores y estaciones de trabajo que pueden estar expuestos a amenazas por un indicador de riesgo concreto.

Haga clic en la aplicación vulnerable que deseé analizar para expandir su panel lateral concreto.



Panel de detalles para aplicaciones vulnerables

Cada panel contiene lo siguiente:

1. Una sección de información con el nombre de la aplicación, el nivel de gravedad, el número de dispositivos a los que afecta y cuántas vulnerabilidades pudieron dañar su entorno.
2. Una sección **Reparación** con acciones de mitigación y una lista de CVE descubiertos:
 - a. Haga clic en el botón **Parchear aplicación** para aplicar los parches disponibles para la aplicación vulnerable.



Importante

La funcionalidad **Parchear aplicación** es solo para dispositivos analizados que tienen instalado el módulo de [Administración de parches](#).

Aparece una nueva ventana donde debe confirmar la acción o cancelarla.

- b. Se creará una nueva tarea para aplicar los parches a aplicaciones vulnerables en todos los dispositivos afectados.



Nota

Puede comprobar el progreso de la tarea en la página [Red > Tareas](#).

- c. El botón **Ignorar riesgo** cambia el estado de la aplicación seleccionada de **Activo** a **Ignorado**.



Nota

Puede volver a cambiarlo al estado activo en cualquier momento que deseé, haciendo clic en el botón **Restaurar aplicación**.

3. Expanda los CVE de la lista y haga clic en el botón **Ver base de datos CVE** para acceder a la base de datos con información específica.

Riesgos humanos

La pestaña **Riesgos humanos** muestra todos los riesgos causados por las acciones imprudentes o involuntarias de los usuarios activos, o la falta de medidas adoptadas para proteger adecuadamente sus sesiones de trabajo mientras están en su red. Proporciona información detallada del nivel de gravedad, el número de usuarios vulnerables, el estado y el tipo de riesgo.



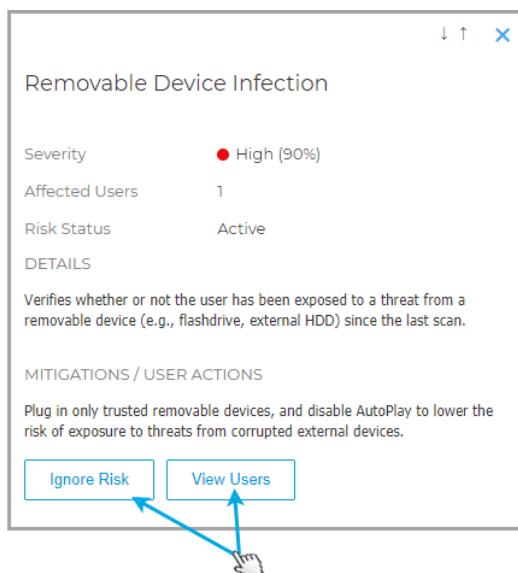
Nota

Consulte [Recopilación de datos sobre riesgos humanos](#) para obtener más detalles sobre cómo procesamos los datos del usuario.

Puede personalizar la información que se muestra en las tarjetas y filtrar los riesgos debidos a los usuarios mediante estas opciones:

Opción de filtrado	Detalles
Riesgos humanos	Esta columna incluye un menú desplegable en el que puede buscar y que le permite filtrar la lista de riesgos humanos por nombre.
Gravedad	Esta columna le permite filtrar la lista de riesgos humanos por su nivel de gravedad. Puede seleccionar entre Bajo, Medio y Alto.
Usuarios vulnerables	Esta columna muestra el número de usuarios que ocasionan riesgos humanos.
Tipo de mitigación	Esta columna le permite filtrar la lista de riesgos que se pueden mitigar de forma manual o automática.
Estado	Esta columna le permite filtrar la lista de riesgos por su estado: Activo o Ignorado.

Haga clic en el riesgo humano que deseé analizar para expandir su panel lateral concreto.



Panel de detalles de riesgos humanos

Cada panel contiene lo siguiente:

1. Una sección de información con el nombre del riesgo, nivel de gravedad, usuarios vulnerables, estado del riesgo y una descripción detallada de este.
2. Una sección **Acciones de usuario/mitigaciones** con acciones de mitigación:
 - a. El botón **Ignorar riesgo** cambia el estado del riesgo seleccionado de **Activo** a **Ignorado**.



Nota

Puede volver a cambiarlo al estado activo en cualquier momento que desee, haciendo clic en el botón **Restaurar riesgo**.

- b. La acción **Ver usuarios** le conduce a la pestaña **Usuarios** para ver todos los usuarios que han desencadenado este riesgo con la actividad en su red.

Dispositivos

La pestaña **Dispositivos** muestra todos los servidores analizados y las estaciones de trabajo que administra. Proporciona información detallada de su nombre, nivel de gravedad, tipo de dispositivo y número de riesgos que le afectan.

Puede personalizar la información que se muestra en las tarjetas y filtrar los dispositivos mediante estas opciones:

Opción de filtrado	Detalles
Dispositivo	Esta columna incluye un menú desplegable en el que puede buscar y que le permite filtrar la lista de servidores y estaciones de trabajo afectados por nombre.
Gravedad	Esta columna le permite filtrar la lista de dispositivos según el nivel de gravedad correspondiente a cada uno de ellos. Puede seleccionar entre Bajo, Medio y Alto.
Configuraciones erróneas	Esta columna muestra el número de configuraciones erróneas descubiertas por dispositivo.
CVE	Esta columna muestra el número de vulnerabilidades o riesgos comunes (CVE) descubiertos por dispositivo.

Opción de filtrado	Detalles
Tipo de dispositivo	Esta columna le permite filtrar la lista de dispositivos por su tipo. Puede seleccionar entre Servidor y Estación de trabajo.

Haga clic en el dispositivo que desee investigar para expandir su panel lateral concreto.

The screenshot shows a detailed view of a device named "VD-W10-1". The top section displays basic statistics: Severity (Medium 57%), Misconfigurations (94), and CVEs (3). Below this, there are two tabs: "Misconfigurations" (selected) and "App Vulnerabilities". Under "Misconfigurations", there is a section titled "Automatically Resolvable Indicators" with a count of 87, accompanied by a green circle icon with a white letter "A". A blue double-headed vertical arrow on the left side of the panel indicates that clicking on the device name will expand this panel. At the bottom of the panel, there are sections for "DETAILS" and "MITIGATIONS / NETWORK ACTIONS".

1

VD-W10-1

Severity: Medium (57%)

Misconfigurations: 94

CVEs: 3

Misconfigurations App Vulnerabilities

87 Automatically Resolvable Indicators

Install ActiveX

DETAILS

Verifies the local group policy "Prevent per-user ActiveX controls", located in "Computer Configuration > Templates > Windows Components > Internet Explorer". This policy setting allows you to prevent the ActiveX controls on a per-user basis. If you enable this policy setting, ActiveX be installed on a per-user basis.

MITIGATIONS / NETWORK ACTIONS

We recommend setting this policy on "Enabled".

2

Panel de detalles para dispositivos

Cada panel contiene lo siguiente:

1. Una sección de información con el nombre del dispositivo, el nivel de gravedad y el número de configuraciones erróneas y vulnerabilidades o riesgos comunes que le afectan.

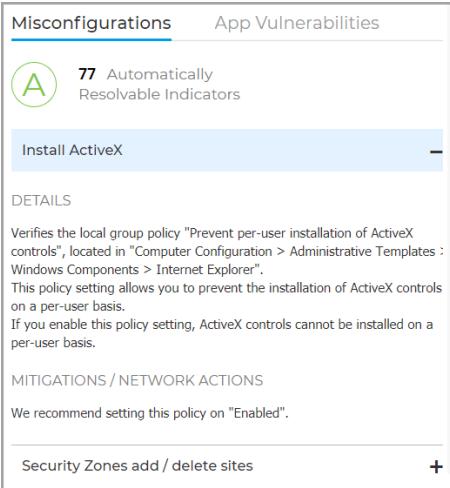
El botón **Ignorar endpoint** cambia el estado del dispositivo seleccionado de **Activo** a **Ignorado**.

Nota

Puede volver a cambiarlo al estado activo en cualquier momento que desee, haciendo clic en el botón **Restaurar endpoint**.

2. Una sección de riesgos que muestra detalladamente cada configuración errónea y aplicación vulnerable descubierta en el dispositivo, agrupadas en dos pestañas.

- La pestaña **Configuraciones erróneas** incluye todas las configuraciones erróneas descubiertas en el dispositivo, agrupadas por indicadores de riesgo que pueden arreglarse automáticamente e indicadores de riesgo que solo pueden resolverse manualmente.



Misconfigurations App Vulnerabilities

 77 Automatically Resolvable Indicators

Install ActiveX

DETAILS

Verifies the local group policy "Prevent per-user installation of ActiveX controls", located in "Computer Configuration > Administrative Templates : Windows Components > Internet Explorer". This policy setting allows you to prevent the installation of ActiveX controls on a per-user basis. If you enable this policy setting, ActiveX controls cannot be installed on a per-user basis.

MITIGATIONS / NETWORK ACTIONS

We recommend setting this policy on "Enabled".

Security Zones add / delete sites +

- a. Haga clic en el botón **Resolver todos los riesgos** para reparar todas las configuraciones erróneas y políticas mal configuradas que afectan a este dispositivo.

Aparece una nueva ventana donde debe confirmar la acción o cancelarla.

- b. Se crea una nueva tarea para aplicar la configuración recomendada en el dispositivo afectado.



Nota

Puede comprobar el progreso de la tarea en la página **Red > Tareas**.

Para los indicadores de riesgo que solo pueden mitigarse manualmente, debe acceder usted mismo al dispositivo afectado y aplicar la configuración recomendada.



Nota

También puede optar por investigar por separado las configuraciones erróneas que afecten al dispositivo actual y resolverlas una por una con el botón **Resolver riesgo**.

- La pestaña **Vulnerabilidades de aplicaciones** incluye todas las aplicaciones vulnerables descubiertas en el dispositivo y el número de CVE que afectan a cada aplicación.

The screenshot shows a user interface for managing application vulnerabilities. At the top, there are two tabs: "Misconfigurations" and "App Vulnerabilities". The "App Vulnerabilities" tab is selected, indicated by a blue underline. Below the tabs, a message says "2 Applications that needs patching". Underneath, there are two entries: "7-zip 16.00" with a minus sign to its right, and "Notepad 7.6.2" with a plus sign to its right. To the left of each entry, there is a "CVEs:" label followed by the number "2".

- a. Haga clic en el botón **Parchear todas las aplicaciones** para aplicar los parches disponibles a todas las aplicaciones vulnerables que exponen el dispositivo seleccionado a las amenazas.



Importante

Parchear todas las aplicaciones funciona solo en los dispositivos analizados que tienen instalado el módulo de [Administración de parches](#).

Aparece una nueva ventana donde debe confirmar la acción o cancelarla.

- b. Se creará una nueva tarea para aplicar los parches a las aplicaciones vulnerables en el dispositivo afectado.

**Nota**

Puede comprobar el progreso de la tarea en la página **Red > Tareas**.

**Nota**

También puede optar por investigar por separado las aplicaciones vulnerables que afecten al dispositivo actual y parchearlas una por una con el botón **Parchear aplicación**.

Usuarios

La pestaña **Usuarios** muestra todos los usuarios que, intencionadamente o no, exponen su entorno a las amenazas. Proporciona información como el nombre de usuario, el nivel de gravedad general del riesgo de ese usuario, el cargo y el departamento del usuario, el número de riesgos a los que están expuestos y su estado al calcular el riesgo general de la empresa.

Puede personalizar la información que se muestra en las tarjetas y filtrar los dispositivos mediante estas opciones:

Opción de filtrado	Detalles
Usuarios	Esta columna incluye un campo en el que puede buscar y que le permite filtrar la lista de usuarios vulnerables por nombre.
Gravedad	Esta columna le permite filtrar la lista de usuarios vulnerables por su nivel de gravedad. Puede seleccionar entre Bajo, Medio y Alto.
N.º de riesgos	Esta columna muestra el número de riesgos humanos correspondiente a cada usuario.
Título	Esta columna le permite filtrar la lista de usuarios por su cargo en la organización.
Departamento	Esta columna le permite filtrar la lista de usuarios por departamento al que pertenecen en la organización.
Estado	Esta columna le permite filtrar la lista de usuarios por su estado: Activo o Ignorado.

Haga clic en el usuario que deseé investigar para expandir su panel lateral concreto.

Panel de detalles para usuarios

Cada panel contiene lo siguiente:

1. Una sección de información con el nombre del usuario, su cargo y departamento, información de contacto, nivel de gravedad y estado.
2. Una sección **Acciones de usuario/mitigaciones** con acciones de mitigación:

- a. El botón **Ignorar usuario** cambia el estado del usuario seleccionado de **Activo** a **Ignorado**.

**Nota**

Puede volver a cambiarlo al estado activo en cualquier momento que desee, haciendo clic en el botón **Restaurar usuario**.

11. 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).

11.1. Tipos de informes

Para cada tipo de endpoint hay disponibles distintos tipos de informe:

- **Informes de equipos y máquinas virtuales**

- [Informes de Exchange](#)

11.1.1. 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 contenido, Antiexploit avanzado y ATC/IDS. 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 y Cortafuego. Aparecerá una ventana de confirmación que le informará de la nueva regla que modificará la política existente para ese endpoint concreto.

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 dispositivo 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.
- Nombre de la empresa.

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.

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.

Uso de licencia mensual

Haga clic en los números en cada columna para ver los detalles de cada módulo y complemento disponible. Puede personalizar fácilmente el informe haciendo clic en el botón **Mostrar/Ocultar columnas**.

Email Security - Uso de licencia mensual

Este informe proporciona el uso de licencia para el servicio Email Security. Todos los intervalos de informes obtienen la información del uso de licencia hasta el final del día anterior. Por ejemplo, genera un informe el lunes a las 12 p. m. y establece el intervalo en **Este mes**. El informe proporcionará información sobre el uso de licencia hasta el final del domingo.

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 reinicio, el código de error devuelto, la descripción de cada reinicio 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. 481).

- 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 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.

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.

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.

11.1.2. 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 - Uso de licencia mensual

Proporciona información detallada concerniente al uso de la licencia de Security for Exchange por parte de su empresa en un período de tiempo determinado.

La tabla debajo del gráfico ofrece detalles sobre el nombre de la empresa y la clave de licencia, así como el mes y el número de buzones protegidos pertenecientes a su empresa.

El número de licencias utilizadas sirve de enlace a una nueva ventana en la que puede encontrar información de uso detallada, como dominios licenciados en su empresa y sus buzones.

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.

11.2. 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. Haga clic en el botón **Añadir** en la parte superior de la tabla. Se muestra una ventana de configuración.

Crear Informe X

Detalles

Tipo:

Nombre: *

Configuración

Ahora
 Programado

Intervalo de informe:

Mostrar: Todos los puntos finales
 Solo los puntos finales con sitios Web bloqueados

Entregar: Enviar por correo a las

Generar **Cancelar**

Opciones de informe

3. Seleccione el tipo de informe deseado desde el menú. Para obtener más información, consulte "[Tipos de informes](#)" (p. 409)
4. Escriba un nombre descriptivo para el informe. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.
5. Configure la recurrencia del informe:
 - Seleccione **Ahora** para crear un informe instantáneo.
 - Seleccione **Programado** para establecer que el informe se genere automáticamente en el intervalo de tiempo que desee:
 - Cada hora, en el intervalo especificado entre horas.
 - Diariamente. En este caso, también puede establecer la hora de inicio (horas y minutos).
 - Semanalmente, en los días especificados de la semana y a la hora de inicio seleccionada (horas y minutos).

- Mensualmente, en los días especificados del mes y a la hora de inicio seleccionada (horas y minutos).
6. Para la mayoría de tipos de informe debe especificar el intervalo de tiempo al que se refieren los datos que contienen. El informe mostrará únicamente información sobre el periodo de tiempo seleccionado.
7. Varios tipos de informes ofrecen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Utilice las opciones de filtrado en la sección **Mostrar** para obtener únicamente la información deseada. Por ejemplo, para un informe de **Estado de actualización** puede seleccionar ver únicamente la lista de objetos de red que no se hayan actualizado, o los que necesiten reiniciarse para completar la actualización.
8. **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.
9. **Seleccionar objetivo.** Desplácese hacia abajo para configurar el objetivo del informe. Seleccione uno o varios grupos de endpoints que desee incluir en el informe.
10. 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**.

11.3. Ver y administrar informes programados

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

Nombre del informe	Tipo	Recurrencia	Ver informe
Informe de estado de actualización	Actualización	Cada hora	25 Sep 2015 - 17:40

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.

11.3.1. 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. 432)

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.

11.3.2. 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.

11.3.3. 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.

11.4. 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:

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.

11.5. Guardar Informes

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

Si necesita que los informes estén disponibles durante períodos 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](#)

11.5.1. 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.

11.5.2. 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.

11.6. 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.

11.7. 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.

12. 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.

12.1. Exploración de la cuarentena

La página **Cuarentena** proporciona información detallada acerca de los archivos en cuarentena de todos los endpoints que usted administra.

Equipo	IP	Empresa	Archivo	Nombre de la amenaza	Aislado en	Estado acción
[Equipment]	10.10.195.199	[Company]	C:\users\astanica\appdata\local\vr	EICAR-Test-File (not a virus)	11 May 2018, 15:45:31	Ninguno
[Equipment]	10.10.195.199	[Company]	C:\delecar\0000001.txt	EICAR-Test-File (not a virus)	11 May 2018, 11:13:16	Ninguno

La página Cuarentena

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.

12.2. 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. 181).

12.2.1. 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.

12.2.2. 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.

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. Marque las casillas de verificación correspondientes a los archivos en cuarentena que deseé restaurar.
3. Haga clic en el botón  **Restaurar** de la zona superior de la tabla.
4. Elija la ubicación donde desea que sean restaurados los archivos seleccionados (bien sea la ubicación original o una personalizada del equipo objetivo).
Si elige restaurar en una ubicación personalizada, debe introducir la ruta absoluta en el campo correspondiente.
5. Seleccione **Añadir exclusión en política automáticamente** para excluir los archivos a restaurar de análisis futuros. La exclusión se aplica a todas las políticas que afecten a los archivos seleccionados, a excepción de la política por defecto, que no se puede modificar.
6. Haga clic en **Guardar** para solicitar la acción de restauración del archivo. Puede observar el estado pendiente en la columna **Acción**.
7. 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.

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. Marque las casillas de verificación correspondientes a los archivos en cuarentena que deseé eliminar.
3. 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. Haga clic en el botón **Vaciar cuarentena**.

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.

12.3. 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.

12.3.1. 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.

12.3.2. 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 guardarla 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 deseé 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 deseé 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” \(p. 182\)](#)”.

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 15 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 deseé 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**.

Se borrarán todos los elementos de la tabla Cuarentena. La acción solicitada se envía inmediatamente a los objetos de la red objetivo.

13. 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:

The screenshot shows the Bitdefender GravityZone interface with the 'Sandbox Analyzer' tab selected. On the left, there's a sidebar with various navigation options like 'Panel de Control', 'Incidentes', 'Lista de Bloqueo', 'Buscar', 'Red', 'Inventario de parches', 'Paquetes', 'Tareas', 'Políticas', 'Reglas de asignación', 'Informes', 'Cuarentena', 'Empresas', 'Cuentas', 'Actividad del usuario', 'Sandbox Analyzer', and 'Envío manual'. The main area has a header with 'Sandbox Analyzer', a search bar, and filter buttons. Below is a chart showing 'Puntuación de gravedad' (Severity Score) from 0 to 100, with a red bar at 0. A legend indicates 'Limpio' (Clean), 'Infected' (Infected), and 'Incompatible'. A 'Tipo de envío' (Type of delivery) section shows 'Manual' and 'Automático'. An 'Estado del envío' (Delivery status) section shows 'Finalizado', 'Análisis pendiente', and 'Fallido'. A 'ATT&CK Techniques' section is empty. The main content area shows a table with three rows of analysis results:

Estado	Nombre del envío	Puntuación de gravedad	Archivos y procesos	Enviado desde	Entorno	Opciones
Limpio	Bitdefender_GravityZone_Inhalation.pdf	0	Indetectado	N/A	Sandbox en la nube	Visualización >
Limpio	https://www.bitdefender.org/	0	Indetectado	N/A	Sandbox en la nube	Visualización >
Incompatible	ad-ID.PNG	N/A	Indetectado	N/A	Sandbox en la nube	Visualización >
NDOS	ad-ID.PNG - N/A	N/A				Eliminar entrada

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 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](#)
- [Eliminar tarjetas de envíos](#)
- [Realizar envíos manuales](#)

13.1. 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. 481).
- **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.
 - **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.
 - **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.

13.2. 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 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.

13.3. 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.

13.4. 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. 17).

Subir Configuración general

Ejemplos

Archivos

Explorar

Proporcione una contraseña para los archivos cifrados:

Ha de añadir las contraseñas una a una. Si carga varios archivos cifrados, Sandbox Analyzer utilizará la misma contraseña para todos.

URL

Ajustes de detonación

Argumentos de línea de comandos: ⓘ

Detonar muestras individualmente

Enviar

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:
 - **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 esta 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**.

14. 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
- Iniciar, finalizar, cancelar y detener procesos de solución de problemas en las máquinas afectadas
- Editar los ajustes de autenticación para las cuentas de GravityZone.

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

Usuario	Rol	Acción	Área	Objetivo	Empresa	PABD	Buscar

Usuario	Rol	Acción	Área	Objetivo	Creado

La página de actividad del usuario

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

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

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

- Objeto de consola concreto afectado por la acción.
- Hora en la que sucedió el evento.

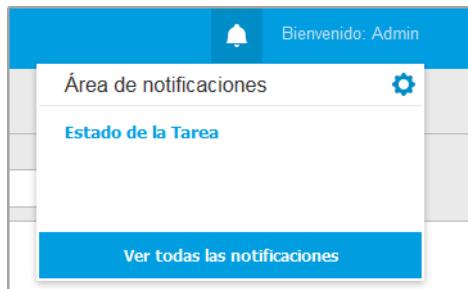
Para ordenar eventos por una columna específica, simplemente haga clic en el encabezado de esa columna. Haga clic en el encabezado de la columna nuevamente para invertir el sentido de ordenación.

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

15. USO DE HERRAMIENTAS

16. 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 ícono  de la esquina superior derecha de Control Center mostrará el número de nuevos eventos detectados. Haciendo clic en dicho ícono se muestra el área de notificaciones que contiene la lista de eventos detectados.

16.1. 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" \(p. 463\)](#)".

Las amenazas detectadas por HyperDetect no se incluyen en esta notificación.

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.

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.

Se ha alcanzado el límite de utilización de licencias de los servidores

Esta notificación se envía cuando el número de servidores protegidos alcanza el límite especificado en su clave de licencia.

Debe tener privilegios de **administración de empresa** para ver esta notificación.

Está a punto de alcanzarse el límite de licencias de los servidores

Esta notificación se envía cuando se ha utilizado el 90 % de los puestos de licencia disponibles para los servidores.

Debe tener privilegios de **administración de empresa** para ver esta notificación.

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.

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 Syslog: CEF

Estado de actualización

Esta notificación se activa semanalmente si se encuentran versiones antiguas de productos en su red.

Antiexploit avanzado

Esta notificación le informa de si el Antiexploit avanzado ha detectado un intento de exploit en su red.

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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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 Syslog: 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.

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.

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.

También puede recibir esta notificación para las tareas de análisis activadas a través de NTSA.

Disponibilidad de formato Syslog: 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 Syslog: 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.

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 la empresa, 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 sobre las muestras enviadas por su empresa está disponible en el informe **Resultados de Sandbox Analyzer (en desuso)**. La información sobre las muestras enviadas por su empresa también está disponible en la sección **Sandbox Analyzer**, en el menú principal de Control Center.

Disponibilidad de formato Syslog: CEF

Actividad de Hiperdetección

Esta notificación le comunica cuándo HyperDetect encuentra cualquier evento de antimalware o sin bloquear en su red. Esta notificación se envía para cada evento de HyperDetect y proporciona la siguiente información:

- Información del endpoint afectado (nombre, IP, agente instalado).
- Tipo y nombre del malware.
- Ruta del archivo infectado. En el caso de los ataques sin archivos, se proporciona el nombre del ejecutable utilizado en el ataque.
- Estado de infección
- El hash SHA256 del ejecutable del malware.
- El tipo de ataque previsto (ataque selectivo, grayware, exploits, ransomware, archivos sospechosos y tráfico de red)
- Nivel de detección (Tolerante, Normal o Agresivo).
- Fecha y hora de la detección.

Disponibilidad de formato Syslog: CEF

Puede ver información detallada sobre la infección y seguir investigando las incidencias generando un informe de **Actividad de HyperDetect** directamente desde la página de **notificaciones**. Para ello:

1. En Control Center, haga clic en el botón  **Notificación** para mostrar el área de notificaciones.
2. Haga clic en el enlace **Mostrar más** al final de la notificación para abrir la página **Notificaciones**.
3. Haga clic en el botón **Ver informe** en los detalles de la notificación. Esto abre la ventana de configuración de informes.
4. Configure el informe en caso necesario. Para más información, diríjase a ["Creando Informes" \(p. 425\)](#).
5. Haga clic en **Generar**.

**Nota**

Para evitar saturar su buzón, recibirá un máximo de una notificación por hora.

Problema de integración de Active Directory

Esta notificación le informa de las incidencias que afectan a la sincronización con Active Directory.

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. La notificación se envía a todas sus cuentas de usuario.

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 Syslog: CEF

Nuevo incidente

Recibe esta notificación cuando se produce un nuevo incidente. Una vez habilitada, la notificación se genera cada vez que se muestra un nuevo incidente en la sección **Incidentes** del Control Center. Para obtener más información, haga clic en el **Nombre del incidente**.

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.

16.2. 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.

Tipo	Creado
<input type="checkbox"/> Estado de la Tarea	19 Ago 2015, 15:15:14

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.

16.3. 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 deseé eliminar.
3. Haga clic en el botón  **Eliminar** de la zona superior de la tabla.

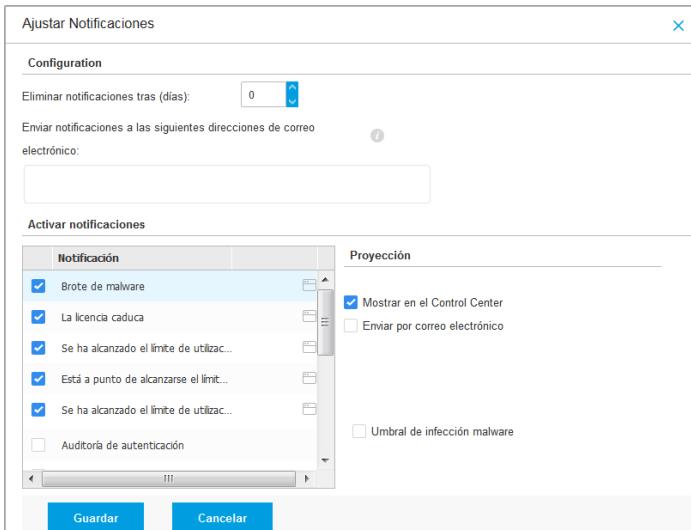
También puede configurar las notificaciones para que se borren automáticamente tras un cierto número de días. Para más información, diríjase a “[Configurar las opciones de notificación](#)” (p. 463).

16.4. 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 ícono  **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 1 y 365 en el campo **Eliminar notificaciones tras (días)**.
 - 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 deseé. Para más información, diríjase a “[Tipo de notificaciones](#)” (p. 456). 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**.
- **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 deseé en el campo **Umbral de infección malware**.

- 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**.

17. 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 proporcionará la asistencia que necesite.

Nota

Puede encontrar información sobre los servicios y políticas de soporte que ofrecemos en nuestro Centro de Soporte técnico.

17.1. 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.

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.

17.2. Solicitar ayuda

Puede solicitar ayuda a través de nuestro Centro de soporte técnico online: Rellene el [formulario de contacto](#) y envíelo.

17.3. 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.

17.3.1. 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_[computernname]_[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_[computernname]_[currentdate]. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

17.3.2. 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.

17.3.3. 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.

17.4. 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.

17.4.1. 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>

17.4.2. 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.

17.4.3. 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 1^a

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; 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; ffp; 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; 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; oox; 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; slidx; 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; xl; 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 ícono determinado.

En la tabla que se muestra a continuación hallará el ícono y la descripción de todos los tipos de objeto disponibles.

ícono	Tipo
	Grupo de red
	Equipo
	Equipo de relay
	Equipo del integrador de Active Directory
	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
	Security Server

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.

ícono	Estado
	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; fpx; 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; rlx; 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; 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. Objetos Sandbox Analyzer

A.6.1. 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.6.2. 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.6.3. Exclusiones predeterminadas del envío automático

`asc`, `avi`, `bmp`, `gif`, `jpeg`, `jpg`, `mkv`, `mp4`, `pgp`, `png` y `txt`.

A.7. Recopilación de datos sobre riesgos humanos

Recopilamos y almacenamos temporalmente datos confidenciales, exclusivamente a nivel local (en la estación de trabajo del usuario), con el único propósito de generar alertas sobre posibles amenazas a las que su empresa pueda verse expuesta por el comportamiento del usuario. No guardamos datos de carácter personal como nombres de usuario y contraseñas en forma de texto sin formato en ninguna base de datos en la nube.

Los datos locales que recopilamos se eliminan periódicamente y pueden incluir solo hashes de nombres de usuario y contraseñas, el número total de sitios web de riesgo a los que se ha accedido en determinado período de tiempo y las URL de algunos de estos sitios web sospechosos, así como las IP de sus dominios.

La siguiente tabla describe los comportamientos de los usuarios que monitoriza el ERA (análisis de riesgos en los endpoints) y la forma en que procesa y recopila los datos de los usuarios.

Nombre Regla	Descripción	Tipo	Información recopilada
Credenciales HTTP estándar	Comprueba si el usuario ha enviado o no credenciales mediante	contraseñas	Comprueba si el usuario usa las mismas contraseñas en diferentes

Nombre Regla	Descripción	Tipo	Información recopilada
	conexiones HTTP inseguras desde el último análisis.		sitios externos. Este escenario se habilita cuando detectamos al menos dos sitios web externos con la misma contraseña.
Contraseña HTTP externa compartida	Comprobamos si el usuario accede a sitios web inseguros (HTTP) y almacenamos el número de sitios web a los que se ha accedido y el momento en que se ha hecho.	contraseñas	Almacenamos localmente el hash de las contraseñas (formato CRC32) introducidas en sitios externos, así como las URL a las que se accede, las IP de los dominios y el nombre de usuario.
Contraseña HTTP interna compartida con externa	Comprueba si el usuario usa las mismas contraseñas compartidas entre sitios web internos y externos.	contraseñas	Almacenamos localmente el hash de las contraseñas (formato CRC32) introducidas en sitios externos e internos, así como las URL a las que se accede y las IP de los dominios.
Navegación de alto riesgo	Comprueba si el usuario ha navegado o no por sitios de phishing o fraude desde el último análisis. Este escenario se activa cuando el número de sitios web inseguros a los que se accede supera el umbral actual.	navegación	Solo almacenamos localmente el número de sitios web de alto riesgo a los que se ha accedido durante un período de tiempo determinado y sus URL.
Gran número de detecciones	Comprueba si el usuario ha estado expuesto a una gran cantidad de	detecciones	Almacenamos localmente el número de detecciones desencadenadas durante

Nombre Regla	Descripción	Tipo	Información recopilada
	amenazas desde el último análisis. El escenario se activa cuando el número de detecciones por usuario supera el umbral preestablecido..		un período de tiempo determinado.
Infección de dispositivos extraíbles	Comprueba si el usuario ha estado expuesto a una amenaza de un dispositivo extraíble (p. ej.: unidades flash o discos duros externos) desde el último análisis.	detecciones	Almacenamos localmente las detecciones desencadenadas durante un período de tiempo determinado y la fuente de la infección (archivo USB/CD/ISO).
Infección de SMB	Comprueba si el usuario ha accedido a algún archivo malicioso en una carpeta compartida de red desde el último análisis.	detecciones	Almacenamos localmente los eventos de acceso a archivos que se originan en carpetas compartidas de red o puntos compartidos.
Infección de navegación	Comprueba si el usuario ha accedido a alguna URL maliciosa desde el último análisis.	detecciones	Almacenamos localmente las URL maliciosas o sospechosas y las contamos.
Gran número de detecciones a lo largo del tiempo	Comprueba si el usuario ha estado expuesto a un número muy alto de amenazas durante un período de tiempo determinado.	detecciones	Almacenamos localmente el número de infecciones durante un período de tiempo determinado.
Contraseña HTTP externa compartida	Comprueba si el usuario no cambia periódicamente las contraseñas de los sitios web externos.	contraseñas	Almacenamos localmente lo siguiente: hashes de contraseña (formato CRC32), hash del nombre de usuario y las URL de sitios web externos que

Nombre Regla	Descripción	Tipo	Información recopilada
Contraseña de usuario antigua	Comprueba si el usuario no ha cambiado la contraseña de inicio de sesión para la cuenta (local o de dominio) desde hace más de treinta días.	contraseñas	desencadenaron este comportamiento, así como las IP de los dominios. No almacenamos nada localmente. Llamamos a una función de Active Directory que devuelve la última vez que se cambió la contraseña de un usuario.

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 contenido ficheros almacenados.

Fichero contenido 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 ícono 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".

IoR

Indicador de riesgo: se refiere a un valor de clave de registro o datos de determinado ajuste del sistema o una vulnerabilidad de aplicación conocida.

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.

Malware

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.

No Heurístico

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

Phishing

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

Puerto

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

En las redes de tipo TCP/IP y UDP representa el 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 periféricos, 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 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.