

IBM QRadar  
Versión 7.4.1

*Guía del usuario*



**Nota**

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 231.

**Información sobre el producto**

Este documento se aplica a IBM® QRadar Security Intelligence Platform 7.4.1 y a los releases subsiguientes a menos que se reemplace por una versión actualizada de este documento.

© Copyright International Business Machines Corporation 2012, 2020.

---

# Contenido

<b>Información preliminar.....</b>	<b>ix</b>
<b>Capítulo 1. Novedades para los usuarios de QRadar.....</b>	<b>1</b>
Nuevas características y mejoras en QRadar 7.4.1.....	1
Nuevas características y mejoras en QRadar 7.4.0.....	1
<b>Capítulo 2. Prestaciones de su producto IBM QRadar.....</b>	<b>3</b>
Navegadores web soportados .....	4
Habilitación del modo de documento y modo de explorador en Internet Explorer.....	5
Inicio de sesión de IBM QRadar.....	5
API RESTful .....	5
Pestañas de interfaz de usuario.....	6
Pestaña Panel de control.....	6
Puede utilizar la pestaña Delitos para ver delitos que se producen en la red.....	6
Pestaña Actividad de registro.....	7
Utilización de la pestaña Actividad de red para investigar flujos.....	8
Pestaña Activos.....	9
Pestaña Informes.....	10
Utilización del dispositivo de QRadar Risk Manager.....	11
Procedimientos comunes de QRadar.....	11
Visualización de notificaciones.....	11
Renovación y pausa de QRadar.....	12
Investigación de direcciones IP.....	13
Hora del sistema.....	15
Actualización de preferencias de usuario.....	15
<b>Capítulo 3. Gestión de panel de control.....</b>	<b>17</b>
Paneles de control predeterminados.....	17
Paneles de control personalizados.....	19
Elementos de la búsqueda de flujos.....	19
Añadir elementos relacionados con delitos al panel de control.....	20
Actividad de registro.....	21
Resumen del sistema.....	22
Panel de control de supervisión de riesgos.....	22
Supervisar el cumplimiento de políticas.....	23
Supervisar el cambio de riesgo.....	25
Elementos de Gestión de vulnerabilidades.....	25
Notificación del sistema.....	26
Centro de información de amenazas de Internet.....	27
Crear un panel de control personalizado.....	27
Investigar actividad de registro o actividad de red.....	27
Configuración de tipos de gráficos de panel de control.....	28
Eliminación de elementos de panel de control.....	29
Desconexión de un elemento del panel de control.....	29
Renombrar un panel de control .....	30
Supresión de un panel de control.....	30
Gestión de notificaciones del sistema.....	30
Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos...	31
<b>Capítulo 4. Gestión de delitos.....</b>	<b>33</b>

Priorización de delitos.....	33
Encadenamiento de delitos.....	33
Indexación de delitos.....	34
Consideraciones sobre la indexación de delitos.....	34
Ejemplo: Detección de irrupciones de programas maliciosos en función de la firma MD5.....	35
Retención de delitos.....	35
Proteger delitos.....	36
Desproteger delitos.....	36
Investigaciones de delitos.....	37
Seleccionar un delito para investigar.....	38
Investigar un delito mediante la información de resumen.....	39
Investigación de sucesos.....	43
Investigación de flujos.....	44
Acciones de delitos.....	45
Añadir notas.....	45
Ocultar delitos.....	45
Mostrar delitos ocultos.....	46
Cerrar delitos.....	46
Exportar delitos.....	47
Asignar delitos a usuarios.....	47
Enviar notificaciones de correo electrónico.....	48
Marcado de un delito para su seguimiento.....	49

## **Capítulo 5. QRadar Analyst Workflow.....51**

Novedades de QRadar Analyst Workflow.....	51
Problemas conocidos.....	51
Instalación de QRadar Analyst Workflow.....	52
Delitos.....	52
Visualización de delitos.....	53
Investigación de delitos.....	54
Acciones de delitos.....	54
Consulta de datos de sucesos y flujos para encontrar delitos específicos.....	56
Sucesos.....	57
Investigación de sucesos.....	57
Filtrado de sucesos.....	58

## **Capítulo 6. Investigación de la actividad de registro..... 59**

Visión general de la pestaña Actividad de registro.....	59
Barra de herramientas de pestaña Actividad de registro.....	59
Opciones de menú que aparecen al pulsar el botón derecho del ratón.....	63
Resultados de barra de estado.....	64
Supervisión de actividad de registro.....	64
Ver sucesos en modalidad continua.....	64
Ver sucesos normalizados.....	65
Ver sucesos en bruto.....	68
Ver sucesos agrupados.....	70
Ver una lista de sucesos y detalles de suceso en diversas modalidades en la página de detalles de suceso.....	75
Funciones de barra de herramientas de detalles de suceso.....	80
Ver delitos asociados.....	81
Modificación de la correlación de sucesos.....	82
Ajustar sucesos de falso positivo para que no generen delitos .....	82
Datos de PCAP.....	83
Visualización de la columna de datos de PCAP.....	83
Visualización de la información de PCAP.....	84
Descarga del archivo de PCAP en el sistema.....	85
Exportación de sucesos.....	85

<b>Capítulo 7. Supervisión de la actividad de red.....</b>	<b>87</b>
Establecimiento de registros de desbordamiento de datos.....	87
Ver flujos continuos en tiempo real desde la pestaña <b>Actividad de red</b> .....	87
Ver flujos normalizados.....	88
Ver flujos agrupados.....	88
<b>Capítulo 8. Utilización de la función Ajuste de falsos positivos para impedir que flujos de falso positivo generen delitos.....</b>	<b>91</b>
<b>Capítulo 9. Exportar flujos.....</b>	<b>93</b>
<b>Capítulo 10. Gestión de activos.....</b>	<b>95</b>
Orígenes de datos de activos.....	96
Flujo de trabajo de datos de activos entrantes.....	97
Actualizaciones de los datos de activos.....	99
Reglas de exclusión de conciliación de activos.....	99
Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra.....	101
Fusión de activos.....	101
Identificación de desviaciones de crecimiento de activos.....	102
Notificaciones del sistema que indican desviaciones de crecimiento de activos.....	103
Ejemplo: Cómo los errores de configuración de las extensiones de origen de registro pueden provocar desviaciones de crecimiento de activos.....	103
Resolución de problemas con perfiles de activo que sobrepasan el umbral de tamaño normal....	104
Los datos de activos nuevos se añaden a las listas negras de activos.....	104
Listas negras y listas blancas de activos.....	105
Listas negras de activos.....	105
Listas blancas de activos.....	106
Perfiles de activo.....	107
Vulnerabilidades.....	107
Visión general de la pestaña Activos.....	108
Visualización de un perfil de activo.....	108
Adición o edición de un perfil de activo.....	110
Búsqueda de perfiles de activo en la página <b>Activo</b> en la pestaña Activos.....	114
Guardar criterios de búsqueda de activos.....	115
Grupos de búsqueda de activos.....	116
Tareas de gestión de perfiles de activo.....	118
Investigar vulnerabilidades de activo.....	119
<b>Capítulo 11. Gestión de gráficos.....</b>	<b>123</b>
Visión general de gráfico de serie temporal.....	123
Leyendas de gráficos.....	124
Configuración de gráficos.....	125
<b>Capítulo 12. Búsquedas de sucesos y flujos.....</b>	<b>127</b>
Creación de una búsqueda personalizada.....	127
Creación de un diseño de columna personalizado.....	132
Supresión de un diseño de columna personalizado.....	133
Guardar criterios de búsqueda .....	133
Búsqueda planificada.....	134
Opciones de búsqueda avanzada.....	135
Ejemplos de series de búsqueda de AQL.....	137
Convertir una búsqueda guardada en una serie de AQL.....	140
Opciones de búsqueda de Filtro rápido.....	141
Identificar si se ha invertido la dirección del flujo o no.....	143

Valores de algoritmo de dirección del flujo.....	144
Personalización de búsquedas para mostrar el algoritmo de dirección del flujo.....	144
Identificación de la definición de campos de aplicación para un flujo.....	144
Valores de algoritmos de determinación de aplicación.....	145
Personalización de búsquedas para mostrar el algoritmo de determinación de aplicación.....	145
Visualización de la descripción de datos de flujo de AWS enumerados.....	146
Información de VLAN en registros de flujo de actividad de red.....	147
Asignar dominios y arrendatarios a flujos con información de VLAN.....	148
Visibilidad de los flujos de MPLS recibidos de los datos de IPFIX.....	148
Búsquedas de delitos.....	152
Buscar delitos en las páginas Mis delitos y Todos los delitos.....	152
Buscar delitos en la página <b>Por IP de origen</b> de la pestaña Delito.....	159
Buscar delitos en la página <b>Por IP de destino</b> de la pestaña <b>Delito</b> .....	161
Buscar delitos en la página <b>Por red</b> de la pestaña <b>Delito</b> .....	163
Guardar criterios de búsqueda en la pestaña <b>Delitos</b> para reutilizarlos en búsquedas futuras.....	163
Buscar delitos indexados en función de una propiedad personalizada.....	164
Buscar IOCs de forma rápida con la búsqueda perezosa.....	165
Supresión de criterios de búsqueda.....	166
Utilización de una sub-búsqueda para refinar los resultados de búsqueda.....	166
Gestión de búsquedas.....	167
Cancelación de una búsqueda.....	167
Supresión de una búsqueda.....	168
Gestión de grupos de búsqueda.....	168
Visualización de grupos de búsqueda.....	168
Creación de un grupo de búsqueda nuevo.....	169
Edición de un grupo de búsqueda.....	169
Copia de una búsqueda guardada en otro grupo.....	170
Eliminación de un grupo o una búsqueda guardada de un grupo.....	170
Ejemplo de búsqueda: Informes de empleados diarios.....	171
<b>Capítulo 13. Propiedades de suceso y de flujo personalizadas.....</b>	<b>173</b>
Creación de una propiedad personalizada.....	174
Modificación o supresión de una propiedad personalizada.....	175
Definición de propiedades personalizadas mediante expresiones de propiedades personalizadas...	175
Caso práctico: Crear un informe que utiliza datos de suceso que no están normalizados.....	180
<b>Capítulo 14. Reglas.....</b>	<b>183</b>
Reglas personalizadas.....	184
Creación de una regla personalizada.....	185
Configuración de un suceso o flujo como falso positivo.....	190
Reglas de detección de anomalías.....	190
Creación de una regla de detección de anomalías.....	193
Configuración de una respuesta de regla para añadir datos a una recopilación de datos de referencia.....	197
Editar componentes básicos.....	198
Visualización del rendimiento de las reglas .....	199
<b>Capítulo 15. Correlación histórica.....</b>	<b>203</b>
Visión general de la correlación histórica.....	203
Creación de un perfil de correlación histórica.....	204
Visualización de la información sobre ejecuciones de correlación histórica.....	205
<b>Capítulo 16. Integración de IBM X-Force.....</b>	<b>207</b>
X-Force datos en el panel de control.....	207
Aplicación IBM Security Threat Content.....	208
Habilitación de reglas de X-Force en IBM QRadar.....	208
Categorías de dirección IP y URL.....	208

Búsqueda de información de direcciones IP y URL en X-Force Exchange.....	209
Creación de una regla de categorización de URL para supervisar el acceso a determinados tipos de sitios web.....	209
Factor de confianza y reputación de dirección IP.....	210
Ajustar falsos positivos con el valor de factor de confianza.....	210
Buscar datos de IBM X-Force Exchange con criterios de búsqueda avanzados.....	211
<b>Capítulo 17. Gestión de informes.....</b>	<b>213</b>
Diseño de informe.....	213
Tipos de gráfico.....	214
Barra de herramientas de la pestaña de informes.....	216
Tipos de gráfico.....	218
Creación de informes personalizados.....	219
Edición de informes que utilizan el Asistente de informes.....	223
Visualización de informes generados.....	223
Supresión de contenido generado.....	224
Generación manual de un informe.....	224
Duplicación de un informe.....	224
Compartición de un informe.....	225
Creación de marca de informes.....	225
Grupos de informes.....	226
Creación de un grupo de informes.....	226
Edición de un grupo.....	226
Compartición de grupos de informes.....	227
Asignar un informe a un grupo.....	228
Copia de un informe en otro grupo.....	228
Eliminación de un informe.....	228
<b>Avisos.....</b>	<b>231</b>
Marcas registradas.....	232
Términos y condiciones de la documentación de producto.....	232
Declaración de privacidad en línea de IBM.....	233
Reglamento general de protección de datos.....	234
<b>Glosario.....</b>	<b>235</b>
A.....	235
B.....	235
C.....	236
D.....	236
E.....	237
F.....	237
G.....	238
H.....	238
I.....	238
K.....	239
L.....	239
M.....	240
N.....	240
O.....	240
P.....	241
Q.....	241
R.....	241
S.....	242
T.....	243
V.....	243
W.....	243

**Índice..... 245**



## Acerca de esta guía

---

La Guía del usuario de IBM QRadar proporciona información sobre la gestión de IBM QRadar SIEM, que incluye los paneles Panel de control, Delitos, Actividad de registro, Actividad de red, Activos, e Informes.

### **Público al que va dirigido esta guía**

Esta guía está pensada para todos los usuarios de QRadar SIEM que están encargados de investigar y gestionar la seguridad de una red. Esta guía presupone que el usuario tiene acceso a QRadar SIEM y conocimientos sobre la red corporativa y las tecnologías de red.

### **Documentación técnica**

Para obtener información sobre cómo acceder a más documentación técnica, notas técnicas y notas de release, consulte [Acceso a la documentación de IBM Security QRadar](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

### **Cómo ponerse en contacto con el servicio de soporte al cliente**

Para obtener información sobre cómo ponerse en contacto con el servicio de soporte al cliente, consulte la [nota técnica de soporte y descarga](http://www.ibm.com/support/docview.wss?uid=swg21616144) (<http://www.ibm.com/support/docview.wss?uid=swg21616144>).

### **Declaración de buenas prácticas de seguridad**

La seguridad de los sistemas de TI implica la protección de los sistemas y la información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado a la información o puede ocasionar daños o un uso erróneo de los sistemas, incluidos los ataques a terceros. Ningún sistema o producto de TI debe ser considerado completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir el acceso o uso inadecuado. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, NI QUE HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALINTENCIONADAS O ILEGALES DE TERCEROS.

### **Tenga en cuenta lo siguiente:**

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM QRadar solamente se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este programa en conformidad con las leyes, regulaciones y políticas aplicables y asume toda la responsabilidad de su cumplimiento. El licenciataria declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM QRadar.



---

# Capítulo 1. Novedades para los usuarios de QRadar

Conozca las nuevas funciones y características de IBM QRadar que le permiten detectar y solucionar problemas de seguridad en la red de su organización de manera más sencilla.

---

## Nuevas características y mejoras en QRadar 7.4.1

---

Para los usuarios de QRadar, IBM QRadar 7.4.1 presenta estas características nuevas.

### **Soporte de la tarjeta Napatech de 40 Gbps**

El componente QFlow de IBM QRadar ahora admite la nueva Napatech NT200A02 (2 x 40 Gbps) SmartNIC. La conectividad de red no es indicativa de los niveles de rendimiento de los datos de los que es capaz cada dispositivo.

Napatech ha desechado el soporte de NT20E SmartNIC.

### **Soporte del campo ID de flujo en los registros de flujo de NetFlow V9**

IBM QRadar ahora da soporte al campo `flowId` (elemento IANA 148) en las exportaciones de datos de NetFlow Versión 9. En QRadar, el campo aparece en el campo **ID de flujo de proveedor** en la ventana **Detalles de flujo**.

El ID de flujo se utiliza como parte del identificador exclusivo del flujo, para que solo se agreguen los registros de flujo con el mismo valor de ID de flujo. Las sesiones con diferentes ID de flujo se mantienen separadas y se correlacionan con diferentes valores de ID de flujo.

Puede utilizar el campo `flowId` en los filtros y las búsquedas para identificar rápidamente todos los registros de flujo en una determinada sesión.

---


## Nuevas características y mejoras en QRadar 7.4.0

---

Para los usuarios de QRadar, IBM QRadar 7.4.0 presenta las siguientes nuevas características.

### **Campos estándar adicionales para los sucesos**

Puede ver detalles adicionales sobre los sucesos. Estos detalles proporcionan una mayor visibilidad sobre cómo QRadar procesa internamente los sucesos.

 [Más información sobre los detalles del suceso...](#)



## Capítulo 2. Prestaciones de su producto IBM QRadar

La documentación del producto IBM QRadar describe funciones tales como delitos, flujos, activos y correlación histórica, que pueden no estar disponibles en todos los productos de QRadar. Dependiendo del producto que esté utilizando, algunas de las características documentadas podrían no estar disponibles en su despliegue.

### IBM QRadar Log Manager

QRadar Log Manager es una solución básica, de alto rendimiento y escalable para recopilar, analizar, almacenar y elaborar información sobre grandes volúmenes de registros de sucesos de red y de seguridad.

### IBM QRadar SIEM

QRadar SIEM es un producto avanzado que incluye la gama completa de prestaciones de inteligencia y seguridad para los despliegues locales. Consolida datos de flujo de red procedentes de miles de activos, dispositivos, puntos finales y aplicaciones de dispositivo distribuidos por la red, y realiza actividades de normalización y correlación inmediata en los datos en bruto para distinguir hebras reales de falsos positivos.

### IBM QRadar on Cloud

QRadar on Cloud permite a los profesionales de la seguridad de IBM gestionar la infraestructura, en tanto que los analistas de seguridad realizan las tareas de detección y gestión de hebras. Puede proteger la red y cumplir los requisitos de supervisión de conformidad y elaboración de información con un coste total de propiedad menor.

### Prestaciones del producto QRadar

Revise la siguiente tabla para comparar las prestaciones de cada producto de QRadar.

Prestación	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Capacidades administrativas completas	Sí	No	Sí
Da soporte a despliegues alojados	No	Sí	No
Paneles de control personalizables	Sí	Sí	Sí
Motor de reglas personalizadas	Sí	Sí	Sí
Gestionar sucesos de red y seguridad	Sí	Sí	Sí
Gestionar registros de aplicación y host	Sí	Sí	Sí
Alertas basadas en umbral	Sí	Sí	Sí
Plantillas de conformidad	Sí	Sí	Sí
Archivado de datos	Sí	Sí	Sí
Integración de canales de información de reputación de IP de IBM Security X-Force Threat Intelligence	Sí	Sí	Sí
Despliegues autónomos de WinCollect	Sí	Sí	Sí
Despliegues gestionados de WinCollect	Sí	No	Sí
Supervisión de la actividad de red	Sí	Sí	No

Tabla 1. Comparación de prestaciones de QRadar (continuación)

Prestación	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Perfilado de activos	Sí	Sí	No <sup>1</sup>
Gestión de delitos	Sí	Sí	No
Captura y análisis de flujo de red	Sí	Sí	No
Correlación histórica	Sí	Sí	No
Integración de QRadar Network Insights	Sí	Sí	No
Integración de QRadar Vulnerability Manager	Sí	Sí	Sí
Integración de QRadar Risk Manager	Sí	No	No
Integración de QRadar Incident Forensics	Sí	No	No
Exploradores de evaluación de vulnerabilidades	Sí	Sí	Sí

<sup>1</sup> QRadar Log Manager solo hace un seguimiento de datos de activos si QRadar Vulnerability Manager está instalado.

Parte de la documentación, como la *Guía de administración* y la *Guía del usuario* es común a varios productos y puede describir las prestaciones que no están disponibles en su despliegue. Por ejemplo, los usuarios de IBM QRadar on Cloud no tienen las capacidades administrativas completas que se describen en la *Guía de administración de IBM QRadar*.

## Navegadores web soportados

Para que las características de los productos de IBM QRadar funcionen correctamente, debe utilizar un navegador web soportado.

La tabla siguiente lista las versiones soportadas de navegadores web.

Tabla 2. Navegadores web soportados para productos de QRadar

Navegador web	Versiones soportadas
Mozilla Firefox de 64 bits	60 Extended Support Release y posterior
Microsoft Edge de 64 bits	38.14393 y posterior
Google Chrome de 64 bits	Más reciente

El navegador web Microsoft Internet Explorer deja de ser compatible a partir de QRadar 7.4.0.

### Excepciones y certificados de seguridad

Si está utilizando el navegador web Mozilla Firefox, debe añadir una excepción a Mozilla Firefox para iniciar una sesión en QRadar SIEM. Para obtener más información, consulte la documentación del navegador web Mozilla Firefox.

### Navegación por la aplicación basada en la web

Cuando utilice QRadar, use las opciones de navegación existentes en la interfaz de usuario de QRadar, en lugar del botón **Atrás** del navegador web.

## Habilitación del modo de documento y modo de explorador en Internet Explorer

Si utiliza Microsoft Internet Explorer para acceder a productos de IBM QRadar, debe habilitar el modo de explorador y el modo de documento.

### Procedimiento

1. En el explorador web de Internet Explorer, pulse F12 para abrir la ventana **Herramientas de desarrollo**.
2. Pulse **Modo de explorador** y seleccione la versión del explorador web.
3. Pulse **Modo de documento** y seleccione el **Estándar Internet Explorer** correspondiente al release de Internet Explorer.

## Inicio de sesión de IBM QRadar

IBM QRadar es una aplicación basada en web. QRadar utiliza la información de inicio de sesión predeterminada para el URL, el nombre de usuario y la contraseña.

Utilice la información de la tabla siguiente cuando inicie la sesión en la consola de IBM QRadar.

Información de inicio de sesión	Valor predeterminado
URL	https://<Dirección IP>, donde <Dirección IP> es la dirección IP de la consola de QRadar.  Para iniciar la sesión en QRadar en un entorno de IPv6 o mixto, escriba la dirección IP entre corchetes:  https://[<Dirección IP>]
Nombre de usuario	admin
Contraseña	La contraseña que se asigna a QRadar durante el proceso de instalación.
Clave de licencia	Una clave de licencia predeterminada le proporciona acceso al sistema durante 5 semanas.

## API RESTful

La API (Interfaz de programación de aplicaciones) de REST (Representational State Transfer) es útil para integrar IBM QRadar con otras soluciones. Puede ejecutar acciones en la QRadar Console enviando solicitudes HTTPS a determinados puntos finales (URL) de la QRadar Console.

Cada punto final contiene el URL del recurso al que desea acceder y la acción que desea realizar en ese recurso. La acción se indica con el método HTTP de la solicitud: GET, POST, PUT o DELETE. Para obtener más información sobre los parámetros y respuestas de cada punto final, consulte *IBM QRadar API Guide*.

### Ejemplos de código y de foro de la API de QRadar

El foro de la API proporciona más información sobre la API REST, incluidas las respuestas a las preguntas más frecuentes y ejemplos de código anotado que puede utilizar en un entorno de prueba. Para obtener más información, consulte el [foro de API \(https://ibm.biz/qradarforos\)](https://ibm.biz/qradarforos).

## Pestañas de interfaz de usuario

La funcionalidad se divide en pestañas. La pestaña **Panel de control** se visualiza cuando se inicia la sesión.

Puede desplazarse fácilmente por las pestañas para localizar los datos o la funcionalidad que necesita.

### Pestaña Panel de control

La pestaña **Panel de control** es un entorno de espacio de trabajo que proporciona información resumida y detallada sobre los sucesos que se producen en la red.

La pestaña **Panel de control** Proporciona un entorno de espacio de trabajo que soporta varios paneles de control en los que puede visualizar las vistas de seguridad de red, la actividad o los datos que recopila QRadar. Están disponibles cinco paneles de control predeterminados. Cada panel de control contiene elementos que proporcionan información detallada y de resumen sobre los delitos que se producen en la red. También puede crear un panel de control personalizado para centrarse en las responsabilidades de las operaciones de red o de seguridad. Para obtener más información sobre el uso de la pestaña **Panel de control**, consulte [Gestión de panel de control](#).

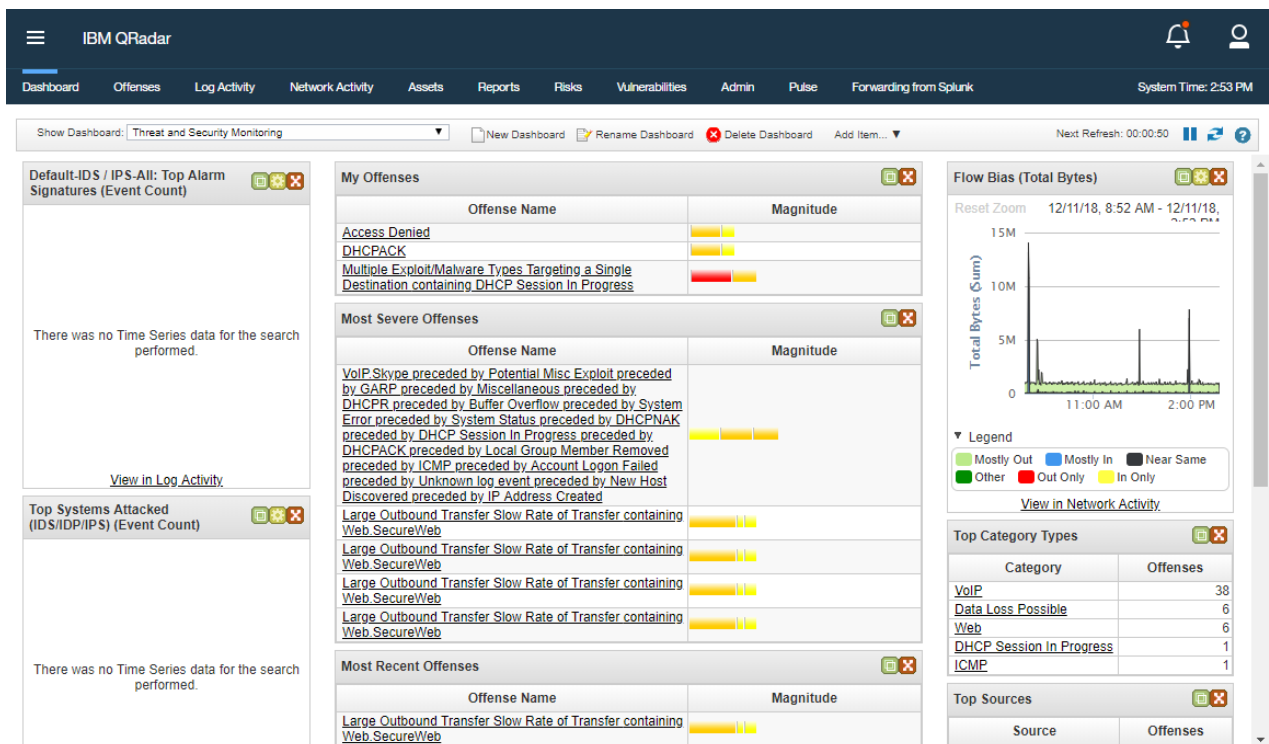


Figura 1. Pestaña Panel de control de la consola de QRadar

### Información relacionada

[Cómo realizar análisis de red utilizando elementos del panel de control de QRadar SIEM](#)

### Pestaña Delitos

Ver los delitos que se producen en la red, los cuales puede localizar mediante diversas opciones de navegación o a través de búsquedas avanzada.

Desde la pestaña **Delitos**, puede investigar un delito para determinar la causa raíz de un problema y trabajar para resolverlo.



The screenshot shows the IBM QRadar console interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', 'Pulse', and 'Forwarding from Splunk'. The 'Offenses' tab is active, displaying a table of offenses. The table has columns for 'Id', 'Description', 'Offense Type', 'Offense Source', 'Magnitude', 'Source IPs', and 'Destination IPs'. The table contains 17 rows of data, including offenses like 'VoIP Skype preceded by Potential Misc Exploit...', 'Large Outbound Transfer Slow Rate of Transfer containing Web...', and 'Multiple Exploit/Malware Types Targeting a Single Destination...'. The interface also shows search parameters, filter options, and pagination controls at the bottom.

Figura 2. Pestaña Delitos de la consola de QRadar

## Conceptos relacionados

[Gestión de delitos](#)

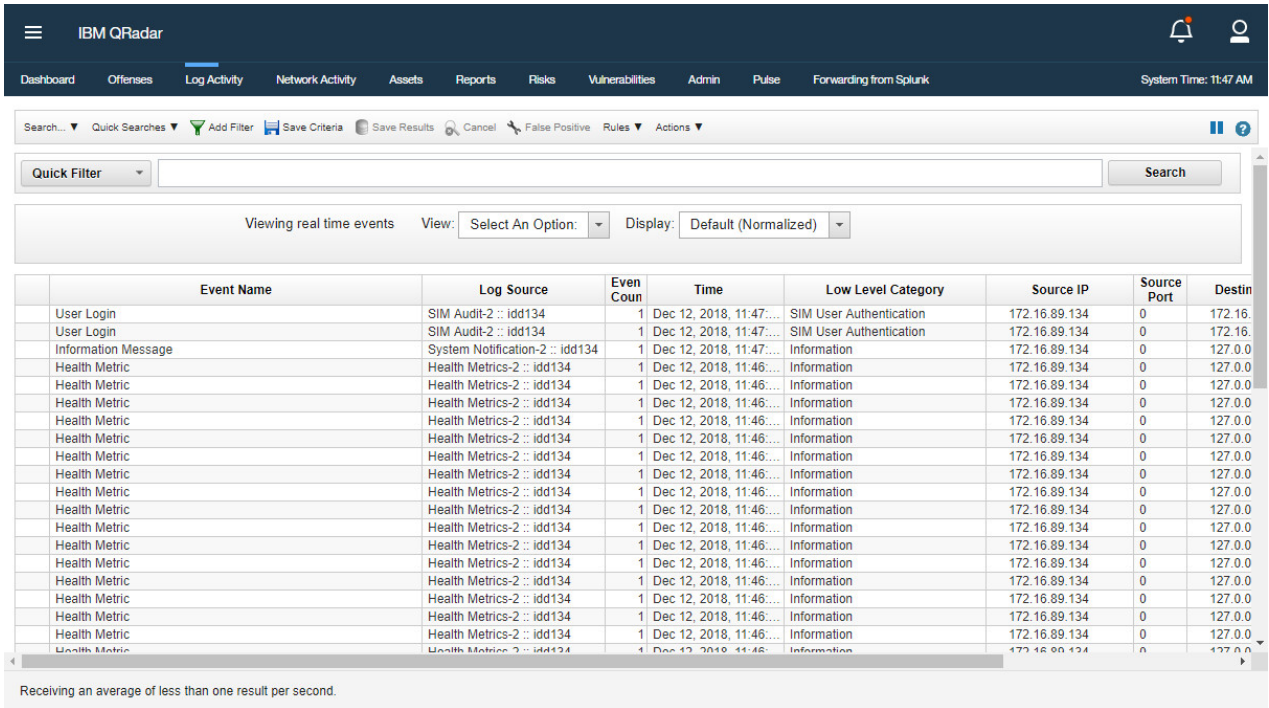
## Información relacionada

[Investigación de QRadar SIEM - Trabajo con delitos](#)

## Pestaña Actividad de registro

Investigar los registros de sucesos que se envían a QRadar en tiempo real, realizar búsquedas potentes y ver la actividad de registro utilizando gráficos de series temporales configurables.

Utilice la pestaña **Actividad de registro** para realizar investigaciones en profundidad sobre los datos de suceso.



Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destin
User Login	SIM Audit-2 :: idd134	1	Dec 12, 2018, 11:47:...	SIM User Authentication	172.16.89.134	0	172.16.
User Login	SIM Audit-2 :: idd134	1	Dec 12, 2018, 11:47:...	SIM User Authentication	172.16.89.134	0	172.16.
Information Message	System Notification-2 :: idd134	1	Dec 12, 2018, 11:47:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0
Health Metric	Health Metrics-2 :: idd134	1	Dec 12, 2018, 11:46:...	Information	172.16.89.134	0	127.0.0

Figura 3. Pestaña Actividad de registro de la consola de QRadar

### Conceptos relacionados

#### Investigación de actividad de registro

Puede supervisar e investigar sucesos en tiempo real o realizar búsquedas avanzadas.

### Información relacionada

#### Orígenes de registro de QRadar SIEM

#### Propiedades personalizadas de origen de registro de QRadar SIEM

### Pestaña Actividad de red

Utilice la pestaña **Actividad de red** para investigar flujos que se envían en tiempo real, realizar búsquedas avanzadas y ver actividad de red mediante gráficos de serie temporal configurables.

Un flujo es una sesión de comunicación entre dos hosts. Visualizar información de flujo le permitirá determinar cómo se transmite el tráfico, qué se transmite (si está habilitada la opción de captura de contenido) y quién está transmitiendo. Los datos de flujo también incluyen detalles tales como protocolos, valores de ASN, valores de IFIndex y prioridades.

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
	Dec 12, 2...	172.16...	41086	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	50182	172.16...	443	tcp_ip	Web.Sec...	17,675	7,377	36	30	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	36050	172.16...	443	tcp_ip	Web.Sec...	1,345	3,805	9	8	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	34797	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	40136	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	58414	172.16...	7800	tcp_ip	Other	141 (C)	140 (C)	2	2	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	33709	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	43164	172.16...	514	tcp_ip	Misc.Syslog	148	78	2	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	60484	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	50690	172.16...	443	tcp_ip	Web.Sec...	946	381	6	4	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	57754	172.16...	443	tcp_ip	Web.Sec...	1,665	2,376	10	7	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	55608	172.16...	53	udp_ip	Misc.dom...	88 (C)	544 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	60052	172.16...	1433	tcp_ip	DataWar...	3,069 (C)	3,369 (C)	17	10	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	50361	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	59761	172.16...	53	udp_ip	Misc.dom...	136 (C)	217 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	48704	172.16...	53	udp_ip	Misc.dom...	90 (C)	164 (C)	1	1	N/A	idd134	idd134.en...
	Dec 12, 2...	172.16...	44295	172.16...	53	udp_ip	Misc.dom...	91 (C)	165 (C)	1	1	N/A	idd134	idd134.en...

Receiving an average of 6 results per second.

Figura 4. Pestaña Actividad de red de la consola de QRadar

## Conceptos relacionados

“Supervisión de la actividad de red” en la página 87

Puede utilizar la pestaña **Actividad de red** para supervisar e investigar actividad de red (flujos) en tiempo real o realizar búsquedas avanzadas.

## Información relacionada

[Principios fundamentales de IBM QRadar SIEM](#)

[Activos y redes de QRadar SIEM](#)

## Pestaña Activos

QRadar descubre automáticamente los activos, servidores y hosts que operan en la red.

El descubrimiento automático se basa en datos de flujo pasivos y datos de vulnerabilidad, permitiendo que QRadar cree un perfil de activo.

Los perfiles de activo proporcionan información sobre cada activo conocido de la red, incluyendo información de identidad, si está disponible, y sobre qué servicios se ejecutan en cada activo. Estos datos de perfil se utilizan para la correlación con el fin de ayudar a reducir falsos positivos.

Por ejemplo, un ataque intenta utilizar un servicio específico que se está ejecutando en un activo específico. En esta situación, QRadar puede determinar si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo. Mediante la pestaña **Activos**, puede ver los activos aprendidos o buscar activos específicos para ver los perfiles.

Id	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services	Last User	User Last Seen
1001	172.16.88.179	172.16.88.179		0.0	0	5		
1002	172.16.131.118	172.16.131.118		0.0	0	0		
1003	172.16.89.185	172.16.89.185		0.0	0	9		
1004	172.16.89.186	172.16.89.186		0.0	0	2		
1005	172.16.88.245	172.16.88.245		0.0	0	4		
1006	172.16.89.134	172.16.89.134		0.0	0	5		
1007	172.16.2.9	172.16.2.9		0.0	0	1		
1008	172.16.210.144	172.16.210.144		0.0	0	1		
1009	172.16.131.66	172.16.131.66		0.0	0	0		
1010	172.16.89.220	172.16.89.220		0.0	0	3		
1011	172.16.89.221	172.16.89.221		0.0	0	2		
1012	172.16.87.113	172.16.87.113		0.0	0	0		
1013	172.16.131.91	172.16.131.91		0.0	0	0		
1014	172.16.89.151	172.16.89.151		0.0	0	5		
1015	172.16.95.175	172.16.95.175		0.0	0	1		
1016	172.16.210.42	172.16.210.42		0.0	0	1		
1017	172.16.131.98	172.16.131.98		0.0	0	0		
1018	172.16.131.100	172.16.131.100		0.0	0	0		
1019	172.16.3.9	172.16.3.9		0.0	0	1		
1020	172.16.75.170	172.16.75.170		0.0	0	1		
1021	172.16.150.31	172.16.150.31		0.0	0	0		
1022	172.16.89.200	172.16.89.200		0.0	0	10		
1023	172.16.198.182	172.16.198.182		0.0	0	0		
1024	172.16.158.160	172.16.158.160		0.0	0	0		
1025	172.16.424.108	172.16.424.108		0.0	0	0		

Figura 5. Pestaña Activos de la consola de QRadar

### Información relacionada

[Activos y redes de QRadar SIEM](#)

## Pestaña Informes

Utilice la pestaña **Informes** para crear, distribuir y gestionar informes para los datos en QRadar.

Crear informes personalizados para uso operativo y ejecutivo. Combinar información (por ejemplo, seguridad o red) en un solo informe. También puede utilizar plantillas de informe preinstaladas que se incluyen con QRadar.

También puede marcar los informes con logotipos personalizados. Esta personalización es beneficiosa para distribuir informes a diferentes públicos.

Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
Weekly Success...	Security	Manual	Manual	Apr 13, 2017, 9:...	admin	admin	None	
Asset Compliance	CIS Benchmark...	Manual	Manual	Aug 12, 2014, 6:...	admin	admin	None	
Scan Overview	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
New Vulnerabili...	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Missing Patches	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Scan Results (...)	Scan Reports	Manual	Manual	May 30, 2014, ...	admin	admin	None	
Scan Summary...	Scan Reports	Manual	Manual	May 6, 2014, 11:...	admin	admin	None	
Accessible files...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Default logon v...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Annual Vulnera...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Monthly Vulner...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Vulnerability Ex...	Vulnerability Ma...	Manual	Manual	Apr 30, 2013, 7:...	admin	admin	None	
Obsolete Envir...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Vulnerability Ov...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Network Vulner...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Last 7 Days Vul...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
Weekly PCI Co...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 6:...	admin	admin	None	
PCI Complianc...	Vulnerability Ma...	Manual	Manual	Apr 28, 2013, 5:...	admin	admin	None	
Weekly Firewall...	Network Manag...	Weekly	4 days 14 hour...	Oct 18, 2010, 7:...	admin	admin	Dec 10, 2018, 2:0	
Top IDS/IPS AI...	Security	Weekly	4 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 10, 2018, 2:0	
Top IDS/IPS AI...	Security	Weekly	4 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 10, 2018, 2:0	
Top Application...	Network Manag...	Weekly	3 days 14 hour...	Sep 23, 2010, 4:...	admin	admin	Dec 9, 2018, 2:01	
Daily User Auth...	Authentication, ...	Daily	13 hours 10 mi...	Sep 23, 2010, 4:...	admin	admin	Dec 12, 2018, 1:0	

Figura 6. Pestaña Informes de la consola de QRadar

### Conceptos relacionados

#### Gestión de informes

Puede utilizar la pestaña **Informes** para crear, editar, distribuir y gestionar informes.

## IBM QRadar Risk Manager

IBM QRadar Risk Manager es un dispositivo instalado por separado para supervisar configuraciones de dispositivo, simular cambios en el entorno de red, y priorizar riesgos y vulnerabilidades de la red.

QRadar Risk Manager utiliza datos recogidos por dispositivos de red y de seguridad, tales como cortafuegos, direccionadores, conmutadores, sistemas de prevención de intrusiones, canales de información de vulnerabilidades y orígenes de seguridad de proveedor. Estos datos se utilizan para determinar los riesgos de seguridad existentes dentro de la infraestructura de seguridad de la red y la probabilidad de que se exploten esos riesgos.

**Nota:** Para obtener más información sobre QRadar Risk Manager, póngase en contacto con el representante de ventas local.

## Procedimientos comunes de QRadar

Los diferentes controles de QRadar son comunes para la mayoría de las pestañas.

### Visualización de notificaciones

El menú **Notificaciones** proporciona acceso a una ventana en la que puede leer y gestionar las notificaciones del sistema.

#### Antes de empezar

Para que las notificaciones del sistema se muestren en la ventana **Notificaciones**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccionar el recuadro de selección **Notificar** en el **Asistente de reglas personalizadas**.

## Acerca de esta tarea

El menú **Mensajes** indica cuántas notificaciones de sistema no leídas tiene en el sistema. Este indicador incrementa el número hasta que se cierran las notificaciones de sistema. Para cada notificación de sistema, la ventana **Mensajes** proporciona un resumen y la indicación de fecha y hora en que se ha creado la notificación de sistema. Puede pasar el puntero del ratón sobre una notificación para ver más detalles. Puede utilizar las funciones de la ventana **Mensajes** para gestionar las notificaciones del sistema.

Las notificaciones del sistema también están disponibles en la pestaña **Panel de control** y en una ventana emergente opcional. Las acciones que se realizan en la ventana **Mensajes** se propagan a la pestaña **Panel de control** y la ventana emergente. Por ejemplo, si cierra una notificación de sistema de la ventana **Mensajes**, la notificación de sistema se elimina de todas las pantallas de notificación de sistema.

## Procedimiento

1. Inicie la sesión en QRadar.
2. Haga clic en **Notificaciones**.
3. En la ventana **Mensajes**, vea los detalles de la notificación de sistema.
4. Para refinar la lista de notificaciones de sistema, pulse una de las opciones siguientes:
  - **Errores**
  - **Avisos**
  - **Info**
5. Para cerrar las notificaciones del sistema, elija una de las opciones siguientes:

Opción	Descripción
<b>Descartar toda la información</b>	Pulse aquí para cerrar todas las notificaciones de sistema.
<b>Descartar</b>	Pulse el icono <b>Descartar</b> junto a la notificación de sistema que desea cerrar.

6. Para ver los detalles de notificación del sistema, pase el puntero del ratón sobre la notificación del sistema.

## Tareas relacionadas

[“Creación de una regla personalizada” en la página 185](#)

[Gestión de notificaciones del sistema](#)

Puede especificar el número de notificaciones que desea visualizar en el elemento de panel de control **Notificación del sistema** y cerrar las notificaciones del sistema después de leerlas.

## Renovación y pausa de QRadar

Puede renovar, poner en pausa y reproducir manualmente los datos que se visualizan en las pestañas.

### Pestaña Panel de control

La pestaña **Panel de control** se renueva automáticamente cada 60 segundos. El temporizador indica el tiempo que queda hasta que la pestaña se renueva automáticamente. Consulte la figura 7 para ver un ejemplo.

Pulse la barra de título de cualquier elemento de panel de control para detener automáticamente el tiempo de renovación. El temporizador parpadea en rojo para indicar que la visualización actual se ha puesto en pausa.

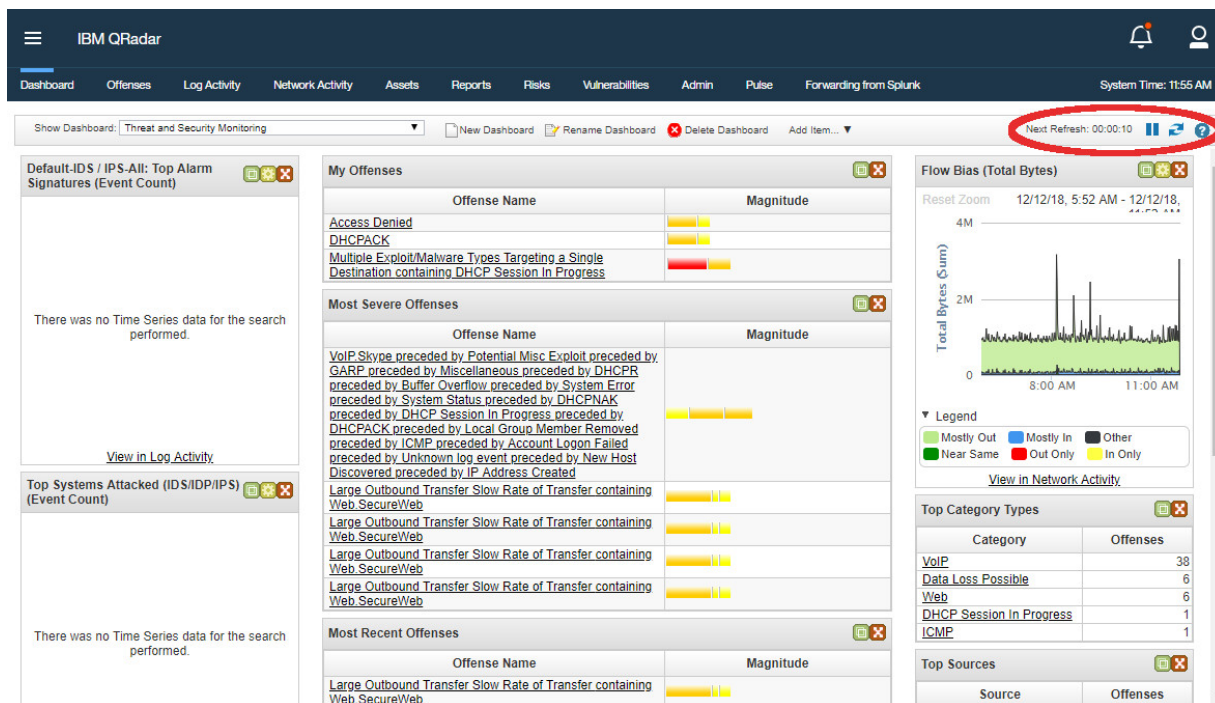


Figura 7. Temporizador en la consola de QRadar

### Pestañas Actividad de registro y Actividad de red

Las pestañas **Actividad de registro** y **Actividad de red** se renuevan automáticamente cada 60 segundos si está viendo la pestaña en modalidad de Último intervalo (renovación automática).

Cuando vea la pestaña **Actividad de registro** o **Actividad de red** en modalidad de Tiempo real (modalidad continua) o de Último minuto (renovación automática), puede utilizar el icono **Pausa** para poner en pausa la visualización actual.

### Pestaña Delitos

La pestaña **Delitos** se debe renovar manualmente. El temporizador indica el tiempo desde que se renovaron los datos por última vez. El temporizador parpadea en rojo cuando se detiene.

## Investigación de direcciones IP

Puede utilizar varios métodos para investigar la información sobre direcciones IP en las pestañas **Panel de control**, **Actividad de registro** y **Actividad de red**.

### Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña que desea ver.
3. Mueva el puntero de ratón sobre una dirección IP para ver la ubicación de la dirección IP.
4. Pulse el botón derecho del ratón en la dirección IP o el nombre de activo y seleccione una de las opciones siguientes:

Tabla 4. Información de direcciones IP	
Opción	Descripción
<b>Navegar &gt; Ver por red</b>	Muestra las redes que están asociadas con la dirección IP seleccionada.
<b>Navegar &gt; Ver resumen de origen</b>	Muestra los delitos que están asociados con la dirección IP de origen seleccionada.

<i>Tabla 4. Información de direcciones IP (continuación)</i>	
<b>Opción</b>	<b>Descripción</b>
<b>Navegar &gt; Ver resumen de destino</b>	Muestra los delitos que están asociados con la dirección IP de destino seleccionada.
<b>Información &gt; Búsqueda de DNS</b>	Busca entradas DNS que están basados en la dirección IP.
<b>Información &gt; Búsqueda de WHOIS</b>	Busca el propietario registrado de una dirección IP remota. El servidor whois predeterminado es whois.arin.net.
<b>Información &gt; Exploración de puertos</b>	Realiza una exploración de Network Mapper (NMAP) de la dirección IP seleccionada. Esta opción solo está disponible si NMAP está instalado en el sistema. Para obtener más información sobre la instalación de NMAP, consulte la documentación de proveedor.
<b>Información &gt; Perfil de activo</b>	<p>Visualiza información de perfil de activo.</p> <p>Esta opción se visualiza si se ha adquirido IBM QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación <i>Guía del usuario de IBM QRadar Vulnerability Manager</i>.</p> <p>Esta opción de menú está disponible si QRadar ha adquirido datos de perfil activamente a través de una exploración o pasivamente a través de orígenes de flujo.</p> <p>Para obtener información, consulte la publicación <i>Guía de administración de IBM QRadar</i>.</p>
<b>Información &gt; Sucesos de búsqueda</b>	Busca los sucesos que están asociados con esta dirección IP.
<b>Información &gt; Buscar flujos</b>	Busca flujos que están asociados con esta dirección IP.
<b>Información &gt; Buscar en conexiones</b>	Busca las conexiones que están asociadas con esta dirección IP. Esta opción solo se visualiza si ha adquirido IBM QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM QRadar Risk Manager. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
<b>Información &gt; Switch Port Lookup</b>	<p>Determina el puerto de conmutador en un dispositivo Cisco IOS para esta dirección IP. Esta opción solo se aplica a conmutadores que se descubren utilizando la opción <b>Discover Devices</b> en la pestaña <b>Riesgos</b>.</p> <p><b>Nota:</b> Esta opción de menú no está disponible en QRadar Log Manager.</p>



*Tabla 4. Información de direcciones IP (continuación)*

Opción	Descripción
<b>Información &gt; Ver topología</b>	Visualiza la pestaña <b>Riesgos</b> , que representa la topología de capa 3 de la red. Esta opción está disponible si ha adquirido IBM QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM QRadar Risk Manager.
<b>Ejecutar Exploración de vulnerabilidad</b>	Seleccione la opción <b>Ejecutar Exploración de vulnerabilidad</b> para realizar una exploración de IBM QRadar Vulnerability Manager en esta dirección IP. Esta opción solo se visualiza cuando se ha adquirido IBM QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación <i>Guía del usuario de IBM QRadar Vulnerability Manager</i> .

## Hora del sistema

La parte superior derecha de la consola de QRadar muestra la hora del sistema, que es la hora local en la consola.

La hora de consola sincroniza los sistemas QRadar en el despliegue de QRadar. La hora de consola se utiliza para determinar qué sucesos de hora se han recibido de otros dispositivos para la correlación de sincronización de hora correcta. En un despliegue distribuido, la consola puede estar en un huso horario diferente del correspondiente al del sistema.

Cuando se aplican filtros y búsquedas basadas en la hora en la pestaña **Actividad de registro** y la pestaña **Actividad de red**, debe utilizar la hora de sistema de la consola para especificar un intervalo de tiempo.

## Actualización de preferencias de usuario

Puede establecer sus preferencias, por ejemplo, el entorno local, en IBM QRadar SIEM.

### Procedimiento

1. Pulse el icono de usuario y, a continuación, haga clic en **Preferencias de usuario** para acceder a la información de usuario.
2. Actualice las preferencias.

Opción	Descripción
<b>Nombre de usuario</b>	Visualiza el nombre de usuario. No puede editar este campo.
<b>Contraseña</b>	Las contraseñas de usuario de QRadar se almacenan como una serie SHA-256 salada. La contraseña debe cumplir los requisitos de longitud mínima y complejidad establecidos.
<b>Contraseña (Confirmar)</b>	Confirmación de la contraseña
<b>Dirección de correo electrónico</b>	La dirección de correo electrónico debe cumplir los requisitos siguientes: <ul style="list-style-type: none"> <li>• Un mínimo de 10 caracteres</li> <li>• Un máximo de 255 caracteres</li> </ul>

<b>Opción</b>	<b>Descripción</b>
<b>Entorno local</b>	<p>QRadar está disponible en los idiomas siguientes: inglés, chino simplificado, chino tradicional, japonés, coreano, francés, alemán, italiano, español, ruso y portugués (Brasil).</p> <p>Si elige otro idioma, la interfaz de usuario se muestra en inglés. Se utilizan otros convenios culturales asociados, como tipo de carácter, clasificación, formato de fecha y hora, y unidad de moneda.</p>
<b>Habilitar notificaciones emergentes</b>	<p>Si desea habilitar las notificaciones de sistema emergentes para que se muestren en la interfaz de usuario, seleccione este recuadro de selección.</p>

3. Pulse **Guardar**.

## Capítulo 3. Gestión de panel de control

La pestaña **Panel de control** es la vista predeterminada cuando se inicia la sesión.

Proporciona un entorno de espacio de trabajo que soporta varios paneles de control en los que puede visualizar las vistas de seguridad de red, la actividad o los datos que se recopilan.

Los paneles de control le permiten organizar los elementos de panel de control en vistas funcionales, que le permiten centrarse en áreas específicas de la red.

Utilice la pestaña Panel de control para supervisar el comportamiento de sucesos de seguridad.

Puede personalizar el panel de control. El contenido que se visualiza en la pestaña **Panel de control** es específico del usuario. Los cambios que se realizan dentro de una sesión solo afectan el sistema.

### Paneles de control predeterminados

Utilice el panel de control predeterminado para personalizar elementos y crear vistas funcionales. Estas vistas funcionales están centradas en áreas determinadas de la red.

La pestaña **Panel de control** proporciona cinco paneles de control predeterminados que están centrados en la seguridad, la actividad de red, la actividad de aplicaciones, la supervisión del sistema y el cumplimiento de las normativas.

Cada panel de control muestra un conjunto predeterminado de elementos de panel de control. Los elementos de panel de control sirven de punto de partida para acceder a datos más detallados. La tabla siguiente define los paneles de control predeterminados.

Panel de control predeterminado	Elementos
Visión general de la aplicación	<p>El panel de control <b>Visión general de la aplicación</b> incluye los elementos predeterminados siguientes:</p> <ul style="list-style-type: none"><li>• Tráfico de entrada por país (bytes totales)</li><li>• Tráfico de salida por país (bytes totales)</li><li>• Aplicaciones principales (bytes totales)</li><li>• Aplicaciones principales de entrada de Internet (bytes totales)</li><li>• Aplicaciones principales de salida a Internet (bytes totales)</li><li>• Servicios principales denegados a través de cortafuegos (recuento de sucesos)</li><li>• DSCP - Prioridad (bytes totales)</li></ul>

Tabla 5. Paneles de control predeterminados (continuación)

Panel de control predeterminado	Elementos
Visión general del cumplimiento de políticas	<p>El panel de control <b>Visión general de conformidad</b> incluye los elementos predeterminados siguientes:</p> <ul style="list-style-type: none"> <li>• Autenticaciones principales por usuario (serie temporal)</li> <li>• Anomalías de autenticación principales por usuario (recuento de sucesos)</li> <li>• Anomalías de inicio de sesión por usuario (en tiempo real)</li> <li>• Conformidad: nombre de usuario implicado en reglas de conformidad (serie temporal)</li> <li>• Conformidad: IPs de origen implicadas en reglas de conformidad (serie temporal)</li> <li>• Informes más recientes</li> <li>•</li> </ul>
Visión general de la red	<p>El panel de control <b>Visión general de la red</b> incluye los elementos predeterminados siguientes:</p> <ul style="list-style-type: none"> <li>• Interlocutores principales (en tiempo real)</li> <li>• Tipo/código de ICMP (paquetes totales)</li> <li>• Redes principales por volumen de tráfico (bytes totales)</li> <li>• Denegación de cortafuegos por puerto de DST (recuento de sucesos)</li> <li>• Denegación de cortafuegos por IP de DST (recuento de sucesos)</li> <li>• Denegación de cortafuegos por IP de SRC (recuento de sucesos)</li> <li>• Aplicaciones principales (bytes totales)</li> <li>• Utilización de enlace (en tiempo real)</li> <li>• DSCP - Prioridad (bytes totales)</li> </ul>
Supervisión del sistema	<p>El panel de control <b>Supervisión del sistema</b> incluye los elementos predeterminados siguientes:</p> <ul style="list-style-type: none"> <li>• Orígenes de registro principales (recuento de sucesos)</li> <li>• Utilización de enlace (en tiempo real)</li> <li>• Notificaciones del sistema</li> <li>• Distribución de procesador de sucesos (recuento de sucesos)</li> <li>• Velocidad de sucesos (sucesos por segundo fusionados – Promedio 1 min)</li> <li>• Velocidad de flujo (flujos por segundo – Máximo 1 min)</li> </ul>

Tabla 5. Paneles de control predeterminados (continuación)

Panel de control predeterminado	Elementos
Supervisión de amenazas y seguridad	<p>El panel de control <b>Supervisión de amenazas y seguridad</b> incluye los elementos predeterminados siguientes:</p> <ul style="list-style-type: none"> <li>• Predeterminado-IDS/IPS-All: Firmas de alarma principales (en tiempo real)</li> <li>• Sistemas atacados principales (recuento de sucesos)</li> <li>• Ataques de provisión de sistemas principales (recuento de sucesos)</li> <li>• Mis delitos</li> <li>• Delitos más graves</li> <li>• Delitos más recientes</li> <li>• Servicios principales denegados a través de cortafuegos (recuento de sucesos)</li> <li>• Centro de información de amenazas de Internet</li> <li>• Sesgo de flujo (bytes totales)</li> <li>• Tipos de categorías principales</li> <li>• Orígenes principales</li> <li>• Destinos locales principales</li> </ul>

## Paneles de control personalizados

Puede personalizar los paneles de control. El contenido que se muestra en la pestaña **Panel de control** es específico del usuario. Los cambios realizados dentro de una sesión de QRadar solo afectan al sistema local del usuario.

Para personalizar la pestaña **Panel de control**, puede realizar las tareas siguientes:

- Cree paneles de control personalizados que sean aplicables a las tareas que tenga asignadas. Se pueden crear un máximo de 255 paneles de control por cada usuario, pero se pueden producir problemas de rendimiento si crea más de 10 paneles de control.
- Añada y elimine elementos de los paneles de control predeterminados o personalizados.
- Mueva y sitúe los elementos de acuerdo con sus necesidades. Cuando sitúa elementos, cada elemento cambia automáticamente de tamaño en proporción al panel de control.
- Añada elementos de panel de control personalizado que están basados en cualquier dato.

Por ejemplo, puede añadir un elemento de panel de control que proporciona un gráfico de serie temporal o un gráfico de barras que representa los 10 elementos principales de actividad de red.

Para crear elementos personalizados, puede crear búsquedas guardadas en **la pestaña Actividad de red** o **la pestaña Actividad de registro** y elegir cómo desea que se representen los resultados en la pestaña de control. Cada gráfico de panel de control muestra datos actualizados en tiempo real. Los gráficos de serie temporal del panel de control se renuevan cada 5 minutos.

### Búsqueda de flujos

Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña **Actividad de red**.

Los elementos de búsqueda de flujos están listados en el menú **Añadir elemento > Actividad de red > Búsqueda de flujos**. El nombre del elemento de búsqueda de flujos coincide con el nombre de los criterios de búsqueda guardados en los que está basado el elemento.

Puede utilizar criterios de búsqueda guardados predeterminados preconfigurados para mostrar elementos de búsqueda de flujos en el menú de la pestaña **Panel de control**. Puede añadir más elementos de panel de control de la búsqueda de flujos al menú de la pestaña **Panel de control**. Para obtener más información, consulte [Añadir elementos de panel de control basados en búsquedas a la lista Añadir elementos](#).

En un elemento de panel de control de búsqueda de flujos, los resultados de la búsqueda muestran datos actualizados en tiempo real en un gráfico. Los tipos de gráfico soportados son series temporales, de tabla, circulares y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar. Para obtener más información sobre la configuración de gráficos, consulte [Configurar gráficos](#).

Los gráficos de serie temporal son interactivos. Mediante los gráficos de serie temporal, puede aumentar el detalle de una línea temporal para investigar actividad de la red.

## Delitos

Puede añadir varios elementos relacionados con delitos al panel de control.

**Nota:** Los delitos ocultos o cerrados se incluyen en los valores que se muestran en la pestaña **Panel de control**. Para obtener más información sobre delitos ocultos o cerrados, consulte [Gestión de delitos](#).

La tabla siguiente describe los elementos de delito:

<i>Tabla 6. Elementos de delito</i>	
<b>Elementos de panel de control</b>	<b>Descripción</b>
Delitos más recientes	Los cinco delitos más recientes se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en el nombre del delito para ver información detallada sobre la dirección IP.
Delitos más graves	Los cinco delitos más graves se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en el nombre del delito para ver información detallada sobre la dirección IP.
Mis delitos	El elemento <b>Mis delitos</b> muestra 5 de los delitos más recientes que tiene asignados el usuario. Los delitos se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.
Orígenes principales	El elemento <b>Delitos principales</b> muestra los orígenes de delitos principales. Cada origen se identifica con una barra de magnitudes para informarle de la importancia del origen. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.

Tabla 6. Elementos de delito (continuación)

Elementos de panel de control	Descripción
Destinos locales principales	El elemento <b>Destinos locales principales</b> muestra los destinos locales principales. Cada destino se identifica con una barra de magnitudes para informarle de la importancia del destino. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.
Categorías	El elemento <b>Tipos de categorías principales</b> muestra las cinco categorías principales correspondientes al número mayor de delitos.

## Actividad de registro

Los elementos de panel de control **Actividad de registro** le permitirán supervisar e investigar sucesos en tiempo real.

**Nota:** Los sucesos ocultos o cerrados no están incluidos en los valores que se visualizan en la pestaña **Panel de control**.

Tabla 7. Elementos de actividad de registro

Elemento de panel de control	Descripción
Búsquedas de suceso	<p>Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña <b>Actividad de registro</b>. Los elementos de búsqueda de sucesos se listan en el menú <b>Añadir elemento &gt; Actividad de red &gt; Búsquedas de suceso</b>. El nombre del elemento de búsqueda de sucesos coincide con el nombre de los criterios de búsqueda guardados en los que se basa el elemento.</p> <p>QRadar incluye criterios de búsqueda guardados predeterminados que están preconfigurados para visualizar elementos de búsqueda de sucesos en el menú de pestaña <b>Panel de control</b>. Puede añadir más elemento de panel de control de búsqueda de sucesos en el menú de pestaña <b>Panel de control</b>. Para obtener más información, consulte Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos Añadir.</p> <p>En un elemento de panel de control <b>Actividad de registro</b>, los resultados de búsqueda visualizan datos de última hora en tiempo real en un gráfico. Los tipos de gráfico soportados son series de tiempo, tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar.</p> <p>Los gráficos de series temporales son interactivos. Puede ampliar y explorar en una línea temporal para investigar la actividad de registro.</p>

Tabla 7. Elementos de actividad de registro (continuación)

Elemento de panel de control	Descripción
Sucesos por gravedad	El elemento de panel de control <b>Sucesos por gravedad</b> visualiza el número de sucesos activos que están agrupados por gravedad. Este elemento le permitirá ver el número de sucesos que se reciben por el nivel de gravedad asignada. La gravedad indica la cantidad de amenaza que representa un origen de delito en relación al grado de preparación del destino ante el ataque. El rango de gravedad es de 0 (baja) a 10 (alta). Los tipos de gráfico soportados son tabla, circular y de barras.
Orígenes de registro principales	El elemento de panel de control <b>Orígenes de registro principales</b> visualiza los 5 orígenes de registro principales que han enviado sucesos a QRadar en los últimos 5 minutos.  El número de sucesos que se envían desde el origen de registro especificado se indica en el gráfico circular. Este elemento le permitirá ver los cambios potenciales en el comportamiento, por ejemplo si un origen de registro de cortafuegos que normalmente no está en la lista de 10 principales ahora contribuye en un gran porcentaje del recuento de mensajes global, debe investigar esta aparición. Los tipos de gráfico soportados son tabla, circular y de barras.

## Resumen del sistema

El elemento de panel de control **Resumen del sistema** proporciona un resumen de alto nivel de la actividad dentro las últimas 24 horas.

Dentro del elemento de resumen, puede ver la información siguiente:

- **Flujos actuales por segundo:** Visualiza la tasa de flujos por segundo.
- **Flujos (tras 24 horas):** Visualiza el número total de flujos activos que se ven dentro de las últimas 24 horas.
- **Sucesos actuales por segundo:** Visualiza la tasa de sucesos por segundo.
- **Sucesos nuevos (pasadas 24 horas):** Visualiza el número total de sucesos nuevos que se reciben dentro de las últimas 24 horas.
- **Delitos nuevos (pasadas 24 horas):** Visualiza el número total de delitos que se han creado o modificado con evidencia nueva dentro de las últimas 24 horas.
- **Tasa de reducción de datos:** Visualiza la tasa de datos reducidos basados en el total de sucesos que se detectan dentro de las últimas 24 horas y el número de delitos modificados dentro de las últimas 24 horas.

## Panel de control de supervisión de riesgos

Utilice el panel de control de **Supervisión de riesgos** para supervisar riesgos para activos, políticas y grupos de políticas.

De forma predeterminada, el panel de control **Supervisión de riesgos** muestra los elementos **Riesgo** y **Cambio de riesgo** que supervisan la puntuación de riesgo de política para activos pertenecientes a los grupos de políticas Vulnerabilidades altas, Vulnerabilidades medias y Vulnerabilidades bajas, así como las



tasas de cumplimiento de políticas y cambios históricos en la puntuación de riesgo de política del grupo de políticas CIS.

Los elementos del panel de control Supervisión de riesgos no muestra ningún resultado a menos que se tenga una licencia de IBM QRadar Risk Manager. Para obtener más información, consulte la Guía del usuario de QRadar Risk Manager.

Para ver el panel de control predeterminado de **Supervisión de riesgos**, seleccione **Mostrar panel de control > Supervisión de riesgos** en la pestaña **Panel de control**.

#### **Tareas relacionadas**

[Supervisar el cumplimiento de políticas](#)

[Supervisar el cambio de riesgo](#)

## **Supervisar el cumplimiento de políticas**

Puede crear un elemento de panel de control que muestra el nivel de cumplimiento de políticas y la puntuación de riesgo de política para activos, políticas y grupos de políticas seleccionados.

### **Procedimiento**

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.
3. Escriba un nombre y una descripción para el panel de control de cumplimiento de políticas.
4. Pulse **Aceptar**.
5. En la barra de herramientas, seleccione **Añadir elemento > Gestor de riesgos > Riesgo**.

Los elementos de panel de control del **Gestor de riesgos** se muestran solamente cuando IBM QRadar Risk Manager se utiliza con una licencia.

6. En la cabecera del elemento de panel de control nuevo, pulse el icono amarillo **Valores**.
7. Utilice las listas **Tipo de gráfico**, **Mostrar parte superior** y **Ordenar** para configurar el gráfico.
8. En la lista **Grupo**, seleccione el grupo que desee supervisar. Para obtener más información, consulte la tabla incluida en el paso 9.

Cuando se selecciona la opción **Activo**, aparece un enlace a la página **Riesgos > Gestión de políticas > Por activo** en la parte inferior del elemento de panel de control **Riesgo**. En la página **Por activo** se muestra información más detallada sobre todos los resultados que se han devuelto para el valor de **Grupo de políticas** seleccionado. Para obtener más información sobre un activo concreto, seleccione **Tabla** en la lista **Tipo de gráfico** y pulse el enlace de la columna **Activo** para ver los detalles sobre el activo en la página **Por activo**.

Cuando se selecciona la opción **Política**, aparece un enlace a la página **Riesgos > Gestión de políticas > Por política** en la parte inferior del elemento de panel de control **Riesgo**. En la página **Por política** se muestra información más detallada sobre todos los resultados que se han devuelto para el valor de **Grupo de políticas** seleccionado. Para obtener más información sobre una política concreta, seleccione **Tabla** en la lista **Tipo de gráfico** y pulse el enlace de la columna **Política** para ver los detalles sobre la política en la página **Por política**.

9. En la lista **Gráfico**, seleccione el tipo de gráfico que desee utilizar. Para obtener más información, consulte la tabla siguiente:

<b>Grupo</b>	<b>Porcentaje de activos aprobados</b>	<b>Porcentaje de controles de política aprobados</b>	<b>Porcentaje de grupos de políticas aprobados</b>	<b>Puntuación de riesgo de política</b>
Todo	Devuelve el porcentaje promedio de cumplimiento para activos, políticas y el grupo de políticas.	Devuelve el porcentaje promedio de cumplimiento de controles de política para activos, políticas y el grupo de políticas.	Devuelve la tasa de cumplimiento promedio de grupo de políticas para todos los activos, políticas y el grupo de políticas.	Devuelve la puntuación de riesgo promedio de política para todos los activos, políticas y el grupo de políticas.
Activo	Indica si un activo ha pasado la prueba de conformidad de activo (100%=cumplimiento 0%=no cumplimiento).  Utilice este valor para mostrar qué activos asociados a un grupo de políticas han pasado la prueba de conformidad.	Indica el porcentaje de controles de política que un activo ha superado.  Utilice este valor para mostrar el porcentaje de controles de política que se han pasado para cada activo que está asociado al Grupo de políticas.	Muestra el porcentaje de subgrupos de políticas que están asociados al activo que ha pasado la prueba de conformidad.	Devuelve la suma de todos los valores de factor de importancia para cuestiones de política que están asociadas a cada activo.  Utilice este valor para ver el riesgo de política para cada activo que está asociado a un grupo de políticas seleccionado.
Política	Indica si todos los activos asociados a cada política de un grupo de políticas han pasado la prueba de conformidad.  Utilice este valor para supervisar si todos los activos asociados a cada política de un grupo de políticas pasan o no la prueba de conformidad.	Devuelve el porcentaje de controles de política superados por cada política del grupo de políticas.  Utilice este valor para supervisar cuántos controles de política fallan para cada política.	Muestra el porcentaje de subgrupos de políticas de los cuales la política es una parte que pasa la prueba de conformidad.	Muestra los valores de factor de importancia para cada pregunta de política del grupo de políticas.  Utilice este valor para ver el factor de importancia de cada política de un grupo de políticas.
Grupo de políticas	Devuelve el porcentaje de activos que pasan la prueba de conformidad para el grupo de políticas global seleccionado.	Devuelve el porcentaje de controles de política que se pasan para cada política del grupo de políticas considerado globalmente.	Devuelve el porcentaje de subgrupos de políticas dentro del grupo de políticas que pasan la prueba de conformidad.	Devuelve la suma de todos los valores de factor de importancia para todas las preguntas de política del grupo de políticas.

10. En la lista **Grupo de políticas**, seleccione los grupos de políticas que desee supervisar.
11. Pulse **Guardar**.

## Supervisar el cambio de riesgo

Puede crear un elemento de panel de control que muestra el cambio de riesgo de política para activos, políticas y grupos de políticas seleccionados para cada día, semana y mes.

### Acerca de esta tarea

Utilice este elemento de panel de control para comparar los cambios en la puntuación de riesgo de política, controles de política y valores de política para un grupo de políticas a lo largo del tiempo.

El elemento de panel de control **Cambio de riesgo** utiliza flechas para indicar cuando un riesgo de política para valores seleccionados ha aumentado, disminuido o permanecido igual durante un periodo de tiempo seleccionado.

- Un número debajo de una flecha roja indica los valores que muestran un riesgo incrementado.
- Un número debajo de una flecha gris indica los valores para los que no ha habido cambio de riesgo.
- Un número debajo de una flecha verde indica los valores que muestran un riesgo reducido.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.
3. Escriba un nombre y una descripción para el panel de control de cumplimiento de políticas histórico.
4. Pulse **Aceptar**.
5. En la barra de herramientas, seleccione **Añadir elemento > Gestor de riesgos > Cambio de riesgo**.

Los elementos de panel de control del **Gestor de riesgos** se muestran solamente cuando IBM QRadar Risk Manager se utiliza con una licencia.

6. En la cabecera del elemento de panel de control nuevo, pulse el icono amarillo **Valores**.
7. En la lista **Grupo de políticas**, seleccione los grupos de políticas que desee supervisar.
8. Seleccione una opción en la lista **Valor para comparar**:
  - Si desea ver los cambios acumulativos en el factor de importancia para todas las preguntas de política dentro de los grupos de políticas seleccionados, seleccione **Puntuación de riesgo de política**.
  - Si desea ver cuántos controles de política han cambiado dentro de los grupos de políticas seleccionados, seleccione **Controles de política**.
  - Si desea ver cuántas políticas han cambiado dentro de los grupos de políticas seleccionados, seleccione **Políticas**.
9. Seleccione el período de cambio de riesgo que desee supervisar en la lista **Variación de tiempo**:
  - Si desea comparar cambios de riesgo de las 12:00 a.m. de hoy con los cambios de riesgo de ayer, seleccione **Día**.
  - Si desea comparar cambios de riesgo de las 12:00 a.m. del lunes de esta semana con los cambios de riesgo de la semana pasada, seleccione **Semana**.
  - Si desea comparar cambios de riesgo de las 12:00 a.m. del primer día del mes actual con los cambios de riesgo del mes pasado, seleccione **Mes**.
10. Pulse **Guardar**.

## Elementos de Gestión de vulnerabilidades

Los elementos de panel de control Gestión de vulnerabilidades solo se visualizan cuando se ha adquirido IBM QRadar Vulnerability Manager y se ha obtenido la licencia.

Para obtener más información, consulte la publicación *Guía del usuario de IBM QRadar Vulnerability Manager*.

Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña **Vulnerabilidades**. Los elementos de búsqueda se listan en el menú **Añadir elemento** > **Gestión de vulnerabilidades** > **Búsqueda de vulnerabilidades**. El nombre del elemento de búsqueda coincide con el nombre de los criterios de búsqueda guardada en los que se basa el elemento.

QRadar incluye criterios de búsqueda guardada predeterminados que se han preconfigurado para visualizar elementos de búsqueda en el menú de la **pestaña Panel de control**. Puede añadir más elementos de panel de control de búsqueda en el menú de la **pestaña Panel de control**.

Los tipos de gráfico soportados son tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar.

## Notificación del sistema

El elemento de panel de control Notificación del sistema muestra notificaciones de sucesos recibidas por el sistema.

Para que las notificaciones se muestren en el panel de control **Notificación del sistema**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccione el recuadro de selección **Notificar** en el Asistente de reglas personalizadas.

Para obtener más información sobre cómo configurar notificaciones de sucesos y crear reglas de suceso, consulte la publicación *Guía de administración de IBM QRadar*.

En el elemento de panel de control **Notificaciones del sistema**, puede ver la información siguiente:

- **Distintivo:** Visualiza un símbolo para indicar el nivel de gravedad de la notificación. Apunte al símbolo para ver más detalle sobre el nivel de gravedad.
  - Icono **Salud**
  - Icono **Información** (?)
  - Icono **Error** (X)
  - Icono **Aviso** (!)
- **Creado:** Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.
- **Descripción:** Visualiza información acerca de la notificación.
- **Icono Descartar (x):** Le permitirá cerrar una notificación del sistema.

Puede apuntar el ratón sobre una notificación para ver más detalles:

- **IP de host:** Visualiza la dirección IP del host que ha originado la notificación.
- **Gravedad:** Visualiza el nivel de gravedad de la incidencia que ha creado esta notificación.
- **Categoría de nivel bajo:** Visualiza la categoría de bajo nivel que está asociada con el incidente que ha generado esta notificación. Por ejemplo: Interrupción de servicio.
- **Carga útil:** Visualiza el contenido de carga útil que está asociado con el incidente que ha generado esta notificación.
- **Creado:** Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.

Cuando se añade el elemento de panel de control **Notificaciones del sistema**, las notificaciones del sistema también se pueden visualizar como notificaciones emergentes en la interfaz de usuario de QRadar. Estas notificaciones emergentes se visualizan en la esquina inferior derecha de la interfaz de usuario, independientemente de la pestaña seleccionada.

Las notificaciones emergentes solo están disponibles para los usuarios con permisos administrativos y están habilitadas de forma predeterminada. Para inhabilitar las notificaciones emergentes, seleccione **Preferencias de usuario** y borre el recuadro de selección **Habilitar notificaciones emergentes**.

En la ventana emergente **Notificaciones del sistema**, se resalta el número de notificaciones de la cola. Por ejemplo, si se visualiza (1 – 12) en la cabecera, la notificación actual es de 1 de 12 de notificaciones a visualizar.

La ventana emergente **Notificación del sistema** proporciona las opciones siguientes:

- **Icono Siguiente (>)**: Visualiza el siguiente mensaje de notificación. Por ejemplo, si el mensaje de notificación actual es 3 de 6, pulse el icono para ver 4 de 6.
- **Icono Cerrar (X)**: Cierra esta ventana emergente de notificación.
- **(detalles)**: Visualiza más información acerca de esta notificación del sistema.

## Centro de información de amenazas de Internet

El elemento de panel de control **Centro de información de amenazas de Internet** es un canal de información RSS que le proporciona avisos sobre problemas de seguridad, evaluaciones diarias sobre amenazas, noticias relacionadas con la seguridad y repositorios de amenazas.

El diagrama **Nivel de peligro actual** indica el nivel de peligro actual y proporciona un enlace que conduce a la página Nivel de peligro actual del sitio web IBM Internet Security Systems.

Los avisos actuales se listan en el elemento de panel de control. Para ver un resumen del aviso, pulse el icono de **Flecha** situado junto al aviso. El aviso se expandirá para mostrar un resumen. Pulse de nuevo el icono de flecha para ocultar el resumen.

Para investigar el aviso completo, pulse el enlace asociado. El sitio web IBM Internet Security Systems se abrirá en una ventana nueva del navegador para mostrar los detalles del aviso completo.

## Crear un panel de control personalizado

---

Puede crear un panel de control personalizado para ver un grupo de elementos de panel de control que cumplen un requisito determinado.

### Acerca de esta tarea

Después de crear un panel de control personalizado, el nuevo panel de control aparece en la pestaña **Panel de control** y en el cuadro de lista **Mostrar panel de control**. De forma predeterminada, un panel de control personalizado nuevo está vacío; por lo tanto, debe añadirle elementos.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. Pulse el icono **Panel de control nuevo**.
3. En el campo **Nombre**, escriba un nombre exclusivo para el panel de control. La longitud máxima es 65 caracteres.
4. En el campo **Descripción**, escriba una descripción del panel de control. La longitud máxima es de 1024 caracteres. Esta descripción se muestra en la ayuda contextual para el nombre de panel de control en el cuadro de lista **Mostrar panel de control**.
5. Pulse **Aceptar**.

## Utilización del panel de control para investigar actividad de registro o actividad de red

---

Los elementos de búsqueda de la pestaña de control proporcionan un enlace a los paneles **Actividad de registro** o **Actividad de red**, lo cual le permite investigar la actividad de registro o de red con más detalle.

### Acerca de esta tarea

Para investigar flujos desde un elemento de panel de control de **Actividad de registro**:

1. Pulse el enlace **Vista en Actividad de registro**. Se abrirá la pestaña **Actividad de registro**, que muestra resultados y dos gráficos correspondientes a los parámetros del elemento de panel de control.

Para investigar flujos desde un elemento de panel de control de **Actividad de red**:

1. Pulse el enlace **Vista en Actividad de red**. Se abrirá la pestaña **Actividad de red**, que muestra resultados y dos gráficos correspondientes a los parámetros del elemento de panel de control.

Los tipos de gráfico que aparecen en la pestaña **Actividad de registro** o **Actividad de red** dependen del gráfico que esté configurado en el elemento de panel de control:

Tipo de gráfico	Descripción
Barras, circular y de tabla	La pestaña <b>Actividad de registro</b> o <b>Actividad de red</b> muestra un gráfico de barras, un gráfico circular y una tabla de detalles de flujo.
Serie temporal	<p>La pestaña <b>Actividad de registro</b> o <b>Actividad de red</b> muestra gráficos de acuerdo con los criterios siguientes:</p> <ol style="list-style-type: none"> <li>1. Si el rango de tiempo que ha definido es menor o igual que 1 hora, se muestra un gráfico de serie temporal, un gráfico de barras y una tabla de detalles de suceso o de flujo.</li> <li>2. Si el rango de tiempo que ha definido es mayor que 1 hora, se muestra un gráfico de serie temporal y puede pulsar Actualizar detalles. Esta acción inicia una búsqueda la cual proporciona los detalles del suceso o flujo y genera un gráfico de barras. Cuando la búsqueda finaliza, se muestran el gráfico de barras y una tabla de detalles de suceso o flujo.</li> </ol>

## Configuración de tipos de gráficos de panel de control

Puede configurar diferentes tipos de gráficos de panel de control para presentar los datos de su organización de forma significativa.

De forma alternativa, utilice la aplicación de panel de control IBM QRadar Pulse para comunicar información y análisis acerca de la red. Visualice delitos, datos de red, amenazas y comportamiento de usuarios maliciosos, así como entornos de nube de todo el mundo en mapas geográficos, un mundo de amenazas en 3D, además de gráficos de actualización automática. Para obtener más información, consulte la aplicación [QRadar Pulse](https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm/Pulseapp.doc/c_Qapps_PulseDashboard_intro.html) (https://www.ibm.com/support/knowledgecenter/SS42VS\_latest/com.ibm/Pulseapp.doc/c\_Qapps\_PulseDashboard\_intro.html).

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el cuadro de lista **Mostrar panel de control**, seleccione el panel de control donde reside el elemento que desee personalizar.
3. En la cabecera del elemento de panel de control que desee configurar, pulse el icono **Valores**.
4. Configure los parámetros del gráfico.
  - a) En el cuadro de lista de **Valor para gráfico**, seleccione el tipo de objeto que desee representar en el gráfico. Las opciones incluyen todos los parámetros de suceso o de flujo normalizados y personalizados que se incluyen en los parámetros de búsqueda.
  - b) Seleccione un tipo de gráfico:
    - Los gráficos de barras, circulares y de tablas solo se encuentran disponibles para los sucesos o flujos agrupados.

- Los datos se acumulan de modo que cuando ejecuta una búsqueda guardada de serie temporal se encontrará disponible una memoria caché de datos de suceso o de flujo para mostrar los datos correspondientes al periodo de tiempo anterior. Los parámetros acumulados se indican mediante un asterisco (\*) en el cuadro de lista **Valor para gráfico**. Si selecciona un valor para representar gráficamente que no está acumulado (sin asterisco), no habrá datos de serie temporal disponibles.

Seleccione el recuadro de selección **Capturar datos de serie temporal** para habilitar la captura de serie temporal. Cuando selecciona este recuadro de selección, la característica de gráfico acumula datos para los gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada.

## Resultados

Las configuraciones para gráficos personalizados se conservan, de modo que se muestran como configurados cada vez que accede a la pestaña **Panel de control**.

## Eliminación de elementos de panel de control

---

Puede eliminar elementos de un panel de control y añadir el elemento de nuevo en cualquier momento.

### Acerca de esta tarea

Cuando se elimina un elemento del panel de control, el elemento no se elimina por completo.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea eliminar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono rojo [x] para eliminar el elemento del panel de control.

## Desconexión de un elemento del panel de control

---

Puede desconectar un elemento del panel de control y visualizar el elemento en una ventana nueva en el sistema.

### Acerca de esta tarea

Al desconectar un elemento de panel de control, el elemento de panel de control original permanece en la pestaña **Panel de control**, mientras que una ventana desconectada con un elemento de la pestaña de control duplicado permanece abierta y se renueva durante intervalos planificados. Si cierra la aplicación de QRadar, la ventana desconectada permanecerá abierta para supervisión y continúa renovándose hasta que se cierra manualmente la ventana o se cierra el sistema.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea desconectar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono verde para desconectar el elemento de panel de control y abrirlo en una ventana independiente.

## Renombrar un panel de control

---

Puede renombrar un panel de control y actualizar la descripción.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea editar.
3. En la barra de herramientas, pulse el icono **Renombrar panel de control**.
4. En el campo **Nombre**, escriba un nuevo nombre para el panel de control. La longitud máxima es de 65 caracteres.
5. En el campo **Descripción**, escriba una nueva descripción del panel de control. La longitud máxima es de 255 caracteres.
6. Pulse **Aceptar**.

## Supresión de un panel de control

---

Puede suprimir un panel de control.

### Acerca de esta tarea

Después de suprimir un panel de control, la pestaña **Panel de control** se renueva y se visualiza el primer panel de control que se lista en el recuadro de lista **Mostrar panel de control**. El panel de control que ha suprimido ya no se visualiza en el recuadro de lista **Mostrar panel de control**.

### Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea suprimir.
3. En la barra de herramientas, pulse **Suprimir panel de control**.
4. Pulse **Sí**.

## Gestión de notificaciones del sistema

---

Puede especificar el número de notificaciones que desea visualizar en el elemento de panel de control **Notificación del sistema** y cerrar las notificaciones del sistema después de leerlas.

### Antes de empezar

Asegúrese de que el elemento de panel de control **Notificación del sistema** se añade al panel de control.

### Procedimiento

1. En la cabecera de elemento de panel de control Notificación del sistema, pulse el icono **Valores**.
2. En el recuadro de lista **Visualizar**, seleccione el número de notificaciones de sistema que desea ver.
  - Las opciones son **5**, **10** (valor predeterminado), **20**, **50** y **Todos**.
  - Para ver todas las notificaciones del sistema que se han registrado en las últimas 24 horas, pulse **Todos**.
3. Para cerrar una notificación del sistema, pulse el icono **Suprimir**.



## Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos

---

Puede añadir elementos de panel de control basados en búsqueda al menú **Añadir elementos**.

### Antes de empezar

Para añadir un elemento de panel de control de búsqueda de sucesos y flujos al menú **Añadir elemento** en la pestaña **Panel de control**, debe acceder a la pestaña **Actividad de registro** o **Actividad de red** para crear criterios de búsqueda que especifiquen que los resultados de búsqueda se pueden visualizar en la pestaña **Panel de control**. Los criterios de búsqueda también deben especificar que los resultados se agrupan en un parámetro.

### Procedimiento

1. Elija:
  - Añadir un elemento de panel de control de búsqueda de flujos, pulse la pestaña **Actividad de red**.
  - Para añadir un elemento de panel de control de búsqueda de sucesos, pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, elija una de las opciones siguientes:
  - Para crear una búsqueda, seleccione **Nueva búsqueda**.
  - Para editar una búsqueda guardada, seleccione **Editar búsqueda**.
3. Configure o edite los parámetros de búsqueda, según sea necesario.
  - En el panel Editar búsqueda, seleccione la opción **Incluir en Panel de control**.
  - En el panel Definición de columna, seleccione una columna y pulse el icono **Añadir columna** para mover la columna a la lista **Agrupar por**.
4. Pulse **Filtro**.

Se visualizan los resultados de búsqueda.
5. Pulse **Guardar criterios**. Consulte Guardar criterios de búsqueda en la pestaña Delito.
6. Pulse **Aceptar**.
7. Verifique que los criterios de búsqueda guardados han añadido satisfactoriamente el elemento de panel de control de búsqueda de sucesos o flujos a la lista de **Añadir elementos**
  - a) Pulse la pestaña **Panel de control**.
  - b) Elija una de las siguientes opciones:
    - a) Para verificar un elemento de búsqueda de sucesos, seleccione **Añadir elemento > Actividad de registro > Búsquedas de suceso > Añadir elemento**.
    - b) Para verificar un elemento de búsqueda de flujo, seleccione **Añadir elemento > Actividad de red > Búsquedas de flujo**.

El elemento de panel de control se visualiza en la lista con el mismo nombre que los criterios de búsqueda guardados.



---

## Capítulo 4. Gestión de delitos

IBM QRadar reduce billones de sucesos y flujos a un número manejable de delitos procesables que se priorizan por su impacto en las operaciones de negocio. Utilice la pestaña **Delitos** para acceder a todos los datos necesarios para entender incluso las amenazas más complejas.

Proporcionando un contexto inmediato para el delito, QRadar ayuda a identificar rápidamente qué delitos son los más importantes y a iniciar una investigación para encontrar el origen del ataque o infracción de política de seguridad sospechosos.

**Restricción:** No puede gestionar delitos en IBM QRadar Log Manager. Para obtener más información sobre las diferencias entre IBM QRadar SIEM y IBM QRadar Log Manager, consulte [Capítulo 2, “Prestaciones de su producto IBM QRadar”](#), en la página 3.

---

### Priorización de delitos

La calificación de magnitud de un delito es una medida de la importancia del delito en el entorno. IBM QRadar utiliza la calificación magnitud para priorizar delitos y ayudarle a determinar qué delitos deben investigarse primero.

La *calificación de magnitud* de un delito se calcula en función de la relevancia, la gravedad y la credibilidad.

- La *relevancia* determina el impacto del delito en la red. Por ejemplo, si un puerto está abierto, la relevancia es alta.
- La *credibilidad* indica la integridad del delito, según lo determinado por la valoración de credibilidad configurada en el origen del registro. La credibilidad aumenta a medida que varios orígenes notifican el mismo suceso.
- La *gravedad* indica el nivel de amenaza que representa un origen en relación al grado de preparación del destino ante el ataque.

QRadar utiliza algoritmos complejos para calcular la calificación de magnitud del delito, y la calificación se reevalúa cuando se añaden nuevos sucesos al delito y también a intervalos planificados. Se tiene en cuenta la información siguiente cuando se calcula la magnitud del delito:

- el número de sucesos y flujos que están asociados con el delito
- el número de orígenes de registro
- la antigüedad del delito
- el peso de los activos asociados con el delito
- las categorías, la gravedad, la relevancia y la credibilidad de los sucesos y los flujos que contribuyen al delito
- las vulnerabilidades y evaluación de la amenaza de los hosts que están involucrados en el delito

La calificación de magnitud de un delito es diferente de la calificación de magnitud de un suceso. Puede influir en la magnitud de un delito estableciendo la magnitud de sucesos en las acciones de regla, pero no puede ignorar los algoritmos de QRadar para establecer la magnitud del delito.

---

### Encadenamiento de delitos

IBM QRadar encadena delitos para reducir el número de delitos que necesita revisar, lo que reduce el tiempo necesario para investigar y remediar la amenaza.

El encadenamiento de delitos ayuda a encontrar la causa raíz de un problema conectando varios síntomas y mostrándolos en un solo delito. Al comprender cómo ha cambiado un delito a lo largo del tiempo, puede ver cosas que pueden haberse ignorado durante el análisis. Algunos sucesos que no habría

valido la pena investigar por sí mismos pueden cobrar interés repentinamente cuando se correlacionan con otros sucesos para mostrar un patrón.

El encadenamiento de delitos se basa en el campo de índice de delito que se especifica en la regla. Por ejemplo, si la regla está configurada para utilizar la dirección IP de origen como el campo de índice de delito, solo hay un delito que tenga esa dirección IP de origen durante el tiempo que el delito está activo.

Puede identificar un delito encadenado buscando precedido por en el campo **Descripción** de la página **Resumen de delito**. En el ejemplo siguiente, QRadar ha combinado todos los sucesos que se han desencadenado para cada una de las tres reglas en un delito y ha añadido los nombres de regla al campo **Descripción**:

```
Exploit Followed By Suspicious Host Activity - Chained  
preceded by Local UDP Scanner Detected  
preceded by XForce Communication to a known Bot Command and Control
```

## Indexación de delitos

La indexación de delitos proporciona la capacidad de agrupar sucesos o flujos de diferentes reglas indexados en la misma propiedad en un solo delito.

IBM QRadar utiliza el parámetro de índice de delitos para determinar qué delitos deben encadenarse. Por ejemplo, un delito que solo tiene una dirección IP de origen y varias direcciones IP de destino indica que la amenaza tiene un solo atacante y múltiples víctimas. Si indexa este tipo de delito por la dirección IP de origen, todos los sucesos y flujos que se originen desde la misma dirección IP se añadirán al mismo delito.

Puede configurar reglas para indexar un delito en función de cualquier parte de información. QRadar incluye un conjunto de campos normalizados predefinidos que puede utilizarse para indexar los delitos. Si el campo en el que desea basar la indexación no está incluido en los campos normalizados, cree un suceso personalizado o una propiedad de flujo personalizada para extraer los datos de la carga útil y utilizarlos como el campo de indexación de delito en la regla. La propiedad personalizada en la que basar el índice puede basarse en una expresión regular, un cálculo o una expresión basada en AQL.

## Consideraciones sobre la indexación de delitos

Es importante comprender cómo afecta la indexación de delitos al despliegue de IBM QRadar.

### Rendimiento del sistema

Asegúrese de optimizar y habilitar todas las propiedades personalizadas que se utilizan para la indexación de delitos. La utilización de propiedades que no están optimizadas puede tener un efecto negativo en el rendimiento.

Al crear una regla, no puede seleccionar propiedades no optimizadas en el campo **Indexar delito según**. Sin embargo, si una regla existente se indexa en una propiedad personalizada y luego la propiedad personalizada se desoptimiza, la propiedad seguirá estando disponible en la lista de índice de delitos. No desoptimice propiedades personalizadas que se utilizan en reglas.

### Acción y respuesta de regla

Cuando el valor de la propiedad indexada es nulo, no se crea un delito aunque se marque el recuadro de selección **Asegurarse de que el suceso detectado forma parte de un delito** en la acción de regla. Por ejemplo, si una regla está configurada para crear un delito que se indexa por nombre de host, pero el nombre de host del suceso está vacío, no se crea un delito aunque se cumplan todas las condiciones de las pruebas de regla.

Cuando el limitador de respuestas utiliza una propiedad personalizada y el valor de propiedad personalizada es nulo, el límite se aplica al valor nulo. Por ejemplo, si la respuesta es **Correo electrónico**, y el limitador dice **Responder no más de 1 vez por 1 hora por propiedad personalizada**, si la regla se activa una segunda vez con una propiedad nula dentro de una hora, no se enviará un correo electrónico.

Al indexar mediante una propiedad personalizada, las propiedades personalizadas que puede utilizar en los campos de índice de regla y limitador de respuestas dependen del tipo de regla que esté creando. Una regla de suceso acepta propiedades de sucesos personalizadas en los campos de índice de regla y limitador de respuestas, mientras que una regla de flujo solo acepta propiedades de flujos personalizadas. Una regla común acepta propiedades de sucesos personalizadas o propiedades de flujos personalizadas en los campos de índice de regla y limitador de respuestas.

No puede utilizar propiedades personalizadas para indexar un delito creado por un suceso asignado.

### Contenido de carga útil

Los delitos indexados mediante Ariel Query Language (AQL), una expresión regular (regex) o mediante una propiedad calculada incluyen la misma carga útil que el suceso inicial que generó el delito.

Los delitos indexados por un campo de suceso normalizado, como por ejemplo una IP de origen o una IP de destino, incluyen el nombre de suceso y la descripción como carga útil de motor de reglas personalizadas (CRE).

## Ejemplo: Detección de irrupciones de programas maliciosos en función de la firma MD5

Como analista de seguridad de red de una gran organización, utiliza QRadar para detectar irrupciones de programas maliciosos. Establece los criterios para una irrupción como una amenaza que se produce en 10 hosts durante 4 horas. Desea utilizar la firma MD5 como base para esta detección de amenazas.

Debe configurar IBM QRadar para evaluar los registros entrantes a fin de determinar si existe una amenaza, y luego agrupar todas las reglas activadas que contienen la misma firma MD5 firma en un solo delito.

1. Cree una propiedad personalizada para extraer la firma MD5 de los registros. Asegúrese de que la propiedad personalizada esté optimizada y habilitada.
2. Cree una regla y configúrela para crear un delito que utilice la propiedad personalizada de firma MD5 como campo de índice de delito. Cuando se activa la regla, se crea un delito. Todas las reglas activadas que tienen la misma firma MD5 se agrupan en un delito.
3. Puede buscar por tipo de delito para encontrar los delitos que están indexadas según la propiedad personalizada de firma MD5.

## Retención de delitos

---

El estado de un delito determina cuánto tiempo IBM QRadar conserva el delito en el sistema. El periodo de retención de delito determina cuánto tiempo se conservan los delitos inactivos y cerrados antes de que se eliminen de la consola de QRadar.

### Delitos activos

Cuando una regla desencadena un delito, el delito está activo. En este estado, QRadar está a la espera de evaluar nuevos sucesos o flujos con respecto a la prueba de regla del delito. Cuando se evalúan sucesos nuevos, el reloj del delito se restablece para mantener el delito activo durante otros 30 minutos.

### Delitos latentes

Un delito pasa a estar latente si no se añaden sucesos o flujos nuevos al delito durante 30 minutos, o si QRadar no ha procesado ningún suceso durante 4 horas. Un delito permanece en estado latente durante 5 días. Si se añade un suceso mientras un delito está latente, se restablece el contador de cinco días.

### Delitos inactivos

Un delito pasa a estar inactivo después de 5 días de permanecer en estado latente. En el estado inactivo, los sucesos nuevos desencadenantes de la prueba de regla de delito no contribuyen al delito inactivo. Se añaden a un delito nuevo.

Los delitos inactivos se eliminan una vez transcurrido el periodo de retención del delito.

## Delitos cerrados

Los delitos cerrados se eliminan una vez transcurrido el periodo de retención del delito. Si se producen más sucesos para un delito que está cerrado, se crea un nuevo delito.

Si incluye delitos cerrados en una búsqueda y el delito no se ha eliminado de la consola de QRadar, el delito se muestra en los resultados de búsqueda.

El periodo de retención de delitos predeterminado es de 30 días. Una vez caducado el periodo de retención de delitos, los delitos cerrados e inactivos se eliminan del sistema. Los delitos que no están cerrados o inactivos se conservan indefinidamente. Puede proteger un delito para impedir que se elimine cuando caduque el periodo de retención.

## Proteger delitos

Puede haber delitos que desee conservar sin importar su periodo de retención. Puede proteger los delitos para impedir que se eliminen delitos de QRadar una vez transcurrido el periodo de retención.

### Acerca de esta tarea

De forma predeterminada, los delitos se conservan durante treinta días. Para obtener más información sobre la personalización del periodo de retención de delitos, consulte el manual *Guía de administración de IBM QRadar*.

### Procedimiento

1. Pulse la pestaña **Delitos** y, a continuación, pulse **Todos los delitos**.
2. Elija una de las siguientes opciones:
  - Seleccione el delito que desee proteger y luego seleccione **Proteger** en la lista **Acciones**.
  - En el cuadro de lista **Acciones**, seleccione **Proteger listados**.
3. Pulse **Aceptar**.

### Resultados

El delito está protegido y no se eliminará de QRadar. En la ventana **Delito**, el delito protegido está indicado por un icono **Protegido** en la columna Distintivo.

## Desproteger delitos

Puede desproteger delitos que anteriormente se habían protegido para impedir que se eliminaran una vez transcurrido su periodo de retención.

### Acerca de esta tarea

Para listar solamente delitos protegidos, puede realizar una búsqueda que aplica filtros para obtener solamente delitos protegidos. Si desmarca la casilla **Protegido** y están seleccionadas todas las demás opciones de la lista **Excluye la opción** en el panel Parámetros de búsqueda, solo se visualizan delitos protegidos.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Opcional: realice una búsqueda que muestra solamente delitos protegidos.
4. Elija una de las siguientes opciones:
  - Seleccione el delito que ya no desea proteger y luego seleccione **Desproteger** en el cuadro de lista **Acciones**.
  - En el cuadro de lista **Acciones**, seleccione **Desproteger listados**.
5. Pulse **Aceptar**.

## Investigaciones de delitos

IBM QRadar utiliza reglas para supervisar los sucesos y flujos de la red para detectar amenazas de seguridad. Cuando los sucesos y los flujos cumplen los criterios de prueba definidos en las reglas, se crea un delito para mostrar que se sospecha un ataque o infracción de la política de seguridad. Sin embargo, saber que un delito se ha producido es solo el primer paso; identificar cómo se ha producido, dónde se ha producido y quién lo ha cometido requiere alguna investigación.

La ventana **Resumen de delito** le ayuda a iniciar la investigación del delito suministrando contexto para ayudarle a comprender qué ha sucedido y determinar cómo aislar y resolver el problema.

The screenshot shows the 'Offense 31' summary page in IBM QRadar. The page is divided into several sections, each with a callout box asking a question:

- Offense Summary:** Contains fields for Magnitude, Status, Relevance (5), Severity (0), and Credibility (3). A callout box asks: "What was the attack?".
- Description:** "Large Outbound Transfer Slow Rate of Transfer preceded by Large Outbound Transfer High Rate of Transfer containing unknown". A callout box asks: "Was it successful?".
- Source Information:** Includes Source IP(s), Destination IP(s), and Network(s). A callout box asks: "Who was responsible?".
- Offense Source Summary:** Includes IP, Location, Magnitude, Vulnerabilities (0), Username (Unknown), Host Name (Unknown), and Asset Name. A callout box asks: "Where can I find them?".
- Top 5 Source IPs:** A table with columns for Source IP, Magnitude, and Offenses. A callout box asks: "How many targets are involved?".
- Top 5 Destination IPs:** A table with columns for Destination IP, Magnitude, Location, Vulnerability, Chained, User, MAC, Weight, Offenses, Source(s), Last EventFlow, and Events. A callout box asks: "Are the targets vulnerable?".
- Last 10 Events:** A table with columns for Event Name, Magnitude, Log Source, Category, Destination, and Time. A callout box asks: "Where is the evidence?".
- Top 5 Annotations:** A section for annotations. A callout box asks: "Why does QRadar consider the event threatening?".

Figura 8. Vista Resumen de delito

QRadar no utiliza permisos de usuario a nivel de dispositivo para determinar qué delitos puede ver cada usuario. Todos los usuarios que tienen acceso a la red pueden ver todos los delitos independientemente de qué origen de registro o el origen de flujo asociado con el delito. Para obtener más información sobre

la restricción del acceso de red, consulte la documentación de perfiles de seguridad en la *Guía de administración de IBM QRadar*.

## Seleccionar un delito para investigar

La pestaña **Delitos** muestra los ataques de seguridad sospechados y las infracciones de políticas que se producen en la red. Los delitos aparecen listados con el delito de mayor magnitud en primer lugar. Investigue los delitos de la parte superior de la lista en primer lugar.

### Acerca de esta tarea

Utilice las opciones de navegación de la izquierda para ver los delitos desde perspectivas diferentes. Por ejemplo, seleccione **Por IP de origen** o **Por IP de destino** para ver información sobre delincuentes reincidentes, direcciones IP que generan muchos ataques o sistemas que están constantemente bajo ataque. Puede refinar los delitos de la lista seleccionando un período de tiempo para los delitos que desea ver o cambiando los parámetros de búsqueda.

También puede buscar delitos que están basados en diversos criterios. Para obtener más información sobre la búsqueda de delitos, consulte [“Búsquedas de delitos”](#) en la página 152.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, seleccione la categoría de delitos que desea ver.
3. Dependiendo de la categoría que haya seleccionado, podrá seleccionar las siguientes opciones de filtrado:
  - a) En la lista **Ver delitos**, seleccione una opción para filtrar la lista de delitos para un intervalo de tiempo determinado.
  - b) En el panel **Parámetros de búsqueda actuales**, pulse los enlaces **Borrar filtro** para refinar la lista de delitos.
4. Para ver todos los delitos que se están produciendo en la red, pulse **Todos los delitos**.
5. Para ver todos los delitos que tiene asignados, pulse **Mis delitos**.
6. Para ver delitos agrupados en la categoría de alto nivel, pulse **Por categoría**.
  - a) Para ver los grupos de categoría de nivel bajo para una categoría de nivel alto, pulse el icono de flecha situado junto al nombre de la categoría de nivel alto.
  - b) Para ver una lista de delitos para una categoría de nivel bajo, haga una doble pulsación en la categoría de nivel bajo.

Los campos de recuento, tales como **Recuento de sucesos/flujo**s y **Recuento de orígenes**, no tienen en cuenta los permisos de red del usuario.
7. Para ver delitos agrupados por dirección IP de origen, pulse **Por IP de origen**.

La lista de delitos solo muestra las direcciones IP de origen con delitos activos.

  - a) Efectúe una doble pulsación en el grupo **IP de origen** que desee ver.
  - b) Para ver una lista de direcciones IP de destino locales para la dirección IP de origen, pulse **Destinos** en la barra de herramientas de página **Origen**.
  - c) Para ver una lista de delitos que están asociados a una dirección IP de origen, pulse **Delitos** en la barra de herramientas de la página **Origen**.
8. Para ver delitos agrupados por dirección IP de destino, pulse **Por IP de destino**.
  - a) Efectúe una doble pulsación en el grupo de direcciones **IP de origen** que desee ver.
  - b) Para ver una lista de delitos que están asociados a la dirección IP de destino, pulse **Delitos** en la barra de herramientas de la página **Destino**.
  - c) Para ver una lista de direcciones IP de origen que están asociadas a la dirección IP de destino, pulse **Orígenes** en la barra de herramientas de la página **Destino**.
9. Para ver delitos agrupados por red, pulse **Por red**.



- a) Efectúe una doble pulsación en la **Red** que desee ver.
  - b) Para ver una lista de direcciones IP de origen que están asociadas a la red, pulse **Orígenes** en la barra de herramientas de la página **Red**.
  - c) Para ver una lista de direcciones IP de destino que están asociadas a la red, pulse **Destinos** en la barra de herramientas de la página **Red**.
  - d) Para ver una lista de delitos que están asociados a la red, pulse **Delitos** en la barra de herramientas de la página **Red**.
10. Efectúe una doble pulsación en el delito para ver más información.

### Qué hacer a continuación

Utilice la información del resumen del delito y los detalles para investigar el delito y realizar las acciones necesarias.

## Investigar un delito mediante la información de resumen

La ventana **Resumen de delito** proporciona la información necesaria para investigar un delito en IBM QRadar. La información que es más importante para usted durante la investigación puede ser diferente dependiendo del tipo de delito que esté investigando.

Para facilitar la investigación de un delito, la parte inferior de la página **Resumen de delito** agrupa información acerca de los contribuyentes principales al delito. Este campo muestra solo las partes de información más recientes o importantes de esa categoría. Muchos campos muestran más información cuando se pasa el puntero del ratón sobre ellos. Algunos campos tienen opciones de menú contextual.

### Procedimiento

1. Pulse la pestaña **Delitos** y efectúe una doble pulsación en el delito que desee investigar.  
Se abre la ventana **Resumen de delito**.
2. Revise la primera fila de datos para conocer el nivel de importancia que QRadar ha asignado al delito.

#### Más información sobre la calificación de magnitud:

Parámetro	Descripción
<b>Magnitud</b>	Indica la importancia relativa del delito. Este valor se calcula en función de las calificaciones de relevancia, gravedad y credibilidad.
<b>Estado</b>	Pase el ratón por encima del icono de estado para ver el estado. QRadar no muestra un icono de estado cuando un delito está activo.
<b>Importancia</b>	Indica la importancia del destino. QRadar determina la importancia por el peso que el administrador ha asignado a las redes y los activos.
<b>Gravedad</b>	Indica la amenaza que un ataque representa en relación a cuán preparado está el destino para el ataque.
<b>Credibilidad</b>	Indica la integridad del delito, según lo determinado por la valoración de credibilidad configurada en el origen del registro. La credibilidad aumenta a medida que varios orígenes notifican el mismo suceso. Los administradores de QRadar configuran la calificación de credibilidad de los orígenes de registro.

3. Revise la información de la parte superior de la ventana **Resumen de delito** para obtener más información sobre el tipo de ataque y el marco de tiempo en que se ha producido.

#### Más información sobre la información de delito:

Parámetro	Descripción
<b>Descripción</b>	Muestra la causa del delito.  Los delitos encadenados muestran <b>Precedido de</b> , que indica que el delito ha cambiado con el paso del tiempo a medida que se han añadido nuevos sucesos y flujos a un delito.
<b>Tipo de delito</b>	El tipo de delito está determinado por la regla que ha creado el delito. El tipo de delito determina qué tipo de información se visualiza en el panel <b>Resumen de origen de delito</b> .
<b>Recuento de sucesos/flujos</b>	Para ver la lista de sucesos y flujos que han contribuido al delito, pulse los enlaces <b>Suceso</b> o <b>Flujo</b> .  Si el flujo muestra <b>N/D</b> , la fecha de inicio del delito podría ser anterior a la fecha en que actualizó a IBM QRadar versión 7.1 (MR1). Los flujos no pueden contarse, pero puede pulsar el enlace <b>N/D</b> para investigar los flujos.
<b>IP(s) de origen</b>	Especifica el dispositivo que intenta violar la seguridad de un componente de la red. El dispositivo puede tener una dirección IPv4 o IPv6.  Los delitos de tipo <b>IP de origen</b> siempre se originan en una única dirección IP de origen. Los delitos de otros tipos puede tener más de una dirección IP de origen. Puede ver más información sobre la dirección IP de origen pasando el ratón por encima de la dirección o mediante las acciones de pulsar el botón derecho y el botón izquierdo del ratón.
<b>IP de destino</b>	Especifica el dispositivo de red al que la dirección IP de origen ha intentado acceder. El dispositivo de red puede tener una dirección IPv4 o IPv6.  Si el delito tiene un solo destino, se visualiza la dirección IP. Si el delito tiene varios destinos, se visualiza el número de direcciones IP locales o remotas de destino. Puede ver más información pasando el ratón por encima de la dirección o mediante las acciones de pulsar el botón derecho y el botón izquierdo del ratón.
<b>Inicio</b>	Especifica la fecha y hora en que se produjo el primer suceso o flujo para el delito.
<b>Duración</b>	Especifica la cantidad de tiempo que ha transcurrido desde la creación del primer suceso o flujo asociado con el delito.
<b>Red(es)</b>	Especifica las redes locales de las direcciones IP de destino local establecidas como destino. QRadar considera como locales todas las redes que están especificadas en la jerarquía de redes. El sistema no asocia redes remotas a un delito, aunque se especifiquen como una red remota o un servicio remoto en la pestaña <b>Admin</b> .

4. En la ventana **Resumen de origen de delito**, revise la información sobre el origen del delito.

La información que se muestra en la ventana **Resumen de origen de delito** depende del campo **Tipo de delito**.

#### Más información sobre el resumen de origen:

Parámetro	Descripción
<b>Encadenado</b>	Especifica si la dirección IP de destino está encadenada.  Una dirección IP encadenada está asociada con otros delitos. Por ejemplo, una dirección IP de destino puede llegar a ser la dirección IP de origen de otro

Parámetro	Descripción
	delito. Si la dirección IP de destino está encadenada, pulse <b>Sí</b> para ver los delitos encadenados.
<b>IP de destino</b>	<p>Especifica el dispositivo de red al que la dirección IP de origen ha intentado acceder. El dispositivo de red puede tener una dirección IPv4 o IPv6.</p> <p>Si el delito tiene un solo destino, se visualiza la dirección IP. Si el delito tiene varios destinos, este campo muestra el número de direcciones IP locales o remotas de destino. Puede ver más información pasando el ratón por encima de la dirección o mediante las acciones de pulsar el botón derecho y el botón izquierdo del ratón.</p>
<b>Ubicación</b>	Especifica la ubicación de red de la dirección IP de origen o destino. Si la ubicación es local, pulse el enlace para ver las redes.
<b>Magnitud</b>	<p>Especifica la importancia relativa de la dirección IP de origen o destino.</p> <p>La barra de magnitudes proporciona una representación visual del valor de riesgo de CVSS del activo que está asociado a la dirección IP. Pase el puntero del ratón sobre la barra de magnitudes para mostrar la magnitud calculada.</p>
<b>Gravedad</b>	<p>Especifica la gravedad del suceso o delito.</p> <p>La gravedad indica el nivel de amenaza que un delito representa en relación a cuán preparada está la dirección IP de destino para el ataque. Este valor está correlacionado directamente con la categoría de suceso que está asociada al delito. Por ejemplo, un ataque de denegación de servicio (DoS) tiene una gravedad de 10, lo que indica un caso grave.</p>
<b>IP(s) de origen</b>	<p>Especifica el dispositivo que ha intentado violar la seguridad de un componente de la red. El dispositivo puede tener una dirección IPv4 o IPv6.</p> <p>Los delitos de tipo <b>IP de origen</b> siempre se originan en una única dirección IP de origen. Los delitos de otros tipos puede tener más de una dirección IP de origen. Puede ver más información sobre la dirección IP de origen pasando el ratón por encima de la dirección o mediante las acciones de pulsar el botón derecho y el botón izquierdo del ratón.</p>
<b>Nombre de usuario</b>	<p>Especifica el nombre de usuario que está asociado al suceso o flujo por el que se creó el delito.</p> <p>Pase el ratón por encima del nombre de usuario para ver la información más reciente de la base de datos de modelo de activos para el usuario.</p> <p>Los sucesos que no incluyen un nombre de usuario en la carga útil, o los sucesos generados por el sistema que pertenecen a un sistema local o una cuenta del sistema, muestran Desconocido.</p> <p>Para acceder a más información asociada con un nombre de usuario seleccionado, pulse el botón derecho del ratón en el nombre de usuario para mostrar las opciones de menú <b>Ver activos</b> y <b>Ver sucesos</b>.</p>
<b>Vulnerabilidades</b>	Especifica el número de vulnerabilidades identificadas que están asociadas a la dirección IP de origen o de destino. Este valor incluye también el número de vulnerabilidades activas y pasivas.

Cuando se visualiza la información de resumen de delitos históricos, los campos de datos **Último conocido** no se llenan.

5. En la parte inferior de la ventana **Resumen de delito**, revise la información adicional sobre los principales contribuyentes al delito, incluidas las notas y anotaciones recopiladas sobre el delito. Para ver toda la información que QRadar ha recopilado en una categoría, pulse los enlaces del lado derecho de la cabecera de categoría.

**Más información sobre la información que se presenta en los detalles del delito:**

<b>Categoría de detalles de delito</b>	<b>Descripción</b>
<b>Últimas 5 notas</b>	Se utilizan notas para el seguimiento de información importante recopilada durante la investigación del delito. Puede añadir una nota a un delito, pero no puede editar o suprimir notas.
<b>5 IPs de origen principales</b>	Muestra las 5 principales direcciones IP con la magnitud más alta, que es donde se ha originado el presunto ataque o infracción de política.  Los delitos que solo tienen una dirección IP de origen muestran solo una entrada en la tabla.
<b>5 IPs de destino principales</b>	Muestra las 5 principales direcciones IP locales con la magnitud más alta, que pueden indicar el destino del delito. Los delitos destinados a menos de 5 direcciones IP locales muestran menos entradas en la tabla.  La columna <b>Encadenado</b> indica si la dirección IP de destino es la dirección IP de origen de otro delito. El valor <b>Sí</b> en esta columna indica que un atacante tiene control sobre el sistema con esta dirección IP y lo está utilizando para atacar a otros sistemas.  La columna <b>Magnitud</b> muestra la puntuación de CVSS (Common Vulnerability Scoring System) de agregado, si existe. Cuando no está disponible la puntuación CVSS, la columna muestra la magnitud más alta de todos los delitos de los que la dirección IP forma parte.  Cuando pase el ratón sobre la dirección IP de destino, la <b>Magnitud de destino</b> mostrará la puntuación CVSS. Cuando no está disponible la puntuación CVSS, se visualiza un cero.
<b>5 orígenes de registro principales</b>	Muestra los orígenes de registro que aportan más sucesos al delito.  El motor de reglas personalizadas (CRE) crea un suceso y lo añade al delito cuando los criterios de prueba especificados en la regla personalizada coinciden con el suceso entrante. Un origen de registro que visualiza <b>Motor de reglas personalizadas</b> en el campo <b>Descripción</b> indica que QRadar ha creado los sucesos a partir de ese origen de registro.  <b>Sucesos totales</b> muestra la suma de todos los sucesos recibidos de este origen de registro mientras el delito estaba activo.
<b>5 usuarios principales</b>	Los sucesos deben incluir información de usuario para que QRadar llene esta tabla.
<b>5 categorías principales</b>	Muestra las categorías de nivel inferior que contienen la mayoría de los sucesos que han contribuido al delito.  <b>Recuento de destinos locales</b> muestra el número de direcciones IP de destino locales afectadas por delitos con sucesos en la categoría. Cuando todas las direcciones IP de destino son remotas, este campo muestra 0.
<b>Últimos 10 sucesos</b>	Muestra información acerca de los últimos 10 sucesos que han contribuido al delito.

Categoría de detalles de delito	Descripción
<b>Últimos 10 flujos</b>	Muestra información acerca de los últimos 10 flujos que han contribuido al delito.  La columna <b>Bytes totales</b> muestra la suma de los bytes transferidos en ambas direcciones.
<b>Anotaciones</b>	Las anotaciones proporcionan información sobre qué QRadar considera el suceso o el tráfico observado como amenazante.  QRadar puede añadir anotaciones cuando añada sucesos o flujos a un delito. La anotación más antigua muestra información que QRadar ha añadido al crear el delito. Los usuarios no pueden añadir, editar o suprimir anotaciones.
<b>Últimos 5 resultados de búsqueda</b>	Muestra información de las últimas cinco búsquedas planificadas.

6. Si ha instalado IBM QRadar Risk Manager, pulse **Ver vía de ataque** para ver qué activos de la red se comunican para permitir que un delito viaje a través de la red.

## Investigación de sucesos

Un suceso es un registro de un origen de registro, como un cortafuegos o dispositivo de direccionador, que describe una acción en una red o un host. Los sucesos que están asociados con un delito proporcionan pruebas de que se está produciendo actividad sospechosa en la red. Examinando los datos de suceso, comprenderá la causa del delito y determinará la mejor manera de aislar y mitigar la amenaza.

### Acerca de esta tarea

Algunos sucesos se crean en función de un suceso en bruto entrante, mientras que otros los crea el Motor de reglas personalizadas (CRE) de QRadar. Los sucesos creados por QRadar no tienen una carga útil porque no están basados en sucesos brutos.

### Procedimiento

1. En la ventana **Resumen de delito**, pulse **Sucesos**.  
La ventana **Lista de sucesos** muestra todos los sucesos que están asociados al delito.
2. Especifique la **Hora de inicio**, la **Hora de finalización** y las opciones **Ver** para ver los sucesos que se han producido dentro de un marco de tiempo específico.
3. Pulse la cabecera de columna del suceso para ordenar la lista de sucesos.
4. En la lista de sucesos, pulse el nombre de suceso con el botón derecho del ratón para aplicar opciones de filtro rápido a fin de reducir el número de sucesos a revisar.

También puede aplicar filtros rápidos a otras columnas de la lista de sucesos.

5. Efectúe una doble pulsación sobre un suceso para ver los detalles del mismo.

Las ventanas **Información de suceso** e **Información de origen y destino** solo muestran la información que se conoce sobre el suceso. En función del tipo de suceso, algunos campos pueden estar vacíos.

### Más información sobre los campos de hora de Información de suceso:

Campo	Descripción
<b>Hora de inicio</b>	La hora a la que QRadar ha recibido el suceso en bruto del origen de registro.
<b>Hora de almacenamiento</b>	La hora a la que QRadar ha almacenado el suceso normalizado.

Campo	Descripción
<b>Hora de origen de registro</b>	La hora registrada en el suceso en bruto desde el origen de registro.

6. En el recuadro **Información de carga útil**, revise el suceso en bruto para obtener información que QRadar no ha normalizado.

La información que no se ha normalizado no aparece en la interfaz de QRadar, pero puede ser útil para la investigación.

### Qué hacer a continuación

Para obtener más información sobre cómo utilizar QRadar para revisar los datos de suceso, consulte “Supervisión de actividad de registro” en la página 64 y [Capítulo 12, “Búsquedas de sucesos y flujos”](#), en la página 127.

### Información relacionada

[QRadar: detalles de suceso y la diferencia entre Hora de inicio, Hora de almacenamiento y Hora de origen de registro](#)

## Investigación de flujos

IBM QRadar correlaciona los flujos con un delito cuando identifica actividad sospechosa en las comunicaciones de red. El análisis de flujo proporciona visibilidad en la capa 7, o la capa de aplicación, para aplicaciones como navegadores web, NFS, SNMP, Telnet y FTP. Un flujo puede incluir información como, por ejemplo, direcciones IP, puertos, aplicaciones, estadísticas de tráfico y carga útil de paquete del tráfico sin cifrar.

De forma predeterminada, QRadar intenta extraer campos normalizados y propiedades de flujo personalizadas de los primeros 64 bytes de datos de flujo, pero los administradores pueden aumentar el tamaño de la captura de contenido para recopilar más datos. Para obtener más información, consulte el manual *Guía de administración de IBM QRadar*.

### Procedimiento

1. En la ventana **Resumen de delito**, pulse **Flujos** en el menú superior derecho.  
La ventana **Lista de flujos** muestra todos los flujos que están asociados al delito.
2. Especifique la **Hora de inicio**, la **Hora de finalización**, y las opciones **Ver** para ver los flujos que se han producido dentro de un marco de tiempo específico.
3. Pulse la cabecera de columna del flujo para ordenar la lista de flujos.
4. En la lista de flujos, pulse el nombre de flujo con el botón derecho del ratón para aplicar opciones de filtro rápido a fin de reducir el número de flujos a revisar.  
También puede aplicar filtros rápidos a otras columnas de la lista de flujos.
5. Efectúe una doble pulsación sobre un flujo para revisar los detalles del mismo.

### Más información acerca de los detalles de flujo:

Campo	Descripción
<b>Descripción del suceso</b>	Cuando la aplicación no está específicamente identificada en la carga útil, QRadar utiliza la decodificación incorporada para determinar la aplicación y muestra Aplicación detectada con decodificación basada en estado en <b>Descripción del suceso</b> .
<b>Carga útil de origen y Carga útil de destino</b>	Muestra el tamaño de la carga útil. Cuando el tamaño supera los 64 bytes, la carga útil puede contener información adicional que no se muestra en la interfaz de QRadar.

Campo	Descripción
<b>Reglas personalizadas coinciden parcialmente</b>	Muestra las reglas para las que no se ha cumplido el valor de umbral, pero por lo demás son coincidentes.
<b>Dirección del flujo</b>	Especifica la dirección del flujo, donde L indica red local y R indica red remota.

### Qué hacer a continuación

Para obtener más información sobre cómo utilizar QRadar para revisar los datos de flujo, consulte [Capítulo 7, “Supervisión de la actividad de red”](#), en la [página 87](#) y [Capítulo 12, “Búsquedas de sucesos y flujos”](#), en la [página 127](#).

## Acciones de delitos

IBM QRadar proporciona la posibilidad de actuar sobre los delitos conforme se investigan. Para ayudarle a rastrear delitos sobre los que se ha actuado, QRadar añade un icono a la columna **Distintivo** cuando se asigna un delito a un usuario, protege u oculta un delito, añade notas o marca el delito para su seguimiento.

Para realizar la misma acción sobre varios delitos, pulse y mantenga pulsada la tecla Control mientras selecciona cada delito sobre el que desea actuar. Para ver detalles de delito en una página nueva, pulse la tecla Control mientras hace una doble pulsación sobre un delito.

### Añadir notas

Añadir notas a un delito para rastrear la información que se recopila durante una investigación. Las notas pueden incluir un máximo de 2000 caracteres.

#### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Seleccione el delito al que desea añadir la nota.  
Para añadir la misma nota a varios delitos, pulse la tecla Control mientras selecciona cada delito.
3. En la lista **Acciones**, seleccione **Añadir nota**.
4. Escriba la nota que desee incluir para el delito.
5. Pulse **Añadir nota**.

#### Resultados

La nota aparecerá en el panel **Últimas 5 notas** de la ventana **Resumen de delitos**. Se mostrará un icono de **Notas** en la columna Distintivo de la lista de delitos.

Pase el puntero del ratón sobre el indicador de notas de la columna **Distintivo** de la lista **Delitos** para ver la nota.

### Ocultar delitos

Ocultar un delito para impedir que se visualice en la lista de delitos. Después de ocultar un delito, éste ya no se visualiza en la pestaña **Delitos** de ninguna lista, incluyendo la lista **Todos los delitos**. Sin embargo, si realiza una búsqueda que incluye delitos ocultos, el delito se visualiza en los resultados de la búsqueda.

#### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Seleccione el delito que desee ocultar.

Para ocultar varios delitos, mantenga pulsada la tecla Control mientras selecciona cada delito.

3. En el cuadro de lista **Acciones**, seleccione **Ocultar**.
4. Pulse **Aceptar**.

## Mostrar delitos ocultos

De forma predeterminada, la lista de delitos de la pestaña **Delitos** se filtra para excluir delitos ocultos. Para ver delitos ocultos, borre el filtro de la pestaña **Delitos** o realice una búsqueda que incluya delitos ocultos. Cuando incluya delitos ocultos en la lista de delitos, los delitos muestran la columna **Oculto** en la columna **Distintivo**.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Para borrar el filtro en la lista de delitos, pulse **Borrar filtro** junto al parámetro de búsqueda **Excluir delitos ocultos**.
3. Para crear una búsqueda nueva que incluya delitos ocultos, siga estos pasos:
  - a) En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
  - b) En la ventana **Parámetros de búsqueda**, quite la marca del recuadro de selección **Delitos ocultos** en la lista de opciones **Excluir**.
  - c) Pulse **Buscar**.
4. Para eliminar el distintivo oculto de un delito, siga estos pasos:
  - a) Seleccione el delito para el que desea eliminar el distintivo oculto.  
Para seleccionar varios delitos, mantenga pulsada la tecla Control mientras pulsa cada delito.
  - b) En el cuadro de lista **Acciones**, seleccione **Mostrar**.

El distintivo oculto se elimina y el delito aparece en la lista de delitos sin tener que borrar el filtro **Excluir delitos ocultos**.

## Cerrar delitos

Cierre un delito para eliminarlo completamente del sistema.

### Acerca de esta tarea

El periodo de retención de delitos predeterminado es de 30 días. Una vez caducado el periodo de retención de delitos, los delitos cerrados se suprimen del sistema. Puede proteger un delito para impedir que se suprima cuando caduque el periodo de retención.

Ya no se visualizan delitos cerrados en la pestaña **Delitos** de ninguna lista, incluyendo la lista **Todos los delitos**. Si incluye delitos cerrados en una búsqueda y el delito sigue estando dentro del periodo de retención, el delito se visualiza en los resultados de la búsqueda. Si se producen más sucesos para un delito que está cerrado, se crea un nuevo delito.

Cuando cierra un delito, debe seleccionar una razón para hacerlo. Si tiene el permiso **Gestionar cierres de delitos**, puede añadir razones de cierre personalizadas. Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *Guía de administración de IBM QRadar*.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Seleccione el delito que desee cerrar.  
Para cerrar varios delitos, mantenga pulsada la tecla Control mientras selecciona cada delito.
3. En la lista **Acciones**, seleccione **Cerrar**.
4. En la lista **Razón del cierre**, especifique una razón de cierre.  
Para añadir una razón de cierre, pulse el icono junto a **Razón del cierre** para abrir el cuadro de diálogo **Razones de cierre de delito personalizado**.



5. En el campo **Notas**, escriba una nota para proporcionar más información.

El campo **Notas** muestra la nota que se entró para el cierre de delito anterior. Las notas pueden tener un máximo de 2.000 caracteres.

6. Pulse **Aceptar**.

## Resultados

Después de cerrar los delitos, los recuentos que se muestran en la ventana **Por categoría** de la pestaña **Delitos** pueden tardar varios minutos en reflejar los delitos cerrados.

## Exportar delitos

Exporte delitos cuando desee reutilizar los datos o cuando desee almacenar los datos externamente. Por ejemplo, puede utilizar los datos de delitos para crear informes en una aplicación de terceros. Puede también exportar delitos como estrategia secundaria de retención a largo plazo. El servicio de soporte al cliente puede solicitarle que exporte delitos con fines de resolución de problemas.

Puede exportar delitos en formato XML (Extensible Markup Language) o CSV (comma-separated values). El archivo XML o CSV resultante incluye los parámetros especificados en el panel **Definición de columna** de los parámetros de búsqueda. El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

## Procedimiento

1. Pulse la pestaña **Delitos**.

2. Seleccione los delitos que desee exportar.

Para seleccionar varios delitos, mantenga pulsada la tecla Control mientras selecciona cada delito.

3. Elija una de las siguientes opciones:

- Para exportar delitos en formato XML, seleccione **Acciones > Exportar a XML**.
- Para exportar delitos en formato CSV, seleccione **Acciones > Exportar a CSV**

**Nota:** Si utiliza Microsoft Excel para importar el archivo CSV, debe seleccionar el entorno local correcto para asegurarse de que los datos se visualizan correctamente.

4. Elija una de las siguientes opciones:

- Para abrir el archivo para verlo de inmediato, seleccione **Abrir con** y seleccione una aplicación de la lista.
- Para guardar el archivo, seleccione **Guardar archivo**.

5. Pulse **Aceptar**.

El archivo `<fecha>-data_export.xml.zip`, se guarda en la carpeta de descarga predeterminada del sistema.

## Asignar delitos a usuarios

De forma predeterminada, ningún delito nuevo está asignado. Puede asignar un delito a un usuario de IBM QRadar a efectos de investigación.

### Acerca de esta tarea

Cuando un asigna un delito a un usuario, el delito se muestra en la página **Mis delitos** de ese usuario. Puede tener el permiso **Asignar delitos a usuarios** para asignar delitos a los usuarios. Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *Guía de administración de IBM QRadar*.

Puede asignar delitos a usuarios desde las páginas **Delitos** o **Resumen de delitos**. Este procedimiento proporciona instrucciones sobre cómo asignar delitos desde la pestaña **Delitos**.

## Procedimiento

1. Pulse la pestaña **Delitos**.
2. Seleccione el delito que desee asignar.  
Para asignar varios delitos, mantenga pulsada la tecla Control mientras selecciona cada delito.
3. En la lista **Acciones**, seleccione **Asignar**.
4. En la lista **Asignar a usuario**, seleccione el usuario que desee asignar al delito.

**Nota:** La lista **Asignar a usuario** muestra solo los usuarios que tienen privilegios para ver la pestaña **Delitos**. Los valores del perfil de seguridad de usuario también se siguen.

5. Pulse **Guardar**.

## Resultados

El delito se asignará al usuario seleccionado. Se mostrará el icono de **Usuario** en la columna Distintivo de la pestaña **Delitos** para indicar que el delito está asignado. El usuario designado podrá ver el delito en la página **Mis delitos**.

## Enviar notificaciones de correo electrónico

Comparta la información de resumen de delito con otra persona enviando un correo electrónico.

El cuerpo del mensaje de correo electrónico incluye la información siguiente, si está disponible:

- Dirección IP origen
- Nombre de usuario de origen, nombre de host o nombre de activo
- Número total de orígenes
- Cinco primeros orígenes por magnitud
- Redes de origen
- Dirección IP destino
- Nombre de usuario de destino, nombre de host o nombre de activo
- Número total de destinos
- Cinco primeros destinos por magnitud
- Redes de destino
- Número total de sucesos
- Delito o suceso que ha provocado la activación de la regla de delito o suceso
- Descripción completa de la regla de delito o suceso
- ID de delito
- Cinco primeras categorías
- Hora de inicio del delito u hora en que se creó el suceso
- Cinco primeras anotaciones
- Enlace a la interfaz de usuario del delito
- Reglas de CRE que intervienen

## Procedimiento

1. Pulse la pestaña **Delitos**.
2. Seleccione el delito para el cual desee enviar una notificación de correo electrónico.
3. En el cuadro de lista **Acciones**, seleccione **Enviar por correo electrónico**.
4. Configure los parámetros siguientes:

Opción	Descripción
Parámetro	Descripción

Opción	Descripción
<b>Para</b>	Escriba la dirección de correo electrónico del usuario al que desee informar cuando se produce un cambio en el delito seleccionado. Utilice una coma para separar las direcciones de correo electrónico.
<b>De</b>	Escriba la dirección de correo electrónico de origen. La dirección predeterminada es root@localhost.com.
<b>Asunto de correo electrónico</b>	Escriba el asunto para el correo electrónico. El valor predeterminado es <b>ID de delito</b> .
<b>Mensaje de correo electrónico</b>	Escriba el mensaje estándar que desea acompañar al correo electrónico de notificación.

5. Pulse **Enviar**.

## Marcado de un delito para su seguimiento

Marque un delito para su seguimiento cuando desee señalarlo para su posterior investigación.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Busque el delito que desea marcar para su seguimiento.
3. Efectúe una doble pulsación en el delito.
4. En la lista **Acciones**, seleccione **Seguimiento**.

### Resultados

El delito muestra ahora el icono de seguimiento en la columna **Distintivo**. Para ordenar la lista de delitos de modo que muestre los delitos señalados en la parte superior, pulse la cabecera de columna **Distintivos**.



---

## Capítulo 5. QRadar Analyst Workflow

IBM Security QRadar Analyst Workflow proporciona nuevos métodos para filtrar delitos, sucesos y representaciones gráficas de delitos por magnitud, asignado y tipo. El flujo de trabajo de delitos mejorado proporciona un método más intuitivo para investigar un delito para determinar la causa raíz de un problema y trabajar para resolverlo. Utilice el creador de consultas incorporado para crear consultas de AQL utilizando ejemplos y búsquedas guardadas o compartidas, o escribiendo texto sin formato en el campo de búsqueda.

### Delitos

La página Delitos muestra una tabla de los delitos en su entorno de QRadar que puede filtrar de muchas maneras diferentes. También incluye representaciones gráficas de delitos, por magnitud, asignado y tipo. En esta página, puede investigar un delito para determinar la causa raíz de un problema y trabajar para resolverlo.

### Buscar

La página Buscar incluye un Creador de consultas que puede utilizar para crear una búsqueda de Ariel Query Language (AQL) para encontrar delitos específicos. Cree una búsqueda utilizando ejemplos, búsquedas guardadas o compartidas, o escribiendo directamente en el Creador de consultas. La página Buscar también incluye enlaces a muchos recursos para obtener información sobre la creación de consultas de AQL.

### Aplicaciones

La lista Aplicaciones incluye las aplicaciones de QRadar que son compatibles con el nuevo Analyst Workflow. El primer release del flujo de trabajo incluye la aplicación QRadar Pulse.

Consulte el anuncio de QRadar Analyst Workflow en el [Blog de anuncio de IBM Security Community](#).

---

## Novedades de QRadar Analyst Workflow

Conozca las nuevas funciones y características que permiten supervisar los delitos en QRadar Analyst Workflow.

### Versión 1.1.0

Puede instalar QRadar Analyst Workflow 1.1.0 en un sistema de alta disponibilidad

Este release soluciona los siguientes problemas conocidos:

- El panel **Detalles de suceso** muestra los detalles de los sucesos anómalos.
- Falta de reglas en el panel **Filtro**.
- La información de la IP externa siempre muestra 1 de enero de 1970.
- El filtrado multidominio no funciona.
- El panel **Filtro** se carga continuamente en algunas búsquedas.
- Fecha de creación incorrecta en la tarjeta Búsqueda reciente.
- En ocasiones, aparecen filtros para `logSources;null` y `logSourceType;null` que no se pueden analizar al actualizar.
- Los datos del gráfico no se actualizan si se aplica un filtro NOT.

---

## Problemas conocidos

QRadar Analyst Workflow incluye información necesaria de problemas conocidos.

QRadar Analyst Workflow 1.1.0 incluye los siguientes problemas conocidos:

- Todos los husos horarios se visualizan en el huso horario del cliente, en lugar del huso horario del servidor.
- El botón **Atrás** del navegador no funciona en la página **Sucesos del delito**.
- Los proxies no están soportados.
- El panel **Suceso** puede fallar cuando un tipo de origen de registro tiene demasiadas propiedades personalizadas.
- El mensaje de error esperado no aparece si Analyst Workflow no se puede conectar a X-Force.

## Instalación de QRadar Analyst Workflow

---

Puede instalar IBM Security QRadar Analyst Workflow en QRadar 7.4.0 o posterior.

### Antes de empezar

Si ha instalado previamente una versión del flujo de trabajo, asegúrese de eliminar las carpetas creadas durante dicho proceso de instalación.

### Procedimiento

1. Si tiene certificados personalizados, ejecute los siguientes mandatos en la consola de QRadar en cualquier directorio:
  - `update-ca-trust`
  - `systemctl restart docker`
2. Descargue la versión más reciente del archivo `QRadarAnalystWorkflow<x.x.x>.zip` desde Fix Central. Consulte las instrucciones de IBM Security [App Exchange](#).
3. Copie el archivo en el host de QRadar utilizando el mandato "Secure Copy" (`scp`) de Linux o un cliente FTP.

**Ejemplo de Secure Copy:** `scp QRadarAnalystWorkflow<x.x.x>.zip <host de QRadar>:/<directorio>`

4. Escriba el siguiente mandato para crear un nuevo directorio en el host de QRadar: `mkdir qradar-ui`

**Nota:** Si este directorio ya existe, de una instalación anterior, suprimalo antes de extraer el archivo `.zip`.

5. Para extraer la versión más reciente del archivo `QRadarAnalystWorkflow<x.x.x>.zip` en el host de QRadar, escriba el mandato siguiente: `unzip QRadarAnalystWorkflow<x.x.x>.zip -d qradar-ui`
6. Ejecute `./qradar-ui/start.sh` y, a continuación, espere a que se ejecuten los registros.
7. Acceda a QRadar Analyst Workflow utilizando uno de los métodos siguientes:

- En el menú de navegación, pulse **Pruebe la nueva interfaz de usuario**.
- Acceda a la nueva interfaz de usuario del navegador en `https://<dirección IP de QRadar>/console/ui`.

**Consejo:** Para obtener más información, consulte este [útil vídeo sobre la instalación de QRadar Analyst Workflow](#).

## Delitos

---

La página Visión general de los delitos muestra una tabla de los delitos en su entorno de QRadar que puede filtrar de muchas maneras diferentes. También incluye representaciones gráficas de delitos, por magnitud, asignado y tipo.

En la página de delitos, puede investigar un delito para determinar la causa raíz de un problema y trabajar para resolverlo.

**Consejo:** Para obtener más información sobre la investigación de delitos en QRadar Analyst Workflow, consulte esta [guía paso a paso en vídeo sobre delitos](#).

## Visualización de delitos

Filtre la tabla Delitos para visualizar los delitos específicos que desee investigar.

### Acerca de esta tarea

Cuando aplica los filtros, la tabla de delitos muestra solo los delitos que cumplen los criterios de filtro. Los gráficos visualizados en la página también cambian para reflejar solo los delitos de la lista filtrada.


**Consejo:** Puede copiar y pegar el URL del navegador para compartir la página de delitos, incluidos todos los filtros y las opciones de configuración.

### Procedimiento

1. Para aplicar un filtro, pulse una de las siguientes categorías para ver las opciones de filtrado de dicha categoría:

- Magnitud
- Gravedad
- Asignado a
- Estado
- Hora de inicio
- Tipo de delito
- Nombre de origen de registro
- Tipo de origen de registro
- Red de destino
- Direcciones de destino locales
- Direcciones de origen
- Reglas
- Seguimiento
- Protegido

2. Para incluir solo delitos con atributos específicos, seleccione ese atributo en la lista de filtros. Para

excluir delitos con atributos específicos, pulse el icono  situado junto al atributo y pulse **Aplicar filtro IS NOT**.

**Consejo:** Puede pulsar con el botón derecho Estado, Tipo, IP de origen o IP de destino en la tabla de delitos y aplicar rápidamente un filtro IS o IS NOT a los delitos.

3. Para ordenar la tabla de delitos en orden ascendente o descendente por un atributo, pulse la cabecera de tabla adecuada.
4. Para borrar filtros individuales, pulse la **X** en el indicador de filtro. Para borrar todos los filtros, pulse **Borrar filtros**.
5. Para configurar el número de delitos que se muestran en la tabla, pulse el menú desplegable **Elementos por página** en la parte inferior de la tabla.
6. Para ordenar la tabla de delitos en orden ascendente o descendente por un atributo, pulse la cabecera de tabla adecuada.

## Investigación de delitos

Inicie la investigación de delitos pulsando un delito en la tabla de delitos. Los detalles del delito proporcionan contexto para ayudarle a comprender lo ocurrido y determinar cómo aislar y resolver el problema.

Además de la información básica incluida en la tabla de delitos, la página de detalles del delito incluye la siguiente información detallada:

Característica	Descripción
Insights	La sección Insights muestra las reglas que han desencadenado el suceso. Pulse una regla para ver los detalles sobre reglas específicas.
Gráfico de sucesos	El gráfico de sucesos muestra el número de sucesos que se han producido en un momento dado en los últimos 7 días activos. Utilice la barra de reproducción en la parte superior del gráfico para ir a horas específicas y los picos de sucesos. Pulse <b>Ver sucesos</b> para ver la lista de sucesos que han contribuido al delito e investigar los detalles del suceso.
IP de origen y destino	Si los delitos incluyen varias IP de origen o destino, puede pulsar las listas de IP para desplazarse por la lista completa de IP. Pulse una dirección IP específica para ver los detalles sobre esa IP.
Magnitud	El gráfico de magnitud proporciona una representación visual de cómo se ha calculado la magnitud, en función de la relevancia, la credibilidad y la gravedad. Pulse el gráfico para ver una descripción detallada de cómo se calcula la magnitud.
Notas	En la sección Notas, puede pulsar una nota larga para ver el texto completo. Pulse <b>Añadir nota</b> para añadir su propia nota a los detalles del delito.

**Consejo:** Si un delito tiene un título largo, pulse el título para ver el título de delito completo.

## Acciones de delitos

Saber que un delito se ha producido es solo el primer paso; identificar cómo se ha producido, dónde se ha producido y quién lo ha cometido requiere una investigación.

Utilice QRadar Analyst Workflow para realizar un seguimiento de los delitos en toda la investigación.

### Marcado de un delito para su seguimiento

Marque un delito para su seguimiento cuando desee señalarlo para su posterior investigación.

### Procedimiento

1. En la tabla Delitos, realice una de las acciones siguientes:
  - Seleccione los delitos que desee marcar.
  - Pulse una lista de delitos para abrir los detalles de los delitos.
2. En la lista **Acciones**, seleccione **Seguimiento**.

**Consejo:** Para eliminar el distintivo, seleccione **Dejar de seguir** en la lista **Acciones**.



## Proteger delitos

Puede haber delitos que desee conservar sin importar su periodo de retención. Puede proteger los delitos para impedir que se eliminen delitos de IBM QRadar una vez transcurrido el periodo de retención.

## Acerca de esta tarea

De forma predeterminada, los delitos se conservan durante treinta días. Para obtener más información sobre la personalización del período de retención de delitos, consulte la *Guía de administración de IBM QRadar*.

## Procedimiento

1. En la tabla Delitos, realice una de las acciones siguientes:
  - Seleccione los delitos que desee proteger.
  - Pulse una lista de delitos para abrir los detalles de los delitos.
2. En la lista **Acciones**, seleccione **Proteger**.

**Consejo:** Para eliminar la protección del delito, seleccione **Desproteger** en la lista **Acciones**.

## Ocultar delitos

Oculte un delito para impedir que se visualice en la tabla de delitos. Después de ocultar un delito, éste solo se visualiza si aplica un filtro IS para **Estado = Oculto**.

## Procedimiento

1. En la tabla Delitos, realice una de las acciones siguientes:
  - Seleccione los delitos que desee ocultar.
  - Pulse una lista de delitos para abrir los detalles de los delitos.
2. En la lista **Acciones**, seleccione **Ocultar**.

**Consejo:** Para desocultar el delito, filtre para ver los delitos ocultos y seleccione **Abrir** en la lista **Acciones**.

## Cerrar delitos

Cierre un delito para eliminarlo completamente del sistema.

## Acerca de esta tarea

El periodo de retención de delitos predeterminado es de 30 días. Una vez caducado el periodo de retención de delitos, los delitos cerrados se suprimen del sistema. Puede proteger un delito para impedir que se suprima cuando caduque el periodo de retención.

Después de cerrar un delito, éste solo se visualiza si aplica un filtro IS para **Estado = Cerrado**. Si se producen más sucesos para un delito que está cerrado, se crea un nuevo delito.

Cuando cierra un delito, debe seleccionar una razón para hacerlo. Si tiene el permiso **Gestionar cierres de delitos**, puede añadir razones de cierre personalizadas. Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *Guía de administración de IBM QRadar*.

## Procedimiento

1. En la tabla Delitos, realice una de las acciones siguientes:
  - Seleccione los delitos que desee cerrar.
  - Pulse una lista de delitos para abrir los detalles de los delitos.
2. En la lista **Acciones**, seleccione **Cerrar**.
3. Especifique una razón de cierre en la lista **Seleccione una opción de resolución**.
4. En el campo de texto, escriba una nota para proporcionar más información.

Las notas pueden tener un máximo de 1.984 caracteres.

5. Pulse **Aceptar**.


## Consulta de datos de sucesos y flujos para encontrar delitos específicos

Busque datos de suceso y flujo específicos mediante la creación de búsquedas de Ariel Query Language (AQL) en el Creador de consultas.

### Acerca de esta tarea

Cree búsquedas utilizando el historial de búsquedas o especifique palabras clave directamente en el Creador de consultas. Esta información rellena una plantilla de consulta que puede personalizar para que se adapte a sus necesidades o crear manualmente sus propias búsquedas.

### Procedimiento

1. En el menú de navegación () pulse **Buscar**.
2. Escriba una de las palabras clave siguientes en **Creador de consultas** para iniciar una consulta:
  - Dirección IP
  - URL
  - Hash MD5/SHA-1/SHA-256
3. Seleccione una de las búsquedas predefinidas en la lista que aparece cuando especifica una palabra clave.
4. Revise y edite la plantilla de consulta para acotar la búsqueda y, a continuación, pulse **Ejecutar consulta**.

#### Consejo:

- Las señales de sintaxis se codifican por colores en función de la clase de señal.
- Para crear una serie AQL sintácticamente correcta, los paréntesis emparejados se subrayan cuando se coloca el cursor entre ellos.

```
(startTime, 'MMM dd hh:mm a')
```

5. Pulse **Filtro** para acotar más los resultados de búsqueda y, a continuación, seleccione un delito para ver más detalles.
6. Para ejecutar un resultado de búsqueda existente, seleccione la consulta en el campo **Última búsqueda** para añadirla al Creador de consultas y, a continuación, pulse **Ejecutar consulta**.
7. Opcional: Expanda la sección **Formación y recursos** para obtener más información sobre las consultas de AQL.

### Ejemplo

A continuación, se muestra un ejemplo de una consulta de AQL.

```
SELECT sourceip, destinationip, username
FROM events
WHERE username = 'test name'
GROUP by sourceip, destinationip
ORDER BY sourceip DESC
LIMIT 10
LAST 2 DAYS
```

Para obtener más información sobre la creación de consultas en QRadar Analyst Workflow, consulte esta [guía paso a paso en vídeo sobre la característica de búsqueda](https://youtu.be/GjIT15aFvPU) (https://youtu.be/GjIT15aFvPU).

Para obtener más información sobre las consultas de AQL, consulte estos recursos de documentación y formación:

- [Introducción a AQL con consultas de ejemplo](https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/r_qradar_aql_intro_AQL_queries.html) (https://www.ibm.com/support/knowledgecenter/SS42VS\_latest/com.ibm.qradar.doc/r\_qradar\_aql\_intro\_AQL\_queries.html)
- [Visión general de Ariel Query Language](https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_aql_introduction.html) (https://www.ibm.com/support/knowledgecenter/SS42VS\_latest/com.ibm.qradar.doc/c\_aql\_introduction.html)
- [Operadores lógicos y de comparación de AQL](https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/r_aql_operators.html) (https://www.ibm.com/support/knowledgecenter/SS42VS\_latest/com.ibm.qradar.doc/r\_aql\_operators.html)
- [Parte 1 de la guía de aprendizaje de QRadar AQL: documentación y sintaxis básica](https://youtu.be/-ZHVubxGO2s) (https://youtu.be/-ZHVubxGO2s)
- [Parte 2 de la guía de aprendizaje de QRadar AQL: funciones de AQL muy útiles](https://youtu.be/KfXrij5hGSM) (https://youtu.be/KfXrij5hGSM)

### Conceptos relacionados

#### Investigación de delitos

Inicie la investigación de delitos pulsando un delito en la tabla de delitos. Los detalles del delito proporcionan contexto para ayudarle a comprender lo ocurrido y determinar cómo aislar y resolver el problema.

### Tareas relacionadas

#### Visualización de delitos

Filtre la tabla Delitos para visualizar los delitos específicos que desee investigar.

## Sucesos

---

Utilice la página Sucesos para continuar investigando sucesos específicos para determinar la causa raíz de un problema y trabajar para resolverlo.

La página Sucesos muestra una tabla de los sucesos que han contribuido a un delito específico. Puede filtrar estos sucesos para que se ajusten a sus necesidades.

### Conceptos relacionados

#### Investigación de delitos

Inicie la investigación de delitos pulsando un delito en la tabla de delitos. Los detalles del delito proporcionan contexto para ayudarle a comprender lo ocurrido y determinar cómo aislar y resolver el problema.

#### Acciones de delitos

Saber que un delito se ha producido es solo el primer paso; identificar cómo se ha producido, dónde se ha producido y quién lo ha cometido requiere una investigación.

## Investigación de sucesos

El gráfico de sucesos de la página de detalles del delito muestra el número de sucesos que se han producido en un momento dado en los últimos 7 días activos.

### Procedimiento

1. En la página de delitos, pulse un delito en la tabla de delitos para abrir la página de detalles.
  - Consejo:** Utilice la barra de reproducción en la parte superior del gráfico de sucesos para ir a horas específicas y los picos de sucesos.
2. Pulse **Ver sucesos** para ver la lista de sucesos que han contribuido al delito e investigar los detalles del suceso.
3. Para configurar el número de sucesos devueltos en los resultados del filtro, pulse las flechas en el indicador Límite de resultados.
4. Para configurar el número de sucesos que se muestran en la tabla, pulse el menú desplegable Elementos por página en la parte inferior de la tabla.
5. Para ordenar la tabla de sucesos en orden ascendente o descendente por un atributo, pulse la cabecera de tabla adecuada.

6. Pulse un suceso para ver más detalles sobre ese suceso. También puede pulsar un origen de registro, una IP de origen o una IP de destino para obtener información específica sobre dicho origen o destino.
7. Pulse **Actualizar sucesos** para renovar los resultados de los sucesos.

**Consejo:** Puede copiar y pegar el URL del navegador para compartir la página de sucesos, incluidos todos los filtros y las opciones de configuración.

## Filtrado de sucesos


Filtre la página Sucesos para visualizar solo los sucesos específicos que desee investigar.

### Acerca de esta tarea

Cuando aplica los filtros, la tabla de sucesos muestra solo los sucesos que cumplen los criterios de filtro.

**Consejo:** Puede copiar y pegar el URL del navegador para compartir la página de sucesos, incluidos todos los filtros y las opciones de configuración.

### Procedimiento

1. Para aplicar un filtro, pulse una de las siguientes categorías para ver las opciones de filtrado de dicha categoría:
  - Hora del suceso
  - Magnitud
  - Nombre de origen de registro
  - Categoría
  - IP de origen
  - Puerto de origen
  - IP de destino
  - Puerto de destino
  - Nombre de suceso
  - Usuario
2. Para incluir solo sucesos con atributos específicos, seleccione ese atributo en la lista de filtros. Para excluir sucesos con atributos específicos, pulse el icono  situado junto al atributo y, a continuación, pulse **Aplicar filtro IS NOT**.

**Consejo:** Puede pulsar con el botón derecho del ratón un Origen de registro, IP de origen, IP de destino, Categoría o Nombre de usuario en la tabla de sucesos y aplicar rápidamente a los sucesos un filtro IS o IS NOT.
3. Para ordenar la tabla de sucesos en orden ascendente o descendente por un atributo, pulse la cabecera de tabla adecuada.
4. Para borrar filtros individuales, pulse la **X** en el indicador de filtro. Para borrar todos los filtros, pulse **Borrar filtros**.
5. Pulse **Actualizar sucesos** para renovar los resultados de los sucesos.

## Capítulo 6. Investigación de la actividad de registro

Puede supervisar e investigar sucesos en tiempo real o realizar búsquedas avanzadas.

Utilizando la pestaña **Actividad de registro**, puede supervisar e investigar la actividad de registro (sucesos) en tiempo real o realizar búsquedas avanzadas.

### Visión general de la pestaña Actividad de registro

Un suceso es un registro de un origen de registro, como un cortafuegos o dispositivo de direccionador, que describe una acción en una red o un host.

La pestaña **Actividad de registro** especifica qué sucesos se asocian con delitos.

Debe tener permiso para ver la pestaña **Actividad de registro**.

### Barra de herramientas de pestaña Actividad de registro

Puede acceder a varias opciones desde la barra de herramientas Actividad de registro

Mediante la barra de herramientas, puede acceder a las siguientes opciones:

Opción	Descripción
Buscar	Pulse <b>Buscar</b> para realizar búsquedas avanzadas en sucesos. Las opciones incluyen: <ul style="list-style-type: none"><li>• <b>Nueva búsqueda:</b> Seleccione esta opción para crear una nueva búsqueda de sucesos.</li><li>• <b>Editar búsqueda:</b> Seleccione esta opción para seleccionar y editar una búsqueda de sucesos.</li><li>• <b>Gestionar resultados de búsqueda:</b> seleccione esta opción para ver y gestionar resultados de búsqueda.</li></ul>
Búsquedas rápidas	Desde este cuadro de lista, puede ejecutar búsquedas guardadas anteriormente. Las opciones se muestran en el recuadro de lista <b>Búsquedas rápidas</b> solo cuando ha guardado los criterios de búsqueda que especifican la opción <b>Incluir en Búsquedas rápidas</b> .
Añadir filtro	Pulse <b>Añadir filtro</b> para añadir un filtro a los resultados de búsqueda actuales.
guardar criterios	Pulse <b>Guardar criterios</b> para guardar los criterios de búsqueda actuales.
Guardar resultados	Pulse <b>Guardar resultados</b> para guardar los resultados de búsqueda actuales. Esta opción solo se muestra después de realizar una búsqueda. Esta opción está inhabilitada en modalidad continua.
Cancelar	Pulse <b>Cancelar</b> para cancelar una búsqueda que está en curso. Esta opción está inhabilitada en modalidad continua.

Tabla 8. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Falso positivo	<p>Pulse <b>Falso positivo</b> para abrir la ventana <b>Ajuste de falsos positivos</b>, que le permitirá impedir que los sucesos que se conoce que son falsos positivos creen delitos.</p> <p>Esta opción está inhabilitada en modalidad continua. Para obtener más información sobre el ajuste de falsos positivos, consulte <a href="#">Ajuste de falsos positivos</a>.</p>
Reglas	<p>La opción Reglas solo es visible si tiene permiso para ver reglas.</p> <p>Pulse <b>Reglas</b> para configurar reglas de suceso personalizadas. Las opciones incluyen:</p> <ul style="list-style-type: none"> <li>• <b>Reglas:</b> Seleccione esta opción para ver o crear una regla. Si solo tiene permiso para ver reglas, se visualiza la página de resumen del asistente de reglas. Si tiene permiso para mantener reglas personalizadas, se visualiza el asistente de reglas y puede editar la regla. Para habilitar las opciones de regla de detección de anomalías (Añadir regla de umbral, Añadir regla conductual y Añadir regla de anomalía), debe guardar los criterios de búsqueda agregados porque los criterios de búsqueda guardados especifican los parámetros necesarios.</li> </ul> <p><b>Nota:</b> Las opciones de regla de detección de anomalías solo están visibles si tiene el permiso <b>Actividad de registro &gt; Mantener reglas personalizadas</b> .</p> <ul style="list-style-type: none"> <li>• <b>Añadir regla de umbral:</b> Seleccione esta opción para crear una regla de umbral. Una regla de umbral prueba en el tráfico de sucesos la actividad que supera un umbral configurado. Los umbrales pueden basarse en los datos que QRadar recopila. Por ejemplo, si crea una regla de umbral que indica que no pueden iniciar la sesión en el servidor más de 220 clientes entre las 08:00 y las 17:00, las reglas generan una alerta cuando el cliente número 221 intenta iniciar la sesión.</li> </ul> <p>Cuando se selecciona la opción <b>Añadir regla de umbral</b>, el asistente de reglas se visualiza, lleno con las opciones adecuadas para crear una regla de umbral.</p>

Tabla 8. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Reglas (continuación)	<ul style="list-style-type: none"> <li data-bbox="862 241 1469 653">• <b>Añadir regla conductual:</b> Seleccione esta opción para crear una regla conductual. Una regla conductual prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, puede crear una regla conductual para comparar el promedio de volumen de tráfico durante los últimos 5 minutos con el promedio de volumen de tráfico durante la última hora. Si se produce un cambio de más del 40%, la regla genera un respuesta.  Cuando se selecciona la opción <b>Añadir regla conductual</b>, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla conductual.</li> <li data-bbox="862 814 1469 1157">• <b>Añadir regla de anomalía:</b> Seleccione esta opción para crear una regla de anomalía. Una regla de anomalía prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, si un área de la red que nunca se comunica con Asia empieza a comunicarse con hosts de ese país, una regla de anomalía genera una alerta.  Cuando se selecciona la opción <b>Añadir regla de anomalía</b>, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla de anomalía.</li> </ul>

Tabla 8. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Acciones	<p>Pulse <b>Acciones</b> para realizar las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• <b>Mostrar todo:</b> Seleccione esta opción para eliminar todos los filtros en los criterios de búsqueda y visualizar todos los sucesos no filtrados.</li> <li>• <b>Imprimir:</b> Seleccione esta opción para imprimir los sucesos que se visualizan en la página.</li> <li>• <b>Exportar a XML &gt; Columnas visibles:</b> Seleccione esta opción para exportar solo las columnas que son visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea <a href="#">Exportación de sucesos</a>.</li> <li>• <b>Exportar a XML &gt; Exportación completa (Todas las columnas):</b> Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea <a href="#">Exportación de sucesos</a>.</li> <li>• <b>Exportar a CSV &gt;Columnas visibles:</b> Seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea <a href="#">Exportación de sucesos</a>.</li> <li>• <b>Exportar a CSV &gt; Exportación completa (Todas las columnas):</b> Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea <a href="#">Exportación de sucesos</a>.</li> <li>• <b>Suprimir:</b> Seleccione esta opción para suprimir un resultado de búsqueda. Consulte <a href="#">Gestión de resultados de búsqueda de sucesos y flujos</a>.</li> <li>• <b>Notificar:</b> seleccione esta opción para especificar que desea recibir una notificación por correo electrónico cuando finalicen las búsquedas seleccionadas. Esta opción solo está habilitada para las búsquedas en curso.</li> </ul> <p><b>Nota:</b> Las opciones <b>Imprimir</b>, <b>Exportar a XML</b> y <b>Exportar a CSV</b> están inhabilitadas en modalidad continua y cuando se ven resultados de búsqueda parciales.</p>



Tabla 8. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Barra de herramientas de búsqueda	<p><b>Búsqueda avanzada</b>                      Seleccione <b>Búsqueda avanzada</b> en el recuadro de lista para entrar una serie de búsqueda AQL (Ariel Query Language) para especificar los campos que desea que se devuelvan.</p> <p><b>Filtro rápido</b>                      Seleccione Filtro rápido en el recuadro de lista para buscar cargas útiles utilizando palabras o frases simples.</p>
Ver	<p>La vista predeterminada de la pestaña <b>Actividad de registro</b> es una corriente de sucesos en tiempo real. La lista <b>Ver</b> contiene opciones para ver también sucesos de periodos de tiempo específicos. Después de elegir un periodo de tiempo especificado de la lista <b>Ver</b> puede modificar el periodo de tiempo visualizado cambiando los valores de fecha y hora en los campos <b>Hora de inicio</b> y <b>Hora de finalización</b>.</p>

### Opciones de menú que aparecen al pulsar el botón derecho del ratón

En la pestaña **Actividad de registro**, puede pulsar el botón derecho del ratón en un suceso para acceder a más información de filtro de sucesos.

Las opciones de menú que aparecen al pulsar el botón derecho del ratón son las siguientes:

Tabla 9. Opciones de menú que aparecen al pulsar el botón derecho del ratón

Opción	Descripción
Filtro en	<p>Seleccione esta opción para filtrar en el suceso seleccionado, en función del parámetro seleccionado del suceso.</p>
Falso positivo	<p>Seleccione esta opción para abrir la ventana <b>Falso positivo</b>, que le permitirá impedir que los sucesos que se conoce que son falsos positivos creen delitos. Esta opción está inhabilitada en la modalidad continua. Consulte <a href="#">Ajustes de falsos positivos</a>.</p>
Más opciones:	<p>Seleccione esta opción para investigar una dirección IP o un nombre de usuario. Para obtener más información sobre la investigación una dirección IP, consulte Investigación de direcciones IP.</p> <p><b>Nota:</b> Esta opción no se visualiza en modalidad continua.</p>
<b>Filtro rápido</b>	<p>Filtrar elementos que coinciden o no coinciden con la selección.</p>

## Barra de estado

Al transmitir sucesos, la barra de estado visualiza el número promedio de resultados que se reciben por segundo.

Este es el número de resultados que la consola ha recibido satisfactoriamente de los procesadores de sucesos. Si este número supera los 40 resultados por segundo, solo se visualizarán 40 resultados. El resto se acumula en el almacenamiento intermedio de resultados. Para ver más información de estado, mueva el puntero del ratón sobre la barra de estado.

Cuando no se transmiten sucesos, la barra de estado muestra el número de resultados de búsqueda que se visualizan actualmente en la pestaña y la cantidad de tiempo que se necesita para procesar los resultados de búsqueda.

## Supervisión de actividad de registro

---

De forma predeterminada, la pestaña **Actividad de registro** visualiza sucesos en modalidad continua, lo que le permite ver los sucesos en tiempo real.

Para obtener más información sobre la modalidad continua, consulte [Visualización de sucesos de modalidad continua](#). Puede especificar un rango de tiempo distinto para filtrar sucesos mediante el recuadro de lista **Ver**.

Si anteriormente ha configurado criterios de búsqueda guardados como el valor predeterminado, los resultados de dicha búsqueda se visualizan automáticamente cuando se accede a la pestaña **Actividad de registro**. Para obtener más información acerca de cómo guardar criterios de búsqueda, consulte [Guardar criterios de búsqueda de sucesos y flujos](#).

## Visualización de sucesos en modalidad continua

La modalidad continua le permitirá ver los datos de sucesos que entran en el sistema. Esta modalidad le proporciona una vista en tiempo real de la actividad actual de sucesos visualizando los últimos 50 sucesos.

### Acerca de esta tarea

Si se aplican filtros en la pestaña **Actividad de registro** o en los criterios de búsqueda antes de habilitar la modalidad continua, los filtros se mantienen en modalidad continua. Sin embargo, la modalidad continua no soporta búsquedas que incluyan sucesos agrupados. Si habilita la modalidad continua en sucesos agrupados o criterios de búsqueda agrupados, la pestaña **Actividad de registro** visualiza los sucesos normalizados. Consulte [Visualización de sucesos normalizados](#).

Cuando desea seleccionar un suceso para ver detalles o realizar una acción, debe poner en pausa la modalidad continua antes de efectuar una doble pulsación en un suceso. Cuando la modalidad continua está en pausa, se visualizan los últimos 1.000 sucesos.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione **Tiempo real (modalidad continua)**.  
Para obtener información sobre las opciones de la barra de herramientas, consulte la Tabla 4-1. Para obtener más información sobre los parámetros que se visualizan en modalidad continua, consulte la Tabla 4-7.
3. Opcional. Poner en pausa o reproducir los sucesos en modalidad continua. Elija una de las siguientes opciones:
  - Para seleccionar un registro de sucesos, pulse el icono de **Pausa** para poner en pausa la modalidad continua.
  - Para reiniciar la modalidad continua, pulse el icono de **Reproducir**.

## Visualización de sucesos normalizados

Los sucesos se recopilan en formato en bruto y, a continuación, se normalizan para visualizarse en la pestaña **Actividad de registro**.

### Acerca de esta tarea

La normalización implica analizar los datos de sucesos en bruto y preparar los datos para visualizar información legible sobre la pestaña. Cuando los sucesos se normalizan, el sistema también normaliza los nombres. Por lo tanto, el nombre que se muestra en la pestaña **Actividad de registro** puede no coincidir con el nombre que se visualiza en el suceso.

**Nota:** Si ha seleccionado que se visualice un intervalo de tiempo, se visualiza un gráfico de serie temporal. Para obtener más información sobre la utilización de gráficos de serie temporal, consulte [Visión general de gráfico de serie temporal](#).

La pestaña **Actividad de registro** muestra de forma predeterminada los parámetros siguientes cuando se visualizan sucesos normalizados:

<b>Parámetro</b>	<b>Descripción</b>
Filtros actuales	En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse <b>Borrar filtro</b> . <b>Nota:</b> Este parámetro solo se muestra después de aplicar un filtro.
Ver	En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.

Tabla 10. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado)  
(continuación)

Parámetro	Descripción
Estadísticas actuales	<p>Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen:</p> <p><b>Nota:</b> Pulse la flecha situada junto a <b>Estadísticas actuales</b> para visualizar u ocultar las estadísticas</p> <ul style="list-style-type: none"> <li>• <b>Resultados totales:</b> Especifica el número total de resultados que coincidían con los criterios de búsqueda.</li> <li>• <b>Archivos de datos buscados:</b> Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Archivos de datos comprimidos buscados:</b> Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado.</li> <li>• <b>Recuento de archivos de índices:</b> Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Duración:</b> Especifica la duración de la búsqueda.</li> </ul> <p><b>Nota:</b> Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.</p>
Gráficos	<p>Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse <b>Ocultar gráficos</b> si desea eliminar los gráficos de la pantalla. Los gráficos solo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. Para obtener más información sobre cómo configurar gráficos, consulte <a href="#">Gestión de gráficos</a>.</p> <p><b>Nota:</b> Si utiliza Mozilla Firefox como navegador y está instalado un bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.</p>

Tabla 10. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado)  
(continuación)

Parámetro	Descripción
Icono de delitos	Pulse este icono para ver detalles del delito que está asociado con este suceso. Para obtener más información, consulte <a href="#">Gestión de gráficos</a> . <b>Nota:</b> Dependiendo del producto, es posible que este icono no esté disponible. Debe tener IBM QRadar SIEM.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se detectan muchos sucesos del mismo tipo para la misma dirección IP de origen y dirección en un breve periodo de tiempo.
Hora	Especifica la fecha y hora en que QRadar ha recibido el suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel que está asociada con este suceso.  Para obtener más información sobre categorías de suceso, consulte la publicación <i>Guía de administración de IBM QRadar</i> .
IP de origen	Especifica la dirección IP de origen del suceso. <b>Nota:</b> Si selecciona la visualización <b>Normalizado (con columnas IPv6)</b> , consulte el parámetro <b>IPv6 de origen</b> para sucesos IPv6.
Puerto de origen	Especifica el puerto de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso. <b>Nota:</b> Si selecciona la visualización <b>Normalizado (con columnas IPv6)</b> , consulte el parámetro <b>IPv6 de destino</b> para sucesos IPv6.
Puerto de destino	Especifica el puerto de destino del suceso.
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso. Normalmente los nombres de usuario están disponibles en sucesos relacionados con la autenticación. Para todos los demás tipos de sucesos donde el nombre de usuario no está disponible, este campo especifica N/A.

Tabla 10. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Magnitud	Especifica la magnitud de este suceso. Las variables incluyen credibilidad, pertinencia y gravedad. Apunte el ratón sobre la barra de magnitud para visualizar los valores y la magnitud calculada.

Si selecciona la visualización **Normalizado (con columnas IPv6)**, la pestaña **Actividad de registro** mostrará los siguientes parámetros extra:

Tabla 11. Parámetros de pestaña Actividad de registro - Normalizado (con columnas IPv6)

Parámetro	Descripción
IPv6 de origen	Especifica la dirección IP de origen del suceso. <b>Nota:</b> Los sucesos de IPv4 muestran 0.0.0.0.0.0.0.0 en las columnas <b>IPv6 de origen</b> e <b>IPv6 de destino</b> .
IPv6 de destino	Especifica la dirección IP de destino del suceso. <b>Nota:</b> Los sucesos de IPv4 muestran 0.0.0.0.0.0.0.0 en las columnas <b>IPv6 de origen</b> e <b>IPv6 de destino</b> .

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional: En el cuadro de lista **Visualizar**, seleccione **Normalizado (con columnas IPv6)**.  
La visualización **Normalizado (con columnas IPv6)** muestra las direcciones IPv6 de origen y destino para sucesos IPv6.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Pulse el icono **Pausa** para poner en pausa la modalidad continua.
5. Efectúe una doble pulsación en el suceso que desea con más detalle. Para obtener más información, consulte [Detalles de suceso](#).

### Visualización de sucesos en bruto

Puede ver los datos de sucesos en bruto, que son los datos de sucesos sin analizar desde el origen de registro.

#### Acerca de esta tarea

Al ver datos de sucesos en bruto, la pestaña **Actividad de registro** proporciona los parámetros siguientes para cada suceso.

Tabla 12. Parámetros de sucesos en bruto

Parámetro	Descripción
Filtros actuales	<p>En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse <b>Borrar filtro</b>.</p> <p><b>Nota:</b> Este parámetro solo se visualiza después de aplicar un filtro.</p>
Ver	<p>En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.</p>
Estadísticas actuales	<p>Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen:</p> <p><b>Nota:</b> Pulse la flecha situada junto a <b>Estadísticas actuales</b> para visualizar u ocultar las estadísticas</p> <ul style="list-style-type: none"> <li>• <b>Resultados totales:</b> Especifica el número total de resultados que coincidirían con los criterios de búsqueda.</li> <li>• <b>Archivos de datos buscados:</b> Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Archivos de datos comprimidos buscados:</b> Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado.</li> <li>• <b>Recuento de archivos de índices:</b> Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Duración:</b> Especifica la duración de la búsqueda.</li> </ul> <p><b>Nota:</b> Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.</p>

Tabla 12. Parámetros de sucesos en bruto (continuación)

Parámetro	Descripción
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse <b>Ocultar gráficos</b> si desea eliminar los gráficos de la pantalla. Los gráficos solo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar.  <b>Nota:</b> Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.
Icono de delitos	Pulse este icono para ver detalles del delito que está asociado con este suceso.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Carga útil	Especifica la información de carga útil de suceso original en formato UTF-8.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Visualizar**, seleccione **Sucesos en bruto**.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Efectúe una doble pulsación en el suceso que desea con más detalle. Consulte [Detalles del suceso](#).

### Visualización de sucesos agrupados

Utilizando la pestaña **Actividad de registro**, puede ver sucesos que están agrupados por diversas opciones. En el recuadro de lista **Visualizar**, puede seleccionar el parámetro por el que desea agrupar los sucesos.

#### Acerca de esta tarea

El recuadro de lista Visualizar no aparece en modalidad continua porque la modalidad continua no soporta los sucesos agrupados. Si ha entrado en modalidad continua utilizando criterios de búsqueda no agrupados, se visualiza esta opción.

El recuadro de lista Visualizar proporciona las opciones siguientes:



Opción de grupo	Descripción
Categoría de nivel bajo	Muestra una lista resumida de sucesos que están agrupados por la categoría de bajo nivel del suceso.  Para obtener más información sobre categorías, consulte el manual <i>Guía de administración de IBM QRadar</i> .
Nombre de suceso	Muestra una lista resumida de sucesos que están agrupados por el nombre normalizado del suceso.
IP de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de destino del suceso.
Puerto de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de destino del suceso.
IP de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de origen del suceso.
Regla personalizada	Muestra una lista resumida de sucesos que están agrupados por la regla personalizada asociada.
Nombre de usuario	Muestra una lista resumida de sucesos que están agrupados por el nombre de usuario que está asociado con los sucesos.
Origen de registro	Muestra una lista resumida de sucesos que están agrupados por los orígenes de registro que han enviado el suceso a QRadar.
Categoría de nivel superior	Muestra una lista resumida de sucesos que están agrupados por la categoría de nivel alto del suceso.
Red	Muestra una lista resumida de sucesos que están agrupados por la red que está asociada con el suceso.
Puerto de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de origen del suceso.

Después de seleccionar una opción en el cuadro de lista **Visualizar**, la disposición de las columnas de datos depende de la opción de agrupación elegida. Cada fila de la tabla de sucesos representa un grupo de sucesos. La pestaña **Actividad de registro** proporciona la siguiente información para cada grupo de sucesos

Parámetro	Descripción
Agrupando por	Especifica el parámetro para el que se agrupa la búsqueda.

Tabla 14. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Filtros actuales	En la parte superior de la tabla se muestran los detalles del filtro que se aplica a los resultados de búsqueda. Para borrar estos valores de filtro, pulse <b>Borrar filtro</b> .
Ver	En el cuadro de lista, seleccione el rango de tiempo para el que desee aplicar el filtro.
Estadísticas actuales	<p>Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen:</p> <p><b>Nota:</b> Pulse la flecha situada junto a <b>Estadísticas actuales</b> para mostrar u ocultar las estadísticas.</p> <ul style="list-style-type: none"> <li>• <b>Resultados totales:</b> Especifica el número total de resultados que coincidían con los criterios de búsqueda.</li> <li>• <b>Archivos de datos buscados:</b> Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Archivos de datos comprimidos buscados:</b> Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado.</li> <li>• <b>Recuento de archivos de índices:</b> Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado.</li> <li>• <b>Duración:</b> Especifica la duración de la búsqueda.</li> </ul> <p><b>Nota:</b> Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para resolver problemas de los sucesos, es posible que se le solicite que proporcione información estadística actual.</p>

Tabla 14. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Gráficos	<p>Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse <b>Ocultar gráficos</b> si desea eliminar el gráfico de la pantalla.</p> <p>Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarlo a asociar los objetos de gráfico con los parámetros que representan. Mediante la característica de leyenda, puede realizar las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• Mueva el puntero del ratón sobre un elemento de leyenda para ver más información sobre los parámetros que representa.</li> <li>• Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente.</li> <li>• Pulse en un elemento de leyenda para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento.</li> <li>• Pulse <b>Leyenda</b> si desea eliminar la leyenda de la pantalla gráfica.</li> </ul> <p><b>Nota:</b> Los gráficos solo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar.</p> <p><b>Nota:</b> Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.</p>
IP de origen (Recuento exclusivo)	Especifica la dirección IP de origen que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.
IP de destino (Recuento exclusivo)	Especifica la dirección IP de destino que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.
Puerto de destino (Recuento exclusivo)	Especifica los puertos de destino que están asociados con este suceso. Si hay varios puertos que están asociados con este suceso, este campo especifica el término Múltiple y el número de puertos.

Tabla 14. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro (Recuento exclusivo)	Especifica los orígenes de registro que han enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Categoría de nivel alto (Recuento exclusivo)	Especifica la categoría de alto nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías.  Para obtener más información sobre las categorías, consulte la publicación <i>IBM QRadar Log Manager Administration Guide</i> .
Categoría de nivel bajo (Recuento exclusivo)	Especifica la categoría de bajo nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías.
Protocolo (Recuento exclusivo)	Especifica el ID de protocolo asociado con este suceso. Si hay varios protocolos que están asociados con este suceso, este campo especifica el término Múltiple y el número de ID de protocolo.
Nombre de usuario (Recuento exclusivo)	Especifica el nombre de usuario que está asociado con este suceso, si está disponible. Si hay varios nombres de usuario que están asociados con este suceso, este campo especifica el término Múltiple y el número de nombres de usuario.
Magnitud (máxima)	Especifica la magnitud máxima calculada para sucesos agrupados. Las variables que se utilizan para calcular la magnitud incluyen la credibilidad, la pertinencia y la gravedad. Para obtener más información sobre credibilidad, relevancia y gravedad, consulte el <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html">Glosario</a> ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html</a> ).
Recuento de sucesos (Suma)	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Recuento	Especifica el número total de sucesos normalizados en este grupo de sucesos.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.

3. En el recuadro de lista Visualizar, elija el parámetro por el que desea agrupar los sucesos. Consulte la Tabla 2.  
Se listan los grupos de sucesos. Para obtener más información sobre los detalles de grupo de sucesos, consulte la Tabla 1.
4. Para ver la página **Lista de sucesos** para un grupo, efectúe una doble pulsación en el grupo de sucesos que desea investigar.  
La página **Lista de sucesos** no conserva las configuraciones de gráfico que pueda haber definido en la pestaña **Actividad de registro**. Para obtener más información sobre los parámetros de página **Lista de sucesos**, consulte la Tabla 1.
5. Para ver los detalles de un suceso, efectúe una doble pulsación en el suceso que desea investigar. Para obtener más información sobre los detalles de suceso, consulte la Tabla 2.

## Visualización de detalles de suceso

Puede ver una lista de sucesos en varias modalidades, incluida la modalidad continua o en grupos de sucesos. Sea cual sea la modalidad que elija para ver sucesos, puede localizar y ver los detalles de un único suceso.

La página de detalles de suceso proporciona la siguiente información:

<i>Tabla 15. Detalles de suceso</i>	
<b>Parámetro</b>	<b>Descripción</b>
Nombre de suceso	Especifica el nombre normalizado del suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel de este suceso.  Para obtener más información sobre las categorías, consulte la publicación <i>Guía de administración de IBM QRadar</i> .
Descripción del suceso	Especifica una descripción del suceso, si está disponible.
Magnitud	Especifica la magnitud de este suceso. Para obtener más información sobre la magnitud, consulte el <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">Glosario</a> ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html</a> ).
Importancia	Especifica la pertinencia de este suceso. Para obtener más información sobre la relevancia, consulte el <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">Glosario</a> ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html</a> ).
Gravedad	Especifica la gravedad de este suceso. Para obtener más información sobre la gravedad, consulte el <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">Glosario</a> ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html</a> ).

Tabla 15. Detalles de suceso (continuación)

Parámetro	Descripción
Credibilidad	Especifica la credibilidad de este suceso. Para obtener más información sobre la credibilidad, consulte el <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">Glosario</a> ( <a href="http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html">http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/r_qradar_product_glossary.html</a> ).
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso, si está disponible.  Para acceder a más información asociada con un nombre de usuario seleccionado, pulse el botón derecho del ratón en el nombre de usuario para mostrar las opciones de menú <b>Ver activos</b> y <b>Ver sucesos</b> .
Hora de inicio	Especifica la hora en que se ha recibido el suceso del origen de registro.
Hora de almacenamiento	Especifica el tiempo que el suceso ha estado almacenado en la base de datos de QRadar.
Hora de origen de registro	Especifica la hora de sistema indicada por el origen de registro en la carga útil de suceso.
Información de detección de anomalía: Este panel solo se visualiza si este suceso lo ha generado una regla de detección de anomalías. Pulse el icono <b>Anomalía</b> para ver los resultados de búsqueda guardados que han hecho que la regla de detección de anomalías generara este suceso.	
Descripción de la regla	Especifica la regla de detección de anomalías que ha generado este suceso.
Descripción de anomalía	Especifica una descripción del comportamiento anómalo que ha sido detectada por la regla de detección de anomalías.
Valor de alerta de anomalía	Especifica el valor de alerta de anomalía.
<b>Información sobre origen y destino</b>	
IP de origen	Especifica la dirección IP de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso.
Nombre de activo de origen	Especifica el nombre de activo definido por el usuario del origen de suceso. Para obtener más información sobre activos, consulte Gestión de activos.
Nombre de activo de destino	Especifica el nombre de activo definido por el usuario del destino de suceso. Para obtener más información sobre activos, consulte Gestión de activos
Puerto de origen	Especifica el puerto de origen de este suceso.
Puerto de destino	Especifica el puerto de destino de este suceso.

Tabla 15. Detalles de suceso (continuación)

<b>Parámetro</b>	<b>Descripción</b>
IP de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT (Network Address Translation - Conversión de direcciones de red), este parámetro especifica la dirección IP de origen antes de que se aplicaran los valores de NAT. NAT convierte una dirección IP de una red en una dirección IP diferente de otra red.
IP de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino antes de que se aplicaran los valores de NAT.
Puerto de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen antes de que se aplicaran los valores de NAT.
Puerto de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino antes de que se aplicaran los valores de NAT.
IP de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de origen después de que se aplicaran los valores de NAT.
IP de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino después de que se aplicaran los valores de NAT.
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
IPv6 de origen	Especifica la dirección IPv6 de origen del suceso.
IPv6 de destino	Especifica la dirección IPv6 de destino del suceso.
MAC de origen	Especifica la dirección MAC de origen del suceso.

Tabla 15. Detalles de suceso (continuación)

Parámetro	Descripción
MAC de destino	Especifica la dirección MAC de destino del suceso.
<b>Información sobre la carga útil</b>	
Carga útil	Especifica el contenido de carga útil del suceso. Este campo ofrece 3 pestañas para ver la carga útil: <ul style="list-style-type: none"> <li>• Universal Transformation Format (UTF) - Pulse UTF.</li> <li>• Hexadecimal: Pulse HEX.</li> <li>• Base64 - Pulse Base64.</li> </ul>
<b>Información adicional</b>	
Protocolo	Especifica el protocolo que está asociado con este suceso.
QID	Especifica el QID para este suceso. Cada suceso tiene un QID exclusivo. Para obtener más información sobre la correlación de un QID, consulte <a href="#">Modificación de correlación de sucesos</a> .
Origen de registro	Especifica el origen de registro que ha enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Reglas personalizadas	Especifica las reglas personalizadas que coinciden con este suceso. .
Reglas personalizadas que coinciden parcialmente	Especifica reglas personalizadas que coinciden parcialmente con este suceso.
Anotaciones	Especifica el anotación para este suceso. Las anotaciones son descripciones de texto que las reglas pueden añadir automáticamente a los sucesos como parte de la respuesta de regla.
Recopilador de sucesos	Especifica el ID del componente Recopilador de sucesos que ha analizado el suceso.
ID de suceso de QID	Valor principal establecido por DSM para identificar un suceso. QRadar utiliza este campo, junto con Categoría de suceso, para establecer una correlación con un registro QID para el suceso.
Categoría de suceso de QID	Valor secundario establecido por DSM para identificar un suceso. QRadar utiliza este campo, junto con ID de suceso, para establecer una correlación con un registro QID para el suceso.



Tabla 15. Detalles de suceso (continuación)

Parámetro	Descripción
Identificador de origen de registro	Especifica el Identificador de origen de registro del origen de registro que ha recibido el suceso. Si el suceso se direcciona a un origen de registro de tipo <b>Registro genérico de SIM</b> , establezca este valor como valor de Identificador de origen de registro cuando cree el origen de registro para recopilar este suceso.
Truncado	Especifica si la carga útil de suceso se ha truncado debido a que superaba el tamaño máximo permitido de 32 KB para QRadar. El parámetro solo se establece en True si la carga útil se trunca antes del almacenamiento porque supera el tamaño máximo permitido para QRadar. El parámetro se establece en False si la carga útil no se trunca. También se establece en False si la carga útil es truncada por el protocolo de origen de registro que la recopiló en función del parámetro de tamaño máximo de la carga útil establecido en la configuración del origen de registro.
Almacenado para rendimiento	Establézcalo en True si un suceso se ha direccionado al almacenamiento directamente debido a problemas de rendimiento. Si el parámetro se establece en False y el suceso tiene una Categoría de nivel bajo de tipo Almacenado, QRadar ha intentado analizarlo, pero el suceso no ha sido reconocido por ninguno de los orígenes de registro disponibles con un Identificador de origen de registro coincidente. En ambos casos, el suceso se almacena sin ningún tipo de análisis o normalización.
<b>Información de identidad:</b> QRadar recopila información de identidad, si está disponible, de los mensajes de origen de registro. La información de identidad proporciona detalles adicionales acerca de los activos en la red. Los orígenes de registro solo generan información de identidad si el mensaje de registro enviado a QRadar contiene una dirección IP y al menos uno de los elementos siguientes: Nombre de usuario o Dirección MAC. No todos los orígenes de registro generan información de identidad.	
Nombre de usuario de identidad	Especifica el nombre de usuario del activo que está asociado con este suceso.
IP de identidad	Especifica la dirección IP del activo que está asociado con este suceso.
Nombre de NetBios de identidad	Especifica el nombre del Sistema básico de entrada/salida de red (NetBios) del activo que está asociado con este suceso.

Tabla 15. Detalles de suceso (continuación)

Parámetro	Descripción
<b>Campo ampliado de identidad</b>	Especifica más información sobre el activo que está asociado con este suceso. El contenido de este campo es texto definido por el usuario y depende de los dispositivos de la red que están disponibles para proporcionar información de identidad. Los ejemplos incluyen: ubicación física de dispositivos, políticas pertinentes, conmutador de red y nombres de puerto.
Tiene identidad (distintivo)	Especifica Verdadero si QRadar ha recopilado información de identificación para el activo que está asociado con este suceso.  Para obtener más información sobre qué dispositivos envían información de identidad, consulte la publicación <i>IBM QRadar DSM Configuration Guide</i> .
Nombre de host de identidad	Especifica el nombre de host del activo que está asociado con este suceso.
MAC de identidad	Especifica la dirección MAC del activo que está asociado con este suceso.
Nombre de grupo de identidad	Especifica el nombre de grupo del activo que está asociado con este suceso.

## Barra de herramientas de detalles de suceso

La barra de herramientas de detalles de sucesos proporciona varias funciones para ver detalles de sucesos.

La barra de herramientas de **detalles de suceso** proporciona las siguientes funciones:

Tabla 16. Barra de herramientas de detalles de suceso

Parámetro	Descripción
<b>Volver a lista de sucesos</b>	Pulse <b>Volver a Lista de sucesos</b> para volver a la lista de sucesos.
<b>Delito</b>	Pulse <b>Delito</b> para visualizar los delitos que están asociadas con el suceso.
<b>Anomalía</b>	Pulse <b>Anomalía</b> para visualizar los resultados de búsqueda guardados que han hecho que la regla de detección de anomalías generara este suceso.  <b>Nota:</b> Este icono solo se visualiza si este suceso ha sido generado por una regla de detección de anomalías.
<b>Correlación de sucesos</b>	Pulse <b>Correlación de suceso</b> para editar la correlación de sucesos. Para obtener más información, consulte <a href="#">Modificación de correlación de sucesos</a> .

Tabla 16. Barra de herramientas de detalles de suceso (continuación)

Parámetro	Descripción
<b>Falso positivo</b>	Pulse <b>Falso positivo</b> para ajustar QRadar a fin de evitar que los sucesos positivos falsos generen delitos.
<b>Extraer propiedad</b>	Pulse <b>Extraer propiedad</b> para crear una propiedad de suceso personalizada a partir del suceso seleccionado.
<b>Anterior</b>	Pulse <b>Anterior</b> para ver el suceso anterior en la lista de sucesos.
<b>Siguiente</b>	Pulse <b>Siguiente</b> para ver el siguiente suceso en la lista de sucesos.
<b>Datos de PCAP</b>	<p><b>Nota:</b> Esta opción solo se visualiza si la consola de QRadar se ha configurado para integrarse con el DSM de Juniper JunOS Platform. Para obtener más información sobre cómo gestionar datos de PCAP, consulte <a href="#">Gestión de datos de PCAP</a>.</p> <ul style="list-style-type: none"> <li>• <b>Ver información de PCAP:</b> Seleccione esta opción para ver la información de PCAP. Para obtener más información, consulte <a href="#">Visualización de información de PCAP</a>.</li> <li>• <b>Descargar archivo de PCAP:</b> Seleccione esta opción para descargar el archivo de PCAP en el sistema de escritorio. Para obtener más información, consulte <a href="#">Descarga del archivo de PCAP en el sistema</a>.</li> </ul>
<b>Imprimir</b>	Pulse <b>Imprimir</b> para imprimir los detalles de suceso.

## Visualización de delitos asociados

En la pestaña Actividad de registro, puede ver el delito que está asociado con el suceso.

### Acerca de esta tarea

Si un suceso coincide con una regla, se puede generar un delito en la pestaña **Delitos**.

Para obtener más información sobre reglas, consulte el manual *Guía de administración de IBM QRadar*.

Cuando vea un delito en la pestaña **Actividad de registro**, es posible que el delito no se visualice si el magistrado aún no se ha guardado en disco el delito que está asociado con el suceso seleccionado o si el delito se ha depurado de la base de datos. Si esto ocurre, el sistema se lo notificará.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Pulse el icono **Delito** junto al suceso que desea investigar.
4. Vea el delito asociado.

## Modificación de la correlación de sucesos

---

Puede correlacionar manualmente un suceso normalizado o en bruto con una categoría de alto nivel y de bajo nivel (o QID).

### Antes de empezar

Esta acción manual se utiliza para correlacionar sucesos de origen de registro desconocidos con sucesos de QRadar conocidos para que se puedan categorizar y procesar adecuadamente.

### Acerca de esta tarea

A efectos de normalización, QRadar correlaciona automáticamente sucesos de orígenes de registro con categorías de alto y bajo nivel.

Para obtener más información sobre categorías de suceso, consulte la publicación *Guía de administración de IBM QRadar*.

Si los sucesos se reciben de orígenes de registro que el sistema no puede categorizar, los sucesos se categorizan como desconocidos. Dichos sucesos se producen por distintos motivos, incluyendo:

- **Sucesos definidos por el usuario:** Algunos orígenes de registro, como Snort, le permiten crear sucesos definidos por el usuario.
- **Sucesos nuevos o antiguos:** Los orígenes de registro de proveedor pueden actualizar el software con releases de mantenimiento para soportar sucesos nuevos que es posible que QRadar no soporte.

**Nota:** El icono **Correlacionar suceso** está inhabilitado para los sucesos cuando la categoría de alto nivel es Auditoría SIM o el tipo de origen de registro es Protocolo de acceso a objetos simple (SOAP).

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Efectúe una doble pulsación en el suceso que desea correlacionar.
4. Pulse **Correlación de suceso**.
5. Si conoce el QID que desea correlacionar con este suceso, escriba el QID en el campo **Especifique los QID**.
6. Si no conoce el QID que desea correlacionar con este suceso, puede buscar un QID específico:
  - a) Elija una de las opciones siguientes: Para buscar un QID por categoría, seleccione la categoría de alto nivel en el recuadro de lista Categoría de alto nivel. Para buscar un QID por categoría, seleccione la categoría de bajo nivel en el recuadro de lista Categoría de bajo nivel. Para buscar un QID por tipo de origen de registro, seleccione un tipo de origen de registro en el recuadro de lista Tipo de origen de registro. Para buscar un QID por nombre, escriba un nombre en el campo QID/Nombre.
  - b) Pulse **Buscar**.
  - c) Seleccione **QID** con el que desea asociar este suceso.
7. Pulse **Aceptar**.

## Ajustar falsos positivos

---

Puede utilizar la función Ajuste de falsos positivos para impedir que sucesos de falso positivo generen delitos.

### Antes de empezar

Puede ajustar sucesos de falso positivo en la página **lista de sucesos** o **detalles de suceso**.

### Acerca de esta tarea

Puede ajustar sucesos de falso positivo en la página **lista de sucesos** o **detalles de suceso**.

Debe tener permisos adecuados para crear reglas personalizadas para ajustar falsos positivos.

Para obtener más información sobre roles, consulte el manual *Guía de administración de IBM QRadar*.

Para obtener más información sobre falsos positivos, consulte el [Glosario](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html) ([http://www.ibm.com/support/knowledgecenter/SS42VS\\_7.2.7/com.ibm.qradar.doc/r\\_qradar\\_siem\\_glossary.html](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html)).

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Seleccione el suceso que desee ajustar.
4. Pulse **Falso positivo**.
5. En el panel Propiedad de suceso/flujo de la ventana **Falso positivo**, seleccione una de las opciones siguientes:
  - Suceso/flujo(s) con un QID específico de <Suceso>
  - Cualquier suceso/flujo(s) con una categoría de bajo nivel de <Suceso>
  - Cualquier suceso/flujo(s) con una categoría de alto nivel de <Suceso>
6. En el panel Dirección de tráfico, seleccione una de las opciones siguientes:
  - <Dirección IP de origen> a <Dirección IP de destino>
  - <Dirección IP de origen> a cualquier destino
  - Cualquier origen a <Dirección IP de destino>
  - Cualquier origen a cualquier destino
7. Pulse **Ajustar**.

## Datos de PCAP

---

Si la consola de QRadar se ha configurado para integrarse con el DSM Juniper JunOS Platform, Packet Capture (PCAP) se puede recibir, procesar y los datos se pueden almacenar de un origen de registro Juniper SRX-Series Services Gateway.

Para obtener más información sobre el DSM Juniper JunOS Platform, consulte la publicación *IBM QRadar DSM Configuration Guide*.

## Visualización de la columna de datos de PCAP

La columna **Datos de PCAP** no se visualiza en la pestaña **Actividad de registro** de forma predeterminada. Al crear criterios de búsqueda, debe seleccionar la columna **Datos de PCAP** en el panel Definición de columna.

### Antes de empezar

Para poder visualizar los datos de PCAP en la pestaña **Actividad de registro**, se debe configurar el origen de registro de Juniper SRX-Series Services Gateway con el protocolo de combinación PCAP Syslog. Para obtener más información sobre cómo configurar protocolos de origen de registro, consulte la publicación *Managing Log Sources Guide*.

### Acerca de esta tarea

Cuando se realiza una búsqueda que incluye la columna **Datos de PCAP**, se visualiza un icono en la columna **Datos de PCAP** de los resultados de búsqueda si hay datos de PCAP disponibles para un suceso. Utilizando el icono de **PCAP**, puede ver los datos de PCAP o descargar el archivo **PCAP** en el sistema.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda**.
3. Opcional. Para buscar sucesos que tienen datos de PCAP, configure los criterios de búsqueda siguientes:
  - a) En el primer recuadro de lista, seleccione **Datos de PCAP**.
  - b) En el segundo recuadro de lista, seleccione **Igual que**.
  - c) En el tercer recuadro de lista, seleccione **Verdadero**.
  - d) Pulse **Añadir filtro**.
4. Configure las definiciones de columna para incluir la columna **Datos de PCAP**:
  - a) En la lista **Columnas disponibles** del panel Definición de columna, pulse **Datos de PCAP**.
  - b) Pulse el icono **Añadir columna** en el conjunto inferior de iconos para mover la columna **Datos de PCAP** a la lista **Columnas**.
  - c) Opcional. Pulse el icono **Añadir columna** en el conjunto superior de iconos para mover la columna **Datos de PCAP** a la lista **Agrupar por**.
5. Pulse **Filtro**.
6. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
7. Efectúe una doble pulsación en el suceso que desee investigar.

### Qué hacer a continuación

Para obtener más información sobre cómo ver y descargar datos de PCAP, consulte las secciones siguientes:

- [Visualización de la información de PCAP](#)
- [Descarga del archivo de PCAP en el sistema](#)

## Visualización de la información de PCAP

En el menú de barra de herramientas **Datos de PCAP**, puede ver una versión legible de los datos en el archivo de PCAP o descargar el archivo de PCAP en el sistema.

### Antes de empezar

Para poder ver información de PCAP, debe realizar o seleccionar una búsqueda que visualice la columna **Datos de PCAP**.

### Acerca de esta tarea

Antes de poder visualizar los datos de PCAP, se debe recuperar el archivo de PCAP para visualizarlo en la interfaz de usuario. Si el proceso de descarga tarda un período de tiempo prolongado, se visualiza la ventana **Downloading PCAP Packet information**. En la mayoría de los casos, el proceso de descarga es rápido y esta ventana no se visualiza.

Una vez recuperado el archivo, una ventana emergente proporciona una versión legible del archivo de PCAP. Puede leer la información que se visualiza en la ventana o descargar la información en el sistema.

### Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:

- Seleccione el suceso y pulse el icono **PCAP**.
  - Pulse el botón derecho del ratón en el icono **PCAP** para el suceso y seleccione **Más opciones > Ver información de PCAP**.
  - Efectúe una doble pulsación en el suceso que desea investigar y, a continuación, seleccione **Datos de PCAP > Ver información de PCAP** en la barra de herramientas de detalles de suceso.
2. Si desea descargar la información en el sistema, seleccione una de las opciones siguientes:
    - Pulse **Descargar archivo de PCAP** para descargar el archivo de PCAP original que se debe utilizar en una aplicación externa.
    - Pulse **Descargar texto de PCAP** para descargar la información de PCAP en formato .TXT
  3. Elija una de las siguientes opciones:
    - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
    - Si desea guardar la lista, seleccione la opción **Save File**.
  4. Pulse **Aceptar**.

## Descarga del archivo de PCAP en el sistema

Puede descargar el archivo PCAP en el sistema para almacenarlo o para utilizar en otras aplicaciones.

### Antes de empezar

Antes de poder ver la información de PCAP, debe realizar o seleccionar una búsqueda que muestre la columna Datos de PCAP. consulte **Visualización de la columna de datos de PCAP**.

### Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:
  - Seleccione el suceso y pulse el icono **PCAP**.
  - Pulse el botón derecho del ratón en el icono de PCAP para el evento y seleccione **Más opciones > Descargar archivo de PCAP**.
  - Efectúe una doble pulsación en el suceso que desea investigar, y, a continuación, seleccione **Datos de PCAP > Descargar archivo de PCAP** en la barra de herramientas de detalles de suceso.
2. Elija una de las siguientes opciones:
  - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
  - Si desea guardar la lista, seleccione la opción **Save File**.
3. Pulse **Aceptar**.

## Exportación de sucesos

---

Puede exportar sucesos en formato XML (Extensible Markup Language - Lenguaje de marcas extensible) o CSV (Valores separados por comas).

### Antes de empezar

El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.

3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:

- **Exportar a XML > Columnas visibles:** seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada.
- **Exportar a XML > Exportación completa (Todas las columnas):** Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
- **Exportar a CSV > Columnas visibles:** Seleccione esta opción para exportar solo las columnas que están visibles en la pestaña **Actividad de registro**. Esta es la opción recomendada.
- **Exportar a CSV > Exportación completa (Todas las columnas):** Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.

4. Si desea reanudar las actividades mientras la exportación está en curso, pulse **Notificar cuando termine**.

### **Resultados**

Cuando la exportación se haya completado, recibirá una notificación de que la exportación se ha completado. Si no ha seleccionado el icono **Notificar cuando termine**, se visualiza la ventana de estado.



---

## Capítulo 7. Supervisión de la actividad de red

Puede utilizar la pestaña **Actividad de red** para supervisar e investigar actividad de red (flujos) en tiempo real o realizar búsquedas avanzadas.

Debe tener permiso para ver la pestaña **Actividad de red**. Para obtener más información sobre permisos y asignar roles, consulte el manual *Guía de administración de IBM QRadar*.

Seleccione la pestaña **Actividad de red** para supervisar e investigar visualmente datos de flujo en tiempo real o realizar búsquedas avanzadas para filtrar los flujos mostrados. Un flujo es una sesión de comunicación entre dos hosts. Puede ver información de flujo para determinar cómo se transmite el tráfico y qué se ha transmitido (si está habilitada la opción de captura de contenido). La información de flujo también puede incluir detalles tales como protocolos, valores de número de sistema autónomo (ASN) o valores de IFIndex (Interface Index). De forma predeterminada, la pestaña **Actividad de red** muestra flujos en modalidad continua.

Si previamente ha configurado una búsqueda guardada predeterminada, los resultados de esa búsqueda se muestran automáticamente cuando abre la pestaña **Actividad de red**. Para obtener más información sobre cómo guardar criterios de búsqueda, consulte [Guardar criterios de búsqueda de sucesos y flujos](#).

---

### Registros de desbordamiento

Si tiene permisos administrativos, puede especificar el número máximo de flujos que desea enviar desde QRadar QFlow Collector a los procesadores de sucesos.

Si tiene permisos administrativos, puede especificar el número máximo de flujos que desea enviar desde QRadar QFlow Collector a los procesadores de sucesos. Una vez que el flujo configurado alcanza su límite, todos los datos que se recopilan se agrupan en un registro de flujo. Este registro de flujo se visualiza entonces en la pestaña **Actividad de red** con una dirección IP de origen de 127.0.0.4 y una dirección IP de destino de 127.0.0.5. Este registro de flujo especifica Desbordamiento en la pestaña **Actividad de red**.

---

### Ver flujos continuos

La modalidad continua le permite ver datos de flujo a medida que entran en el sistema en tiempo real. Esta modalidad le proporciona una visión en tiempo real de la actividad de flujo actual al mostrar los últimos 50 flujos.

#### Acerca de esta tarea

Si aplica filtros en la pestaña **Actividad de red** o en los criterios de búsqueda antes de habilitar la modalidad continua, los filtros se conservan en la modalidad continua. Pero la modalidad continua no permite realizar búsquedas que incluyen flujos agrupados. Si habilita la modalidad continua para flujos agrupados o criterios de búsqueda agrupados, la pestaña **Actividad de red** muestra los flujos normalizados.

#### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En el cuadro de lista Ver, seleccione **Tiempo real (modalidad continua)**.
3. Opcional. Ponga en pausa o inicie los flujos continuos. Cuando la modalidad continua está en pausa, se muestran los últimos 1.000 flujos.

**Nota:** Para los flujos de modalidad, la barra de estado muestra el número promedio de resultados que se reciben por segundo. Esta pantalla es el número de resultados que la consola ha recibido correctamente de los procesadores de flujos. Si este número es mayor que 40 resultados por

segundo, solo se visualizarán 40 resultados. El resto se acumula en el almacenamiento intermedio de resultados. Para ver más información de estado, mueva el puntero del ratón sobre la barra de estado.

Cuando los flujos no son de modalidad continua, la barra de estado muestra el número de resultados de búsqueda que se muestran actualmente y la cantidad de tiempo necesaria para procesar los resultados de la búsqueda.

## Ver flujos normalizados

---

El flujo de datos se captura, normaliza y luego visualiza en la pestaña **Actividad de red**.

### Acerca de esta tarea

La normalización implica preparar datos de flujo para visualizar información legible en la pestaña.

**Nota:** Si selecciona un intervalo de tiempo para visualizar, se muestra un gráfico de serie temporal. Para obtener más información sobre el uso de gráficos de serie temporal, consulte [Visión general de los gráficos de serie temporal](#).

### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En el cuadro de lista **Visualización**, seleccione **Normalizado (con columnas IPv6)** o **Valor predeterminado (normalizado)**.

La visualización **Normalizado (con columnas IPv6)** muestra las direcciones IPv6 de origen y destino para flujos IPv6.

3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Pulse el icono **Pausar** para detener la modalidad continua.
5. Opcional: Pulse **Ocultar gráficos** para eliminar los gráficos de la pantalla.

El parámetro Gráficos de la pestaña **Actividad de red** muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Los gráficos solo se muestran después de seleccionar un rango de tiempo de Último intervalo (renovación automática) o superior, y una opción de agrupación para visualizar. Para obtener más información sobre la configuración de gráficos, consulte [Configurar gráficos](#).

Si utiliza Mozilla Firefox como navegador y está instalado un bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe desinstalar el bloqueador de anuncios. Para obtener más información, consulte la documentación del navegador.

6. Efectúe una doble pulsación en el flujo que desee ver con mayor detalle.

## Ver flujos agrupados

---

Ver flujos agrupados por varias opciones.

### Acerca de esta tarea

El cuadro de lista **Visualizar** no aparece en la modalidad continua porque esta modalidad no da soporte a los flujos agrupados. Si ha entrado en modalidad continua utilizando criterios de búsqueda no agrupados, se visualiza esta opción.

Después de seleccionar una opción en el cuadro de lista **Visualizar**, la disposición de las columnas de datos depende de la opción de agrupación elegida. Cada fila de la tabla de flujos representa un grupo de flujos.

### Procedimiento

1. Pulse la pestaña **Actividad de red**.

2. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
3. En el recuadro de lista **Visualizar**, seleccione el parámetro para el que desee agrupar flujos.
4. Para ver la página **Lista de flujos** para un grupo, haga una doble pulsación en el grupo de flujos que desee investigar.  
La página **Lista de flujos** no conserva las configuraciones de gráficos que pueda definir en la pestaña **Actividad de red**.
5. Para ver los detalles de un flujo, haga una doble pulsación en el flujo que desee investigar.



---

## Capítulo 8. Ajustar falsos positivos

Puede impedir que flujos de falso positivo generen delitos. Puede ajustar flujos de falso positivo en la página lista de flujos o detalles de flujo.

### Acerca de esta tarea

Debe tener permisos adecuados para crear reglas personalizadas para ajustar falsos positivos.

### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. Opcional. Si está viendo flujos en la modalidad continua, pulse el icono **Pausar** para detener la modalidad continua.
3. Seleccione el flujo que desee ajustar.
4. Pulse **Falso positivo**.
5. En el panel Propiedad de suceso/flujo de la página **Falso positivo**, seleccione una de las opciones siguientes:
  - Suceso/flujo(s) con un QID específico de <Suceso>
  - Cualquier suceso/flujo(s) con una categoría de bajo nivel de <Suceso>
  - Cualquier suceso/flujo(s) con una categoría de alto nivel de <Suceso>
6. En el panel Dirección de tráfico, seleccione una de las opciones siguientes:
  - <Dirección IP de origen> a <Dirección IP de destino>
  - <Dirección IP de origen> a cualquier destino
  - Cualquier origen a <Dirección IP de destino>
  - Cualquier origen a cualquier destino
7. Pulse **Ajustar**.



---

## Capítulo 9. Exportar flujos

Puede exportar flujos en formato XML (Extensible Markup Language) o CSV (Comma Separated Values). El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. Opcional. Si está viendo flujos en la modalidad continua, pulse el icono **Pausar** para detener la modalidad continua.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
  - **Exportar a XML > Columnas visibles**: seleccione esta opción para exportar solo las columnas que son visibles en la pestaña Actividad de registro. Esto es la acción recomendada.
  - **Exportar a XML > Exportación completa (Todas las columnas)**: seleccione esta opción para exportar todos los parámetros de flujo. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
  - **Exportar a CSV > Columnas visibles**: seleccione esta opción para exportar solo las columnas que son visibles en la pestaña Actividad de registro. Esto es la acción recomendada.
  - **Exportar a CSV > Exportación completa (Todas las columnas)**: seleccione esta opción para exportar todos los parámetros de flujo. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
4. Si desea reanudar las actividades, pulse **Notificar al terminar**.

### Resultados

Cuando la exportación se haya completado, recibirá una notificación de que la exportación se ha completado. Si no ha seleccionado el icono **Notificar al terminar**, se mostrará la ventana **Estado**.





## Capítulo 10. Gestión de activos

La recopilación y la visualización de datos de activos le ayuda a identificar las amenazas y las vulnerabilidades. Una base de datos de activos precisa facilita la conexión de los delitos que se desencadenan en el sistema a activos físicos o virtuales en la red.

**Restricción:** QRadar Log Manager solo hace un seguimiento de datos de activo si QRadar Vulnerability Manager está instalado. Para obtener más información sobre las diferencias entre IBM QRadar SIEM y IBM QRadar Log Manager, consulte [Capítulo 2, “Prestaciones de su producto IBM QRadar”](#), en la [página 3](#).

### Datos de activos

Un *activo* es cualquier punto final de la red que envía o recibe datos a través de la infraestructura de la red. Por ejemplo, son activos los portátiles, los servidores, las máquinas virtuales y los dispositivos portátiles. A cada activo de la base de datos de activos se le asigna un identificador exclusivo para que pueda distinguirse de los demás registros de activos.

La detección de dispositivos también es útil para crear un conjunto de datos de información histórica sobre el activo. Hacer un seguimiento de la información de activos a medida que cambia le ayuda a supervisar el uso de los activos en la red.

### Límites de activos

La base de datos de activos tiene una capacidad limitada. Cuando se alcanza el límite de activos de su hardware, no puede crear activos nuevos hasta que haya suficiente espacio disponible en la base de datos. En la tabla siguiente, se describen los límites de activos para cada tipo de hardware:

*Tabla 17. Límites de activos para el hardware*

Tipo de hardware	Límite de activos solo para consola	Límite de activos para consola con host gestionado
xx05	200.000	600.000
xx24	300.000	700.000
xx28	500.000	1.000.000
xx29	500.000	1.000.000
xx48	500.000	1.000.000
Otro hardware	60.000	60.000

### Perfiles de activo

Un *perfil de activo* es una recopilación de toda la información que IBM QRadar SIEM ha recogido a lo largo del tiempo acerca de un activo específico. El perfil incluye información acerca de los servicios que se están ejecutando en el activo y toda la información de identidad que se conozca.

QRadar SIEM crea automáticamente perfiles de activo a partir de los sucesos de identidad y los datos de flujos bidireccionales o, si están configuradas, las exploraciones de evaluación de vulnerabilidades. Los datos se correlacionan a través de un proceso que se denomina *conciliación de activos* y el perfil se actualiza a medida que llega información nueva a QRadar. El nombre del activo se deriva de la información de la actualización del activo en el siguiente orden de prioridad:

- Nombre
- Nombre de host NETBios
- Nombre de host DNS

- Dirección IP

### **Recopilación de datos de activos**

Los perfiles de activos se construyen dinámicamente a partir de información de identidad que se absorbe pasivamente de datos de sucesos o de flujos o de datos que QRadar busca activamente durante una exploración de vulnerabilidad. También puede importar datos de activo o editar manualmente el perfil de activo.

## **Orígenes de datos de activos**

---

Se reciben datos de activos de diversos orígenes en el despliegue de IBM QRadar.

Los datos de activos se escriben en la base de datos de activos de forma incremental, normalmente 2 o 3 datos a la vez. A excepción de las actualizaciones de los exploradores de vulnerabilidades de red, cada actualización de activo contiene información sobre un solo activo.

Los datos de activos generalmente provienen de uno de los orígenes de datos de activos siguientes:

### **Sucesos**

Las cargas útiles de sucesos, tales como las creadas por DHCP o servidores de autenticación, a menudo contienen inicios de sesión de usuario, direcciones IP, nombres de hosts, direcciones MAC y otro tipo de información de activos. Estos datos se proporcionan inmediatamente a la base de datos de activos para ayudar a determinar a qué activo se aplica la actualización de activo.

Los sucesos son la causa principal de las desviaciones de crecimiento de activos.

### **Flujos**

Las cargas útiles de flujo contienen información de comunicación, como la dirección IP, el puerto y el protocolo, que se recopila a intervalos regulares configurables. Al final de cada intervalo, los datos se proporcionan a la base de datos de activos, una dirección IP cada vez.

Puesto que los datos de activos de los flujos están emparejados con un activo según un solo identificador, la dirección IP, los datos de flujo nunca son la causa de las desviaciones de crecimiento de activos.

### **Exploradores de vulnerabilidades**

QRadar se integra tanto con exploradores de vulnerabilidades de IBM como de terceros que puedan proporcionar datos de activos tales como el sistema operativo, el software instalado y la información de parches. El tipo de datos varía de un explorador a otro y puede variar de una exploración a otra. A medida que se descubren nuevos activos, nueva información de puertos y nuevas vulnerabilidades, los datos se llevan al perfil de activo en función de los rangos de CIDR que están definidos en la exploración.

Los exploradores pueden añadir desviaciones de crecimiento de activos, pero no es habitual.

### **Interfaz de usuario**

Los usuarios que tienen el rol de activos pueden importar o proporcionar información de activos directamente a la base de datos de activos. Las actualizaciones de activos proporcionadas directamente por un usuario son para un activo específico. Por lo tanto, la etapa de conciliación de activos se omite.

Las actualizaciones de activos proporcionadas por los usuarios no añaden desviaciones de crecimiento de activos.

### **Datos de activos que tienen en cuenta el dominio**

Cuando un origen de datos de activos está configurado con información de dominio, todos los datos de activos que provienen de ese origen de datos se etiquetan automáticamente con el mismo dominio. Puesto que los datos del modelo de activos tienen en cuenta el dominio, la información de dominio se aplica a todos los componentes de QRadar, incluidos las identidades, los delitos, los perfiles de activo y el descubrimiento de servidores.

Cuando vea el perfil de activo, algunos campos podrían estar en blanco. Los campos en blanco existen cuando el sistema no ha recibido esta información en una actualización de activo o la información ha sobrepasado el periodo de retención de activos. El periodo predeterminado de retención es 120 días. Una dirección IP que aparezca como 0.0.0.0 indica que el activo no contiene información de dirección IP.

## **Flujo de trabajo de datos de activos entrantes**

---

IBM QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

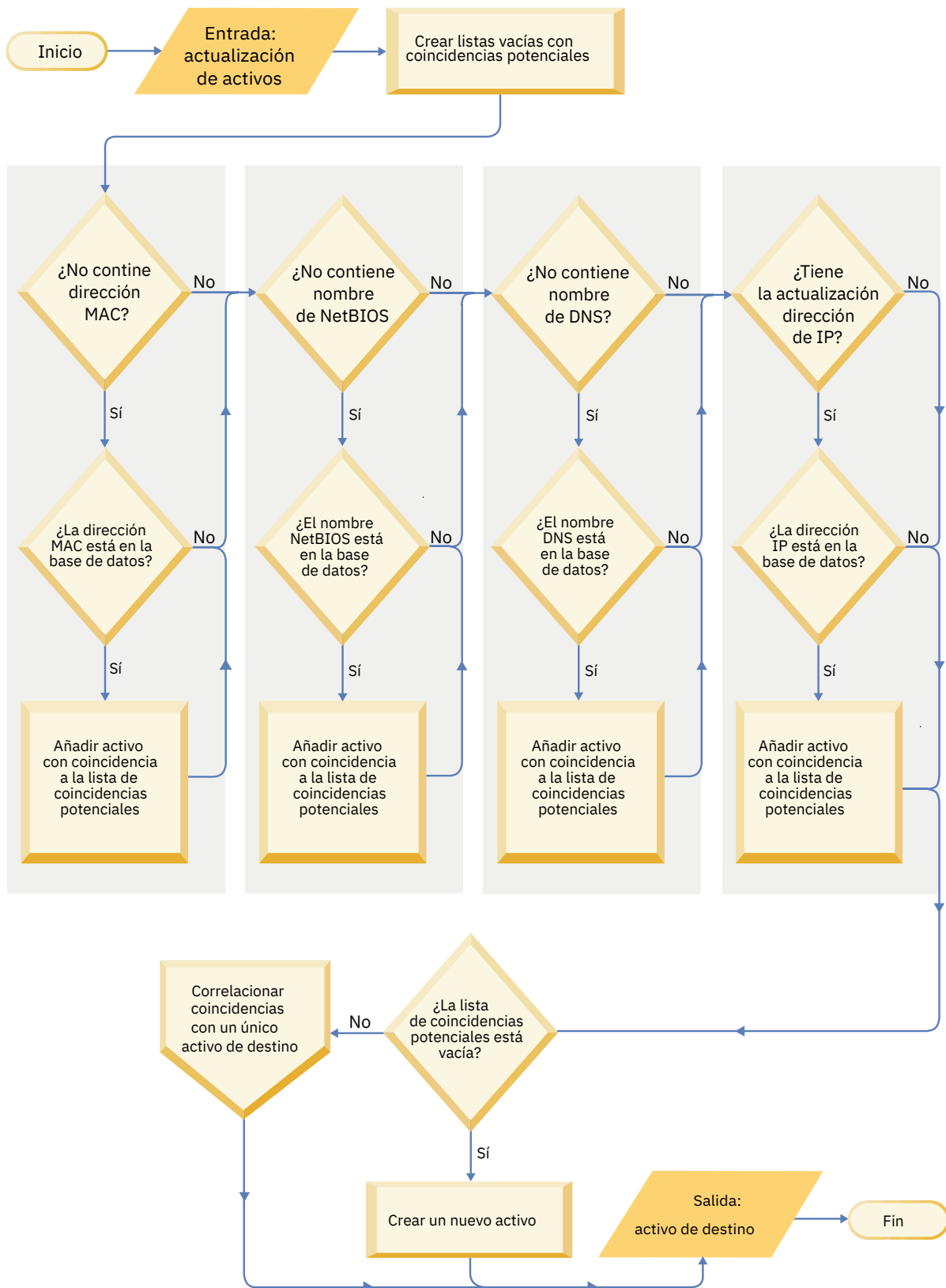


Figura 9. Diagrama de flujo de trabajo de datos de activos

1. QRadar recibe el suceso. El perfilador de activos examina la carga útil del suceso para obtener la información de identidad.

2. Si la información de identidad incluye una dirección MAC, un nombre de host NetBIOS o un nombre de host DNS que ya están asociados con un activo en la base de datos de activos, entonces ese activo se actualiza con la información nueva.
3. Si la única información de identidad disponible es una dirección IP, el sistema concilia la actualización del activo existente que tenga la misma dirección IP.
4. Si una actualización de activo tiene una dirección IP que coincide con un activo existente, pero también el resto de información de identidad no coincide, el sistema utiliza otra información para descartar un falso positivo en la coincidencia antes de que el activo existente se actualice.
5. Si la información de identidad no coincide con un activo existente en la base de datos, entonces se crea un nuevo activo basado en la información de la carga útil del suceso.

## Actualizaciones de los datos de activos

---

IBM QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

Cada actualización de activo debe contener información de confianza acerca de un único activo. Cuando QRadar recibe una actualización de activo, el sistema determina a qué activo se aplica la actualización.

La *conciliación de activos* es el proceso mediante el cual se determina la relación entre las actualizaciones de activos y el activo relacionado en la base de datos de activos. La conciliación de activos se produce después de que QRadar reciba la actualización, pero antes de que la información se escriba en la base de datos de activos.

### Información de identidad

Cada activo debe contener al menos un dato de identidad. Las actualizaciones posteriores que contengan un dato o más de los mismos datos de identidad se concilian con el activo propietario de los datos. Las actualizaciones que se basan en las direcciones IP se manejan con cuidado para evitar coincidencias de activos que sean falsos positivos. Los falsos positivos en las coincidencias de activos se producen cuando a un activo físico se le asigna la propiedad de una dirección IP que anteriormente era propiedad de otro activo del sistema.

Cuando se proporcionan varios datos de identidad, el perfilador de activos da prioridad a la información, de la más a la menos determinista, en el orden siguiente:

- Dirección MAC
- Nombre de host NetBIOS
- Nombre de host DNS
- Dirección IP

Las direcciones MAC, los nombres de host NetBIOS y los nombres de host DNS son exclusivos y, por lo tanto, se consideran datos de identidad definitivos. Las actualizaciones entrantes cuyas coincidencias con un activo existente solamente sean la dirección IP se manejan de forma diferente que las actualizaciones que coincidan con los datos de identidad más definitivos.

### Conceptos relacionados

[Reglas de exclusión de conciliación de activos](#)

## Reglas de exclusión de conciliación de activos

Con cada actualización de activo que entra en IBM QRadar, las reglas de exclusión de conciliación de activos aplican pruebas a la dirección MAC, el nombre de host NetBIOS, el nombre de host DNS y la dirección IP en la actualización de activo.

De forma predeterminada, se hace un seguimiento de cada dato de activos durante un periodo de dos horas. Si algún dato de identidad de la actualización de activo muestra un comportamiento sospechoso dos o más veces en un plazo de dos horas, ese dato se añade a las listas negras de activos. Cada tipo de datos de activos de identidad que se prueba genera una lista negra nueva.

**Consejo:** QRadar excluye los sucesos basándose en los datos que se reciben en el suceso, no en los datos que se infieren o enlazan posteriormente con el suceso.

En los entornos que tienen en cuenta el dominio, las reglas de exclusión de conciliación de activos hacen un seguimiento del comportamiento de los datos de activos por separado en cada dominio.

Las reglas de exclusión de conciliación de activos prueban los escenarios siguientes:

<i>Tabla 18. Pruebas y respuestas de Regla</i>	
<b>Escenario</b>	<b>Respuesta de regla</b>
Cuando una dirección MAC se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos

Puede ver estas reglas en la pestaña **Delitos** pulsando **Reglas** y, a continuación, seleccionando el grupo **Exclusión de conciliación de activos** en la lista desplegable.

## Conceptos relacionados

Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra  
Puede excluir direcciones IP de las listas negras ajustando las reglas de exclusión de activos.

## Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra

Puede excluir direcciones IP de las listas negras ajustando las reglas de exclusión de activos.

Como administrador de seguridad de red, gestiona una red corporativa que incluye un segmento de red wifi pública en el que las cesiones de direcciones IP son generalmente breves y frecuentes. Los activos en este segmento de la red tienden a ser transitorios, principalmente sistemas portátiles y dispositivos portátiles que inician y finalizan sesión en la wifi pública con frecuencia. Normalmente, una dirección IP individual la utilizan varias veces distintos dispositivos durante un breve periodo de tiempo.

En el resto del despliegue tiene una red cuidadosamente gestionada que consta únicamente de dispositivos de la empresa con nombres correctos e inventariados. Las cesiones de direcciones IP duran mucho más tiempo en esta parte de la red y a las direcciones IP se accede únicamente a través de la autenticación. En este segmento de red, desea saber inmediatamente cuando hay desviaciones de crecimiento de activos y desea conservar los valores predeterminados para las reglas de exclusión de conciliación de activos.

### Elaboración de la lista negra de direcciones IP

En este entorno, las reglas de exclusión de conciliación de activos predeterminadas incluyen inadvertidamente en una lista negra la red entera durante un breve periodo de tiempo.

Su equipo de seguridad observa que las notificaciones relacionadas con el activo generadas por el segmento de wifi son una molestia. Desea evitar que la wifi desencadene más notificaciones de desviaciones del crecimiento de activos.

### Ajuste de las reglas de conciliación de activos para ignorar algunas actualizaciones de activos

Revisa el informe **Desviaciones de activo por origen de registro** en la última notificación del sistema. Determina que los datos de la lista negra proceden del servidor DHCP de la wifi.

Los valores de la columna **Recuento de sucesos**, la columna **Recuento de flujos** y la columna **Delitos** de la fila correspondiente a la regla **AssetExclusion: Excluir IP por dirección MAC** indican que el servidor DHCP de la wifi desencadena esta regla.

Añade una prueba a las reglas de conciliación de activos existentes para hacer que las reglas dejen de añadir datos de la wifi a la lista negra.

```
Aplicar AssetExclusion:Excluir IP por Dirección MAC en sucesos detectados por el sistema Local y NO cuando los sucesos los ha detectado uno o varios MicrosoftDHCP @ microsoft.dhcp.test.com y NO cuando cualquiera de Dominio es la clave y cualquiera de IP de identidad es el valor en cualquiera de Lista blanca de IPv4 del dominio de conciliación de activos - Lista negra de IPv4 del dominio de conciliación de activos - IP y cuando al menos 3 sucesos se han visto con la misma IP de identidad y diferente MAC de identidad en 2 horas.
```

La regla actualizada prueba solamente los sucesos de los orígenes de registro que no están en el servidor DHCP de la wifi. Para evitar que los sucesos DHCP de la wifi pasen más pruebas costosas de análisis de comportamiento y conjunto de referencia, también ha movido esta prueba al principio de la pila de pruebas.

## Fusión de activos

La *fusión de activos* es el proceso según el cual la información de un activo se combina con la información de otro activo bajo la premisa de que son realmente el mismo activo físico.

La fusión de activos se produce cuando una actualización de activo contiene datos de identidad que coinciden con dos perfiles de activo diferentes. Por ejemplo, una única actualización que contiene un nombre de host NetBIOS que coincide con un perfil de activo y una dirección MAC que coincide con otro perfil de activo diferente podría desencadenar una fusión de activos.

En algunos sistemas se puede observar un gran volumen de fusión de activos porque tienen orígenes de datos de activos que inadvertidamente combinan en una misma actualización de activo información de identidad de dos activos físicos diferentes. Como ejemplos de estos sistemas cabe citar los entornos siguientes:

- Servidores syslog centrales que actúan como proxy de sucesos
- Máquinas virtuales
- Entornos de instalación automatizada
- Nombres de host no exclusivos, frecuentes con activos como iPads y iPhones.
- Redes privadas virtuales que tienen direcciones MAC compartidas
- Extensiones de origen de registro cuyo campo de identidad es `OverrideAndAlwaysSend=true`

Los activos que tienen muchas direcciones IP, direcciones MAC o nombres de host presentan desviaciones en el crecimiento de los activos y pueden desencadenar notificaciones del sistema.

### **Conceptos relacionados**

Identificación de desviaciones de crecimiento de activos

## **Identificación de desviaciones de crecimiento de activos**

---

A veces los orígenes de datos de activos generan actualizaciones que IBM QRadar no puede manejar correctamente sin intervención manual. En función de la causa del crecimiento anormal de los activos, puede arreglar el origen de datos de activos que está causando el problema o puede bloquear las actualizaciones de activos que provienen de ese origen de datos.

Las *desviaciones de crecimiento de activos* se dan cuando el número de actualizaciones de activos de un único dispositivo supera el límite establecido en el umbral de retención para un tipo concreto de información de identidad. El manejo adecuado de las desviaciones de crecimiento de activos es de vital importancia para mantener un modelo de activos preciso.

En la base de cada desviación de crecimiento de activos se encuentra un origen de datos de activos cuyos datos no son de confianza para actualizar el modelo de activos. Cuando se identifica una desviación potencial del crecimiento de los activos, debe examinar el origen de la información para determinar si hay una explicación razonable para que un activo acumule grandes cantidades de datos de identidad. La causa de una desviación de crecimiento de activos es específica de un entorno.

### **Ejemplo del servidor DHCP de crecimiento de activo anormal en un perfil de activo**

Supongamos que hay un servidor de VPN (red privada virtual) en una red DHCP (Protocolo de configuración dinámica de hosts). El servidor de VPN está configurado para asignar direcciones IP a los clientes de VPN entrantes enviando mediante un proxy las solicitudes DHCP en nombre del cliente al servidor DHCP de la red.

Desde la perspectiva del servidor DHCP, la misma dirección MAC solicita muchas asignaciones de direcciones IP en repetidas ocasiones. En el contexto de las operaciones de red, el servidor VPN delega las direcciones IP a los clientes, pero el servidor DHCP no puede distinguir cuándo una solicitud la realiza un activo en nombre de otro.

El registro del servidor DHCP, que está configurado como un origen de registro de QRadar, genera un suceso de acuse de recibo DHCP (DHCP ACK) que asocia la dirección MAC del servidor VPN con la dirección IP que se asigna al cliente de VPN. Cuando se produce la conciliación de activos, el sistema concilia este evento por dirección MAC, lo que da como resultado un activo existente único que crece con una dirección IP cada vez que se analiza un suceso DHCP ACK.



Finalmente, un solo perfil de activo contiene todas las direcciones IP que se han asignado al servidor de VPN. Esta desviación de crecimiento de activos está causada por las actualizaciones de activos que contienen información acerca de más de un activo.

### **Valores de umbral**

Cuando un activo de la base de datos alcanza un número determinado de propiedades, tales como varias direcciones IP o direcciones MAC, QRadar bloquea ese activo para que no reciba más actualizaciones.

Los valores de umbral del perfilador de activos indican las condiciones bajo las cuales un activo está bloqueado frente a las actualizaciones. El activo se actualiza normalmente hasta el valor del umbral. Cuando el sistema recopila datos suficientes para superar el umbral, el activo muestra una desviación de crecimiento de activo. Las futuras actualizaciones del activo se bloquean hasta que la desviación de crecimiento se corrija.

## **Notificaciones del sistema que indican desviaciones de crecimiento de activos**

IBM QRadar genera notificaciones del sistema para ayudarle a identificar y gestionar las desviaciones de crecimiento de activos en su entorno.

Los siguientes mensajes del sistema indican que QRadar ha identificado posibles desviaciones de crecimiento de activos:

- El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal
- Las reglas de listas negras de activos han añadido datos de activo nuevos a las listas negras de activos

Los mensajes de notificación del sistema incluyen enlaces a los informes para que sea más fácil identificar los activos que presentan desviaciones de crecimiento.

### **Datos de activos que cambian con frecuencia**

El crecimiento de activos puede estar causado por grandes volúmenes de datos de activos que cambian de forma correcta, como en las situaciones siguientes:

- Un dispositivo móvil que va de una oficina a otra con frecuencia al que se le asigna una dirección IP nueva cada vez que inicia sesión.
- Un dispositivo que se conecta a una wifi pública con cesiones breves de direcciones IP, como por ejemplo en un campus universitario, puede recopilar grandes volúmenes de datos de activos durante un semestre.

## **Ejemplo: Cómo los errores de configuración de las extensiones de origen de registro pueden provocar desviaciones de crecimiento de activos**

Las extensiones de origen de registro personalizado que están configuradas incorrectamente pueden provocar desviaciones de crecimiento de activos.

Configura una extensión de origen de registro personalizado para proporcionar actualizaciones de activos a IBM QRadar mediante el análisis de los nombres de usuario de la carga útil de suceso que se encuentra en un servidor de registro central. Configura la extensión de origen de registro para alterar temporalmente la propiedad de nombre de host de sucesos para que las actualizaciones de activos generadas por el origen de registro personalizado siempre especifiquen el nombre del host DNS del servidor de registro central.

En lugar de que QRadar reciba una actualización que tiene el nombre de host del activo en el que el usuario ha iniciado sesión, el origen de registro genera muchas actualizaciones de activos que tienen el mismo nombre de host.

En esta situación, la desviación de crecimiento de activos está causada por un solo perfil de activo que contiene muchas direcciones IP y muchos nombres de usuario.

## Resolución de problemas con perfiles de activo que sobrepasan el umbral de tamaño normal

IBM QRadar genera la notificación del sistema siguiente cuando la acumulación de datos bajo un único activo supera los límites de umbral configurados para los datos de identidad.

```
El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal
```

### Explicación

La carga útil muestra una lista de los cinco activos que presentan desviaciones con más frecuencia y proporciona información sobre por qué el sistema ha marcado cada activo como una desviación de crecimiento. Tal como se muestra en el ejemplo siguiente, la carga útil también muestra el número de veces que el activo ha intentado crecer más allá del umbral del tamaño de activo.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q11labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
Los cinco activos que presentan desviaciones con más frecuencia entre
el 13 de febrero de 2015 8:10:23 PM AST y el 13 de febrero de 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Cuando los datos de activos exceden el umbral configurado, QRadar bloquea el activo frente a actualizaciones futuras. Esta intervención evita que el sistema reciba más datos dañados y mitiga el impacto en el rendimiento que podría producirse si el sistema intenta conciliar las actualizaciones de entrada con un perfil de activo anormalmente grande.

### Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar los activos que contribuyen a la desviación de crecimiento de activo y determinar qué está provocando el crecimiento anormal. La notificación proporciona un enlace a un informe de todos los activos que han experimentado una desviación del crecimiento durante las últimas 24 horas.

Después de resolver la desviación de crecimiento de activo en su entorno, puede ejecutar el informe de nuevo.

1. Pulse la pestaña **Actividad de registro** y pulse **Buscar > Nueva búsqueda**.
2. Seleccione la búsqueda guardada **Desviación de crecimiento de activos: Informe de activos**.
3. Utilice el informe para identificar y reparar los datos de activos inexactos que se han creado durante la desviación.

## Los datos de activos nuevos se añaden a las listas negras de activos

IBM QRadar genera la notificación del sistema siguiente cuando un dato de activos concreto presenta un comportamiento que puede deberse a la desviación del crecimiento de activos.

```
Las reglas de lis. neg. act. han añadido datos de activo nuevos a las lis. neg. act.
```

### Explicación

Las reglas de exclusión de activos supervisan los datos de activos para comprobar la coherencia y la integridad. Las reglas hacen un seguimiento de datos de activos concretos a lo largo del tiempo para asegurarse de que están siendo observados siempre con el mismo subconjunto de datos dentro de un plazo de tiempo razonable.

Por ejemplo, si una actualización de activo incluye una dirección MAC y un nombre de host DNS, la dirección MAC está asociada con ese nombre de host DNS durante un periodo de tiempo concreto. Las actualizaciones de activos posteriores que contengan esa dirección MAC también contienen ese nombre de host DNS si se incluye alguno en la actualización de activo. Si la dirección MAC de repente se asocia

con un nombre de host DNS diferente durante un periodo breve de tiempo, el cambio se supervisa. Si la dirección MAC cambia de nuevo dentro de un periodo breve, la dirección MAC se marca para indicar que contribuye a una instancia de crecimiento de activo anormal o con desviaciones.

### Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar las reglas que se utilizan para supervisar los datos de activos. Pulse el enlace **Desviaciones de activo por origen de registro** en la notificación para ver las desviaciones de activo que se han producido en las últimas 24 horas.

Si los datos de activos son válidos, los administradores de QRadar pueden configurar QRadar para resolver el problema.

- Si las listas negras se llenan demasiado rápido, puede ajustar las reglas de exclusión de conciliación de activos que las llenan.
- Si desea añadir los datos a la base de datos de activos, puede eliminar los datos de activos de la lista negra y añadirlos a la lista blanca de activos correspondiente. Al añadir datos de un activo a la lista blanca se impide que reaparezcan inadvertidamente en la lista negra.

## Listas negras y listas blancas de activos

IBM QRadar utiliza un grupo de reglas de conciliación de activos para determinar si los datos de activos son de confianza. Cuando los datos de activos son cuestionables, QRadar utiliza listas negras y listas blancas de activos para determinar si deben actualizarse los perfiles de activo con los datos de activos.

Una *lista negra de activos* es un conjunto de datos que IBM QRadar considera no fiables. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

El administrador de QRadar puede modificar los datos de la lista negra y la lista blanca de activos para evitar futuras desviaciones de crecimiento de activos.

### Listas negras de activos

Una *lista negra de activos* es un conjunto de datos que IBM QRadar considera no fiables según las reglas de exclusión de conciliación de activos. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Cada actualización de activo en QRadar se compara con las listas negras de activos. Los datos de activos en listas negras se aplican globalmente en todos los dominios. Si la actualización de activo contiene información de identidad (dirección MAC, nombre de host NetBIOS, nombre de host DNS o dirección IP) que se encuentra en una lista negra, la actualización de entrada se descarta y la base de datos de activos no se actualiza.

En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

Tipo de datos de identidad	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Direcciones IP (v4)	Lista negra de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]

Tabla 19. Nombres de recopilación de referencia para los datos de las listas negras de activos (continuación)

Tipo de datos de identidad	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Nombres de host DNS	Lista negra de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista negra de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista negra de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
* ALNIC es un tipo alfanumérico que puede dar cabida tanto al nombre de host como a los valores de dirección MAC.		

El administrador de QRadar puede modificar las entradas de lista negra para asegurarse de que los nuevos datos de activos se manejan correctamente.

## Listas blancas de activos

Puede utilizar listas blancas de activos para evitar que los datos de activos de IBM QRadar reaparezcan inadvertidamente en las listas negras de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

El administrador de QRadar puede modificar las entradas de lista blanca para asegurarse de que los nuevos datos de activos se manejan correctamente.

### Ejemplo de caso práctico de lista blanca

La lista blanca es útil si tiene datos de activos que siguen apareciendo en las listas negras aunque se trate de una actualización de activo válido. Por ejemplo, podría tener un equilibrador de carga DNS con rotación que está configurado para rotar en un conjunto de cinco direcciones IP. Las reglas de exclusión de conciliación de activos podrían determinar que el hecho de que haya varias direcciones IP asociadas con el mismo nombre de host DNS es una indicación de que existe una desviación de crecimiento de activos, y el sistema podría añadir el equilibrador de carga DNS a la lista negra. Para resolver este problema, puede añadir el nombre de host DNS a la lista blanca de DNS de conciliación de activos.

### Entradas en masa a la lista blanca de activos

Una base de datos de activos precisa facilita la conexión de los delitos que se desencadenan en el sistema a activos físicos o virtuales en la red. Pasar por alto las desviaciones de activos añadiendo entradas en masa a la lista blanca de activos no es útil para la creación de una base de datos de activos precisa. En lugar de añadir entradas en masa a la lista blanca, revise la lista negra de activos para determinar qué está contribuyendo a la desviación de crecimiento de activos y luego determine cómo solucionar el problema.

### Tipos de listas blancas de activos

Cada tipo de datos de identidad se mantiene en una lista blanca por separado. En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

*Tabla 20. Nombre de recopilación de referencia para los datos de las listas blancas de activos*

<b>Tipo de datos</b>	<b>Nombre de recopilación de referencia</b>	<b>Tipo de recopilación de referencia</b>
Direcciones IP	Lista blanca de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]
Nombres de host DNS	Lista blanca de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista blanca de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista blanca de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]

\* ALNIC es un tipo alfanumérico que puede dar cabida al nombre de host y a valores de dirección MAC.

## Perfiles de activo

Los perfiles de activo proporcionan información sobre cada activo conocido en la red, incluyendo qué servicios se ejecutan en cada activo.

La información del perfil de activo se utiliza a efectos de correlación para ayudar a reducir los falsos positivos. Por ejemplo, si un origen intenta atacar un servicio específico que se ejecuta en un activo, QRadar determina si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo.

Los perfiles de activo se descubren automáticamente si tiene exploraciones de datos de flujo o de evaluación de vulnerabilidad (VA) configuradas. Para que los datos de flujo llenen los perfiles de activo, se necesitan flujos bidireccionales. Los perfiles de activo también se pueden crear automáticamente a partir de los sucesos de identidad. Para obtener más información sobre la VA, consulte *Guía de configuración de evaluación de vulnerabilidades de IBM QRadar*.

Para tener más información sobre los orígenes de flujo, consulte la publicación *Guía de administración de IBM QRadar*.

## Vulnerabilidades

Puede utilizar exploradores de QRadar Vulnerability Manager y de terceros para identificar vulnerabilidades.

Los exploradores de terceros identifican e informan de las vulnerabilidades descubiertas utilizando referencias externas, como Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB) y Critical Watch. Los exploradores de terceros incluyen, por ejemplo, QualysGuard y nCircle ip360. OSVDB asigna un identificador de referencia exclusiva (OSVDB ID) a cada vulnerabilidad. Las referencias externas asignan un identificador de referencia exclusiva a cada vulnerabilidad. Los ID de referencia de datos externos incluyen, por ejemplo, el ID de Common Vulnerability and Exposures (CVE) o el ID de Bugtraq. Para obtener más información sobre exploradores y evaluación de vulnerabilidad, consulte la publicación *Guía del usuario de IBM QRadar Vulnerability Manager*.

QRadar Vulnerability Manager es un componente que puede comprarse por separado y habilitarse utilizando una clave de licencia. QRadar Vulnerability Manager es una plataforma de exploración de red que proporciona conocimiento de las vulnerabilidades que existen en las aplicaciones, sistemas o dispositivos de la red. Después de que las exploraciones identifiquen las vulnerabilidades, puede buscar y revisar datos de vulnerabilidad, remediar vulnerabilidades y volver a ejecutar exploraciones para evaluar el nuevo nivel de riesgo.

Cuando se habilita QRadar Vulnerability Manager, puede realizar tareas de evaluación de vulnerabilidades en la pestaña **Vulnerabilidades**. En la pestaña **Activos**, puede ejecutar exploraciones en los activos seleccionados.

Para obtener más información, consulte la publicación *Guía del usuario de IBM QRadar Vulnerability Manager*

## Visión general de la pestaña Activos

La pestaña **Activos** le proporciona un espacio de trabajo desde el que puede gestionar los activos de red e investigar las vulnerabilidades de un activo, los puertos, las aplicaciones, el historial y otras asociaciones.

Mediante el uso de la pestaña **Activos**, puede:

- Ver todos los activos descubiertos.
- Añadir manualmente perfiles de activo.
- Buscar activos específicos.
- Ver información sobre activos descubiertos.
- Editar perfiles de activo para activos añadidos o descubiertos manualmente.
- Ajustar vulnerabilidades positivas falsas.
- Importar activos.
- Imprimir o exportar perfiles de activo.
- Descubrir activos.
- Configurar y gestionar exploración de volumen de terceros.
- Iniciar exploraciones de QRadar Vulnerability Manager.

Para obtener información sobre la opción de descubrimiento de servidores en el panel de navegación, consulte la publicación *Guía de administración de IBM QRadar*

Para obtener más información sobre la opción de Exploración de VA en el panel de navegación, consulte la publicación *IBM QRadar Risk Manager User Guide*.

## Visualización de un perfil de activo

En la lista de activos de la pestaña **Activos**, puede seleccionar y ver un perfil de activo. Un perfil de activo proporciona información sobre cada perfil.

### Acerca de esta tarea

La información de perfil de activo se descubre automáticamente a través del servidor de descubrimiento o se configura manualmente. Puede editar la información de perfil de activo generada automáticamente.

La página **Perfil de activo** proporciona la información sobre el activo que se organiza en varios paneles. Para ver un panel, puede pulsar la flecha (>) en el panel para ver más detalles o seleccionar el panel en el recuadro de lista **Visualizar** en la barra de herramientas.

La barra de herramientas de página **Perfil de activo** proporciona las funciones siguientes:

Opciones	Descripción
<b>Volver a lista de activos</b>	Pulse esta opción para volver a la lista de activos.
<b>Visualizar</b>	En el recuadro de lista, puede seleccionar el panel que desea ver en el panel Perfil de activo. Los paneles Resumen de activo y Resumen de interfaz de red se visualizan siempre.
<b>Editar activo</b>	Pulse esta opción para editar el Perfil de activo. Consulte <a href="#">“Adición o edición de un perfil de activo”</a> en la página 110.

Tabla 21. Funciones de barra de herramientas de página Perfil de activo (continuación)

Opciones	Descripción
<b>Ver por red</b>	Si este activo está asociado con un delito, esta opción le permitirá ver la lista de redes que están asociadas con este activo. Al pulsar <b>Ver por red</b> , se visualiza la ventana <b>Lista de redes</b> .
<b>Ver resumen de origen</b>	Si este activo es el origen de un delito, esta opción le permitirá ver la información de resumen de origen. Al pulsar <b>Ver resumen de origen</b> , se visualiza la ventana <b>Lista de delitos</b> .
<b>Ver resumen de destino</b>	Si este activo es el destino de un delito, esta opción le permitirá ver información de resumen de destino.  Al pulsar <b>Ver resumen de destino</b> , se visualiza la ventana <b>Lista de destinos</b> .
<b>Historial</b>	Pulse <b>Historial</b> para ver información de historial de sucesos para este activo. Al pulsar el icono <b>Historial</b> , se visualiza la ventana <b>Búsqueda de sucesos</b> , previamente rellena con los criterios de búsqueda de sucesos:  Si es necesario, puede personalizar los parámetros de búsqueda. Pulse <b>Buscar</b> para ver información de historial de sucesos.
<b>Aplicaciones</b>	Pulse <b>Aplicaciones</b> para ver información de aplicación para este activo. Al pulsar el icono <b>Aplicaciones</b> , se visualiza la ventana <b>Búsqueda de flujos</b> , previamente rellena con criterios de búsqueda de sucesos.  Si es necesario, puede personalizar los parámetros de búsqueda. Pulse <b>Buscar</b> para ver la información de aplicación.
<b>Buscar en conexiones</b>	Pulse <b>Buscar en conexiones</b> para buscar conexiones. Se visualiza la ventana <b>Búsqueda de conexión</b> .  Esta opción solo se visualiza cuando se ha adquirido IBM QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
<b>Ver topología</b>	Pulse <b>Ver topología</b> para investigar el activo adicionalmente. Se visualiza la ventana <b>Topología actual</b> .  Esta opción solo se visualiza cuando se ha adquirido IBM QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
<b>Acciones</b>	En la lista <b>Acciones</b> , seleccione <b>Historial de vulnerabilidades</b> .  Esta opción solo se visualiza cuando se ha adquirido IBM QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**
3. Efectúe una doble pulsación en el activo que desea ver.
4. Utilice las opciones de la barra de herramientas para visualizar los diversos paneles de información de perfil de activo. Consulte [Edición de un perfil de activo](#).
5. Para investigar las vulnerabilidades asociadas, pulse cada vulnerabilidad en el panel Vulnerabilidades. Consulte la Tabla 10-10
6. Si es necesario, edite el perfil de activo. Consulte [Edición de un perfil de activo](#).
7. Pulse **Volver a lista de activos** para seleccionar y ver otro activo, si es necesario.

## Adición o edición de un perfil de activo

Los perfiles de activo se descubren y añaden automáticamente; sin embargo, puede ser necesario añadir manualmente un perfil

### Acerca de esta tarea

Cuando se descubren activos mediante la utilización de la opción Descubrimiento de servidores, algunos detalles de perfil de activo se rellenan automáticamente. Se puede añadir manualmente información al perfil de activo y se pueden editar determinados parámetros.

Solo se pueden editar los parámetros que se han entrado manualmente. Los parámetros generados por el sistema aparecen en cursiva y no son editables. Los parámetros generados por el sistema pueden suprimirse, si es necesario.

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Elija una de las siguientes opciones:
  - Para añadir un activo, pulse **Añadir activo** y escriba la dirección IP o el rango de CIDR del activo en el campo **Nueva dirección IP**.
  - Para editar un activo, efectúe una doble pulsación en el activo que desea ver y pulse **Editar activo**.
4. Configure los parámetros del panel MAC y dirección MAC. Configure una o varias de las opciones siguientes:
  - Pulse el icono **Nueva dirección MAC** y escriba una dirección MAC en el recuadro de diálogo.
  - Pulse el icono **Nueva dirección IP** y escriba una dirección IP en el recuadro de diálogo.
  - Si se lista **NIC desconocido**, puede seleccionar este elemento, pulsar el icono **Editar** y escribir una nueva dirección MAC en el recuadro de diálogo.
  - Seleccione una dirección MAC o IP en la lista, pulse el icono **Editar** y escriba una dirección MAC nueva en el recuadro de diálogo.
  - Seleccione una dirección MAC o IP en la lista y pulse el icono **Eliminar**.
5. Configure los parámetros del panel Nombres y descripción. Configure una o varias de las opciones siguientes:



Parámetro	Descripción
DNS	<p>Elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• Escriba un nombre DNS y pulse <b>Añadir</b>.</li> <li>• Seleccione un nombre de DNS en la lista y pulse <b>Editar</b>.</li> <li>• Seleccione un nombre de DNS en la lista y pulse <b>Eliminar</b>.</li> </ul>
NetBIOS	<p>Elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• Escriba un nombre NetBIOS y pulse <b>Añadir</b>.</li> <li>• Seleccione un nombre de NetBIOS en la lista y pulse <b>Editar</b>.</li> <li>• Seleccione un nombre de NetBIOS en la lista y pulse <b>Eliminar</b>.</li> </ul>
Nombre	Escriba un nombre para este perfil de activo.
Ubicación	Escriba una ubicación para este perfil de activo.
Descripción	Escriba una descripción para este perfil de activo.
AP inalámbrico	Escriba el punto de acceso (AP) inalámbrico para este perfil de activo.
SSID inalámbrico	Escriba el identificador de conjunto de servicios (SSID) inalámbrico para este perfil de activo.
ID de conmutador	Escriba el ID de conmutador para este perfil de activo.
ID de puerto de conmutador	Escriba el ID de puerto de conmutador para este perfil de activo.

6. Configure los parámetros del panel Sistema operativo:

- a) En el recuadro de lista **Proveedor**, seleccione un proveedor de sistema operativo.
- b) En el recuadro de lista **Producto**, seleccione el sistema operativo para el perfil de activo.
- c) En el recuadro de lista **Versión**, seleccione la versión del sistema operativo seleccionado.
- d) Pulse el icono **Añadir**.
- e) En el recuadro de lista **Alterar temporalmente**, seleccione una de las opciones siguientes:
  - **Hasta próxima exploración:** Seleccione esta opción para especificar que el explorador proporciona información de sistema operativo y la información se puede editar temporalmente. Si edita los parámetros de sistema operativo, el explorador restaura la información en su próxima exploración.
  - **Siempre:** Seleccione esta opción para especificar que desea entrar manualmente la información del sistema operativo e impedir que el explorador actualice información.
- f) Seleccione un sistema operativo de la lista.
- g) Seleccione un sistema operativo y pulse en el icono **Conmutar alteración temporal**.

7. Configure los parámetros del panel CVSS y peso. Configure una o varias de las opciones siguientes:

Parámetro	Descripción
Potencial de daños colaterales	<p>Configure este parámetro para indicar la posibilidad de pérdida de vidas humanas o activos físicos a través de daños o robo de este activo. También puede utilizar este parámetro para indicar el potencial de pérdida económica de productividad o ingresos. El mayor potencial de daños colaterales aumenta el valor calculado en el parámetro de puntuación de CVSS.</p> <p>En el recuadro de lista <b>Potencial de daños colaterales</b>, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Ninguno</li> <li>• Bajo</li> <li>• Medio bajo</li> <li>• Medio alto</li> <li>• Alto</li> <li>• No definido</li> </ul> <p>Al configurar el parámetro <b>Potencial de daños colaterales</b>, el parámetro <b>Peso</b> se actualizará automáticamente.</p>
Requisito de confidencialidad	<p>Configure este parámetro para indicar el impacto en la confidencialidad de una vulnerabilidad atacada con éxito en este activo. Un mayor impacto de confidencialidad aumenta el valor calculado en el parámetro Puntuación de CVSS.</p> <p>En el recuadro de lista <b>Requisito de confidencialidad</b>, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Bajo</li> <li>• Medio</li> <li>• Alto</li> <li>• No definido</li> </ul>

Parámetro	Descripción
Requisito de disponibilidad	<p>Configure este parámetro para indicar el impacto en la disponibilidad del activo cuando una vulnerabilidad se ataca con éxito. Los ataques que consumen ancho de banda de red, ciclos de procesador o espacio de disco impactan la disponibilidad de un activo. Un mayor impacto de disponibilidad aumenta el valor calculado en el parámetro Puntuación de CVSS.</p> <p>En el recuadro de lista <b>Requisito de disponibilidad</b>, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Bajo</li> <li>• Medio</li> <li>• Alto</li> <li>• No definido</li> </ul>
Requisito de integridad	<p>Configure este parámetro para indicar que el impacto en la integridad del activo cuando una vulnerabilidad se ataca con éxito. La integridad hace referencia a la fiabilidad y la veracidad garantizada de la información. Un mayor impacto de integridad aumenta el valor calculado en el parámetro Puntuación de CVSS.</p> <p>En el recuadro de lista <b>Requisito de integridad</b>, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Bajo</li> <li>• Medio</li> <li>• Alto</li> <li>• No definido</li> </ul>
Peso	<p>En el recuadro de lista <b>Peso</b> , seleccione un peso para este perfil de activo. El rango de valores es de 0 a 10.</p> <p>Cuando configure el parámetro <b>Peso</b>, el parámetro <b>Potencial de daños colaterales</b> se actualiza automáticamente.</p>

8. Configure los parámetros del panel Propietario. Elija una o varias de las opciones siguientes:

Parámetro	Descripción
Propietario del negocio	<p>Escriba el nombre del propietario del negocio del activo. Un propietario de negocio es, por ejemplo, un director de departamento. La longitud máxima es de 255 caracteres.</p>
Contacto del propietario del negocio	<p>Escriba la información de contacto para el propietario de negocio. La longitud máxima es de 255 caracteres.</p>

Parámetro	Descripción
Propietario técnico	Escriba el propietario técnico del activo. Un propietario técnico es, por ejemplo, el director o gestor de TI. La longitud máxima es de 255 caracteres.
Contacto de propietario técnico	Escriba la información de contacto para el propietario técnico. La longitud máxima es de 255 caracteres.
Usuario técnico	En el recuadro de lista, seleccione el nombre de usuario que desea asociar con este perfil de activo.  También puede utilizar este parámetro para habilitar la remediación de vulnerabilidad automática para IBM Security QRadar Vulnerability Manager. Para obtener más información sobre la remediación automática, consulte la publicación <i>Guía del usuario de IBM QRadar Vulnerability Manager</i> .

9. Pulse **Guardar**.

## Búsqueda de perfiles de activo

Puede configurar parámetros de búsqueda para mostrar solo los perfiles de activo que desea investigar en la página **Activo** en la pestaña **Activos**.

### Acerca de esta tarea

Al acceder a la pestaña **Activos**, se visualiza la página **Activo** llena con todos los activos descubiertos en la red. Para refinar esta lista, puede configurar parámetros de búsqueda para visualizar solo los perfiles de activo que desea investigar.

En la página **Búsqueda de activo**, puede gestionar Grupos de búsqueda de activos. Para obtener más información sobre Grupos de búsqueda de activos, consulte [Grupos de búsqueda de activos](#).

La característica de búsqueda le permitirá buscar perfiles de host, activos e información de identidad. La información de identidad proporciona más detalles sobre los orígenes de registro en la red, incluyendo información de DNS, inicios de sesión de usuario y direcciones MAC.

Mediante la característica de búsqueda de activos, puede buscar activos por referencias de datos externas para determinar si existen vulnerabilidades conocidas en el despliegue.

Por ejemplo:

Recibe una notificación de que el ID de CVE: CVE-2010-000 está siendo utilizado activamente en el campo. Para verificar si los hosts del despliegue son vulnerables a este ataque, puede seleccionar **Referencia externa de vulnerabilidad** en la lista de parámetros de búsqueda, seleccionar **CVE** y, a continuación, escribir

2010-000

para ver una lista de todos los hosts que son vulnerables a ese ID de CVE específico.

**Nota:** Para obtener más información acerca de OSVDB, consulte <http://osvdb.org/>. Para obtener más información acerca de NVDB, consulte <http://nvd.nist.gov/>.

### Procedimiento

1. Pulse la pestaña **Activos**.

2. En el menú de navegación, pulse **Perfiles de activo**.
3. En la barra de herramientas, pulse **Buscar > Nueva búsqueda**.
4. Elija una de las siguientes opciones:
  - Para cargar una búsqueda guardada anteriormente, vaya al Paso 5.
  - Para crear una nueva búsqueda, vaya al Paso 6.
5. Seleccione una búsqueda guardada anteriormente:
  - a) Elija una de las siguientes opciones:
    - Opcional. En el recuadro de lista **Grupo**, seleccione el grupo de búsqueda de activos que desea visualizar en la lista **Búsquedas guardadas disponibles**.
    - En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desea cargar.
    - En el campo **Escriba la búsqueda guardada o seleccione en la lista**, escriba el nombre de la búsqueda que desea cargar.
  - b) Pulse **Cargar**.
6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
  - a) En el primer recuadro de lista, seleccione el parámetro de activo que desea buscar. Por ejemplo, **Nombre de host**, **Clasificación de riesgo de vulnerabilidad** o **Propietario técnico**.
  - b) En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda.
  - c) En el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.
  - d) Pulse **Añadir filtro**.
  - e) Repita estos pasos para cada filtro que desee añadir a los criterios de búsqueda.
7. Pulse **Buscar**.

## Resultados

Puede guardar los criterios de búsqueda de activos. Consulte [Guardar criterios de búsqueda de activos](#).

## Guardar criterios de búsqueda de activos

En la pestaña **Activo**, puede guardar criterios de búsqueda configurados para poder reutilizar los criterios. Los criterios de búsqueda guardados no caducan.

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Realice una búsqueda.
4. Pulse **Guardar criterios**.
5. Entre valores para los parámetros:

Parámetro	Descripción
<b>Especifique el nombre de esta búsqueda</b>	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.
<b>Gestionar grupos</b>	Pulse <b>Gestionar grupos</b> para gestionar grupos de búsqueda. Esta opción solo se visualiza si tiene permisos administrativos.

Parámetro	Descripción
<b>Asignar búsqueda a grupo(s)</b>	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo <b>Otros</b> de forma predeterminada.
<b>Incluir en Búsquedas rápidas</b>	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista <b>Búsqueda rápida</b> , que se encuentra en la barra de herramientas de la pestaña <b>Activos</b> .
<b>Establecer como valor predeterminado</b>	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada cuando accede a la pestaña <b>Activos</b> .
<b>Compartir con todos</b>	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

## Grupos de búsqueda de activos

Utilizando la ventana **Grupos de búsqueda de activos**, puede crear y gestionar grupos de búsqueda de activos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en la pestaña **Activos**.

### Visualización de grupos de búsqueda

Utilice la ventana **Grupos de búsqueda de activos** para ver una lista de grupos y subgrupos.

### Acerca de esta tarea

En la ventana **Grupos de búsqueda de activos**, puede ver detalles acerca de cada grupo, incluyendo una descripción y la fecha en que se ha modificado por última vez el grupo.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

La ventana **Grupos de búsqueda de activos** muestra los parámetros siguientes para cada grupo:

<i>Tabla 22. Funciones de barra de herramientas de ventanas Grupos de búsqueda de activos</i>	
Función	Descripción
<b>Grupo nuevo</b>	Para crear un nuevo grupo de búsqueda, puede pulsar <b>Grupo nuevo</b> . Consulte <a href="#">Creación de un grupo de búsqueda nuevo</a> .
<b>Editar</b>	Para editar un grupo de búsqueda existente, puede pulsar en <b>Editar</b> . Consulte <a href="#">Edición de un grupo de búsqueda</a> .
<b>Copiar</b>	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en <b>Copiar</b> . Consulte <a href="#">Copia de una búsqueda guardada en otro grupo</a> .
<b>Eliminar</b>	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse <b>Eliminar</b> . Consulte <a href="#">Eliminación de un grupo o una búsqueda guardada de un grupo</a> .

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar > Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Vea los grupos de búsqueda.

### Creación de un grupo de búsqueda nuevo

En la ventana **Grupos de búsqueda de activos**, puede crear un nuevo grupo de búsqueda.

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar > Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
6. Pulse **Grupo nuevo**.
7. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
8. Opcional. En el campo **Descripción**, escriba una descripción.
9. Pulse **Aceptar**.

### Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar > Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione el grupo que desea editar.
6. Pulse **Editar**.
7. Escriba un nombre nuevo en el campo **Nombre**.
8. Escriba una nueva descripción en el campo **Descripción**.
9. Pulse **Aceptar**.

### Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en otro grupo. También puede copiar la búsqueda guardada en más de un grupo.

## Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar > Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea copiar.
6. Pulse **Copiar**.
7. En la ventana **Grupos de elementos**, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
8. Pulse **Asignar grupos**.

## Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

### Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar los grupos siguientes del sistema:

- Grupos de búsqueda de activos
- Otros

### Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar > Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea eliminar del grupo:
  - Seleccione la búsqueda guardada que desea eliminar del grupo.
  - Seleccione el grupo que desea eliminar.

## Tareas de gestión de perfiles de activo

Puede suprimir, importar y exportar perfiles de activos utilizando la pestaña **Activos**.

### Acerca de esta tarea

Utilizando la pestaña **Activos**, puede suprimir, importar y exportar perfiles de activos.

### Supresión de activos

Puede suprimir activos específicos o todos los perfiles de activo listados.

### Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione el activo que desea suprimir y, a continuación, seleccione **Suprimir activo** en el recuadro de lista **Acciones**.
4. Pulse **Aceptar**.

### Importación de perfiles de activo

Puede importar información de perfil de activo.

### Antes de empezar

El archivo importado debe ser un archivo CSV con el formato siguiente:

```
ip,nombre,peso,descripción
```

Donde:

- **IP:** Especifica cualquier dirección IP válida en formato decimal con puntos. Por ejemplo: 192.168.5.34.
- **Nombre:** Especifica el nombre de este activo con una longitud de hasta 255 caracteres. Las comas no son válidas en este campo e invalidan el proceso de importación. Por ejemplo: WebServer01 es correcto.



- **Peso:** Especifica un número de 0 a 10, que indica la importancia de este activo en la red. Un valor de 0 indica una importancia baja y 10 es muy alta.
- **Descripción:** Especifica una descripción textual para este activo con una longitud de hasta 255 caracteres. Este valor es opcional.

Por ejemplo, las siguientes entradas se pueden incluir en un archivo CSV:

- 192.168.5.34,WebServer01,5,Main Production Web Server
- 192.168.5.35,MailServ01,0,

El proceso de importación fusiona los perfiles de activo importados con la información de perfil de activo que está actualmente almacenada en el sistema.

### Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el recuadro de lista **Acciones**, seleccione **Importar activos**.
4. Pulse **Examinar** para localizar y seleccionar el archivo CSV que desea importar.
5. Pulse **Importar activos** para empezar el proceso de importación.

### Exportación de activos

Puede exportar perfiles de activo listados a un archivo XML (Extended Markup Language - Lenguaje de marcado extensible) o CSV (Comma-Separated Value - Valor separado por comas).

### Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
  - Exportar a XML
  - Exportar a CSV
4. Vea la ventana de estado para el estado del proceso de exportación.
5. Opcional: Si desea utilizar otras pestañas y páginas mientras la exportación está en curso, pulse el enlace **Notificar cuando termine**.  

Cuando la exportación se haya completado, se visualizará la ventana **Descarga de archivo**.
6. En la ventana **Descarga de archivo**, elija una de las opciones siguientes:
  - **Abrir:** Seleccione esta opción para abrir los resultados de exportación en el navegador que haya elegido.
  - **Guardar:** Seleccione esta opción para guardar los resultados en el escritorio.
7. Pulse **Aceptar**.

## Investigar vulnerabilidades de activo

El panel Vulnerabilidades en la página **Perfil de activo** visualiza una lista de vulnerabilidades descubiertas para el activo.

### Acerca de esta tarea

Puede efectuar una doble pulsación en la vulnerabilidad a mostrar más detalles de vulnerabilidad.

La ventana **Investigar detalles de vulnerabilidad** proporciona los detalles siguientes:

<b>Parámetro</b>	<b>Descripción</b>
ID de vulnerabilidad	Especifica el ID de la vulnerabilidad. El ID de vulnerabilidad es un identificador exclusivo generado por VIS (Vulnerability Information System - Sistema de información de vulnerabilidad).
Fecha de publicación	Especifica la fecha en la que los detalles de vulnerabilidad se han publicado en la OSVDB.
Nombre	Especifica el nombre de la vulnerabilidad.
Activos	Especifica el número de activos de la red que tienen esta vulnerabilidad. Pulse el enlace para ver la lista de activos.
Activos, incluyendo excepciones	Especifica el número de activos de la red que tienen excepciones de vulnerabilidad. Pulse el enlace para ver la lista de activos.
CVE	Especifica el identificador de CVE para la vulnerabilidad. Los identificadores de CVE los proporciona la NVDB.  Pulse el enlace para obtener más información. Al pulsar en el enlace, el sitio web NVDB se visualiza en una ventana de navegador nueva.
xforce	Especifica el identificador de X-Force para la vulnerabilidad.  Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web de IBM Internet Security Systems se visualiza en una ventana de navegador nueva.
OSVDB	Especifica el identificador de OSVDB para la vulnerabilidad.  Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web OSVDB se visualiza en una ventana de navegador nueva.
Detalles de plug-in	Especifica el ID de QRadar Vulnerability Manager.  Pulse el enlace para ver definiciones de Oval, entradas de Windows Knowledge Base o avisos de UNIX para la vulnerabilidad.  Esta característica proporciona información sobre cómo QRadar Vulnerability Manager comprueba los detalles de vulnerabilidad durante una exploración de parches. Puede utilizarla para identificar por qué se ha generado una vulnerabilidad en un activo o por qué no se ha generado.

Parámetro	Descripción
Puntuación base CVSS	<p>Visualiza la puntuación de CVSS (Common Vulnerability Scoring System) de agregado de las vulnerabilidades en este activo. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades.</p> <p>La puntuación de CVSS se calcula utilizando los siguientes parámetros definidos por el usuario:</p> <ul style="list-style-type: none"> <li>• Potencial de daños colaterales</li> <li>• Requisito de confidencialidad</li> <li>• Requisito de disponibilidad</li> <li>• Requisito de integridad</li> </ul> <p>Para obtener más información sobre cómo configurar estos parámetros, consulte <a href="#">“Adición o edición de un perfil de activo” en la página 110.</a></p> <p>Para obtener más información acerca de CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</p>
Impacto	Visualiza el tipo de daño o perjuicio que se puede esperar si se aprovecha esta vulnerabilidad.
Medidas base de CVSS	<p>Muestra las medidas que se utilizan para calcular la puntuación base de CVSS, incluyendo:</p> <ul style="list-style-type: none"> <li>• Vector de acceso</li> <li>• Complejidad de acceso</li> <li>• Autenticación</li> <li>• Impacto de confidencialidad</li> <li>• Impacto de integridad</li> <li>• Impacto de disponibilidad</li> </ul>
Descripción	Especifica una descripción de la vulnerabilidad detectada. Este valor solo está disponible cuando el sistema integra herramientas de VA.
Problema	Especifica los efectos que la vulnerabilidad puede tener en la red.
Solución	Siga las instrucciones que se proporcionan para resolver la vulnerabilidad.
Parcheo virtual	Visualiza la información de parche virtual asociada con esta vulnerabilidad, si está disponible. Un parche virtual es una solución de mitigación a corto plazo para una vulnerabilidad descubierta recientemente. Esta información se deriva de los sucesos de IPS (Intrusion Protection System - Sistema de prevención de intrusiones). Si desea instalar el parche virtual, consulte la información de proveedor de IPS.

Parámetro	Descripción
Referencia	<p>Visualiza una lista de referencias externas, incluyendo:</p> <ul style="list-style-type: none"> <li>• <b>Tipo de referencia:</b> Especifica el tipo de referencia que se lista, por ejemplo una lista de envío de correo o URL de advertencia.</li> <li>• <b>URL:</b> Especifica el URL que puede pulsar para ver la referencia.</li> </ul> <p>Pulse el enlace para obtener más información. Al pulsar el enlace, el recurso externo se visualiza en una ventana de navegador nueva.</p>
Productos	<p>Visualiza una lista de productos que están asociados con esta vulnerabilidad.</p> <ul style="list-style-type: none"> <li>• <b>Proveedor:</b> Especifica el proveedor del producto.</li> <li>• <b>Producto:</b> Especifica el nombre de producto.</li> <li>• <b>Versión:</b> Especifica el número de versión del producto.</li> </ul>

### Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione un perfil de activo.
4. En el panel de vulnerabilidades, pulse el valor de parámetro **ID o Vulnerabilidad** para la vulnerabilidad que desea investigar.

---

# Capítulo 11. Gestión de gráficos

Puede utilizar varias opciones de configuración de gráficos para ver los datos.

Si selecciona un intervalo de tiempo o una opción de agrupación para ver los datos, los gráficos se visualizan sobre la lista de sucesos o de flujos.

Los gráficos no se visualizan mientras se está en modalidad continua.

Puede configurar un gráfico para seleccionar los datos que desea trazar. Puede configurar gráficos independientemente el uno del otro para visualizar los resultados de búsqueda desde diferentes perspectivas.

Los tipos de gráfico incluyen:

- Gráfico de barras: Visualiza los datos en un gráfico de barras. Esta opción solo está disponible para sucesos agrupados.
- Gráfico circular: Visualiza datos en un gráfico circular. Esta opción solo está disponible para sucesos agrupados.
- Tabla: Visualiza datos en una tabla. Esta opción solo está disponible para sucesos agrupados.
- Serie temporal: Visualiza un gráfico de líneas interactivo que representa los registros que se comparan por un intervalo de tiempo especificado. Para obtener información sobre cómo configurar criterios de búsqueda de serie temporal, consulte [Visión general de gráfico de serie temporal](#).

Después de configurar un gráfico, las configuraciones de gráfico se conservan al:

- Cambiar la vista utilizando el recuadro de lista **Visualizar**.
- Aplicar un filtro.
- Guardar criterios de búsqueda.

Las configuraciones de gráfico no se conservan al:

- Iniciar una búsqueda nueva.
- Acceder a una búsqueda rápida.
- Ver los resultados agrupados en una ventana de rama.
- Guarde los resultados de búsqueda.

**Nota:** Si utiliza el navegador web Mozilla Firefox y se instala una extensión de navegador de bloqueador de anuncios, no se visualizan gráficos. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.

---

## Visión general de gráfico de serie temporal

Los gráficos de serie temporal son representaciones gráficas de la actividad a lo largo del tiempo.

Los picos y valles que se visualizan en los gráficos describen la actividad de volumen alto y bajo. Los gráficos de serie temporal son útiles para las tendencias de corto plazo y largo plazo de los datos.

Mediante el uso de gráficos de serie temporal, puede acceder, navegar e investigar la actividad de registro o de red desde diversas vistas y perspectivas.

**Nota:** Debe tener los permisos de rol adecuados para gestionar y ver gráficos de serie temporal.

Para visualizar gráficos de serie temporal, debe crear y guardar una búsqueda que incluya opciones de agrupación y serie temporal. Puede guardar hasta 100 búsquedas de serie temporal.

Las búsquedas guardadas de serie temporal predeterminadas son accesibles desde la lista de búsquedas disponibles en la página de búsqueda de sucesos o flujos.

Puede identificar fácilmente las búsquedas de serie temporal guardadas en el menú **Búsquedas rápidas**, porque el nombre de búsqueda se añade con el rango de tiempo especificado en los criterios de búsqueda.

Si los parámetros de búsqueda coinciden con una búsqueda guardada anteriormente para las opciones de agrupación y definición de columna, es posible que se visualice automáticamente un gráfico de serie temporal para los resultados de búsqueda. Si no se visualiza automáticamente un gráfico de series temporal para los criterios de búsqueda no guardados, no existen criterios de búsqueda guardados anteriormente que coincidan con los parámetros de búsqueda. Si esto ocurre, debe habilitar la captura de datos de serie temporal y guardar los criterios de búsqueda.

Puede ampliar y explorar una línea temporal en un gráfico de series temporal para investigar la actividad. La tabla siguiente proporciona funciones que puede utilizar para ver gráficos de serie temporal.

<i>Tabla 23. Funciones de gráficos de serie temporal</i>	
<b>Función</b>	<b>Descripción</b>
Ver datos con mayor detalle	<p>Utilizando la característica de zoom, puede investigar segmentos de tiempo más pequeños del tráfico de sucesos.</p> <ul style="list-style-type: none"> <li>• Mueva el puntero del ratón sobre el gráfico y, a continuación, utilice la rueda del ratón para ampliar el gráfico (girar la rueda del ratón hacia arriba).</li> <li>• Resalte el área del gráfico que desea ampliar. Cuando suelte el botón del ratón, el gráfico muestra un segmento de tiempo más pequeño. Ahora puede pulsar y arrastrar el gráfico para explorar el gráfico.</li> </ul> <p>Al ampliar un gráfico de series temporal, el gráfico se renueva para mostrar un segmento de tiempo más pequeños.</p>
Ver un intervalo de tiempo mayor de datos	<p>Utilizando la característica de zoom, puede investigar segmentos de tiempo más grandes o volver al rango de tiempo máximo. Puede expandir un rango de tiempo utilizando una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Pulsar en el restablecimiento de zoom en la esquina superior izquierda del gráfico.</li> <li>• Mover el puntero de ratón sobre el gráfico y, a continuación, utilizar la rueda del ratón para expandir la vista (girar la rueda del ratón hacia abajo).</li> </ul>
Explorar el gráfico	<p>Cuando haya aumentado un gráfico de series temporal, puede pulsar y arrastrar el gráfico a la izquierda o a la derecha para explorar la línea temporal.</p>

## Leyendas de gráficos

Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarle a asociar los objetos de gráfico con los parámetros que representan.

Mediante la característica de leyenda, puede realizar las acciones siguientes:

- Mueva el puntero del ratón sobre un elemento de leyenda o el bloque de color de leyenda para ver más información sobre los parámetros que representa.
- Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente.
- Pulse un elemento de leyenda de gráfico circular o de barras para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento.
- Pulse **Leyenda**, o la flecha que se encuentra junto a ella, si desea eliminar la leyenda de la pantalla de gráfico.

## Configuración de gráficos

Puede utilizar opciones de configuración para cambiar el tipo de gráfico, el tipo de objeto del que desea crear el gráfico y el número de objetos que se representan en el gráfico. Para gráficos de serie temporal, también puede seleccionar un intervalo de tiempo y habilitar la captura de datos de serie temporal.

### Acerca de esta tarea

Los datos se pueden acumular para que cuando se realice una búsqueda de serie temporal, esté disponible una memoria caché de datos para visualizar datos para el periodo de tiempo anterior. Después de habilitar la captura de datos de serie temporal para un parámetro seleccionado, se visualiza un asterisco (\*) junto al parámetro en el recuadro de lista Valor para gráfico.

**Restricción:** Los gráficos no se visualizan cuando se visualizan sucesos o flujos en modalidad de tiempo real (modalidad continua). Para visualizar gráficos, debe acceder a la pestaña **Actividad de registro** o **Actividad de red** y realizar una búsqueda agrupada que especifica un rango de tiempo.

### Procedimiento

1. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
2. Para crear una búsqueda agrupada, siga estos pasos:
  - a) En la barra de herramientas, pulse **Buscar** > **Nueva búsqueda**.
  - b) En **Búsquedas guardadas disponibles**, seleccione una búsqueda y pulse **Cargar**.
  - c) Vaya al panel Definición de columna y si el cuadro de lista **Agrupar por** está vacío, en la lista **Columnas disponibles** seleccione una columna.
  - d) Pulse **Buscar**.
3. Para utilizar una búsqueda agrupada, en la barra de herramientas pulse **Búsquedas rápidas** y seleccione una búsqueda agrupada.
4. En el panel Gráficos, pulse el icono **Configurar** (⚙️).
5. Configure los parámetros siguientes:

Parámetro	Descripción
<b>Valor para gráfico</b>	El tipo de objeto que desea trazar en el eje Y del gráfico.  Las opciones incluyen todos los parámetros de suceso o de flujo normalizados y personalizados que se incluyen en los parámetros de búsqueda.
<b>Mostrar parte superior</b>	El número de objetos que desea ver en el gráfico. El valor predeterminado es 10. Si incluye más de 10 elementos en el gráfico, los datos serán ilegibles.
<b>Tipo de gráfico</b>	Si el gráfico de barras, circular o de tabla se basa en criterios de búsqueda guardados con un rango

Parámetro	Descripción
	de tiempo de más de 1 hora, debe pulsar <b>Actualizar detalles</b> para actualizar el gráfico y llenar los detalles de suceso.
<b>Capturar datos de serie temporal</b>	Habilita la captura de datos de series temporales. Cuando se selecciona este recuadro de selección, el gráfico empieza a acumular datos para gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada.  Esta opción solo está disponible en los gráficos de Serie temporal.
<b>Rango de tiempo</b>	El rango de tiempo que desea ver.  Esta opción solo está disponible en gráficos de serie temporal.

6. Si ha seleccionado la opción de gráfico **Serie temporal** y ha habilitado la opción **Capturar datos de serie temporal**, en el panel Gráficos, pulse **Guardar** .
7. Para ver la lista de sucesos o flujos si el rango de tiempo es mayor que 1 hora, pulse **Actualizar detalles**.




## Capítulo 12. Búsquedas de sucesos y flujos

Puede realizar búsquedas en las pestañas **Actividad de registro**, **Actividad de red** y **Delitos**.

Utilice las opciones de búsqueda e índice de IBM QRadar que mejoran el rendimiento de la búsqueda y devuelven resultados con más rapidez. Para buscar criterios específicos, las búsquedas avanzadas utilizan series de búsqueda de AQL.

Puede especificar criterios de filtro para buscar sucesos, flujos y delitos. Después de realizar una búsqueda, puede guardar los criterios de búsqueda y los resultados de la búsqueda.

Si el administrador de QRadar ha configurado restricciones de recursos para establecer limitaciones de

tiempo o datos sobre búsquedas de sucesos y de flujo, el icono de restricción de recursos () aparece junto al criterio de búsqueda.

### Conceptos relacionados

Opciones de búsqueda de Filtro rápido

Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

## Creación de una búsqueda personalizada

Puede buscar datos que coincidan con sus criterios utilizando opciones de búsqueda más específicas. Por ejemplo, puede especificar columnas para su búsqueda, que puede agrupar y reordenar para navegar más eficazmente por los resultados de la búsqueda.

### Acerca de esta tarea

La duración de la búsqueda varía dependiendo del tamaño de la base de datos.

Puede añadir nuevas opciones de búsqueda para filtrar los resultados de búsqueda y encontrar el suceso o flujo específico que desea.

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de suceso y de flujo:

Opciones	Descripción
Grupo	Seleccione un grupo de búsqueda de sucesos o un grupo de búsqueda de flujos para verlo en la lista <b>Búsquedas guardadas disponibles</b> .
Escriba la búsqueda guardada o seleccione en la lista	Escriba el nombre de una búsqueda guardada o una palabra clave para filtrar la lista <b>Búsquedas guardadas disponibles</b> .
Búsquedas guardadas disponibles	Esta lista muestra todas las búsquedas disponibles, a menos que utilice las opciones <b>Agrupe o Escriba la búsqueda guardada o Seleccione en la lista</b> para aplicar un filtro a la lista. Puede seleccionar una búsqueda guardada en esta lista para visualizarla o editarla.

Tabla 24. Opciones de búsqueda (continuación)

Opciones	Descripción
Buscar	El icono <b>Buscar</b> está disponible en varios paneles de la página de búsqueda. Puede pulsar <b>Buscar</b> cuando haya terminado de configurar la búsqueda y desee ver los resultados.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el menú <b>Búsqueda rápida</b> .
Incluir en Panel de control	Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña <b>Panel de control</b> . Para obtener más información sobre la pestaña <b>Panel de control</b> , consulte <a href="#">Gestión de panel de control</a> . <b>Nota:</b> Este parámetro solo se visualiza si se agrupa la búsqueda.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.
Compartir con todos	Marque este recuadro de selección para compartir esta búsqueda con todos los demás usuarios.
Tiempo real (modalidad continua)	Visualiza resultados en modalidad continua. <b>Nota:</b> Cuando se habilita Tiempo real (modalidad continua), no puede agrupar los resultados de búsqueda. Si selecciona cualquier opción de agrupación en el panel Definición de columna, se abre un mensaje de error.
Último intervalo (renovación automática)	Se produce una renovación de la pestaña <b>Actividad de registro</b> y de la pestaña <b>Actividad de red</b> a intervalos de un minuto para visualizar la información más reciente.
Reciente	Después de seleccionar esta opción, debe seleccionar una opción de rango de tiempo en la lista. <b>Nota:</b> Es posible que los resultados del último minuto no estén disponibles. Seleccione la opción <i>&lt;Intervalo específico&gt;</i> si desea ver todos los resultados.
Intervalo específico	Después de seleccionar esta opción, debe seleccionar el rango de fecha y hora en los calendarios <b>Hora de inicio</b> y <b>Hora de finalización</b> .

Tabla 24. Opciones de búsqueda (continuación)

Opciones	Descripción
Acumulación de datos	<p>Se visualiza cuando se carga una búsqueda guardada.</p> <p>Si no se acumulan datos para esta búsqueda guardada, se visualiza el siguiente búsqueda: No se están acumulando datos para esta búsqueda.</p> <p>Si se acumulan datos se acumulan para esta búsqueda guardada, se visualizan las opciones siguientes:</p> <p>Al pulsar el enlace de columna o pasar el puntero del ratón sobre él, se abre una lista de las columnas que están acumulando datos.</p> <p>Utilice el enlace <b>Habilitar recuentos exclusivos/ Inhabilitar recuentos exclusivos</b> para visualizar recuentos de sucesos y flujos exclusivos en lugar de promedios de recuentos a lo largo del tiempo. Después de pulsar el enlace <b>Habilitar recuentos exclusivos</b>, se abre un recuadro de diálogo que indica qué informes y búsquedas guardadas comparten los datos acumulados.</p>
Filtros actuales	Muestra los filtros que se aplican a esta búsqueda.
Guardar resultados cuando finalice la búsqueda	Guarda los resultados de búsqueda.
Visualizar	Especifica una columna predefinida que se ha establecido para visualizarse en los resultados de búsqueda.
Nombre	El nombre del diseño de columna personalizado.
Guardar diseño de columna	Guarda un diseño de columna personalizado que se ha modificado.
Suprimir diseño de columna	Suprime un diseño de columna personalizado que se ha guardado.
Escriba la columna o seleccione en la lista	<p>Filtra las columnas que figuran en la lista Columnas disponibles.</p> <p>Por ejemplo, escriba Device para visualizar una lista de columnas que incluyan Device en el nombre de columna.</p>
Columnas disponibles	Las columnas que se están utilizando actualmente para esta búsqueda guardada se resaltan y se visualizan en la lista de <b>Columnas</b> .

Tabla 24. Opciones de búsqueda (continuación)

Opciones	Descripción
Añadir y eliminar flechas de columna (conjunto superior)	<p>Utilice el conjunto superior de flechas para personalizar la lista <b>Agrupar por</b>.</p> <ul style="list-style-type: none"> <li>• Para añadir una columna, seleccione una o más columnas de la lista <b>Columnas disponibles</b> y pulse la flecha derecha.</li> <li>• Para eliminar una columna, seleccione una o más columnas de la lista <b>Agrupar por</b> y pulse la flecha izquierda.</li> </ul>
Añadir y eliminar flechas de columna (conjunto inferior)	<p>Utilice el conjunto inferior de flechas para personalizar la lista <b>Columnas</b>.</p> <ul style="list-style-type: none"> <li>• Para añadir una columna, seleccione una o más columnas de la lista <b>Columnas disponibles</b> y pulse la flecha derecha.</li> <li>• Para eliminar una columna, seleccione una o más columnas de la lista <b>Columnas</b> y pulse la flecha izquierda.</li> </ul>
Agrupar por	<p>Especifica las columnas en las que la búsqueda guardada agrupa los resultados.</p> <ul style="list-style-type: none"> <li>• Para subir una columna en la lista de prioridad, seleccione una columna y pulse la flecha arriba. También puede arrastrar la columna hacia arriba en la lista.</li> <li>• Para bajar una columna en la lista de prioridad, seleccione una columna y pulse la flecha abajo. También puede arrastrar la columna hacia abajo en la lista.</li> </ul> <p>La lista de prioridad especifica en qué orden se agrupan los resultados. Los resultados de búsqueda se agrupan por la primera columna de la lista <b>Agrupar por</b> y, a continuación, se agrupan por la columna siguiente de la lista.</p> <p><b>Nota:</b> Es posible que la búsqueda no devuelva los resultados correctos si se incluyen dominios de la lista <b>Agrupar por</b>.</p>

Tabla 24. Opciones de búsqueda (continuación)

Opciones	Descripción
Columnas	<p>Especifica las columnas que se han elegido para la búsqueda. Puede seleccionar más columnas de la lista <b>Columnas disponibles</b>. Puede personalizar adicionalmente la lista <b>Columnas</b> utilizando las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Para subir una columna en la lista de prioridad, seleccione una columna y pulse la flecha arriba. También puede arrastrar la columna hacia arriba en la lista.</li> <li>• Para bajar una columna en la lista de prioridad, seleccione una columna y pulse la flecha abajo. También puede arrastrar la columna hacia abajo en la lista.</li> </ul> <p>Si el tipo de columna es numérico o está basado en el tiempo y hay una entrada en la lista <b>Agrupar por</b>, la columna incluye una lista. Utilice el cuadro de lista para elegir cómo desea agrupar la columna.</p> <p>Si el tipo de columna es grupo, la columna incluye una lista para elegir cuántos niveles desea incluir para el grupo.</p>
Mover columnas entre la lista Agrupar por y la lista Columnas	<p>Mueva columnas entre la lista <b>Agrupar por</b> y la lista <b>Columnas</b> seleccionando una columna de una lista y arrastrándola a la otra.</p>
Ordenar por	<p>En la primera lista, seleccione la columna por la que desee ordenar los resultados de búsqueda. A continuación, en la segunda lista, seleccione el orden que desea para visualizar para los resultados de búsqueda.</p>
Límite de resultados	<p>Especifique el número de filas que una búsqueda devuelve en la ventana <b>Editar búsqueda</b>. El campo <b>Límite de resultados</b> también aparece en la ventana <b>Resultados</b>.</p> <ul style="list-style-type: none"> <li>• Para una búsqueda guardada, el límite se almacena en la búsqueda guardada y se vuelve a aplicar al cargar la búsqueda.</li> <li>• Cuando ordena una columna del resultado de búsqueda que tiene un límite de filas, la ordenación se realiza dentro de las filas limitadas que se muestran en la cuadrícula de datos.</li> <li>• En el caso de una búsqueda agrupada por con el gráfico de serie temporal activado, el límite de filas solo se aplica a la cuadrícula de datos. La lista <b>N principales</b> del gráfico de serie temporal controla cuántas series temporales se dibujan en el gráfico.</li> </ul>

## Procedimiento

1. Elija una opción de búsqueda:

- Para buscar sucesos, pulse la pestaña **Actividad de registro**.
- Para buscar flujos, pulse la pestaña **Actividad de red**.

2. En la lista **Buscar**, seleccione **Búsqueda nueva**.

3. Seleccione una búsqueda guardada anteriormente.

4. Para crear una búsqueda, en el panel Rango de tiempo, seleccione las opciones para el rango de tiempo que desea capturar para esta búsqueda.

**Nota:** El rango de tiempo que selecciona puede afectar al rendimiento, cuando el rango de tiempo es grande.

5. Habilite recuentos exclusivos en el panel **Acumulación de datos**.

**Nota:** La habilitación de recuentos exclusivos en datos acumulados que se comparten con muchos otros informes y búsquedas guardadas puede disminuir el rendimiento del sistema.

6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda.

- a) En la primera lista, seleccione un parámetro que desee buscar.
- b) En la segunda lista, seleccione el modificador que desea utilizar para la búsqueda.

### Nota:

Para buscar un suceso o un flujo cuya propiedad personalizada no tenga ningún valor, utilice el operador "is N/A". Para buscar un suceso o un flujo cuya propiedad personalizada tenga un valor, utilice el operador "is not N/A".

- c) Desde el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.
  - d) Pulse **Añadir filtro**.
  - e) Repita estos pasos para cada filtro que vaya a añadir a los criterios de búsqueda.
7. Para guardar automáticamente los resultados de búsqueda cuando la búsqueda se ha completado, marque el recuadro de selección **Guarde los resultados cuando finalice la búsqueda** y, a continuación, escriba un nombre para la búsqueda guardada.
8. En el panel Definición de columna, defina las columnas y el diseño de columna que desea utilizar para ver los resultados:
- a) En la lista **Visualizar**, seleccione la columna preconfigurada establecida para asociarse con esta búsqueda.
  - b) Pulse la flecha situada junto a **Definición de vista avanzada** para visualizar parámetros de búsqueda avanzada.
  - c) Personalice las columnas que se visualizarán en los resultados de búsqueda.
  - d) En el campo **Límite de resultados**, escriba el número de filas que desea que devuelva la búsqueda.
9. Pulse **Filtro**.

## Creación de un diseño de columna personalizado

Crear un diseño de columna personalizado añadiendo o eliminando columnas en un diseño existente.

### Procedimiento

1. En la pestaña **Actividad de registro** o la pestaña **Actividad de red**, pulse **Buscar > Editar búsqueda**.
2. En el panel **Definición de columna**, seleccione un diseño de columna existente en la lista **Visualizar**.

Cuando modifica el diseño, el nombre de la lista **Visualizar** se cambia automáticamente por *Personalizado*.

3. Modifique el agrupamiento de búsquedas.

- a) Para añadir una columna al grupo de búsquedas, seleccione una columna de la lista **Columnas disponibles** y pulse la flecha derecha para mover la columna a la lista **Agrupar por**.
  - b) Para mover una columna de la lista **Columnas** al grupo de búsquedas, seleccione una columna de la lista **Columnas** y arrástrela a la lista **Agrupar por**.
  - c) Para eliminar una columna del grupo de búsquedas, seleccione la columna de la lista **Agrupar por** y pulse la flecha izquierda.
  - d) Para cambiar el orden de los agrupamientos de columna, utilice las flechas arriba y abajo o arrastre las columnas a su sitio.
4. Modifique el diseño de la columna.
- a) Para añadir una columna a su diseño personalizado, seleccione una columna de la lista **Columnas disponibles** y pulse la flecha derecha para mover la columna a la lista **Columnas**.
  - b) Para mover una columna de la lista **Agrupar por** a su diseño personalizado, seleccione una columna en la lista **Agrupar por** y arrástrela a la lista **Columnas**.
  - c) Para eliminar una columna del diseño personalizado, seleccione la columna de la lista **Columnas** y pulse la flecha izquierda.
  - d) Para cambiar el orden de sus columnas, utilice las flechas arriba y abajo o arrastre las columnas a su sitio.
5. En el campo **Nombre**, especifique el nombre de su diseño de columna personalizado.
6. Pulse **Guardar diseño de columna**.

## Supresión de un diseño de columna personalizado

Puede suprimir un diseño de columna creado por el usuario existente.

### Procedimiento

1. En la pestaña **Actividad de registro** o la pestaña **Actividad de red**, pulse **Buscar > Editar búsqueda**.
2. En el panel **Definición de columna**, seleccione un diseño de columna creado por el usuario existente en la lista **Visualizar**.
3. Pulse **Suprimir diseño de columna**.

## Guardar criterios de búsqueda

---

Puede guardar los criterios de búsqueda configurados para poder reutilizar los criterios y utilizar los criterios de búsqueda guardados en otros componentes como, por ejemplo, informes. Los criterios de búsqueda guardados no caducan.

### Acerca de esta tarea

Si se especifica un rango temporal para la búsqueda, el nombre de búsqueda se añade con el rango de tiempo especificado. Por ejemplo, una búsqueda guardada denominada Explotaciones por origen con un rango de tiempo de Últimos 5 minutos se convierte en Explotaciones por origen - Últimos 5 minutos.

Si cambia una columna establecida en una búsqueda guardada anteriormente y luego guarda los criterios de búsqueda utilizando el mismo nombre, se perderán las acumulaciones anteriores de gráficos de series temporales.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. Realice una búsqueda.
3. Pulse **Guardar criterios**.

4. Entre valores para los parámetros:

Opción	Descripción
<b>Parámetro</b>	Descripción
<b>Nombre de búsqueda</b>	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.
<b>Asignar búsqueda a grupo(s)</b>	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo Otros de forma predeterminada. Para obtener más información, consulte <a href="#">Gestión de grupos de búsqueda</a> .
<b>Gestionar grupos</b>	Pulse <b>Gestionar grupos</b> para gestionar grupos de búsqueda. Para obtener más información, consulte <a href="#">Gestión de grupos de búsqueda</a> .
<b>Opciones de intervalo de tiempo:</b>	<p>Elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <b>Tiempo real (modalidad continua):</b> Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad continua.</li> <li>• <b>Último intervalo (renovación automática):</b> Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad de renovación automática. Se produce una renovación de la pestaña <b>Actividad de registro</b> y de la pestaña <b>Actividad de red</b> a intervalos de un minuto para visualizar la información más reciente.</li> <li>• <b>Reciente:</b> Seleccione esta opción y, desde este recuadro de lista, seleccione el rango de tiempo por el que desea filtrar.</li> <li>• <b>Intervalo específico:</b> Seleccione esta opción y, en el calendario, seleccione el rango de fecha y hora por el que desea filtrar.</li> </ul>
<b>Incluir en Búsquedas rápidas</b>	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista <b>Búsqueda rápida</b> en la barra de herramientas.
<b>Incluir en Panel de control</b>	<p>Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña <b>Panel de control</b>. Para obtener más información sobre la pestaña <b>Panel de control</b>, consulte <a href="#">Gestión de panel de control</a>.</p> <p><b>Nota:</b> Este parámetro solo se visualiza si se agrupa la búsqueda.</p>
<b>Establecer como valor predeterminado</b>	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.
<b>Compartir con todos</b>	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

5. Pulse **Aceptar**.

## Búsqueda planificada

Utilice la opción de búsqueda planificada para planificar una búsqueda y ver los resultados.

Puede planificar que una búsqueda se ejecute a una hora específica del día o de la noche. Si planifica que una búsqueda se ejecute por la noche, puede investigar por la mañana. A diferencia de los informes, tiene la opción de agrupar los resultados de búsqueda e investigar adicionalmente. Puede buscar el número de inicios de sesión anómalos en el grupo de red. Si el resultado es generalmente 10 y el resultado de la búsqueda es 100, puede agrupar los resultados de búsqueda para facilitar la investigación. Para ver qué usuario tiene la mayoría de inicios de sesión anómalos, puede agruparlos por nombre de usuario. Puede continuar investigando adicionalmente.

Puede planificar una búsqueda en sucesos o flujos desde la pestaña **Informes**. Debe seleccionar un conjunto de criterios de búsqueda previamente guardado para la planificación.



## 1. Cree un informe

Especifique la siguiente información en la ventana **Asistente de informes**:

- El tipo de gráfico es Sucesos/Archivos de registro o Flujos.
- El informe se basa en una búsqueda guardada.

**Nota:** QRadar no admite informes basados en búsquedas de AQL que contengan sentencias de subselección.

- Genere un delito.

Puede elegir la opción **Crear un delito individual** o la opción **Añadir resultado a un delito existente**.

También puede generar una búsqueda manual.

## 2. Vea los resultados de búsqueda

Puede ver los resultados de la búsqueda planificada desde la pestaña **Delitos**.

- Los delitos de búsqueda planificada se identifican por la columna **Tipo de delito**.

Si crea un delito individual, se genera un delito cada vez que se ejecuta el informe. Si añade el resultado de búsqueda guardada en un delito existente, se crea un delito la primera vez que se ejecuta el informe. Las ejecuciones de informe subsiguientes se añaden a este delito. Si no se devuelven resultados, el sistema no añade o crea un delito.

- Para ver el resultado de búsqueda más reciente en la ventana **Resumen de delitos**, efectúe una doble pulsación en un delito de búsqueda planificada de la lista de delitos. Para ver la lista de todas las ejecuciones de búsqueda planificada, pulse **Resultados de búsqueda** en el panel **Últimos 5 resultados de búsqueda**.

Puede asignar un delito de búsqueda planificada a un usuario.

### Tareas relacionadas

#### Creación de una búsqueda personalizada

Puede buscar datos que coincidan con sus criterios utilizando opciones de búsqueda más específicas. Por ejemplo, puede especificar columnas para su búsqueda, que puede agrupar y reordenar para navegar más eficazmente por los resultados de la búsqueda.

#### Asignar delitos a usuarios

De forma predeterminada, ningún delito nuevo está asignado. Puede asignar un delito a un usuario de IBM QRadar a efectos de investigación.

## Opciones de búsqueda avanzada

---

Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

**Nota:** Cuando teclee una consulta de AQL, utilice apóstrofes para una comparación de series y comillas para una comparación de valor de propiedad.

El campo **Búsqueda avanzada** tiene finalización automática y resaltado de sintaxis.

Utilice la finalización automática y el resaltado de sintaxis para ayudar a crear consultas. Para obtener información sobre los navegadores web soportados, consulte [“Navegadores web soportados”](#) en la [página 4](#)

**Nota:** Si utiliza un filtro rápido en la pestaña **Actividad de registro**, debe renovar la ventana del navegador antes de ejecutar una búsqueda avanzada.

### Acceso a búsqueda avanzada

Acceda a la opción **Búsqueda avanzada** desde la barra de herramientas **Buscar** que está en las pestañas **Actividad de red** y **Actividad de registro** para escribir una consulta de AQL.

Seleccione **Búsqueda avanzada** desde el recuadro de lista de la barra de herramientas **Buscar**.

Expanda el campo **Búsqueda avanzada** siguiendo estos pasos:

1. Arrastre el icono de expansión que se encuentra a la derecha del campo.
2. Pulse Mayús + Intro para ir a la línea siguiente.
3. Pulse Intro.

Puede pulsar el botón derecho del ratón en cualquier valor del resultado de búsqueda y filtrar por ese valor.

Efectúe una doble pulsación en cualquier fila del resultado de búsqueda para ver más detalles.

Todas las búsquedas, incluidas las búsquedas de AOL, se incluyen en el registro de auditoría.

### Ejemplos de serie de búsqueda de AQL

La tabla siguiente proporciona ejemplos de las series de búsqueda de AOL.

<i>Tabla 25. Ejemplos de series de búsqueda de AOL</i>	
<b>Descripción</b>	<b>Ejemplo</b>
Seleccionar columnas predeterminadas en sucesos. Seleccionar columnas predeterminados en flujos.	SELECT * FROM events SELECT * FROM flows
Seleccionar columnas específicas.	SELECT sourceip, destinationip FROM events
Seleccionar columnas específicas y ordenar los resultados.	SELECT sourceip, destinationip FROM events ORDER BY destinationip
Ejecutar una consulta de búsqueda agregada.	SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip
Ejecutar una llamada de función en una cláusula SELECT.	SELECT CATEGORYNAME(category) AS namedCategory FROM events
Filtrar los resultados de búsqueda utilizando una cláusula WHERE.	SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1
Buscar sucesos que han desencadenado una regla específica, que se basa en el nombre de regla o el texto parcial en el nombre de regla.	SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creventlist) ILIKE '%suspicious%'
Hacer referencia a nombres de campo que contienen caracteres especiales, por ejemplo caracteres aritméticos o espacios, poniendo el nombre de campo entre comillas.	SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'

La tabla siguiente proporciona ejemplos de las series de búsqueda de AQL para X-Force.

<i>Tabla 26. Ejemplos de series de búsqueda de AQL para X-Force</i>	
<b>Descripción</b>	<b>Ejemplo</b>
Comparar una dirección IP con una categoría de X-Force con un valor de confianza.	select * from events where XFORCE_IP_CONFIDENCE('Spam', sourceip) > 3

Tabla 26. Ejemplos de series de búsqueda de AQL para X-Force (continuación)

Descripción	Ejemplo
Buscar las categorías de URL de X-Force asociadas con un URL.	<code>select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL</code>
Recuperar las categorías de IP de X-Force que están asociadas con una IP.	<code>select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL</code>

Para obtener más información acerca de las funciones y los campos y operadores de búsqueda, consulte la publicación *Ariel Query Language guide*.

## Ejemplos de series de búsqueda de AQL

Utilice Ariel Query Language (AQL) para recuperar campos determinados de los sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.

**Nota:** Cuando construye una consulta AQL, si copia texto que contiene apóstrofes de cualquier documento y lo pega en IBM QRadar, la consulta no se analizará. Como solución, puede pegar el texto en QRadar y volver a teclear los apóstrofes o puede copiar y pegar el texto de IBM Knowledge Center.

### Informes de uso de cuenta

Comunidades de usuarios diferentes pueden tener indicadores de amenazas y de uso diferentes.

Utilice datos de referencia para informar sobre diversas propiedades de usuario, tales como departamento, ubicación o gestor. Puede utilizar datos de referencia externos.

La consulta siguiente devuelve información de metadatos sobre el usuario a partir de sucesos de inicio de sesión.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

### Identificadores de cuenta múltiples

En este ejemplo, los usuarios tienen varias cuentas en la red. La empresa necesita tener una vista individual de la actividad de un usuario.

Utilice datos de referencia para correlacionar un ID de usuario local con un ID global.

La consulta siguiente devuelve las cuentas de usuario que son utilizadas por un ID global en sucesos que están marcados como sospechosos.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

La consulta siguiente muestra las actividades que se han realizado mediante un ID global.

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

### Identificar una emisión larga de señales de baliza sospechosa

Muchas amenazas utilizan mandato y control para transmitir periódicamente durante días, semanas y meses.

Las búsquedas avanzadas pueden identificar patrones de conexión a lo largo del tiempo. Por ejemplo, puede investigar conexiones breves, constantes y de pequeño volumen que se realizan cada día/semana/mes entre direcciones IP o entre una dirección IP y una ubicación geográfica.

La consulta siguiente detecta posibles casos de emisiones de señales de baliza realizadas cada hora.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'HH')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING "different hours" > 20
AND "total flows" < 25
LAST 24 hours
```

**Consejo:** Puede modificar esta consulta para trabajar en archivos de registro de proxy y otros tipos de sucesos.

La consulta siguiente detecta posibles casos de emisiones diarias de señales de baliza.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING "different days" > 4
AND "total flows" < 14
LAST 7 days
```

La consulta siguiente detecta la emisión diaria de señales de baliza entre una dirección IP de origen y una dirección IP de destino. Las horas de emisión de señales de baliza no son las mismas cada día. El intervalo de tiempo entre emisiones es corto.

```
SELECT
sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and "total flows" < 10
LAST 7 days
```

La consulta siguiente detecta la emisión diaria de señales de baliza hacia un dominio utilizando sucesos de registro de proxy. Las horas de emisión de señales de baliza no son las mismas cada día. El intervalo de tiempo entre emisiones es corto.

```
SELECT sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
```

```
WHERE LOGSOURCEGROUPNAME(devicegroupplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and "total events" < 10
LAST 7 days
```

La propiedad **url\_domain** es una propiedad personalizada de los archivos de registro de proxy.

### Datos de inteligencia sobre amenazas externas

Los datos de uso y de seguridad que están correlacionados con datos de inteligencia sobre amenazas externas pueden proporcionar indicadores importantes sobre amenazas.

Las búsquedas avanzadas pueden asociar indicadores de amenazas externas con otros sucesos de seguridad y datos de uso.

Esta consulta muestra cómo puede analizar datos de amenazas externas durante muchos días, semanas o meses para identificar y priorizar el nivel de riesgo de activos y cuentas.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

### Inteligencia y configuración de activos

Los indicadores de amenazas y de uso varían según el tipo de activo, sistema operativo, vulnerabilidad, tipo de servidor, clasificación y otros parámetros.

La consulta siguiente utiliza búsquedas avanzadas y el modelo de activos para obtener conocimientos operativos respecto a una ubicación.

La función **Assetproperty** obtiene valores de propiedad de activos, lo cual permite incluir datos de activos en los resultados.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

La consulta siguiente muestra cómo puede utilizar búsquedas avanzadas y el seguimiento de identidades de usuario en el modelo de activos.

La función **AssetUser** obtiene el nombre de usuario a partir de la base de datos de activos.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY "Total Flows" DESC
LAST 3 HOURS
```

### Función de búsqueda de red

Puede utilizar la función de **búsqueda de red** para obtener el nombre de red que está asociado a una dirección IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

## **Función de búsqueda de regla**

Puede utilizar la función de **búsqueda de regla** para obtener el nombre de una regla por su identificador.

```
SELECT RULENAME(123) FROM events
```

La consulta siguiente devuelve los sucesos que activaron un nombre de regla determinado.

```
SELECT * FROM events  
WHERE RULENAME(createEventList) ILIKE '%my rule name%'
```

## **Búsqueda de texto completo TEXT SEARCH**

Puede utilizar el operador TEXT SEARCH para realizar búsquedas de texto completo mediante la opción **Búsqueda avanzada**.

En este ejemplo, hay un número de sucesos que contienen la palabra "firewall" en la carga útil. Puede buscar estos sucesos con la opción **Filtro rápido** y la opción **Búsqueda avanzada** en la pestaña **Actividad de registro**.

- Para utilizar la opción **Filtro rápido**, escriba el texto siguiente en el cuadro **Filtro rápido**: 'firewall'
- Para utilizar la opción **Búsqueda avanzada**, escriba la consulta siguiente en el cuadro **Búsqueda avanzada**:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

## **Propiedad personalizada**

Puede acceder a las propiedades personalizadas para sucesos y flujos cuando utiliza la opción **Búsqueda avanzada**.

La consulta siguiente utiliza la propiedad personalizada "MyWebsiteUrl" para ordenar sucesos por un URL web determinada:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

## **Tareas relacionadas**

[Creación de una propiedad personalizada](#)

Cree una propiedad personalizada para extraer datos que IBM QRadar no suele mostrar procedentes del suceso o de las cargas útiles del flujo. Es necesario activar las propiedades personalizadas y las propiedades personalizadas basadas en extracción deben analizarse para poder utilizarlas e las reglas, las búsquedas, los informes y para indexar los delitos.

## **Convertir una búsqueda guardada en una serie de AQL**

Convierta una búsqueda guardada en una serie de AQL y modifíquela para crear sus propias búsquedas y encontrar rápidamente los datos que desea. Ahora puede crear búsquedas más rápido que tecleando los criterios de búsqueda. También puede guardar la búsqueda para su uso futuro.

### **Procedimiento**

1. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
2. En la lista **Buscar**, seleccione **Nueva búsqueda** o **Editar búsqueda**.
3. Seleccione una búsqueda guardada anteriormente.
4. Pulse **Mostrar AQL**.
5. En la ventana **AQL**, pulse **Copiar en portapapeles**.
6. En la sección **Modalidad de búsqueda**, pulse **Búsqueda avanzada**.
7. Pegue el texto de la serie AQL en el cuadro de texto **Búsqueda avanzada**.

8. Modifique la serie para que incluya los datos que desea encontrar.
9. Pulse **Buscar** para mostrar los resultados.

### Qué hacer a continuación

Guarde los criterios de búsqueda para que la búsqueda aparezca en su lista de búsquedas guardadas y pueda volver a usarse.

### Conceptos relacionados

“Opciones de búsqueda avanzada” en la página 135

Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

“Ejemplos de series de búsqueda de AQL” en la página 137

Utilice Ariel Query Language (AQL) para recuperar campos determinados de los sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.

### Tareas relacionadas

“Creación de una búsqueda personalizada” en la página 127

Puede buscar datos que coincidan con sus criterios utilizando opciones de búsqueda más específicas. Por ejemplo, puede especificar columnas para su búsqueda, que puede agrupar y reordenar para navegar más eficazmente por los resultados de la búsqueda.

“Guardar criterios de búsqueda” en la página 133

Puede guardar los criterios de búsqueda configurados para poder reutilizar los criterios y utilizar los criterios de búsqueda guardados en otros componentes como, por ejemplo, informes. Los criterios de búsqueda guardados no caducan.

## Opciones de búsqueda de Filtro rápido

---

Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

El filtro rápido es uno de los métodos más rápidos que puede utilizar para datos específicos en cargas útiles de sucesos o flujos. Por ejemplo, puede utilizar el filtro rápido para buscar el tipo de información siguiente:

- Cada dispositivo de cortafuegos asignado a un rango de direcciones específico durante la semana pasada
- Una serie de archivos PDF enviados por una cuenta de Gmail en los últimos cinco días
- Todos los registros de un periodo de dos meses que coinciden exactamente con un nombre de usuario con guiones
- Una lista de direcciones de sitios web que terminan en .ca

Puede filtrar las búsquedas desde estas ubicaciones:

### Barra de herramientas Actividad de registro y barras de herramientas Actividad de red

Seleccione **Filtro rápido** en el recuadro de lista de la barra de herramientas **Buscar** para escribir una serie de búsqueda de texto. Pulse el icono **Filtro rápido** para aplicar el **Filtro rápido** a la lista de sucesos o flujos.

### Recuadro de diálogo Añadir filtro

Pulse el icono **Añadir filtro** en la pestaña **Actividad de registro** o **Actividad de red**.

Seleccione **Filtro rápido** como parámetro de filtro y escriba una serie de búsqueda de texto.

### Páginas de búsqueda de flujos

Añada un filtro rápido a la lista de filtros.

**Nota:** Las búsquedas de Filtro rápido que usan un intervalo de tiempo fuera del valor Retención de índice de carga útil pueden activar respuestas del sistema lentas y que consumen muchos recursos. Por

ejemplo, si la retención de índice de carga útil está establecida para 1 día y se utiliza como intervalo de tiempo en la búsqueda las últimas 30 horas.

Cuando vea **flujos** en tiempo real (modalidad continua) o modalidad del último intervalo, puede escribir solo palabras o frases simples en el campo **Filtro rápido**. Cuando vea **sucesos** o **flujos** en un rango de tiempo, siga estas directrices de sintaxis:

<i>Tabla 27. Directrices de sintaxis de filtro rápido</i>	
<b>Descripción</b>	<b>Ejemplo</b>
Incluir cualquier texto sin formato que se espera encontrar en la carga útil.	Firewall
Buscar frases exactas incluyendo varios términos entre comillas.	"Denegación de cortafuegos"
Incluir caracteres comodín individuales y múltiples. El término de búsqueda no puede empezar con un comodín.	F?rewall o F??ew*
Agrupar términos con expresiones lógicas, por ejemplo AND, OR y NOT. Para que se reconozca como expresiones lógicas y no como términos de búsqueda, la sintaxis y los operadores deben estar en mayúsculas.	(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)
Al crear criterios de búsqueda que incluyen la expresión lógica NOT, debe incluir al menos otro tipo de expresión lógica, de lo contrario, no se devuelven resultados.	(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)
Preceder los siguientes caracteres por una barra inclinada invertida para indicar que el carácter es parte del término de búsqueda: + - &&    ! ( ) {} [] ^ " ~ * ? : \.	"%PIX\ -5\ -304001"

### **Limitaciones**

Las búsquedas de filtro rápido funcionan sobre datos de sucesos o flujos en bruto y no distinguen entre campos. Por ejemplo, las búsquedas de filtro rápido devuelven coincidencias tanto para direcciones IP de origen como para direcciones IP de destino, a menos que incluya términos que puedan restringir los resultados.

Los términos de búsqueda se comparan en secuencia desde el primer carácter de la palabra o frase de carga útil. El término de búsqueda `user` coincide con `user_1` y `user_2`, pero no coincide con las frases siguientes: `ruser`, `myuser` o `anyuser`.

Las búsquedas de Filtro rápido utilizan el entorno local inglés. El *entorno local* es un valor que identifica el idioma o la geografía y determina los convenios de formato como ordenación, conversión de mayúsculas y minúsculas, clasificación de caracteres, idioma de los mensajes, representación de la fecha y la hora y representación numérica.

El entorno local lo establece el sistema operativo. Puede configurar QRadar para alterar temporalmente el valor del entorno local del sistema operativo. Por ejemplo, puede establecer el entorno local en **Inglés** y QRadar Console puede establecerse en **Italiano**.

Si utiliza caracteres Unicode en la consulta de búsqueda de filtro rápido, podrían devolverse resultados de búsqueda inesperados.

Si elige un entorno local que no sea inglés, puede utilizar la opción Búsqueda avanzada en QRadar para realizar búsquedas en los datos de sucesos y carga útil.



## ¿Cómo funcionan la búsqueda de filtro rápido y las señales de carga útil?

El texto de la carga útil se divide en palabras, frases, símbolos u otros elementos. Estas señales se delimitan por espacio y puntuación. Las señales no coinciden siempre con los términos de búsqueda especificados por el usuario lo que hace que algunos términos no se encuentren cuando no coinciden con la señal generada. Los caracteres delimitadores se descartan pero existen excepciones como por ejemplo las siguientes:

- Los periodos que no van seguidos por un espacio en blanco se incluyen como parte de la señal.  
Por ejemplo, `192.0.2.0:56` se señala como la señal de host `192.0.2.0` y la señal de puerto `56`.
- Las palabras se dividen en los guiones, a menos que la palabra contenga un número, en cuyo caso la señal no se divide y los números y los guiones se retienen como una señal.
- Los nombres de dominio de internet y las direcciones de correo electrónico se conservan como una sola señal.

`192.0.2.0/home/www` se señala como una señal y el URL no se separa.

`192.0.2.7:/calling1/www2/scp4/path5/fff` se señala como host `192.0.2.7` y el resto es una señal `/calling1/www2/scp4/path5/fff`

Los nombres de archivo y los nombres de URL que contienen más de un signo de subrayado se dividen antes de un punto (.).

Ejemplo de varios signos de subrayado en un nombre de archivo:

Si utiliza `hurricane_katrina_ladm118.jpg` como término de búsqueda, se divide en las señales siguientes:

- `hurricane`
- `katrina_ladm118.jpg`

Busque el término de búsqueda completo en la carga útil poniendo comillas alrededor del término de búsqueda: `"hurricane_katrina_ladm118.jpg"`

Ejemplo de varios signos de subrayado en una vía de acceso de archivo relativa:

`thumb.ladm1180830/thumb.ladm11808301806.hurricane_katrina_ladm118.jpg` se divide en las señales siguientes:

- `thumb.ladm1180830/thumb.ladm11808301806.hurricane`
- `katrina_ladm118.jpg`

Para buscar `hurricane_katrina_ladm118.jpg`, que consta de una señal parcial y una señal completa, ponga un asterisco frente al término de consulta `*hurricane_katrina_ladm118.jpg`

### Conceptos relacionados

[Búsquedas de sucesos y flujos](#)

Puede realizar búsquedas en las pestañas **Actividad de registro**, **Actividad de red** y **Delitos**.

## Identificar si se ha invertido la dirección del flujo o no

Cuando esté viendo un flujo en QRadar Console, es posible que desee saber si QRadar ha modificado la dirección del flujo o no y qué proceso ha llevado a cabo. Este algoritmo proporciona información sobre la presentación original del tráfico en la red y qué características del tráfico han hecho que se revirtiera, si ha habido una inversión.

Cuando el Recopilador de flujos detecte algún flujo, comprobará algunas de sus propiedades antes de actuar. En algunos casos, la comunicación o los flujos entre dispositivos es bidireccional (el cliente se comunica con el servidor y este responde al cliente). En este escenario, tanto el cliente como el servidor funcionan como si uno fuera el origen y el otro, el destino. En realidad, QRadar normaliza la comunicación y todos los flujos entre estas dos entidades siguen la misma convención: "destino" siempre se refiere al servidor y "origen" siempre se refiere al cliente.

Esta normalización se realiza revirtiendo la dirección de todos los flujos que van desde el servidor al cliente. El Recopilador de flujos inspecciona los flujos que ve y utiliza diferentes algoritmos para determinar qué entidad es el destino (intentando identificar qué entidad tiene más probabilidades de ser el servidor). Por ejemplo, supongamos que el Recopilador de flujos identifica el puerto de origen en un flujo de entrada como un puerto de destino común y revierte la dirección utilizando el algoritmo "1 - Single common destination port". Si el algoritmo es "3 - Arrival Time" or "4 - Flow Exporter", sabrá que el flujo no se ha modificado. Al conocer el flujo que se ha invertido y el algoritmo que ha activado esa inversión, podrá deducir cómo ha aparecido originalmente el flujo en la red.

## Valores de algoritmo de dirección del flujo

En la siguiente tabla se muestran los valores que se utilizan en el algoritmo de dirección del flujo.

Valor numérico	Descripción
0	Desconocido
1	Puerto de destino común único
2	Ambos puertos de destino comunes, se prefiere RFC 1700
3	Hora de llegada
4	Exportador de flujos

## Personalización de búsquedas para mostrar el algoritmo de dirección del flujo

Utilice la función de búsqueda para añadir el algoritmo de dirección del flujo a la pantalla **Detalles de flujo** en la pestaña **Actividad de red**. A continuación, puede investigar cada flujo para identificar si la dirección del flujo se ha invertido y, en caso afirmativo, qué algoritmo ha activado la inversión.

### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En la lista **Buscar**, seleccione **Búsqueda nueva**.
3. En la sección **Definición de columnas**, desplácese a la parte de abajo de la lista de columnas disponibles y añada **Algoritmo de dirección del flujo** a la lista de columnas para mostrar en la pestaña.
4. Pulse **Filtro**. La columna **Algoritmo de dirección del flujo** aparece en la pestaña **Actividad de red**, con un valor que representa el algoritmo que se ha utilizado.
5. Ponga en pausa el streaming de sucesos y haga clic en el flujo que desee para investigarlo con más profundidad en la pantalla **Detalles de flujo**.

### Resultados

La columna **Algoritmo de dirección del flujo** aparece ahora en la pantalla **Detalles de flujo** con todos los flujos.

## Identificación de la definición de campos de aplicación para un flujo

Cuando esté viendo un flujo en QRadar Console, es posible que desee saber si QRadar ha modificado el nombre de aplicación del flujo o no y si se ha producido algún proceso. Puede utilizar esta información para conocer con qué algoritmo se ha clasificado la aplicación y para asegurarse de que los algoritmos extraigan correctamente las características del flujo.

Cuando Recopilador de flujos detecta un flujo, utiliza diferentes algoritmos para determinar la aplicación de la que procede el flujo. Cuando el Recopilador de flujos identifica la aplicación, define la propiedad "Application" que aparece en la pantalla Detalles de flujo.

Es posible que tenga aplicaciones que no son estándar o personalizadas en su empresa que ha añadido con anterioridad a los archivos `/opt/qradar/conf/user_application_mapping.conf` o `signatures.xml` para que estas aplicaciones se identifiquen en QRadar. Ahora podrá usar el campo **Algoritmo de determinación de aplicación** para comprobar que sus aplicaciones personalizadas han sido identificadas por el algoritmo correcto. Por ejemplo, comenzará a ver flujos procedentes de esa aplicación identificados por el algoritmo "5 – User Port Based Mapping". A continuación, puede asignar un nivel de confianza a la definición de aplicación ahora que puede ver cómo se ha definido.

## Valores de algoritmos de determinación de aplicación

En la siguiente tabla se muestran los valores que se utilizan en el algoritmo de determinación de aplicación.

Valor numérico	Descripción
1	Desconocido
2	Firmas de aplicación
3	Decodificación basada en estado
4	Correlación basada en puertos de QRadar
5	Correlación de aplicaciones de usuario
6	Correlación de protocolos de mensajes de control de Internet
7	Exportador de flujos
8	Firmas de aplicación QNI
9	Inspectores QNI
10	Clasificación de aplicaciones web de X-Force

## Personalización de búsquedas para mostrar el algoritmo de determinación de aplicación

### Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En la lista **Buscar**, seleccione **Búsqueda nueva**.
3. En la sección **Definición de columnas**, desplácese a la parte de abajo de la lista de columnas disponibles y añada **Algoritmo de determinación de aplicación** a la lista de columnas para mostrar en la pestaña.
4. Pulse **Filtro**. La columna **Algoritmo de determinación de aplicación** aparece en la pestaña **Actividad de red**, con uno de los valores para representar el algoritmo que se ha utilizado.
5. Ponga en pausa el streaming de sucesos y haga clic en el flujo que desee para investigarlo con más profundidad en la pantalla **Detalles de flujo**.

**Nota:** Cuando utilice el **Algoritmo de determinación de aplicación**, el campo **Descripción de suceso** dejará de aparecer porque el algoritmo de aplicación contiene esa información.

## Resultados

La columna **Algoritmo de determinación de aplicación** aparece ahora en la pantalla **Detalles de flujo** con todos los flujos.

## Visualización de la descripción de datos de flujo de AWS enumerados

Los flujos que se reciben a través de las integraciones de Web Service (AWS) incluyen propiedades adicionales en la información de flujo.

### Acerca de esta tarea

Además de las propiedades de flujo normalizado estándar, por los flujos de AWS se muestran las propiedades siguientes:

- Nombre de interfaz (disponible para todos los flujos de IPFIX que envían este campo)
- Suceso de cortafuegos (enumerado, disponible para todos los flujos de IPFIX que envían este campo)
- Acción de AWS (enumerado)
- Estado de registro de AWS (enumerado)
- ID de cuenta de AWS

La tabla siguiente muestra la descripción de serie de cada uno de los campos enumerados.

<i>Tabla 28. Series enumeradas de AWS</i>	
<b>Campo enumerado</b>	<b>Descripción de serie</b>
<b>Suceso de cortafuegos</b>	Los valores numéricos del campo <b>Suceso de cortafuegos</b> se correlacionan con las descripciones siguientes: <ul style="list-style-type: none"><li>• 0 = Ignorar</li><li>• 1 = Flujo creado</li><li>• 2 = Flujo suprimido</li><li>• 3 = Flujo denegado</li><li>• 4 = Alerta de flujo</li><li>• 5 = Actualización de flujo</li></ul>
<b>Acción de AWS</b>	Los valores numéricos del campo <b>Acción de AWS</b> se correlacionan con las descripciones siguientes: <ul style="list-style-type: none"><li>• 0 = N/A</li><li>• 1 = Aceptar</li><li>• 2 = Rechazar</li></ul>
<b>Estado de registro de AWS</b>	Los valores numéricos del campo <b>Estado de registro de AWS</b> se correlacionan con las descripciones siguientes: <ul style="list-style-type: none"><li>• 0 = N/A</li><li>• 1 = Aceptar</li><li>• 2 = No hay datos</li><li>• 3 = Saltar datos</li></ul>

### Procedimiento

Para incluir la descripción de la propiedad enumerada en los resultados de la consulta, debe incluir la función LOOKUP en la serie de búsqueda de AQL.

a) Pulse la pestaña **Actividad de red**.

b) En el recuadro **Búsqueda avanzada**, cree la consulta de AQL que incluye LOOKUP para el campo que desea incluir en la búsqueda.

Los ejemplos siguientes muestran las sentencias LOOKUP para cada uno de los campos enumerados del flujo de AWS:

```
LOOKUP('firewall event', "firewall event")
```

```
LOOKUP('aws action', "aws action")
```

```
LOOKUP('aws log status', "aws log status")
```

Por ejemplo, la consulta siguiente utiliza LOOKUP en una cláusula WHERE y agrupa los flujos aceptados por aplicación.

```
SELECT APPLICATIONNAME(applicationid), count(*) as NumFlows FROM flows
WHERE LOOKUP('aws action', "aws action") == 'Accept'
GROUP BY applicationid ORDER BY NumFlows DESC
```

En este ejemplo la consulta utiliza LOOKUP en la cláusula SELECT para mostrar el número de los flujos aceptados frente a los flujos rechazados en el entorno de AWS:

```
SELECT LOOKUP('aws action', "aws action"), count(*) as NumFlows
FROM flows WHERE "aws action" > 0 GROUP BY "aws action"
ORDER BY NumFlows DESC LAST 7 DAYS
```

## Información de VLAN en registros de flujo de actividad de red

---

QRadar conserva la información de la red de área local virtual (VLAN) que se exporta en registros de flujos externos (IPFIX, NetFlow V9, sFlow V5 o J-Flow V9) o se visualiza en flujos internos (Napatech, Network Interface Card) o un dispositivo de IBM QRadar Network Insights). A continuación, puede consultar, filtrar, buscar o escribir reglas personalizadas con esta información de VLAN.

Los siguientes campos VLAN son compatibles con IPFIX, Netflow versión 9 y J-Flow.

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI (solo paquetes en bruto)
- dot1qCustomerDEI (solo paquetes en bruto)

Los siguientes campos de VLAN son compatibles con paquetes en bruto y sFlow versión 5.

- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- dot1qDEI
- dot1qCustomerDEI

Todos los flujos con información de VLAN contienen dos campos específicos de IBM que se pueden utilizar para definir dominios exclusivos en QRadar:

- ID de VLAN de empresa
- ID de VLAN de cliente

Por ejemplo, un flujo UDP se envía de 10.0.0.1:123 a 10.0.0.2:456 en la VLAN 10. Otro flujo de UDP se envía de 10.0.0.1:123 a 10.0.0.2:456 en la VLAN 20. En QRadar, el identificador exclusivo de cada flujo incluye los campos de VLAN anidados (incluidos los campos **post**). Esto significa que los dos flujos anteriores se tratan de forma independiente, cada uno con su propia definición de VLAN.

## Asignar dominios y arrendatarios a flujos con información de VLAN

---

Con el soporte de gestión de dominios de los flujos de VLAN, puede definir dominios en QRadar en función de la información de VLAN de su red.

En QRadar, puede asignar dominios a los flujos entrantes basándose en la información de VLAN que está incluida en el flujo. Los flujos entrantes se correlacionan con dominios que contienen la misma definición de VLAN. También puede filtrar y consultar los dominios para el dominio basado en VLAN.

Puede asignar arrendatarios a definiciones de dominio para obtener multitenencia. Las definiciones de dominio basadas en VLAN habilitan la multitenencia entre diferentes VLAN, si es necesario.

Por ejemplo, se crean dos definiciones de dominio y se correlacionan con dos arrendatarios de red:

- Para *arrendatario ABC*, el tráfico se envía en el ID de VLAN de empresa = 0, y el ID de VLAN de cliente = 10.
- Para *arrendatario DEF*, el tráfico se envía en el ID de VLAN de empresa = 0, y el ID de VLAN de cliente = 20.

La primera definición de dominio se crea para *arrendatario ABC*, que contiene una definición de VLAN de flujo de ID de VLAN de empresa = 0 y el ID de VLAN de cliente = 10.

Se crea una segunda definición de dominio para *arrendatario DEF*, que contiene una definición de VLAN de flujo de ID de VLAN de empresa = 0 y el ID de VLAN de cliente = 20.

Los flujos entrantes con los campos ID de VLAN de empresa y ID de VLAN de cliente establecidos en 0 y 10 solo puede verlos el *arrendatario ABC*. De forma similar, los flujos entrantes con los campos ID de VLAN de empresa y ID de VLAN de cliente de 0 y 20 solo puede verlos el *arrendatario DEF*. Esto refleja la propiedad de tráfico de cada arrendatario de la red.

## Visibilidad de los flujos de MPLS recibidos de los datos de IPFIX

---

Internet Protocol Flow Information Export (IPFIX) es un protocolo común que permite la exportación de información de flujo de los dispositivos de red. Multiprotocol Label Switching (MPLS) es una técnica de direccionamiento que se ejecuta en cualquier protocolo.

Con el soporte de MPLS para los registros de flujo de IPFIX en QFlow, puede filtrar y buscar flujos de IPFIX en IBM QRadar, que contiene campos de MPLS y reglas de grabación basadas en los valores de estos campos de MPLS.

Por ejemplo, un flujo de IPFIX se exporta desde un conmutador en una red que utiliza MPLS. El flujo de IPFIX que se exporta desde el direccionador contiene información sobre la pila de MPLS, que ahora se guarda como parte del flujo en QRadar®. La pila MPLS puede contener hasta 10 capas y cada una de ellas muestra información sobre el direccionamiento de flujos. Estos campos de MPLS se incluyen en reglas, búsquedas y filtros, y se pueden ver en la ventana **Detalles de flujo**.

### Filtrar en campos de MPLS

Utilice la opción **Añadir filtro** de la pestaña **Actividad de red** para filtrar los campos de MPLS.

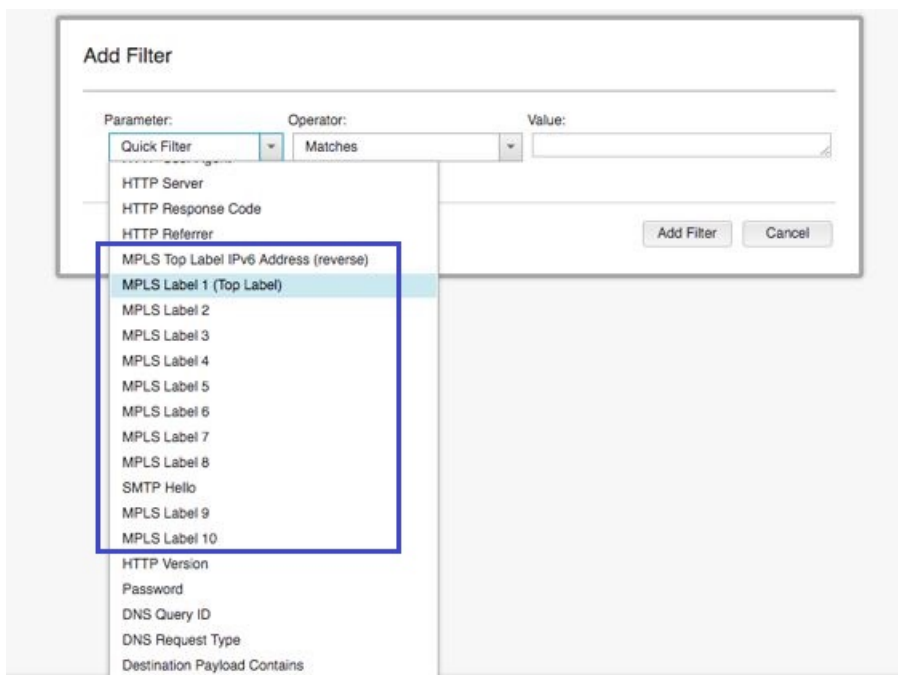


Figura 10. Filtrar en campos de MPLS

Para obtener más información sobre el uso de la opción de búsqueda **Añadir filtro**, consulte el tema [“Opciones de búsqueda de Filtro rápido”](#) en la página 141.

### Buscar campos de MPLS

Utilice la opción **Búsqueda avanzada** de la pestaña **Actividad de red** para buscar campos de MPLS.

The screenshot displays the IBM QRadar interface. At the top, the navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', and 'Admin'. The system time is 11:29 am. Below the navigation bar, there is a search bar with a dropdown menu set to 'Advanced Search'. The search query is 'select "mpls label 1 (top label)" from Flows LAST 3 HOURS'. The search parameters are: Start Time: 9/11/2018 8:30 AM, End Time: 9/11/2018 11:30 AM. The search is completed. Below the search bar, there is a 'Current Statistics' section and a 'Records Matched Over Time' chart. The chart shows a single peak at 9:30 AM. Below the chart, there is a table with the following data:

mpls label 1 (top label)	
000012	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	
N/A	

Figura 11. Buscar campos de MPLS

Para obtener más información sobre el uso de la opción **Búsqueda avanzada**, consulte el tema “Opciones de búsqueda avanzada” en la página 135.

### Ver información sobre los campos de MPLS

Para ver información sobre los campos de MPLS, efectúe una doble pulsación en un flujo en la ventana **Detalles de flujo** de la pestaña **Actividad de red**.




Flow Information			
Protocol	hopopt	Application	Other
Magnitude	 (4)	Relevance	1
Severity	6	Credibility	5
First Packet Time	23 Dec. 2017, 6:59:46 am	Last Packet Time	23 Dec. 2017, 11:32:13 am
Storage Time	11 Sep. 2018, 9:32:46 am		
Event Name	Unknown Application		
Low Level Category	Unknown Flow		
MPLS Top Label Type	Pseudowire (2)		
MPLS Top Label IPv4 Address	10.0.0.3		
MPLS Label 1 (Top Label)	Label Value: 1; Experimental Use: 001; Bottom of Stack: 0 (0x000012)		
MPLS Label 2	Label Value: 2; Experimental Use: 001; Bottom of Stack: 0 (0x000022)		
MPLS Label 3	Label Value: 3; Experimental Use: 001; Bottom of Stack: 0 (0x000032)		
MPLS Label 4	Label Value: 4; Experimental Use: 001; Bottom of Stack: 0 (0x000042)		
MPLS Label 5	Label Value: 5; Experimental Use: 001; Bottom of Stack: 0 (0x000052)		
MPLS Label 6	Label Value: 6; Experimental Use: 001; Bottom of Stack: 0 (0x000062)		
MPLS Label 7	Label Value: 7; Experimental Use: 001; Bottom of Stack: 0 (0x000072)		
MPLS Label 8	Label Value: 8; Experimental Use: 001; Bottom of Stack: 0 (0x000082)		
MPLS Label 9	Label Value: 9; Experimental Use: 001; Bottom of Stack: 0 (0x000092)		
MPLS Label 10	Label Value: 10; Experimental Use: 001; Bottom of Stack: 1 (0x0000a3)		
MPLS VPN Route Distinguisher	0101010101010101		
MPLS Top Label Prefix Length	4		
MPLS Top Label IPv6 Address	102:304:506:708:90a:b0c:d0e:f10		
MPLS Payload Length	255		
MPLS Top Label TTL	7		
MPLS Label Stack Length	30		
MPLS Label Stack Depth	10		
MPLS Top Label Exp	1		
Post MPLS Top Label Exp	1		
Pseudo Wire Type	4		
Pseudo Wire	10000		

Figura 12. Campos de MPLS en Información de flujo

### Elementos de información MPLS de IPFIX

En la tabla siguiente se describen los elementos de información MPLS de IPFIX que están admitidos. Todos estos elementos tienen el número de empresa privada (PEN): 0.

Campo	ID de elemento
mplsTopLabelType	46
mplsTopLabelIPv4Address	47
mplsTopLabelStackSection	70
mplsLabelStackSection2	71
mplsLabelStackSection3	72
mplsLabelStackSection4	73
mplsLabelStackSection5	74
mplsLabelStackSection6	75

<b>Campo</b>	<b>ID de elemento</b>
mplsLabelStackSection7	76
mplsLabelStackSection8	77
mplsLabelStackSection9	78
mplsLabelStackSection10	79
mplsVpnRouteDistinguisher	90
mplsTopLabelPrefixLength	91
mplsTopLabelIPv6Address	140
mplsPayloadLength	194
mplsTopLabelTTL	200
mplsLabelStackLength	201
mplsLabelStackDepth	202
mplsTopLabelExp	203
postMplsTopLabelExp	237
pseudoWireType	250
pseudoWireControlWord	251
mplsLabelStackSection	316
mplsPayloadPacketSection	317
sectionOffset	409
sectionExportedOctets	410

Para obtener más información sobre cada campo, consulte la asignación de elemento de información de IANA en [IP Flow Information Export \(IPFIX\) Entities](https://www.iana.org/assignments/ipfix/ipfix.xhtml) (<https://www.iana.org/assignments/ipfix/ipfix.xhtml>).

## Búsquedas de delitos

Puede buscar delitos utilizando criterios específicos para visualizar, en una lista de resultados, los delitos que coinciden con los criterios de búsqueda.

Puede crear una búsqueda nueva o cargar un conjunto de criterios de búsqueda que previamente se han guardado.

### Buscar delitos en las páginas **Mis delitos** y **Todos los delitos**

En las páginas **Mis delitos** y **Todos los delitos** de la pestaña **Delito**, puede buscar delitos que coinciden con los criterios de búsqueda especificados.

#### Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en las páginas **Mis delitos** y **Todos los delitos**.

Para obtener información sobre las categorías, consulte la publicación *Guía de administración de IBM QRadar*.

Tabla 29. Opciones de búsqueda de las páginas *Mis delitos* y *Todos los delitos*

Opciones	Descripción
<b>Grupo</b>	Este cuadro de lista le permite seleccionar un grupo de búsqueda de delito en la lista <b>Búsquedas guardadas disponibles</b> para su visualización.
<b>Escriba la búsqueda guardada o seleccione en la lista</b>	Este campo le permite escribir el nombre de una búsqueda guardada o una palabra clave para filtrar la lista <b>Búsquedas guardadas disponibles</b> .
<b>Búsquedas guardadas disponibles</b>	Esta lista muestra todas las búsquedas disponibles, a menos que aplique un filtro a la lista utilizando las opciones Grupo o <b>Escriba la búsqueda guardada o seleccione en la lista</b> . Puede seleccionar una búsqueda guardada en esta lista para visualizarla o editarla.
<b>Todos los delitos</b>	Esta opción le permite buscar todos los delitos sin importar el rango de tiempo.
<b>Reciente</b>	Esta opción le permite seleccionar un rango de tiempo predefinido que desee utilizar como filtro. Después de seleccionar esta opción, debe seleccionar una opción de rango de tiempo en el cuadro de lista.
<b>Intervalo específico</b>	Esta opción le permite definir un rango de tiempo personalizado para la búsqueda. Después de seleccionar esta opción, debe seleccionar una de las opciones siguientes. <ul style="list-style-type: none"> <li>• <b>Fecha de inicio entre:</b> seleccione esta casilla para buscar delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.</li> <li>• <b>Último suceso/flujo entre:</b> seleccione esta casilla para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.</li> </ul>
<b>Buscar</b>	El icono <b>Buscar</b> está disponible en varios paneles de la página de búsqueda. Puede pulsar <b>Buscar</b> cuando termine de configurar la búsqueda y desee ver los resultados.
<b>ID de delito</b>	En este campo, puede escribir el ID de delito que desee buscar.
<b>Descripción</b>	En este campo, puede escribir la descripción para la que desee buscar.
<b>Asignado a usuario</b>	En este cuadro de lista, puede seleccionar el nombre de usuario para el que desee buscar.

Tabla 29. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
<b>Dirección</b>	<p>En este cuadro de lista, puede seleccionar la dirección de delito para la que desee buscar. Las opciones son:</p> <ul style="list-style-type: none"> <li>• Local a local</li> <li>• Local a remoto</li> <li>• Remoto a local</li> <li>• Remoto a remoto</li> <li>• Local a remoto o local</li> <li>• Remoto a remoto o local</li> </ul>
<b>IP de origen</b>	<p>En este campo, puede escribir la dirección IPv4 o IPv6 de origen o rango de CIDR para el que desee buscar.</p>
<b>IP de destino</b>	<p>En este campo, puede escribir la dirección IPv4 o IPv6 de destino o rango de CIDR para el que desee buscar.</p>
<b>Magnitud</b>	<p>En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.</p>
<b>Gravedad</b>	<p>En este cuadro de lista, puede especificar un valor de gravedad y luego seleccionar que solamente se muestren los delitos cuya gravedad sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.</p>
<b>Credibilidad</b>	<p>En este cuadro de lista, puede especificar un valor de credibilidad y luego seleccionar que solamente se muestren los delitos cuya credibilidad sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.</p>
<b>Importancia</b>	<p>En este cuadro de lista, puede especificar un valor de importancia y luego seleccionar que solamente se muestren los delitos cuya importancia sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.</p>
<b>Contiene nombre de usuario</b>	<p>En este campo, puede escribir una sentencia de expresión regular (regex) para buscar delitos que contienen un nombre de usuario determinado. Cuando defina patrones de expresión de regular personalizados, siga las reglas de expresión regular tal como están definidas por el lenguaje de programación Java™. Para obtener más información, puede consultar las guías de aprendizaje sobre expresiones regulares que encontrará en la web.</p>
<b>Red de origen</b>	<p>En este cuadro de lista, puede seleccionar la red de origen para la que desee buscar.</p>

Tabla 29. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
<b>Red de destino</b>	En este cuadro de lista, puede seleccionar la red de destino para la que desee buscar.
<b>Categoría de nivel alto</b>	En este cuadro de lista, puede seleccionar la categoría de nivel alto para la que desee buscar. .
<b>Categoría de nivel bajo</b>	En este cuadro de lista, puede seleccionar la categoría de nivel bajo para la que desee buscar.
<b>Excluir</b>	<p>Las opciones de este panel le permiten excluir delitos en los resultados de búsqueda. Las opciones son:</p> <ul style="list-style-type: none"> <li>• Delitos activos</li> <li>• Delitos ocultos</li> <li>• Delitos cerrados</li> <li>• Delitos inactivos</li> <li>• Delitos protegidos</li> </ul>
<b>Cerrado por usuario</b>	<p>Este parámetro solo se muestra cuando la casilla <b>Delitos cerrados</b> está en blanco en el panel Excluir.</p> <p>En este cuadro de lista, puede seleccionar el nombre de usuario para el que desee buscar delitos cerrados, o seleccionar <b>Cualquiera</b> para mostrar todos los delitos cerrados.</p>
<b>Razón del cierre</b>	<p>Este parámetro solo se muestra cuando la casilla <b>Delitos cerrados</b> está en blanco en el panel Excluir.</p> <p>En este cuadro de lista, puede seleccionar una razón para la que desee buscar delitos cerrados, o seleccionar <b>Cualquiera</b> para mostrar todos los delitos cerrados.</p>
<b>Sucesos</b>	En este cuadro de lista, puede especificar un valor de recuento de sucesos y luego seleccionar que solamente se muestren los delitos cuyo recuento de sucesos sea igual, menor o mayor que el valor configurado.
<b>Flujos</b>	En este cuadro de lista, puede especificar un valor de recuento de flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento de flujos sea igual, menor o mayor que el valor configurado.
<b>Sucesos/flujos totales</b>	En este cuadro de lista, puede especificar un valor de recuento total de sucesos y flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento total de sucesos y flujos sea igual, menor o mayor que el valor configurado.

Tabla 29. Opciones de búsqueda de las páginas *Mis delitos* y *Todos los delitos* (continuación)

Opciones	Descripción
<b>Destinos</b>	En este cuadro de lista, puede especificar un valor de recuento de direcciones IP de destino y luego seleccionar que solamente se muestren los delitos cuyo recuento de direcciones IP de destino sea igual, menor o mayor que el valor configurado.
<b>Grupo de origen de registro</b>	En este cuadro de lista, puede seleccionar un grupo de origen de registro que contiene el origen de registro para el que desee buscar. El cuadro de lista <b>Origen de registro</b> muestra todos los orígenes de registro que se han asignado al grupo de origen de registro seleccionado.
<b>Origen de registro</b>	En este cuadro de lista, puede seleccionar el origen de registro para el que desee buscar.
<b>Grupo de reglas</b>	En este cuadro de lista, puede seleccionar un grupo de reglas que contiene la regla contribuyente para la que desee buscar. El cuadro de lista <b>Regla</b> muestra todas las reglas que están asignadas al grupo de reglas seleccionado.
<b>Regla</b>	En este cuadro de lista, puede seleccionar la regla contribuyente para la que desee buscar.
<b>Tipo de delito</b>	En este cuadro de lista, puede seleccionar un tipo de delito para el que desee buscar. Para obtener más información sobre las opciones del cuadro de lista <b>Tipo de delito</b> , consulte la Tabla 2.

La tabla siguiente describe las opciones disponibles en el cuadro de lista **Tipo de delito**:

Tabla 30. Opciones de tipo de delito

Tipos de delito	Descripción
<b>Cualquiera</b>	Esta opción busca todos los orígenes de registro.
<b>IP de origen</b>	Para buscar delitos con una dirección IP de origen determinada, puede seleccionar esta opción y luego escribir la dirección IP de origen para la que desee buscar.
<b>IP de destino</b>	Para buscar delitos con una dirección IP de destino determinada, puede seleccionar esta opción y luego escribir la dirección IP de destino para la que desee buscar.

Tabla 30. Opciones de tipo de delito (continuación)

Tipos de delito	Descripción
<p><b>Nombre de suceso</b></p>	<p>Para buscar delitos con un nombre de suceso determinado, puede pulsar el icono <b>Examinar</b> para abrir el Explorador de sucesos y seleccionar el nombre de suceso (QID) para el que desee buscar.</p> <p>Puede buscar un QID determinado utilizando una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Para buscar un QID por categoría, seleccione la casilla <b>Examinar por categoría</b> y seleccione la categoría de nivel alto o bajo en los cuadros de lista.</li> <li>• Para buscar un QID por tipo de origen de registro, seleccione la casilla <b>Examinar por origen de registro</b> y seleccione un tipo de origen de registro en el cuadro de lista <b>Tipo de origen de registro</b>.</li> <li>• Para buscar un QID por tipo de origen de registro, seleccione la casilla <b>Examinar por tipo de origen de registro</b> y seleccione un tipo de origen de registro en el cuadro de lista <b>Tipo de origen de registro</b>.</li> <li>• Para buscar un QID por nombre, seleccione la casilla <b>Búsqueda de QID</b> y escriba un nombre en el campo <b>QID/Nombre</b>.</li> </ul>
<p><b>Nombre de usuario</b></p>	<p>Para buscar delitos con un nombre de usuario determinado, puede seleccionar esta opción y luego escribir el nombre de usuario para el que desee buscar.</p>
<p><b>Dirección MAC de origen</b></p>	<p>Para buscar delitos con una dirección MAC de origen determinada, puede seleccionar esta opción y luego escribir la dirección MAC de origen para la que desee buscar.</p>
<p><b>Dirección MAC de destino</b></p>	<p>Para buscar delitos con una dirección MAC de destino determinada, puede seleccionar esta opción y luego escribir la dirección MAC de destino para la que desee buscar.</p>
<p><b>Origen de registro</b></p>	<p>En el cuadro de lista <b>Grupo de origen de registro</b>, puede seleccionar el grupo de origen de registro que contiene el origen de registro para el que desee buscar. El cuadro de lista <b>Origen de registro</b> muestra todos los orígenes de registro que se han asignado al grupo de origen de registro seleccionado.</p> <p>En el cuadro de lista <b>Origen de registro</b>, seleccione el origen de registro para el que desee buscar.</p>

Tabla 30. Opciones de tipo de delito (continuación)

Tipos de delito	Descripción
<b>Nombre de host</b>	Para buscar delitos con un nombre de host determinado, puede seleccionar esta opción y luego escribir el nombre de host para el que desee buscar.
<b>Puerto de origen</b>	Para buscar delitos con un puerto de origen determinado, puede seleccionar esta opción y luego escribir el puerto de origen para el que desee buscar.
<b>Puerto de destino</b>	Para buscar delitos con un puerto de destino determinado, puede seleccionar esta opción y luego escribir el puerto de destino para el que desee buscar.
<b>IPv6 de origen</b>	<p>Este tipo de delito existe para la compatibilidad con versiones anteriores y solo aparece si se ha creado un índice IPv6 de origen en la versión 7.3.0 o versiones anteriores. Para buscar un delito más antiguo con una dirección IPv6 de origen, seleccione esta opción y escriba la dirección IPv6 de origen.</p> <p>Para buscar delitos IPv4 e IPv6 creados en la versión 7.3.1 o versiones posteriores, seleccione en su lugar la opción IP de origen.</p>
<b>IPv6 de destino</b>	<p>Este tipo de delito existe para la compatibilidad con versiones anteriores y solo aparece si se ha creado un índice IPv6 de destino en la versión 7.3.0 o versiones anteriores. Para buscar un delito más antiguo con una dirección IPv6 de destino, seleccione esta opción y escriba la dirección IPv6 de destino.</p> <p>Para buscar delitos IPv4 e IPv6 creados en la versión 7.3.1 o versiones posteriores, seleccione la opción de IP de destino en su lugar.</p>
<b>ASN de origen</b>	Para buscar delitos con un ASN de origen determinado, puede seleccionar el ASN de origen en el cuadro de lista <b>ASN de origen</b> .
<b>ASN de destino</b>	Para buscar delitos con un ASN de destino determinado, puede seleccionar el ASN de destino en el cuadro de lista <b>ASN de destino</b> .
<b>Regla</b>	Para buscar delitos que están asociados a una regla determinada, puede seleccionar el grupo de reglas donde reside la regla que desee buscar en el cuadro de lista <b>Grupo de reglas</b> . El cuadro de lista <b>Grupo de reglas</b> muestra todas las reglas que están asignadas al grupo de la reglas seleccionado. En el cuadro de lista <b>Regla</b> , seleccione la regla para la que desee buscar.



Tabla 30. Opciones de tipo de delito (continuación)

Tipos de delito	Descripción
ID de aplicación	Para buscar delitos con un ID de aplicación, puede seleccionar el ID de aplicación en el cuadro de lista <b>ID de aplicación</b> .

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
3. Elija una de las siguientes opciones:
  - Para cargar una búsqueda guardada anteriormente, vaya al Paso 4.
  - Para crear una búsqueda nueva, vaya al Paso 7.
4. Seleccione una búsqueda guardada anteriormente utilizando una de estas opciones:
  - En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desee cargar.
  - En el campo **Escriba la búsqueda guardada** o **Seleccione en la lista**, escriba el nombre de la búsqueda que desee cargar.
5. Pulse **Cargar**.
6. Opcional. Seleccione la casilla **Establecer como valor predeterminado** en el panel Editar búsqueda para establecer la búsqueda actual como búsqueda predeterminada. Si establece esta búsqueda como búsqueda predeterminada, la búsqueda se ejecutará automáticamente y mostrará resultados cada vez que acceda a la pestaña **Delitos**.
7. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
8. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
9. En el panel Origen de delito, especifique el tipo de delito y origen de delito que desee buscar:
  - a) En el cuadro de lista, seleccione el tipo de delito para el que desee buscar.
  - b) Escriba los parámetros de búsqueda. Consulte la Tabla 2.
10. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
  - a) En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
  - b) En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son Ascendente y Descendente.
11. Pulse **Buscar**.

### Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

## Buscar delitos en la página Por IP de origen

Este tema describe cómo buscar delitos en la página **Por IP de origen** de la pestaña **Delito**.

### Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página **Por IP de origen**:

Tabla 31. Opciones de búsqueda de la página Por IP de origen

Opciones	Descripción
<b>Todos los delitos</b>	Puede seleccionar esta opción para buscar todas las direcciones IP de origen sin importar el rango de tiempo.
<b>Reciente</b>	Puede seleccionar esta opción y, desde este cuadro de lista, seleccionar el rango de tiempo para el que desee buscar.
<b>Intervalo específico</b>	<p>Para especificar un intervalo para el que buscar, puede seleccionar la opción Intervalo específico y luego seleccionar una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• <b>Fecha de inicio entre:</b> seleccione esta casilla para buscar direcciones IP de origen asociadas a delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.</li> <li>• <b>Último suceso/flujo entre:</b> seleccione esta casilla para buscar direcciones IP de origen asociadas con delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.</li> </ul>
<b>Buscar</b>	El icono <b>Buscar</b> está disponible en varios paneles de la página de búsqueda. Puede pulsar <b>Buscar</b> cuando termine de configurar la búsqueda y desee ver los resultados.
<b>IP de origen</b>	En este campo, puede escribir la dirección IPv4 o IPv6 de origen o rango de CIDR para el que desee buscar.
<b>Magnitud</b>	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
<b>Riesgo de VA</b>	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
<b>Sucesos/flujos</b>	En este cuadro de lista, puede especificar un valor de recuento de sucesos o flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.

Tabla 31. Opciones de búsqueda de la página Por IP de origen (continuación)

Opciones	Descripción
<b>Excluir</b>	<p>Puede seleccionar las casillas correspondientes a los delitos que desee excluir de los resultados de búsqueda. Las opciones son:</p> <ul style="list-style-type: none"> <li>• <b>Delitos activos</b></li> <li>• <b>Delitos ocultos</b></li> <li>• <b>Delitos cerrados</b></li> <li>• <b>Delitos inactivos</b></li> <li>• <b>Delitos protegidos</b></li> </ul>

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por IP de origen**.
3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
5. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
6. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
  - a) En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
  - b) En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
7. Pulse **Buscar**.

### Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

## Buscar delitos en la página Por IP de destino

En la página **Por IP de destino** de la pestaña **Delito**, puede buscar delitos que están agrupados por la dirección IP de destino.

### Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página **Por IP de destino**:

Tabla 32. Opciones de búsqueda de la página Por IP de destino

Opciones	Descripción
<b>Todos los delitos</b>	Puede seleccionar esta opción para buscar todas las direcciones IP de destino sin importar el rango de tiempo.
<b>Reciente</b>	Puede seleccionar esta opción y, desde este cuadro de lista, seleccionar el rango de tiempo para el que desee buscar.

Tabla 32. Opciones de búsqueda de la página Por IP de destino (continuación)

Opciones	Descripción
<b>Intervalo específico</b>	<p>Para especificar un intervalo determinado para el que buscar, puede seleccionar la opción <b>Intervalo específico</b> y luego seleccionar una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Para especificar un intervalo determinado para el que buscar, puede seleccionar la opción <b>Intervalo específico</b> y luego seleccionar una de las opciones siguientes:</li> <li>• <b>Último suceso/flujo entre:</b> seleccione esta casilla para buscar direcciones IP de destino asociadas con delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar</li> </ul>
<b>Buscar</b>	El icono <b>Buscar</b> está disponible en varios paneles de la página de búsqueda. Puede pulsar <b>Buscar</b> cuando termine de configurar la búsqueda y desee ver los resultados.
<b>IP de destino</b>	Puede escribir la dirección IPv4 o IPv6 de destino o rango de CIDR para el que desee buscar.
<b>Magnitud</b>	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado.
<b>Riesgo de VA</b>	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
<b>Sucesos/flujo</b>	En este cuadro de lista puede especificar una magnitud de recuento de suceso o flujo y seleccionar que solamente se visualicen los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Por IP de destino**.
3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
5. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
6. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
  - a) En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.

- b) En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.

7. Pulse **Buscar**.

### Qué hacer a continuación

#### Guardar criterios de búsqueda en la pestaña Delito

## Buscar delitos en la página Por red

En la página **Por red** de la pestaña **Delito**, puede buscar delitos que están agrupados por la red asociada.

### Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página **Por Red**:

<i>Tabla 33. Opciones de búsqueda para buscar datos de delito en la página Por red</i>	
<b>Opción</b>	<b>Descripción</b>
<b>Red</b>	En este cuadro de lista, puede seleccionar la red para la que desee buscar.
<b>Magnitud</b>	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado.
<b>Riesgo de VA</b>	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado.
<b>Suceso/flujo</b>	En este cuadro de lista puede especificar un recuento de suceso o flujo y seleccionar que solamente se visualicen los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por red**.
3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
5. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
  - a) En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
  - b) En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
6. Pulse **Buscar**.

### Qué hacer a continuación

#### Guardar criterios de búsqueda en la pestaña Delito

## Guardar criterios de búsqueda en la pestaña Delitos

En la pestaña **Delitos**, puede guardar criterios de búsqueda configurados para reutilizarlos en búsquedas futuras. Los criterios de búsqueda guardados no caducan.

## Procedimiento

1. Procedimiento
2. Realice una búsqueda. Consulte Búsquedas de delitos.
3. Pulse **Guardar criterios**.
4. Escriba valores para los parámetros siguientes:

Opción	Descripción
Parámetro	Descripción
Nombre de búsqueda	Escriba un nombre que desee asignar a los criterios de búsqueda.
Gestionar grupos	Pulse <b>Gestionar grupos</b> para gestionar grupos de búsqueda. Consulte <a href="#">Gestionar grupos de búsqueda</a> .
Opciones de rango de tiempo:	<p>Elija una de las siguientes opciones:</p> <ul style="list-style-type: none"><li>• <b>Todos los delitos:</b> seleccione esta opción para buscar todos los delitos sin importar el rango de tiempo.</li><li>• <b>Reciente:</b> seleccione esta opción y, desde este cuadro de lista, seleccione el rango de tiempo para el que desee buscar.</li><li>• <b>Intervalo específico:</b> para especificar un intervalo determinado para el que buscar, seleccione la opción <b>Intervalo específico</b> y luego seleccione una de las opciones siguientes: Fecha de inicio entre: seleccione esta casilla para buscar delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar. Último suceso/flujo entre: seleccione esta casilla para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de marcar este recuadro de selección, utilice los cuadros de lista para seleccionar las fechas en las que desea buscar. Último suceso entre: marque este recuadro de selección para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.</li></ul>
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.

5. Pulse **Aceptar**.

## Buscar delitos indexados en función de una propiedad personalizada

Defina criterios de búsqueda para filtrar la lista de delitos y facilitar la decisión de qué delitos es necesario investigar. Puede utilizar el tipo de delito en los criterios de búsqueda para buscar todos los delitos que se basan en una propiedad personalizada. Puede filtrar los resultados de la consulta para mostrar los delitos que tienen un resultado captura de propiedad personalizada específica.

### Antes de empezar

La propiedad personalizada debe utilizarse como índice de regla. Para obtener más información, consulte ["Indexación de delitos"](#) en la página 34.

## Procedimiento

1. Pulse la pestaña **Delitos**.
2. En la lista **Buscar**, seleccione **Búsqueda nueva**.
3. En el panel **Origen de delito**, seleccione la propiedad personalizada en la lista **Tipo de delito**.  
La lista **Tipo de delito** muestra solo los campos normalizados y propiedades personalizadas que se utilizan como índices de regla. No puede utilizar **Origen de delito** para buscar en las propiedades DateTime.
4. Opcional: Para buscar delitos que tienen un valor específico en el resultado de la captura de propiedad personalizada, escriba el valor que desea buscar en el recuadro de filtro.
5. Configure otros parámetros de búsqueda para satisfacer los requisitos de la búsqueda.
6. Pulse **Buscar**.

## Resultados

Todos los delitos que cumplan los criterios de búsqueda se mostrarán en la lista de delitos. Cuando visualice el resumen del delito, la propiedad personalizada en la que ha basado la búsqueda se mostrará en el campo **Tipo de delito**. El resultado de la captura de propiedad personalizada se muestra en el campo **Valor de propiedad personalizada** del panel **Resumen de origen de delito**.

## Buscar IOCs de forma rápida con la búsqueda perezosa

---

Puede utilizar la *búsqueda perezosa* de IBM QRadar para buscar un indicador de compromiso (IOC), como por ejemplo tráfico de red de salida inusual o anomalías en la actividad de cuentas de usuario con privilegios.

### Antes de empezar

La *búsqueda perezosa* devuelve los primeros 1000 sucesos que están relacionados con el criterio de búsqueda. Por ejemplo, si necesita buscar un MD5 determinado como parte de una investigación de irrupción de programa malicioso, no es necesario revisar todos los sucesos relacionados. Realice una *búsqueda perezosa* para devolver rápidamente un conjunto de resultados limitado.

Para aprovechar la *búsqueda perezosa*, debe tener el perfil de seguridad Admin o un perfil de seguridad de no administrador que esté configurado de la siguiente manera:

- Prioridad de permiso establecida en **Sin restricciones**.
- Acceso a todas las redes y orígenes de registro.

La búsqueda perezosa no puede ser utilizada por usuarios con perfiles de seguridad de no administrador en redes en las que haya dominios configurados.

## Procedimiento

1. Para realizar una búsqueda perezosa para filtros rápidos, siga estos pasos:
  - a) En la pestaña **Actividad de registro**, en el campo **Filtro rápido**, especifique un valor.
  - b) En la lista **Ver**, seleccione un rango de tiempo.
2. Para realizar una búsqueda perezosa para búsquedas básicas, siga estos pasos:
  - a) En la pestaña **Actividad de registro**, pulse **Buscar > Nueva búsqueda**.
  - b) Seleccione un rango de tiempo **Reciente** o establezca un **Intervalo específico**.
  - c) Asegúrese de que el valor del campo **Ordenar por** esté establecido en **Hora de inicio** y el valor del campo **Límite de resultados** sea 1000 como máximo. Las columnas agregadas no deben incluirse en la búsqueda.
  - d) Especifique un valor para el parámetro **Filtro rápido** y pulse **Añadir filtro**.
3. Para inhabilitar completamente la búsqueda perezosa, siga estos pasos:

- a) Pulse **Valores del sistema** en la pestaña **Admin**.
- b) En la ventana **Valores del sistema**, elimine los valores del campo **Límite de búsqueda predeterminado**.

## Supresión de criterios de búsqueda

---

Puede suprimir criterios de búsqueda.

### Acerca de esta tarea

Al suprimir una búsqueda guardada, es posible que los objetos que están asociados con la búsqueda guardada no funcionen. Los informes y las reglas de detección de anomalías son objetos de QRadar que utilizan criterios de búsqueda guardada. Después de suprimir una búsqueda guardada, edite los objetos asociados para asegurarse de que siguen funcionando.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda** o **Editar búsqueda**.
3. En el panel Búsquedas guardadas, seleccione una búsqueda guardada en el recuadro de lista **Búsquedas guardadas disponibles**.
4. Pulse **Suprimir**.
  - Si los criterios de búsqueda guardada no están asociado con otros objetos de QRadar, se visualiza una ventana de confirmación.
  - Si los criterios de búsqueda guardada están asociado con otros objetos, se visualiza la ventana **Suprimir búsqueda guardada**. La ventana lista objetos que están asociados con la búsqueda guardada que desea suprimir. Tome nota de los objetos asociados.
5. Pulse **Aceptar**.
6. Elija una de las siguientes opciones:
  - Pulse **Aceptar** para continuar.
  - Pulse **Cancelar** para cerrar la ventana **Suprimir búsqueda guardada**.

### Qué hacer a continuación

Si los criterios de búsqueda guardada estaban asociados con otros objetos de QRadar, acceda a los objetos asociados que ha anotado y edite los objetos para eliminar o sustituir la asociación con la búsqueda guardada suprimida.

## Utilización de una sub-búsqueda para refinar los resultados de búsqueda

---

Puede utilizar una sub-búsqueda para buscar en un conjunto de resultados de búsqueda completada. La sub-búsqueda se utiliza para refinar los resultados de búsqueda, sin buscar de nuevo en la base de datos.

### Antes de empezar

Al definir una búsqueda que desea utilizar como base para realizar una sub-búsqueda, asegúrese de que la opción Tiempo real (modalidad continua) está inhabilitada y la búsqueda no se ha agrupado.

### Acerca de esta tarea

Esta característica no está disponible para búsquedas agrupados, búsquedas en curso o en modalidad continua.



## Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. Realice una búsqueda.
3. Cuando la búsqueda se haya completado, añada otro filtro:
  - a) Pulse **Añadir filtro**.
  - b) En el primer recuadro de lista, seleccione un parámetro que desee buscar.
  - c) En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda. La lista de modificadores que están disponibles depende del atributo que se ha seleccionado en la primera lista.
  - d) En el campo de entrada, escriba información específica que esté relacionada con la búsqueda.
  - e) Pulse **Añadir filtro**.

## Resultados

El panel Filtros originales especifica los filtros originales que se aplican a la búsqueda de base. El panel Filtros actuales especifica los filtros que se aplican a la sub-búsqueda. Puede borrar filtros de sub-búsqueda sin reiniciar la búsqueda de base. Pulse el enlace **Borrar filtro** junto al filtro que desea borrar. Si borra un filtro en el panel Filtros originales, se reinicia la búsqueda de base.

Si suprime los criterios de búsqueda de base para los criterios de sub-búsqueda guardados, seguirá teniendo acceso a los criterios de sub-búsqueda guardados. Si añade un filtro, la sub-búsqueda busca en la base de datos entera porque la función de búsqueda ya no basa la búsqueda en un conjunto de datos buscado previamente.

### Qué hacer a continuación

[Guardar criterios de búsqueda](#)

## Gestión de resultados de búsqueda

---

Puede iniciar varias búsquedas y, a continuación, ir a otras pestañas para realizar otras tareas mientras las búsquedas se completan en segundo plano.

Puede configurar una búsqueda para que, al finalizarse, envíe una notificación por correo electrónico.

En cualquier momento mientras una búsqueda está en curso, puede volver a la pestaña **Actividad de registro** o la pestaña **Actividad de red** para ver resultados de búsqueda parciales o completos.

## Cancelación de una búsqueda

Mientras una búsqueda está en cola o en curso, puede cancelar la búsqueda en la página **Gestionar resultados de búsqueda**.

### Acerca de esta tarea

Si la búsqueda está en curso cuando se cancela, se mantienen los resultados que se han acumulado hasta que la cancelación.

## Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.

3. Seleccione el resultado de búsqueda en cola o en curso que desea cancelar.
4. Pulse **Cancelar**.
5. Pulse **Sí**.

## Supresión de una búsqueda

Si un resultado de búsqueda ya no es necesario, puede suprimir el resultado de búsqueda de la página **Gestionar resultados de búsqueda**.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Seleccione el resultado de búsqueda que desea suprimir.
4. Pulse **Suprimir**.
5. Pulse **Sí**.

## Gestión de grupos de búsqueda

Utilizando la ventana **Grupos de búsqueda**, puede crear y gestionar grupos de búsqueda de sucesos, flujos y delitos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en las pestañas **Actividad de registro**, **Actividad de red** y **Delitos** y en el asistente de informes.

## Visualización de grupos de búsqueda

Está disponible un conjunto predeterminado de grupos y subgrupos.

### Acerca de esta tarea

Puede ver grupos de búsqueda en las ventanas **Grupos de búsqueda de sucesos**, **Grupos de búsqueda de flujos** o **Grupos de búsqueda de delitos**.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

Las ventanas **Grupos de búsqueda de sucesos**, **Grupos de búsqueda de flujos** y **Grupos de búsqueda de delitos** muestran los parámetros siguientes para cada grupo.

<i>Tabla 34. Parámetros de ventanas de grupos de búsqueda</i>	
<b>Parámetro</b>	<b>Descripción</b>
<b>Nombre</b>	Especifica el nombre del grupo de búsqueda.
<b>Usuario</b>	Especifica el nombre del usuario que ha creado el grupo de búsqueda.
<b>Descripción</b>	Especifica la descripción del grupo de búsqueda.
<b>Fecha de modificación</b>	Especifica la fecha en que se ha modificado el grupo de búsqueda.

Las barras de herramienta de las ventanas **Grupos de búsqueda de sucesos**, **Grupos de búsqueda de flujos** y **Grupos de búsqueda de delitos** proporcionan las funciones siguientes.

Tabla 35. Funciones de barra de herramientas de ventanas de grupos de búsqueda

Función	Descripción
<b>Grupo nuevo</b>	Para crear un nuevo grupo de búsqueda, puede pulsar <b>Grupo nuevo</b> . Consulte <a href="#">Creación de un grupo de búsqueda nuevo</a> .
<b>Editar</b>	Para editar un grupo de búsqueda existente, puede pulsar en <b>Editar</b> . Consulte <a href="#">Edición de un grupo de búsqueda</a> .
<b>Copiar</b>	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en <b>Copiar</b> . Consulte <a href="#">Copia de una búsqueda guardada en otro grupo</a> .
<b>Eliminar</b>	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse <b>Eliminar</b> . Consulte <a href="#">Eliminación de un grupo o una búsqueda guardada de un grupo</a> .

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. **Seleccionar búsqueda > Editar búsqueda.**
3. Pulse **Gestionar grupos**.
4. Vea los grupos de búsqueda.

### Creación de un grupo de búsqueda nuevo

Puede crear un grupo de búsqueda nuevo.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. **Seleccionar búsqueda Editar búsqueda.**
3. Pulse **Gestionar grupos**.
4. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
5. Pulse **Grupo nuevo**.
6. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
7. Opcional. En el campo **Descripción**, escriba una descripción.
8. Pulse **Aceptar**.

### Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.

- Pulse la pestaña **Actividad de red**.
2. Seleccione **Buscar > Editar búsqueda**.
  3. Pulse **Gestionar grupos**.
  4. Seleccione el grupo que desea editar.
  5. Pulse **Editar**.
  6. Edite los parámetros:
    - Escriba un nombre nuevo en el campo **Nombre**.
    - Escriba una nueva descripción en el campo **Descripción**.
  7. Pulse **Aceptar**.

## Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en uno o varios grupos.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. Seleccione **Buscar > Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione la búsqueda guardada que desea copiar.
5. Pulse **Copiar**.
6. En la ventana **Grupos de elementos**, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
7. Pulse **Asignar grupos**.

## Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

### Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar los grupos siguientes del sistema:

- Grupos de búsqueda de sucesos
- Grupos de búsqueda de flujos
- Grupos de búsqueda de delitos
- Otros

### Procedimiento

1. Elija una de las siguientes opciones:
  - Pulse la pestaña **Actividad de registro**.
  - Pulse la pestaña **Actividad de red**.
2. Seleccione **Buscar > Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Elija una de las siguientes opciones:
  - Seleccione la búsqueda guardada que desea eliminar del grupo.

- Seleccione el grupo que desea eliminar.
5. Pulse **Eliminar**.
  6. Pulse **Aceptar**.

## Ejemplo de búsqueda: Informes de empleados diarios

---

El ejemplo siguiente describe cómo utilizar una consulta de búsqueda avanzada para consultar información de empleado específica.

Para la gestión de identidades, puede optar por generar un informe diario de la actividad de usuario en QRadar. El informe debe incluir información sobre el empleado, como por ejemplo el nombre de usuario, el número de serie, el jefe y la actividad.

Un empleado puede tener varios nombres de usuario en QRadar. Puede utilizar la API RESTful para construir una correlación de referencia que devuelve todos los nombres de usuario del nombre del empleado `Global_User`. Para el número de serie y el nombre del gestor, puede crear otro conjunto de datos de referencia y añadirlo a la correlación de referencia.

Las actividades del empleado pueden ir desde anomalías de inicio de sesión a tareas de QRadar, como por ejemplo la supresión de objetos. Estos sucesos los registra QRadar. Especificando la frecuencia de los sucesos en la correlación, puede calibrar las actividades sospechosas. Puede agrupar los datos por nombre de empleado y nombre de suceso y después ordenarlos por la frecuencia más elevada dentro de un periodo de 24 horas.

Para ver este informe diario, puede iniciar la sesión en QRadar Console. En el recuadro de texto Búsqueda avanzada de la pestaña **Actividad de registro**, puede teclear la consulta de búsqueda siguiente:

```
select REFERENCEMAP('GlobalID_Mapping', username) as Global_User, QIDNAME(qid)
as 'Nombre de suceso', count(*) as 'Recuento de sucesos', FIRST(username) as
UserId, REFERENCETABLE('employee_data', 'SerialNum', Global_user) as 'Serial
Number', REFERENCETABLE('employee_data', 'Manager', Global_User) as Manager from
events where (Global_User IS NOT NULL) GROUP BY Global_user, 'Nombre de suceso'
ORDER BY 'Recuento de sucesos' DESC last 1 DAYS
```



---

## Capítulo 13. Propiedades de suceso y de flujo personalizadas

IBM QRadar normaliza la información estándar que analiza el DSM, como nombres de usuarios, direcciones IP y puertos.

Algunos orígenes de sucesos envían información exclusiva que no está normalizada. Puede utilizar propiedades personalizadas para extraer esos datos del suceso o de la carga útil del flujo y después utilizar los datos no normalizados en las reglas personalizadas, las búsquedas y los informes.

El tipo de propiedad personalizada que cree dependerá del método que desee utilizar para definir los datos no normalizados en la carga útil.

### Propiedades basadas en extracción

Cree una propiedad basada en extracción cuando desee utilizar un valor de propiedad o una expresión JSON para analizar los valores de propiedad procedentes del suceso o de las cargas útiles de flujo.

Por ejemplo, supongamos que tiene un informe que muestra todos los usuarios que han cambiado los permisos de otro usuario en un servidor de Oracle. El informe utiliza datos normalizados para mostrar la lista de usuarios que han realizado los cambios de permiso y el número de cambios que han realizado. La cuenta de usuario que se ha modificado no está normalizada y no se puede mostrar en el informe. Puede crear una propiedad personalizada basada en expresión regular para extraer esta información de los registros y, a continuación, utilizar la propiedad en las búsquedas y los informes.

Cuando se analiza el suceso o el flujo, se prueba el patrón de expresión con la carga útil hasta que el patrón coincide. El primer patrón que coincida con el suceso o la carga útil del flujo determina los datos que se extraerán.

Cuando defina patrones de expresión de regular personalizados, siga las reglas de expresión regular tal como están definidas por el lenguaje de programación Java. Para obtener más información sobre las reglas de expresiones regulares, vea tutoriales sobre las expresiones regulares en Internet.

### Propiedades basadas en cálculo

Cree una propiedad basada en cálculo cuando desee realizar cálculos en los sucesos numéricos existentes o las propiedades de flujo. Por ejemplo, puede crear una propiedad basada en cálculo que divida una propiedad numérica por otra propiedad numérica para mostrar un valor de porcentaje.

### Propiedades basadas en AQL

Cree una propiedad basada en AQL cuando desee combinar varias propiedades de extracción y basadas en cálculos en una sola. Por ejemplo, puede utilizar propiedades personalizadas basadas en AQL para combinar URL basadas en extracción, nombres de virus o nombres de usuario secundarios y combinarlos en una única propiedad.

```
CONCAT( 'Src=', sourceip, ' | ', 'User=', username, ' | ', 'Domain=',  
DOMAINNAME(domainid) )
```

**Nota:** La expresión AQL puede incluir funciones AQL.

No admite expresiones que utilicen SELECT, FROM o nombres de base de datos.

No puede utilizar funciones agregadas, como SUM o GROUP ni otras propiedades personalizadas basadas en AQL.

## Creación de una propiedad personalizada

---

Cree una propiedad personalizada para extraer datos que IBM QRadar no suele mostrar procedentes del suceso o de las cargas útiles del flujo. Es necesario activar las propiedades personalizadas y las propiedades personalizadas basadas en extracción deben analizarse para poder utilizarlas e las reglas, las búsquedas, los informes y para indexar los delitos.

### Antes de empezar

QRadar incluye varias propiedades de suceso personalizadas existentes que no están habilitadas ni analizadas de forma predeterminada. Pida a su administrador que revise la propiedad de suceso personalizada que desea crear y asegúrese de que no exista.

Para crear propiedades de suceso personalizadas, debe tener permiso para las **Propiedades de suceso definidas por el usuario**. Para crear propiedades de flujo personalizadas, debe tener permiso para las **Propiedades de suceso definidas por el usuario**.

Los usuarios con capacidad de administración pueden crear propiedades de suceso y de flujo personalizadas seleccionando **Propiedades de suceso personalizadas** o **Propiedades de flujo personalizadas** en la pestaña **Admin**.

### Acerca de esta tarea

Aunque haya varias propiedades personalizadas predeterminadas que tengan el mismo nombre y el mismo origen de registro, pueden tener diferentes expresiones regulares, nombres de suceso o categorías. Por ejemplo, hay varias propiedades personalizadas para el registro de sucesos de seguridad de Microsoft Windows denominadas **AccountName**, pero cada una está definida por una expresión regular única.

### Procedimiento

1. Haga clic en la pestaña **Actividad de registro** o **Actividad de red**.
2. Si está viendo los sucesos o flujos en modalidad continua, pulse el icono **Pausa** para poner en pausa la modalidad continua.
3. Haga doble clic en el suceso o el flujo que contenga los datos que desea extraer y, a continuación, en **Extraer propiedad**.
4. En el panel **Selección de tipo de propiedad**, seleccione el tipo de propiedad personalizada que desee crear.
5. Configure los parámetros de propiedad personalizada.

Haga clic en el icono de ayuda ( ? ) para ver información sobre los parámetros de propiedades personalizadas.

6. Si está creando una propiedad personalizada basada en extracción que se va a utilizar en las reglas, los índices de búsqueda o los perfiles de reenvío, asegúrese de que el recuadro de selección **Analizar reglas, informes y búsquedas por adelantado** esté seleccionado.
7. Pulse **Probar** para probar la expresión con la carga útil.
8. Pulse **Guardar**.

### Qué hacer a continuación

[“Modificación o supresión de una propiedad personalizada” en la página 175](#)

### Conceptos relacionados

Ejemplos de series de búsqueda de AQL

Utilice Ariel Query Language (AQL) para recuperar campos determinados de los sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.



## Modificación o supresión de una propiedad personalizada

---

Edite una propiedad cuando desee cambiar los parámetros de propiedad, como la expresión regular o el tipo de origen de registro.

### Acerca de esta tarea

Puede buscar una propiedad concreta con el campo **Propiedades de búsqueda**. La búsqueda no distingue entre mayúsculas y minúsculas.

Copie una propiedad personalizada cuando desee modificarla y después guárdela con otro nombre.

Para eliminar una propiedad, debe suprimir primero todas sus dependencias. El hecho de eliminar una propiedad personalizada no elimina los campos de propiedad indexados de la base de datos de Ariel.

### Procedimiento

1. Elija una de las siguientes opciones:
  - Para editar o suprimir una propiedad de suceso personalizada, haga clic en la pestaña **Actividad de registro**.
  - Para editar o suprimir una propiedad de flujo personalizada, haga clic en la pestaña **Actividad de red**.
2. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
3. Pulse **Gestionar propiedades personalizadas**.
4. Seleccione la propiedad en la lista y haga clic en **Editar**, **Copiar** o **Eliminar**.
5. Realice los cambios necesarios en la propiedad y haga clic en **Guardar**.

## Definición de propiedades personalizadas mediante expresiones de propiedades personalizadas

---

Defina una propiedad personalizada para una carga útil de suceso utilizando una expresión de propiedad personalizada. Puesto que el análisis de JSON comienza cuando se detecta un objeto JSON válido, no es necesario que el suceso completo esté en formato JSON. De forma similar, el análisis de LEEF y CEF solo se inicia cuando se detecta un mensaje LEEF/CEF válido dentro del suceso. El análisis de Regex se ejecuta para toda la carga útil.

### Acerca de esta tarea

IBM QRadar soporta los siguientes tipos de expresión de propiedad personalizada:

- Expresión regular
- JSON
- LEEF
- CEF
- Par nombre-valor
- Lista genérica
- XML

Puede utilizar expresiones diferentes para capturar diversas propiedades personalizadas para el mismo suceso. También puede utilizar una combinación de tipos de expresión para capturar la misma propiedad personalizada si esa propiedad se puede capturar a partir de varios formatos de suceso.

## Procedimiento

1. Inicie sesión en QRadar y pulse la pestaña **Admin**.
2. En la sección **Orígenes de datos**, pulse **Propiedades de sucesos personalizadas** y, a continuación, haga clic en **Añadir**.
3. En la sección **Selección de tipo de propiedad**, haga clic en **Basado en las extracciones**.
4. En **Campo de prueba**, especifique la carga útil de suceso que desea utilizar para probar la propiedad personalizada.
5. En la sección **Definición de propiedad**, haga lo siguiente:
  - a) Si va a añadir una expresión a una propiedad existente, seleccione **Propiedad existente** y seleccione una propiedad en la lista.
  - b) Si va a definir una propiedad nueva, seleccione **Nueva propiedad** y especifique el nombre de la propiedad.
  - c) Para utilizar la propiedad para las reglas, los informes y las búsquedas, marque el recuadro de selección **Analizar por adelantado para reglas, informes y búsquedas**.  
Debe marcar este recuadro de selección para utilizar la propiedad para las reglas y los índices. Cuando se marca el recuadro de selección, aumenta la eficiencia de los informes y las búsquedas, pero no es necesario seleccionarlo para utilizar la propiedad en los informes y las búsquedas. Si marca el recuadro de selección, las propiedades se analizarán cuando se reciba inicialmente el suceso y antes de almacenarse. Como resultado de ello, las cargas se colocan en el servicio de recopilación de sucesos.
  - d) Seleccione un **Tipo de campo** para la propiedad.  
Si elige IP como tipo para la propiedad personalizada, QRadar solo da soporte a IPv4.
  - e) Opcional: Especifique una descripción para la propiedad.
6. En la sección **Definición de expresión de propiedad**, haga lo siguiente:
  - a) Mantenga seleccionado el recuadro de selección **Habilitado**; de lo contrario, elimine la marca del recuadro de selección para inhabilitar la propiedad.
  - b) En la lista **Tipo de origen de registro**, seleccione un tipo de origen de registro para la propiedad.
  - c) Si la expresión solo se evalúa en los sucesos de un origen de registro específico, seleccione el origen de registro en la lista **Origen de registro**. Si desea que se evalúe en todos los orígenes de registro, no lo seleccione.
  - d) Si la expresión solo se evalúa con respecto a sucesos que tienen un nombre de suceso o QID específico, haga clic en **Nombre de suceso** y busque un QID con el que asociar la expresión.
  - e) Si la expresión se evalúa respecto a cualquier evento con una categoría específica de nivel inferior, seleccione **Categoría** y haga clic en **Categoría de alto nivel** y después en **Categoría de nivel bajo** para el suceso.  
**Consejo:** Si la expresión se evalúa para todos los sucesos del tipo de origen de registro y el origen de registro seleccionados, asegúrese de establecer la **Categoría de nivel bajo** y la **Categoría de alto nivel** en **Cualquiera**.
  - f) En el campo **Extraer utilizando**, seleccione el método de extracción que desea utilizar con la propiedad.

Método de extracción	Formato de expresión válido	Ejemplo
Expresión regular	Introduzca la expresión regular y el número del grupo de captura.	

Tabla 36. Métodos de extracción de propiedades (continuación)

Método de extracción	Formato de expresión válido	Ejemplo
<p>Vía de acceso clave JSON</p>	<p>Una expresión JSON válida tiene el formato:</p> <pre data-bbox="613 331 985 394">/"&lt;nombre de campo de nivel superior&gt;"</pre> <p>Para un suceso en un formato JSON anidado, una expresión JSON válida tiene el formato:</p> <pre data-bbox="613 531 985 657">/"&lt;name of top-level field&gt;"/"&lt;nombre de un campo de subnivel_1&gt;".../"&lt;nombre de campo de subnivel_n&gt;"</pre> <p>Para extraer el campo 'user', escriba /"user" en el campo <b>JsonKeypath</b>.</p> <p>Para extraer solo el valor 'last_name' del subobjeto 'user', escriba esta expresión:</p> <pre data-bbox="613 909 985 951">/"user"/"last_name"</pre>	<p>El ejemplo siguiente es un caso simple de un suceso para un registro JSON sin formato:</p> <pre data-bbox="1031 363 1468 426">{ "action": "login", "user": "Firstname Lastname" }</pre> <p>El ejemplo siguiente es un caso complejo de un suceso para un registro JSON con objetos anidados:</p> <pre data-bbox="1031 573 1468 636">{ "action": "login", "user": { "first_name": "Firstname", "last_name": "Lastname" } }</pre>

Tabla 36. Métodos de extracción de propiedades (continuación)

Método de extracción	Formato de expresión válido	Ejemplo
<p>Clave LEEF</p>	<p>Las expresiones LEEF válidas tienen la forma de una sola referencia de clave o de una referencia de campo de cabecera LEEF especial.</p> <p>Para extraer la propiedad 'usrName', escriba usrName en el campo <b>Clave LEEF</b>.</p> <p>Las posibles claves que se pueden extraer en estos ejemplos son las siguientes:</p> <ul style="list-style-type: none"> <li>• devTimeFormat</li> <li>• devTime</li> <li>• usrName</li> <li>• name</li> <li>• authType</li> <li>• src</li> </ul> <p>Para extraer una propiedad de clave de cabecera, escriba la clave con el formato siguiente en el campo <b>Clave LEEF</b>:</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$eventid\$</pre> <p>Los valores de cabecera LEEF se pueden extraer utilizando las expresiones siguientes:</p> <ul style="list-style-type: none"> <li>• \$leefversion\$</li> <li>• \$vendor\$</li> <li>• \$product\$</li> <li>• \$version\$</li> <li>• \$eventid\$</li> </ul>	<p>El ejemplo siguiente es un caso simple de un suceso con formato LEEF V1.0:</p> <pre style="background-color: #f0f0f0; padding: 5px;">LEEF:1.0 ABC Company  SystemDefender 1.13  console_login devTimeFormat=yyyy- MM-dd'T'HH:mm:ss.SSSZ devTime=2017-10-18T11:26:03.060+0 200    usrName=flastname name=Firstname Lastname authType=interactivePassword src=192.168.0.1</pre> <p>El ejemplo siguiente es un caso simple de un suceso con formato LEEF V2.0 con el carácter separador de caret (^), y contiene las mismas claves que el ejemplo LEEF V1.0:</p> <pre style="background-color: #f0f0f0; padding: 5px;">LEEF:2.0 ABC Company  SystemDefender 1.13  console_login ^  devTimeFormat=yyyy- MMdd'T'HH:mm:ss.SSSZ^ devTime=2017-10-18T11:26:03.060+0 200^usrName=flastname^name=Firstn ame Lastname ^authType=interactivePassword^src =192.168.0.1</pre>

Tabla 36. Métodos de extracción de propiedades (continuación)

Método de extracción	Formato de expresión válido	Ejemplo
<p>Clave CEF</p>	<p>Las expresiones CEF válidas tienen la forma de una sola referencia de clave o de una referencia de campo de cabecera CEF especial.</p> <p>Para extraer la propiedad 'cs1', escriba cs1 en el campo <b>Clave CEF</b>.</p> <p>Las claves posibles que se pueden extraer en el ejemplo son las siguientes:</p> <ul style="list-style-type: none"> <li>• start</li> <li>• duser</li> <li>• cs1</li> <li>• cs1Label</li> <li>• cs2</li> <li>• cs2Label</li> <li>• src</li> </ul> <p>Para extraer una propiedad de clave de cabecera, escriba la clave con el formato siguiente en el campo <b>Clave CEF</b>:</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$id\$</pre> <p>Los valores de cabecera CEF se pueden extraer utilizando las expresiones siguientes:</p> <ul style="list-style-type: none"> <li>• \$cefversion\$</li> <li>• \$vendor\$</li> <li>• \$product\$</li> <li>• \$version\$</li> <li>• \$id\$</li> <li>• \$name\$</li> <li>• \$severity\$</li> </ul>	<p>El ejemplo siguiente muestra un suceso en formato CEF:</p> <pre style="background-color: #f0f0f0; padding: 5px;">CEF:0 ABC Company SystemDefender 1.13 console_login Console Login 1 start=Oct 18 2017 11:26:03 duser=flastname cs1=Firstname Lastname cs1Label=Person Name cs2=interactivePassword cs2Label=authType src=192.168.0.1</pre>
<p>Clave de par nombre-valor</p>	<p>Las expresiones de par nombre valor válidas tienen el formato de una referencia de clave única.</p>	<p>El ejemplo siguiente muestra un suceso cuyo formato es par nombre valor:</p> <pre style="background-color: #f0f0f0; padding: 5px;">Company=ABC Company;Product=SystemDefender; Version=1.13;EventID=console_login; Username=jsmith;Name=John Smith;authType=interactivePassword;</pre>

Tabla 36. Métodos de extracción de propiedades (continuación)		
Método de extracción	Formato de expresión válido	Ejemplo
Vía de acceso clave de lista genérica	Las expresiones de lista genérica tienen el formato de una notación \$<número>. Por ejemplo, \$0 representa la primera propiedad de la lista, \$1 es la segunda propiedad, etc.	El ejemplo siguiente muestra un suceso cuyo formato es lista genérica.  <pre>ABC Company;1.13;console_login;jsmith ; John Smith;interactivePassword;</pre>
Clave XML	Las expresiones XML válidas tienen el formato de una referencia de clave única.  Especifique la vía de acceso del campo XML que desea utilizar para rellenar el valor de la propiedad. Una vía de acceso de clave XML debe empezar por una barra inclinada (/) para indicar la raíz del objeto XML e ir seguida de uno o varios nombres de campo XML entre comillas dobles.	El ejemplo siguiente muestra un suceso en formato XML:  <pre>&lt;EPOEvent&gt;&lt;MachineInfo&gt; &lt;MachineName&gt;NEPTUNE&lt;/ MachineName&gt; &lt;MachineName&gt;VALUE23&lt;/ MachineName&gt;&lt;AgentGUID&gt; 9B-B5-A6-A8-37-B3&lt;/ AgentGUID&gt;&lt;IPAddress someattrib="someattribvalue"&gt; 192.0.2.0&lt;/IPAddress&gt; &lt;OSName&gt;Windows 7&lt;/ OSName&gt;&lt;UserName&gt;I am a test user&lt;/UserName&gt;&lt;/ MachineInfo&gt;&lt;/EPOEvent&gt;</pre>

- g) Si ha elegido Numérico en **Tipo de campo** en la sección **Definición de propiedad**, seleccione un formato de número en el campo **Formato de número extraído** en la sección **Formato** para definir separadores de grupos digitales para el entorno local de a propiedad personalizada.
- h) Si ha elegido Fecha/Hora en **Tipo de campo** en la sección **Definición de propiedad**, seleccione un formato de número en los campos **Formato de fecha/hora extraído** y **Entorno local** en la sección **Formato** para definir separadores de grupos digitales para el entorno local de a propiedad personalizada.
- i) Pulse **Probar** para probar la definición de expresión de propiedad.

7. Pulse **Guardar**.

## Caso práctico: Crear un informe que utiliza datos de suceso que no están normalizados

Puede utilizar una propiedad personalizada para extraer datos que no están normalizados procedentes de una carga útil y utilícelos para generar un informe. Por ejemplo, puede generar un informe que se base en la información de interfaz que se encuentra en los mensajes de denegación de cortafuegos de Cisco ASA.

En este ejemplo, usaremos los siguientes sucesos de cortafuegos de Cisco ASA para demostrar cómo extraer el valor de interfaz de la carga útil de sucesos y generar después un informe que utilice esos datos.

```
<162>Sep 02 2014 11:49:41: %ASA-2-106001: Inbound TCP connection denied
from 10.10.10.128/58826 to 10.11.11.11/9100 flags SYN on interface External
<162>Sep 02 2014 11:49:40: %ASA-2-106001: Inbound TCP connection denied
from 10.10.10.128/58826 to 10.11.11.11/9100 flags SYN on interface Loopback
<162>Sep 02 2014 11:49:17: %ASA-2-106001: Inbound TCP connection
denied from 10.10.10.128/58821 to 10.11.11.11/9100 flags SYN on interface Internal
```

### 1. Crear la propiedad personalizada.

En los sucesos de ejemplo indicado más arriba, puede ver que la carga útil de suceso incluye el término `interface` seguido del valor que desea extraer. Para capturar la información de interfaz de

los sucesos indicados más arriba, cree una propiedad personalizada basada en extracción y configúrela para que utilice la expresión regular `interface\s(.*)\b`.

Para asegurarse de que la nueva propiedad personalizada esté disponible para utilizarla en una búsqueda, seleccione la casilla de verificación **Analizar por adelantado para reglas, informes y búsquedas** y habilite la propiedad personalizada.

2. Cree una búsqueda y en el campo **Agrupar por**, seleccione la nueva propiedad de suceso personalizada.

Para asegurarse de que los resultados de la búsqueda solo incluirán sucesos de Cisco ASA, añada el origen de registro y una opción de filtro en los parámetros de búsqueda. Guarde los criterios de búsqueda para utilizarlos en un informe. Asigne la búsqueda guardada a un grupo para que le resulte más fácil encontrarla más tarde.

3. Cree un informe y configure el contenido del gráfico para que utilice la nueva búsqueda guardada.

Si no se ha configurado el informe para ejecutarse después de guardarlo, puede ejecutarlo de forma inmediata seleccionando **AccionesEjecutar informe**.





---

## Capítulo 14. Reglas

Las reglas, a veces llamadas reglas de correlación, se aplican a los sucesos, flujos o delitos para buscar o detectar anomalías. Si se cumplen todas las condiciones de una prueba, la regla genera una respuesta.

### ¿Qué son las reglas?

Las reglas personalizadas realizan pruebas sobre sucesos, flujos y delitos para detectar actividad inusual en la red. Puede crear reglas nuevas utilizando combinaciones AND y OR de las pruebas de regla existentes. Las reglas de detección de anomalías realizan pruebas sobre los resultados de búsquedas guardadas de flujos o de sucesos para detectar patrones de tráfico inusuales en la red. Las reglas de detección de anomalías requieren una búsqueda guardada agrupada alrededor de un parámetro común.

### ¿Qué son los componentes básicos?

Un componente básico es una recopilación de pruebas que no dan como resultado una respuesta o una acción.

Un componente básico agrupa pruebas utilizadas habitualmente para construir una lógica compleja, de modo que se pueda reutilizar en las reglas. Con frecuencia, un componente básico prueba direcciones IP, nombres de usuario privilegiados o recopilaciones de nombres de suceso. Por ejemplo, un componente básico puede incluir las direcciones IP de todos los servidores DNS. Posteriormente, las reglas pueden utilizar este componente básico.

QRadar contiene reglas predeterminadas, y también puede descargar más reglas desde [IBM Security App Exchange](#) para crear nuevas reglas.

### ¿Cómo funcionan las reglas?

Los recopiladores de sucesos de QRadar recopilan sucesos de orígenes locales y remotos, normalizan estos sucesos y los clasifican en categorías de bajo y alto nivel. Para los flujos, los QRadar QFlow Collectors leen paquetes desde la conexión o reciben flujos de otros dispositivos y luego convierten los datos de red en registros de flujo. Cada Procesador de sucesos procesa sucesos o datos de flujo de los recopiladores de sucesos de QRadar. Los Procesadores de flujos examinan y correlacionan la información para indicar cambios de comportamiento o violaciones de políticas. El motor de reglas personalizadas (CRE) procesa sucesos y los compara con las reglas definidas para buscar anomalías. Cuando se cumple una condición de regla, el Procesador de sucesos genera una acción que se define en la respuesta de regla. El CRE realiza un seguimiento de los sistemas que están involucrados en incidentes, aporta sucesos a los delitos y genera notificaciones.

### ¿Cómo se crea un delito a partir de una regla?

QRadar crea un delito cuando los sucesos, flujos o ambos cumplen los criterios de prueba que se especifica en las reglas.

QRadar analiza la información siguiente:

- Sucesos y flujos entrantes
- Información de activos
- Vulnerabilidades conocidas

La regla que ha creado el delito determina el tipo de delito.

El magistrado prioriza los delitos y asigna el valor de magnitud en función de varios factores, que incluyen el número de sucesos, la gravedad, la relevancia y la credibilidad.

**Nota:** Los bloques de construcción se prueban antes de probar las reglas.

Por ejemplo, tiene un bloque de construcción definido para desencadenar un delito en sucesos de alta magnitud. La actividad de registro puede mostrar que hay sucesos de alta magnitud, pero no se ha

desencadenado ningún suceso. Esto puede ocurrir porque cuando se probó el bloque de construcción, la magnitud del suceso no era alta. La magnitud del suceso no aumentó hasta que se probaron las reglas.

Una solución es establecer una regla para buscar la diferencia en Gravedad, Credibilidad y Pertinencia en lugar de utilizar un bloque de construcción.

## Reglas personalizadas

---

IBM QRadar incluye reglas que detectan una amplia gama de actividades, tales como denegaciones de cortafuegos excesivas, múltiples intentos fallidos de inicio de sesión y una posible actividad de red de robots. También puede crear sus propias reglas para detectar actividad inusual.

### ¿Qué son las reglas personalizadas?

Personalice las reglas predeterminadas para detectar actividad inusual en la red.

### Tipos de reglas

Cada uno de los tipos de regla de suceso, flujo, comunes y de delito se prueba contra los datos entrantes de diferentes orígenes en tiempo real. Hay varios tipos de pruebas de regla. Algunas comprueban propiedades simples del conjunto de datos. Otras pruebas de regla son más complicadas. Rastreadores múltiples secuencias de suceso, flujo y delito durante un periodo de tiempo y utilizan un "contador", formado por uno o varios parámetros, antes de que se desencadene una respuesta de regla.

#### Reglas de suceso

Realizan pruebas en datos de origen de registro entrantes que el Procesador de sucesos de QRadar procesa en tiempo real. Se crea una regla de suceso para detectar un suceso individual o secuencias de sucesos. Por ejemplo, para supervisar la red para detectar intentos fallidos de inicio de sesión, el acceso a varios hosts o un suceso de reconocimiento seguido de una explotación, debe crear una regla de suceso. Es habitual que las reglas de suceso creen delitos como respuesta.

#### Reglas de flujo

Realizan pruebas en los datos de flujo de entrada procesados por el Procesador de flujos de QRadar. Puede crear una regla de flujo para detectar un flujo individual o secuencias de flujos. Es habitual que las reglas de flujo creen delitos como respuesta.

#### Reglas comunes

Realizan pruebas en datos de sucesos y flujos. Por ejemplo, puede crear una regla común para detectar sucesos y flujos que tienen una dirección IP de origen determinada. Es habitual que las reglas comunes creen delitos como respuesta.

#### Reglas de delito

Prueban los parámetros de un delito para desencadenar más respuestas. Por ejemplo, se genera una respuesta cuando un delito se produce en una fecha y hora específicas. Una regla de delito procesa delitos solo cuando se realizan cambios en el delito. Por ejemplo, cuando se añaden nuevos sucesos o el sistema ha planificado la reevaluación del delito. Es habitual que las reglas de delito envíen una notificación de correo electrónico como respuesta.

### Gestionar reglas

Puede crear, editar, asignar reglas a grupos y suprimir grupos de reglas. La categorización de reglas y componentes básicos en grupos permite ver las reglas y realizar su seguimiento de forma eficiente. Por ejemplo, puede ver todas las reglas que están relacionados con la conformidad.

### Reglas específicas de dominio

Si una regla tiene una prueba de dominio, puede restringir esa regla para que se aplique solo a los sucesos que están ocurriendo dentro de un dominio especificado. Un suceso que tenga una etiqueta de dominio que es diferente del dominio que está establecido en la regla no desencadena una respuesta.

Para crear una regla que prueba condiciones en todo el sistema, establezca la condición de dominio en **Cualquier dominio**.

### Condiciones de regla

La mayoría de las pruebas de regla evalúan una sola condición, como por ejemplo la existencia de un elemento en una recopilación de datos de consulta o la prueba de un valor contra una propiedad de un suceso. Para comparaciones complejas, puede probar reglas de suceso creando una consulta de Ariel Query Language (AQL) con condiciones de cláusula WHERE. Puede utilizar todas las funciones de cláusula WHERE para escribir criterios complejos que pueden eliminar la necesidad de ejecutar numerosas pruebas individuales. Por ejemplo, utilice una cláusula WHERE de AQL para comprobar si se está realizando un seguimiento del tráfico web o SSL entrante en un conjunto de referencia.

Puede ejecutar pruebas en la propiedad de un suceso, flujo o delito, por ejemplo dirección IP de origen, gravedad de suceso o análisis de ritmo.

Con las funciones, puede utilizar componentes básicos y otras reglas para crear una función de varios sucesos, varios flujos o varios delitos. Puede conectar reglas utilizando funciones que soportan operadores booleanos, por ejemplo OR y AND. Por ejemplo, si desea conectar reglas de suceso, puede utilizar la función **cuando un suceso coincide con alguna|todas las reglas siguientes**.

## Creación de una regla personalizada

---

IBM QRadar incluye reglas que detectan una amplia gama de actividades, tales como denegaciones de cortafuegos excesivas, múltiples intentos fallidos de inicio de sesión y una posible actividad de red de robots. También puede crear sus propias reglas para detectar actividad inusual.

### Antes de empezar

Antes de crear una regla nueva, debe tener el permiso **Delitos > Mantener reglas personalizadas**.

### Acerca de esta tarea

Cuando defina pruebas de regla, realice pruebas con el volumen de datos más pequeño posible. Al realizar las pruebas de esta manera, se obtiene un mejor rendimiento de las pruebas de regla y se asegura de no crear reglas costosas. Para optimizar el rendimiento, empiece con categorías amplias que restrinjan los datos que evalúa la prueba de regla. Por ejemplo, empiece con una prueba de regla para un tipo de origen de registro, una ubicación de red, un origen de flujo o un contexto (R2L, L2R, L2L) específico. Las pruebas de nivel medio serán direcciones IP, tráfico de puerto u otras pruebas asociadas. La regla debe probar la carga útil y las últimas expresiones regex.

Las reglas similares se agrupan por categorías. Por ejemplo, Auditoría, Explotación, Denegación de servicio distribuido (DDoS), Reconocimiento, etc. Cuando se suprime un elemento de un grupo, la regla o el componente básico solo se suprime del grupo; sigue estando disponible en la página **Reglas**. Cuando se suprime un grupo, las reglas o los componentes básicos de ese grupo permanecen disponibles en la página **Reglas**.

### Procedimiento

1. En **Delitos**, pestañas **Actividad de registro** o **Actividad de red**, pulse **Reglas**.
2. En la lista **Visualizar**, seleccione **Reglas** para crear una nueva regla.
3. Opcional: En la lista **Visualizar**, seleccione **Componentes básicos** para crear una nueva regla utilizando componentes básicos.
4. En la lista **Acciones**, seleccione un tipo de regla.

Cada tipo de regla se prueba contra los datos entrantes de diferentes orígenes en tiempo real. Por ejemplo, las reglas de suceso prueban datos de origen de registro entrante y las reglas de delito prueban los parámetros de un delito para desencadenar más respuestas.

5. En la página **Editor de pila de prueba de regla**, en el panel **Regla**, teclee un nombre exclusivo que desee para asignar a esta regla en el cuadro de texto **Aplicar**.
6. En el recuadro de lista, seleccione **Local** o **Global**.
  - Si selecciona **Local**, todas las reglas se procesan en el Procesador de sucesos en el que se recibieron y solo se crean delitos para los sucesos que se procesan localmente.
  - Si selecciona **Global**, todos los sucesos coincidentes se envían a la QRadar Console para su proceso y, por tanto, la QRadar Console utiliza más ancho de banda y recursos de proceso.

**Más información sobre las reglas locales y globales:**

**Pruebas de regla globales**

Utilice reglas globales para detectar cosas como "varias anomalías de inicio de sesión de usuario", donde los sucesos de ese usuario pueden aparecer en varios Procesadores de sucesos. Por ejemplo, si ha configurado esta regla para 5 anomalías de inicio de sesión en 10 minutos desde el mismo nombre de usuario, y lo establece como regla **Local**, esas 5 anomalías de inicio de sesión deben aparecer en el mismo Procesador de sucesos. Por tanto, si 3 anomalías de inicio de sesión estaban en un Procesador de sucesos y 2 en otro, no se genera ningún delito. Sin embargo, si establece esta regla como **Global**, se genera un delito.

7. En la lista **Grupo de pruebas**, seleccione una o varias pruebas que desea añadir a esta regla. El CRE evalúa las pruebas de regla en orden, línea por línea. La primera prueba se evalúa y cuando es verdadera, se evalúa la línea siguiente hasta que se alcanza la prueba final.

Si selecciona la prueba **cuando el suceso coincide con esta consulta de filtro de AQL** para una regla de suceso nueva, especifique una consulta de cláusula WHERE de AQL en el cuadro de texto **Especifique una consulta de filtro de AQL**.

**Obtenga más información sobre la utilización de reglas para sucesos que no se detectan:**

Las pruebas de regla siguiente se pueden desencadenar individualmente pero no se actúa sobre las pruebas de regla de la misma pila de pruebas de reglas.

- **cuando uno o varios de estos tipos de origen de registro no han detectado los sucesos durante este número de segundos**
- **cuando uno o varios de estos orígenes de registro no han detectado los sucesos durante este número de segundos**
- **cuando uno o varios de estos grupos de origen de registro no han detectado los sucesos durante este número de segundos**

Estas pruebas de regla no se ven activadas por un suceso entrante, sino que se activan cuando no se ve un suceso específico durante un intervalo de tiempo específico configurado. QRadar utiliza una *tarea observadora* que consulta periódicamente la última vez que se vio un suceso (hora de última visualización) y almacena esta hora del suceso para cada origen de registro. La regla se desencadena cuando la diferencia entre la hora de última visualización y la hora actual sobrepasa el número de segundos configurado en la regla.

8. Para exportar la regla configurada como un bloque básico a utilizar con otras reglas, pulse **Exportar como componente básico**.
9. En la página **Respuestas de regla**, configure las respuestas que desea que genere esta regla.

**Obtenga más información sobre los parámetros de la página de respuesta de regla:**

<i>Tabla 37. Parámetros de página Respuesta de regla de suceso, flujo, común y delito</i>	
<b>Parámetro</b>	<b>Descripción</b>
Descartar el suceso detectado	Fuerza al suceso o flujo coincidentes a omitir todas las demás reglas del motor de reglas y evita que se cree un delito. El suceso se graba en el almacenamiento para utilizarlo en las búsquedas y en la elaboración de informes.

<i>Tabla 37. Parámetros de página Respuesta de regla de suceso, flujo, común y delito (continuación)</i>	
<b>Parámetro</b>	<b>Descripción</b>
Asignar suceso nuevo	<p>Marque este recuadro de selección para asignar un suceso nuevo además del suceso o flujo original, que se procesa igual que todos los demás sucesos en el sistema.</p> <p>Asigna un suceso nuevo con el suceso original, y se procesa como todos los demás sucesos del sistema.</p> <p>Los parámetros <b>Asignar suceso nuevo</b> se visualizan cuando se marca este recuadro de selección. De forma predeterminada, el recuadro de selección no está marcado.</p>
Gravedad	Nivel de gravedad que desea asignar al suceso, donde 0 representa el nivel más bajo y 10 el más alto. La gravedad se muestra en el panel <b>Anotación</b> de detalles del suceso.
Credibilidad	La credibilidad que desee asignar al origen de registro. Por ejemplo, ¿es el origen de registro ruidoso o caro? El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La credibilidad se visualiza en el panel <b>Anotación</b> de los detalles de suceso.
Pertinencia	La relevancia que desea asignar al peso del activo. Por ejemplo, ¿cuánto le importa el activo? El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La pertinencia se visualiza en el panel <b>Anotación</b> de los detalles de suceso.
Correo electrónico	Para cambiar el valor <b>Entorno local del correo electrónico</b> , seleccione <b>Valores del sistema</b> en la pestaña <b>Admin</b> .
Especifique las direcciones de correo electrónico que se deben notificar:	Utilice una coma para separar varias direcciones de correo electrónico.
Condición de excepción de SNMP	<p>Habilite esta función para enviar una notificación de SNMP (condición de excepción).</p> <p>La salida de condición de excepción SNMP incluye la hora del sistema, el OID de condición de excepción y los datos de notificación, como los define el MIB. Puede acceder a la MIB desde <code>/opt/qradar/conf/Q1LABS-MIB.txt</code>.</p>
Enviar a SysLog Local	<p>Si desea registrar el suceso o flujo localmente, seleccione este recuadro de selección.</p> <p>De forma predeterminada, este recuadro de selección no está marcado.</p> <p><b>Nota:</b> Solo los sucesos normalizados se pueden registrar localmente en un dispositivo. Si desea enviar datos de sucesos en bruto, debe utilizar la opción Enviar a destinos de reenvío para enviar los datos a un host de syslog remoto.</p>

<i>Tabla 37. Parámetros de página Respuesta de regla de suceso, flujo, común y delito (continuación)</i>	
<b>Parámetro</b>	<b>Descripción</b>
Enviar a destinos de reenvío	<p>Si desea registrar el suceso o flujo en un destino de reenvío, seleccione este recuadro de selección.</p> <p>Un destino de reenvío es un sistema de proveedor, por ejemplo SIEM, tíquets o sistemas de alerta. Al marcar este recuadro de selección, se visualiza una lista de destinos de reenvío.</p> <p>Para añadir, editar o suprimir un destino de reenvío, pulse el enlace <b>Gestionar destinos</b>.</p>
Notificar	<p>Visualiza los sucesos que se generan como resultado de esta regla en el elemento Notificaciones del sistema en la pestaña Panel de control.</p> <p>Si habilita las notificaciones, configure el parámetro <b>Limitador de respuestas</b>.</p>
Añadir a un conjunto de referencia	<p>Añade los sucesos que se generan como resultado de esta regla a un conjunto de referencia. Debe ser administrador para añadir datos a un conjunto de referencia.</p> <p>Para añadir datos a un conjunto de referencia, siga estos pasos:</p> <ol style="list-style-type: none"> <li>En la primera lista, seleccione la propiedad del suceso o flujo que desea añadir.</li> <li>En la segunda lista, seleccione el conjunto de referencia al que desea añadir los datos especificados.</li> </ol>
Añadir a datos de referencia	<p>Para utilizar esta respuesta de regla, debe crear la recopilación de datos de referencia.</p>
Eliminar de conjunto de referencia	<p>Marque este recuadro de selección si desea que esta regla elimine datos de un conjunto de referencia.</p> <p>Para eliminar datos de un conjunto de referencia:</p> <ol style="list-style-type: none"> <li>En el primer recuadro de lista, seleccione la propiedad del suceso o flujo que desea eliminar. Las opciones incluyen todos los datos normalizados o personalizados.</li> <li>En el segundo recuadro de lista, seleccione el conjunto de referencia del que desea eliminar los datos especificados.</li> </ol> <p>La respuesta de la regla <b>Eliminar de conjunto de referencia</b> proporciona las funciones siguientes:</p> <p><b>Renovar</b>  Pulse <b>Renovar</b> para renovar el primer recuadro de lista para asegurarse de que la lista es actual.</p>
Eliminar de datos de referencia	<p>Para utilizar esta respuesta de regla, debe tener una recopilación de datos de referencia.</p>

Tabla 37. Parámetros de página Respuesta de regla de suceso, flujo, común y delito (continuación)	
Parámetro	Descripción
Ejecutar una acción personalizada	Puede escribir scripts que realizan acciones específicas en respuesta a los sucesos de red. Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquea una dirección IP de origen concreta de la red en respuesta a repetidos intentos fallidos de inicio de sesión.  Puede añadir y configurar acciones personalizadas utilizando el icono <b>Definir acciones</b> en la pestaña <b>Admin</b> .
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de suceso sobre el servidor IF-MAP.
Limitador de respuestas	Configura la frecuencia con la que desea que responda esta regla.
Nombre del delito	Si desea que la información de <b>Nombre de suceso</b> contribuya al nombre del delito, seleccione la opción <b>Esta información debe contribuir al nombre del delito</b> .  Si desea que el <b>Nombre de suceso</b> configurado sea el nombre del delito, seleccione la opción <b>Esta información debe establecer o sustituir el nombre del delito</b> .  <b>Nota:</b> Esta opción no cambia el nombre de un delito existente. Para cambiar el nombre de un delito existente, debe usar la opción Regla del delito <b>Esta información debe establecer o sustituir el nombre del delito</b> .

Una notificación SNMP puede tener el aspecto siguiente:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
ICMP Destination Unreachable Communication with Destination Host is
Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
Offense description"
```

Una salida de syslog puede tener este aspecto:

```
Sep 28 12:39:01 localhost.localdomain ECS:
Rule 'Name of Rule' Fired: 172.16.60.219:12642
-> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
1000398, Category: 1011, Notes: Event description
```

### Qué hacer a continuación

Para probar las reglas, ejecute [Capítulo 15, “Correlación histórica”](#), en la página 203.

Para verificar que el suceso desencadena la prueba de regla basada en el bloque de construcción, puede crear una respuesta de correo electrónico. Consulte [“Enviar notificaciones de correo electrónico”](#) en la página 48.

### Información relacionada

[Gestión de reglas personalizadas en QRadar SIEM](#)

## Configuración de un suceso o flujo como falso positivo

---

Puede tener tráfico de red legítimo que desencadene sucesos y flujos de falsos positivos que dificulte identificar verdaderos incidentes de seguridad. Puede impedir que los sucesos y los flujos se correlacionen con delitos configurándolos como falsos positivos.

### Procedimiento

1. En las pestañas **Actividad de registro** o **Actividad de red**, pulse la pausa en la parte superior derecha para detener la modalidad continua en tiempo real de sucesos o flujos.
2. Seleccione el suceso que desee ajustar.
3. Pulse **Falso positivo**.
4. Seleccione una opción de propiedad de suceso o flujo.
5. Seleccione una opción de dirección de tráfico.
6. Pulse **Ajustar**.

### Resultados

El suceso o flujo que coincida con los criterios especificados ya no se correlacionará con los delitos. Para editar el ajuste de falsos positivos, utilice el componente básico **User-BB\_FalsePositive: Ajustes de positivos definidos por el usuario** de la sección **Reglas** de la pestaña **Delitos**.

## Reglas de detección de anomalías

---

Las reglas de detección de anomalías realizan pruebas sobre los resultados de búsquedas guardadas de flujos o de sucesos para detectar patrones de tráfico inusuales en la red.

Las reglas de detección de anomalías requieren una búsqueda guardada agrupada alrededor de un parámetro común y un gráfico de serie temporal habilitado. Generalmente, la búsqueda necesita acumular datos antes de que la regla de anomalía devuelva resultados que identifiquen patrones de anomalías, umbrales o cambios de comportamiento.

### Reglas de anomalía

Puede probar el tráfico de sucesos y flujos para detectar los cambios en los sucesos a corto plazo en comparación con un intervalo más largo. Por ejemplo, nuevos servicios o aplicaciones que aparecen en una red, un servidor web que se bloquea o cortafuegos que empiezan a denegar el tráfico.

**Ejemplo:** Puede que desee que se le notifique cuando uno de los dispositivos de cortafuegos informa más a menudo de lo normal, porque la red podría estar bajo ataque. Desea que se le notifique cuando se reciba el doble de sucesos en 1 hora. Debe seguir estos pasos:

1. Cree y guarde una búsqueda que agrupe por origen de registro y muestre solo la columna de recuento.
2. Aplique la búsqueda guardada a una regla de anomalía y añada la prueba de regla **y cuando el valor promedio (por intervalo) del recuento durante la última 1 hora sea como mínimo 100% diferente del valor promedio (por intervalo) de la misma propiedad durante las últimas 24 horas**.

### Reglas de umbral

Puede probar sucesos o flujos con respecto a una actividad que sea superior o inferior a un rango especificado. Utilice estas reglas para detectar cambios en el uso de ancho de banda en las aplicaciones, servicios anómalos, el número de usuarios conectados a una VPN y detectar grandes transferencias de salida.

**Ejemplo:** Un usuario que ha estado implicado en un incidente anterior tiene una transferencia de salida de grandes dimensiones.



Cuando un usuario está involucrado en un delito anterior, establezca automáticamente la respuesta de regla para añadirla al conjunto de referencia. Si tiene una lista de observación de usuarios, añádalos al conjunto de referencia. Ajuste límites aceptables en la regla de umbral.

Son necesarios un conjunto de referencia, WatchUsers, y Key:username para la búsqueda.

Realice la búsqueda siguiente y luego aplíquela a una regla de umbral.

```
select assetuser(sourceip, now()) as 'srcAssetUser',
Applicationname(applicationid)as 'AppName', long(sum(sourcebytes
+destinationbytes)) as 'flowsun' from flows where flowdirection = 'L2R' and
REFERENCESETCONTAINS('Watchusers', username)group by 'srcAssetUser',
applicationid order by 'flowsun' desc last 24 hours
```

## Reglas conductuales

Puede probar sucesos o flujos para detectar cambios de volumen que se producen en patrones regulares para detectar valores atípicos. Por ejemplo, un servidor de correo que tiene una retransmisión abierta y que de repente se comunica con muchos hosts o un IPS (sistema de prevención de intrusiones) que empieza a generar numerosas actividades de alerta.

Una regla conductual aprende la frecuencia o volumen de una propiedad durante un periodo predefinido. El período define la línea temporal de comparación de línea base para lo que se está evaluando. Si se establece un período de 1 semana, el comportamiento de la propiedad durante esa semana se aprende y, a continuación, puede utilizar pruebas de regla para recibir alertas de los cambios importantes.

Una vez establecida una regla conductual, el período se ajusta automáticamente. Cuando se aprenden los datos del período, se evalúan continuamente para perfilar el crecimiento empresarial dentro del período; no es necesario cambiar las reglas. Cuanto más tiempo se ejecute una regla conductual, más precisa será. A continuación, puede ajustar las respuestas de regla para capturar cambios más sutiles.

La tabla siguiente describe las opciones de parámetro de prueba de regla conductual.

<i>Tabla 38. Definiciones de prueba de regla conductual</i>	
<b>Parámetro de prueba de regla</b>	<b>Descripción</b>
Período	El valor más importante. El período define el comportamiento de línea base de la propiedad que está probando y que utilizan las otras pruebas de regla. Para definir un período, considere el tipo de tráfico que está supervisando. Por ejemplo, para tráfico de red o procesos que incluyan interacción humana, 1 semana es un buen intervalo de período. Para el seguimiento de servicios automatizados donde los patrones son coherentes, puede que desee crear un período únicamente de 1 día para definir ese patrón de comportamiento.
Nivel de tráfico actual	<p>Peso de los datos originales contabilizando los cambios periódicos y los errores aleatorios. Esta prueba de regla plantea la pregunta: "¿son los datos iguales que ayer a la misma hora"?</p> <p>El peso debe estar en el rango de 1 a 100. Un valor más alto coloca más peso en el valor registrado anteriormente.</p>

Tabla 38. Definiciones de prueba de regla conductual (continuación)

Parámetro de prueba de regla	Descripción
Tendencia de tráfico actual	<p>Peso de los cambios en los datos para cada intervalo de tiempo. Esta prueba de regla plantea la pregunta: "¿en qué medida cambian los datos al comparar este minuto con el minuto anterior"?</p> <p>El peso debe estar en el rango de 1 a 100. Un valor más alto coloca más peso en las tendencias de tráfico que el comportamiento calculado.</p>
Comportamiento de tráfico actual	<p>Peso del efecto estacional para cada período. Esta prueba de regla plantea la pregunta: "¿han aumentado los datos en la misma cantidad de la semana 2 a la semana 3, que de la semana 1 a la semana 2?"</p> <p>El peso debe estar en el rango de 1 a 100. Un valor más alto coloca más peso en el comportamiento aprendido.</p>
Valor pronosticado	<p>Utilice valores pronosticados para escalar líneas base para hacer que las alertas sean más o menos sensibles.</p> <p>La sensibilidad debe estar en el rango de 1 a 100. Un valor 1 indica que el valor medido no puede ser distinto del valor pronosticado. Un valor 100 indica que el tráfico puede ser más de cuatro veces mayor que el valor predicho.</p>

El pronóstico del valor del intervalo (n + 1)<sup>th</sup> se calcula utilizando la fórmula siguiente:

$$F_{n+1} = B_n + T_n + T_{n+1-s}$$

Donde F es el valor pronosticado, B es el valor base del intervalo n, T es el valor de tendencia del intervalo n y T es el valor de tendencia de los intervalos de período transcurridos y s es el número de intervalos dentro del período.

El valor base se calcula utilizando la fórmula siguiente:

$$B_{n+1} = (0.2 + 0.3 * (\langle \text{Nivel de tráfico actual} \rangle / 100.0)) * (\text{value}_{n+1} - T_{n+1-s}) + (1 - (0.2 + 0.3 * (\langle \text{Nivel de tráfico actual} \rangle / 100.0))) * T_n$$

El valor de tendencia se calcula utilizando la fórmula siguiente:

$$T_{n+1} = (0.2 + 0.3 * (\langle \text{Tendencia de tráfico actual} \rangle / 100.0)) * (B_{n+1} - B_n) + (1 - (0.2 + 0.3 * (\langle \text{Tendencia de tráfico actual} \rangle / 100.0))) * T_n$$

La desviación suavizada D se calcula utilizando la fórmula siguiente:

$$D_{n+1} = (0.2 + 0.3 * (\langle \text{Comportamiento de tráfico actual} \rangle / 100.0)) * |\text{value}_{n+1} - F_{n+1}| + (1 - (0.2 + 0.3 * (\langle \text{Comportamiento de tráfico actual} \rangle / 100.0))) * D_{n+1-s}$$

La regla conductual genera una alerta para el intervalo si la siguiente expresión es falsa:

$$F - (1 + (\text{sensibilidad} / 100.0) * 3) * D \leq \text{value} \leq F + (1 + (\text{sensibilidad} / 100.0) * 3) * D$$

Durante el primer período, la regla conductual aprende para los cálculos futuros y no genera ninguna alerta.

## Creación de una regla de detección de anomalías

Las reglas de detección de anomalías prueban el resultado de búsquedas guardadas de flujos o de sucesos para buscar patrones de tráfico inusuales que se producen en la red. Las reglas conductuales prueban el tráfico de sucesos y flujos según tendencias y niveles de tráfico "estacionales". Las reglas de umbral realizan pruebas sobre el tráfico de sucesos y de flujos para detectar actividad que es menor, igual o mayor que un valor umbral configurado, o que está dentro de un rango especificado.

### Antes de empezar

Para crear reglas de detección de anomalías en la pestaña **Actividad de registro**, debe tener el permiso de rol de **Actividad de registro Mantener reglas personalizadas**.

Para crear reglas de detección de anomalías en la pestaña **Actividad de red**, debe tener el permiso de rol de **Actividad de red Mantener reglas personalizadas**.

Para gestionar reglas de detección de anomalías predeterminadas y creadas anteriormente, utilice la página **Reglas** en la pestaña **Delitos**.

### Acerca de esta tarea

Cuando se crea una regla de detección de anomalías, la regla se rellena con una pila de prueba predeterminada en función de los criterios de búsqueda guardada. Puede editar las pruebas predeterminadas o añadir pruebas a la pila de prueba. Al menos se debe incluir una prueba de **Propiedad acumulada** en la pila de prueba.

De forma predeterminada, la opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** está seleccionada en la página **Editor de pila de prueba de regla**.


Una regla de detección de anomalías prueba la propiedad acumulada seleccionada para cada grupo de sucesos o flujos por separado. Por ejemplo, si el valor acumulado seleccionado es **UniqueCount(sourceIP)**, la regla prueba cada dirección IP de origen exclusiva para cada grupo de sucesos o flujos.

La opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** es dinámica. El valor **[Propiedad acumulada seleccionada]** depende de la opción que seleccione para el campo **esta prueba de propiedad acumulada** de la pila de prueba predeterminada. El valor **[grupo]** depende de las opciones de agrupación que se han especificado en los criterios de búsqueda guardados. Si se incluyen varias opciones de agrupación, es posible que el texto se trunque. Mueva el puntero del ratón sobre el texto para ver todos los grupos.

### Procedimiento

1. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
2. Realice una búsqueda agrupada.

Puede añadir una propiedad a **agrupar por** en una búsqueda histórica nueva o seleccionar una propiedad de la lista **Visualizar** en la página de búsqueda actual.

3. En la página de resultados de búsqueda, pulse **Configurar**  y, a continuación, configure las opciones siguientes:
  - a) Seleccione una propiedad de la lista **Valor para gráfico**.
  - b) Seleccione **serie temporal** como tipo de gráfico en la lista **Valor para gráfico**.
  - c) Habilite el recuadro de selección **Capturar datos de serie temporal**.
  - d) Pulse **Guardar** y, a continuación, especifique un nombre para la búsqueda.
  - e) Pulse **Aceptar**.
  - f) Seleccione los últimos 5 minutos en la lista **Rango de tiempo**, mientras espera que se cargue el gráfico de serie temporal.

Debe tener datos de serie temporal para la propiedad que ha seleccionado en la lista **Valor para gráfico** para ejecutar una prueba de regla en esa propiedad acumulada.

4. En el menú **Reglas**, seleccione el tipo de regla que desea crear.
  - Añadir regla de anomalía
  - Añadir regla de umbral
  - Añadir regla conductual
5. En el campo **especifique aquí el nombre de la regla** de la página **Editor de pila de prueba de regla**, escriba un nombre exclusivo que desee asignar a esta regla.
6. Para aplicar la regla mediante la prueba predeterminada, seleccione la primera regla en la lista **Grupo de pruebas** de anomalía.

Puede que tenga que establecer el parámetro de propiedad acumulada en la propiedad que ha seleccionado en la lista **Valor para gráfico** que ha guardado en los criterios de búsqueda. Si desea ver el resultado antes, establezca el porcentaje en un valor inferior, por ejemplo, 10%. Cambie **últimas 24 horas** por un período de tiempo inferior, por ejemplo 1 hora. Debido a que una detección de anomalías realiza pruebas en campos agregados en tiempo real para notificar actividad anómala en la red, es posible que desee aumentar o disminuir los eventos o flujos del tráfico de red.

7. Añada una prueba a una regla.
  - a) Para filtrar las opciones de la lista **Grupo de pruebas**, escriba el texto por el que desea filtrar en el campo **Tipo por filtrar**.
  - b) En la lista **Grupo de pruebas**, seleccione el tipo de prueba que desea añadir a esta regla.
  - c) Para identificar una prueba como prueba excluida, pulse **and** al principio de la prueba en el panel Regla. **and** se visualiza como **and not**.
  - d) Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.
  - e) En el recuadro de diálogo, seleccione valores para la variable y, a continuación, pulse **Enviar**.
8. Para probar las propiedades acumuladas seleccionadas totales para cada grupo de sucesos o flujos, inhabilite el recuadro de selección **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado**.
9. En el panel Grupos, habilite los grupos a los que desea asignar esta regla.
10. En el campo **Notas**, escriba las notas que desee incluir para esta regla y pulse **Siguiente**.
11. En la página **Respuestas de regla**, configure las respuestas que desea que genere esta regla.

**Obtenga más información sobre los parámetros de la página de reglas de detección de anomalías:**

La tabla siguiente proporciona los parámetros de página **Respuesta de regla** si el tipo de regla es Anomalía.

<i>Tabla 39. Parámetros de página de respuesta de regla de detección de anomalías</i>	
<b>Parámetro</b>	<b>Descripción</b>
Asignar suceso nuevo	Especifica que esta regla asigna un suceso nuevo con el suceso o flujo original, que se procesa como todos los demás sucesos del sistema. De forma predeterminada, este recuadro de selección está seleccionado y no se puede borrar.

Tabla 39. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Denominación de delito	<p>Si desea que la información de Nombre de suceso contribuya al nombre del delito, seleccione la opción <b>Esta información debe contribuir al nombre de los delitos asociados</b>.</p> <p>Si desea que el Nombre de suceso configurado contribuya al delito, seleccione la opción <b>Esta información debe establecer o sustituir el nombre de los delitos asociados</b>.</p> <p><b>Nota:</b> Una vez sustituido el nombre del delito, éste no cambiará hasta que se cierre el delito. Por ejemplo, si un delito está asociado a más de una regla y el último suceso no desencadena la regla configurada para sustituir temporalmente el nombre del delito, el último suceso no actualizará el nombre del delito. En lugar de esto, el nombre del delito sigue siendo el nombre establecido por la regla de alteración temporal.</p>
Gravedad	Nivel de gravedad que desea asignar al suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Gravedad se visualiza en el panel Anotaciones de los detalles de suceso.
Credibilidad	La credibilidad que desee asignar al origen de registro. Por ejemplo, ¿es el origen de registro ruidoso o caro? Utilizando los recuadros de lista, seleccione la credibilidad del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Credibilidad se visualiza en el panel Anotaciones de los detalles de suceso.
Pertinencia	La relevancia que desea asignar al peso del activo. Por ejemplo, ¿cuánto le importa el activo? Utilizando los recuadros de lista, seleccione la pertinencia del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Pertinencia se visualiza en el panel Anotaciones de los detalles de suceso.
Asegúrese de que el suceso asignado forma parte de un delito	Como resultado de esta regla, el suceso se reenvía al magistrado. Si existe un delito, se añade este suceso. Si no se ha creado ningún delito en la pestaña Delitos, se crea un delito nuevo.
Notificar	Los sucesos que se generan como resultado de esta regla se visualizan en el elemento Notificaciones del sistema de la pestaña <b>Panel de control</b> . Si habilita las notificaciones, configure el parámetro <b>Limitador de respuestas</b> .
Enviar a SysLog Local	<p>Marque este recuadro de selección si desea registrar el suceso o flujo localmente. De forma predeterminada, el recuadro de selección no está marcado.</p> <p><b>Nota:</b> Solo los sucesos normalizados se pueden registrar localmente en un dispositivo de QRadar. Si desea enviar datos de sucesos en bruto, debe utilizar la opción <b>Enviar a destinos de reenvío</b> para enviar los datos a un host de syslog remoto.</p>

<i>Tabla 39. Parámetros de página de respuesta de regla de detección de anomalías (continuación)</i>	
<b>Parámetro</b>	<b>Descripción</b>
Añadir a un conjunto de referencia	<p>Añade los sucesos que se generan como resultado de esta regla a un conjunto de referencia. Debe ser administrador para añadir datos a un conjunto de referencia.</p> <p>Para añadir datos a un conjunto de referencia, siga estos pasos:</p> <ol style="list-style-type: none"> <li>En la primera lista, seleccione la propiedad del suceso o flujo que desea añadir.</li> <li>En la segunda lista, seleccione el conjunto de referencia al que desea añadir los datos especificados.</li> </ol>
Añadir a datos de referencia	Para utilizar esta respuesta de regla, debe crear la recopilación de datos de referencia.
Eliminar de conjunto de referencia	<p>Marque este recuadro de selección si desea que esta regla elimine datos de un conjunto de referencia.</p> <p>Para eliminar datos de un conjunto de referencia, siga estos pasos:</p> <ol style="list-style-type: none"> <li>En la primera lista, seleccione la propiedad del suceso o flujo que desea eliminar.</li> <li>En la segunda lista, seleccione el conjunto de referencia del que desea eliminar los datos especificados.</li> </ol>
Eliminar de datos de referencia	Para utilizar esta respuesta de regla, debe tener una recopilación de datos de referencia.
Ejecutar una acción personalizada	<p>Puede escribir scripts que realizan acciones específicas en respuesta a los sucesos de red. Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquea una dirección IP de origen concreta de la red en respuesta a repetidos intentos fallidos de inicio de sesión.</p> <p>Marque este recuadro de selección y seleccione una acción personalizada de la lista <b>Acción personalizada a ejecutar</b>.</p> <p>Puede añadir y configurar acciones personalizadas utilizando el icono <b>Definir acciones</b> en la pestaña <b>Admin</b>.</p>
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de delito sobre el servidor IF-MAP.
Limitador de respuestas	Marque este recuadro de selección y utilice los recuadros de lista para configurar la frecuencia con la que desea que responda esta regla
Habilitar regla	Marque este recuadro de selección para habilitar esta regla. De manera predeterminada, el recuadro de selección aparece seleccionado.

Una notificación SNMP puede tener el aspecto siguiente:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
ICMP Destination Unreachable Communication with Destination Host is
```

```
Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
Offense description"
```

Una salida de syslog puede tener este aspecto:

```
Sep 28 12:39:01 localhost.localdomain ECS:
Rule 'Name of Rule' Fired: 172.16.60.219:12642
-> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
1000398, Category: 1011, Notes: Event description
```

12. Pulse **Siguiente**.
13. Pulse **Finalizar**.

## Configuración de una respuesta de regla para añadir datos a una recopilación de datos de referencia

---

Configure reglas que utilicen datos de referencia para avisarle de actividad sospechosa. Por ejemplo, incluya una lista de usuarios privilegiados en los datos de referencia y luego configure una regla que se desencadene para avisarle cuando se produzcan anomalías de usuario privilegiado.

### Antes de empezar

Antes de enviar datos a un conjunto de referencia, el administrador de QRadar debe crear el conjunto de referencias.

### Acerca de esta tarea

QRadar soporta los siguientes tipos de recopilación de datos:

#### Conjunto de referencia

Un conjunto de elementos, por ejemplo una lista de direcciones IP o nombres de usuario, que se derivan de los sucesos y flujos que se producen en la red.

#### Correlación de referencia

Los datos se almacenan en registros que correlacionan una clave con un valor. Por ejemplo, para correlacionar la actividad de usuario en la red, cree una correlación de referencia que utilice el parámetro **Nombre de usuario** como clave y el **ID global** del usuario como valor.

#### Correlación de referencia de conjuntos

Los datos se almacenan en registros que correlacionan una clave con varios valores. Por ejemplo, para probar el acceso autorizado a una patente, utilice una propiedad de suceso personalizada para **ID de patente** como clave y el parámetro **Nombre de usuario** como valor. Utilice una correlación de conjuntos para llenar una lista de usuarios autorizados.

#### Correlación de referencia de correlaciones

Los datos se almacenan en registros que correlacionan una clave a otra clave, que a continuación se correlaciona con un valor único. Por ejemplo, para probar las violaciones de ancho de banda de red, debe crear una correlación de correlaciones. Utilice el parámetro **IP de origen** como la primera clave, el parámetro **Aplicación** como segunda clave y el parámetro **Bytes totales** como valor.

#### Tabla de referencia

En una tabla de referencia, los datos se almacenan en una tabla que correlaciona una clave con otra clave, que a continuación se correlaciona con un valor único. La segunda clave tiene un tipo asignado. Esta correlación es similar a una tabla de base de datos donde cada columna de la tabla está asociada con un tipo. Por ejemplo, debe crear una tabla de referencia que almacena el parámetro **Nombre de usuario** como primera clave y tiene varias claves secundarias que tienen un tipo asignado definido por el usuario como **Tipo de IP** con el parámetro **IP de origen** o **Puerto de origen** como valor. Puede configurar una respuesta de regla para añadir una o más claves definidas en la tabla. También puede añadir valores personalizados a la respuesta de regla. El valor personalizado debe ser válido para el tipo de la clave secundaria.

## Procedimiento

1. Cree la recopilación de datos de referencia utilizando el widget **Gestión de conjuntos de referencia** de la pestaña **Admin**.

También puede crear una recopilación de datos de referencia utilizando el script `ReferenceDataUtil.sh`.

2. Cree una regla utilizando el asistente **Reglas**.
3. Cree una respuesta de regla que envíe datos a una recopilación de datos de referencia. Puede añadir los datos como datos compartidos o datos específicos de dominio.

### Más información sobre los parámetros de Añadir a datos de referencia:

#### Añadir a una correlación de referencia

Envía datos a una recopilación de pares de clave única/múltiples valores. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccione la correlación de referencia a la que desea añadir el registro de datos.

#### Añadir a una correlación de referencia de conjuntos

Envía datos a una recopilación de pares de clave/valor único. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccione la correlación de referencia de conjuntos a los que desea añadir el registro de datos.

#### Añadir a una correlación de referencia de correlaciones

Envía datos a una recopilación de pares de varias claves/valor único. Debe seleccionar una clave para la primera correlación, una clave para la segunda correlación y, a continuación, el valor para el registro de datos. También debe seleccionar la correlación de referencia de correlaciones a la que desea añadir el registro de datos.

#### Añadir a una tabla de referencia

Envía datos a una recopilación de pares de múltiples claves/valor único, donde se ha asignado un tipo a las claves secundarios. Seleccione la tabla de referencia a la que desea añadir datos y, a continuación, seleccione una clave primaria. Seleccione las claves internas (claves secundarias) y sus valores para los registros de datos.

## Editar componentes básicos

---

Puede editar cualquiera de los componentes básicos predeterminados para utilizarlo en varias reglas o para crear reglas complejas o lógicas. Puede guardar un grupo de pruebas como componentes básicos para utilizarlas con reglas.

Por ejemplo, puede editar el componente básico **BB:HostDefinition: Servidores de correo** para identificar todos los servidores de correo del despliegue. A continuación, puede configurar cualquier regla para excluir los servidores de correo de las pruebas de regla.

### Procedimiento

1. Pulse la pestaña **Delitos** o **Actividad de red**.
2. Pulse **Reglas**.
3. En la lista **Visualizar**, seleccione **Componentes básicos**.
4. Efectúe una doble pulsación en el componente básico que desea editar.
5. Actualice el componente básico, como sea necesario.
6. Pulse **Siguiente**.
7. Continúe con el asistente.
8. Pulse **Finalizar**.

### Información relacionada

[Descripción general de los bloques de construcción en QRadar SIEM](#)



## Visualización del rendimiento de las reglas

La visualización del rendimiento de la regla amplía el registro actual en torno a la degradación del rendimiento y las reglas personalizadas caras en el conducto QRadar. Con la visualización del rendimiento de las reglas, puede determinar fácilmente la eficiencia de las reglas del conducto de QRadar directamente en la página **Reglas**.

**Nota:** Debe ser administrador para activar la visualización del rendimiento de las reglas. Una vez que la visualización del rendimiento de la regla esté activada, los usuarios podrán ver las métricas de rendimiento de las reglas. Para obtener más información sobre cómo activar la visualización del rendimiento, consulte *Guía de administración de IBM QRadar*.

Cuando la visualización del rendimiento de la regla está activada, la columna **Rendimiento** se añade a la página **Reglas**. La columna **Rendimiento** permanecerá vacía hasta que se produzca un problema de rendimiento en el motor de reglas personalizado.

Performance ▲	Rule Name	Group	Rule Category
	Devices with High...	Anomaly	Custom Rule
	This rule has not yet had a detailed analysis.		Custom Rule
	Anomaly: Excessiv...	Recon	Custom Rule
	Excessive Firewall...	Anomaly	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule

Figura 13. Columna de rendimiento de la página **Reglas**

Cuando los sucesos o los flujos se dirigen al almacenamiento, QRadar empieza a recopilar las métricas en las reglas habilitadas para las medidas de la eficiencia. Las métricas se recopilan en todas las reglas de suceso, comunes y de flujo. Cuando guarde las actualizaciones de las reglas, las métricas se borrarán de las reglas que haya actualizado para evitar que puedan confundirse el rendimiento y las reglas personalizadas. Esta opción puede configurarla un administrador.

Puede ordenar las reglas por sus métricas de rendimiento e identificar las reglas más caras. Cuando revise las reglas, puede ajustar las pruebas para optimizar cada una de las reglas y reducir la carga del sistema.

Con la visualización del rendimiento de las reglas, podrá ver lo caras que son las reglas. Los equipos de operaciones de QRadar pueden supervisar cualquier regla cara y asegurarse de que no originen problemas de rendimiento futuros.

Si las reglas se ejecutan de forma eficiente, la carga de trabajo del sistema puede disminuir. Con el tiempo, esta eficiencia puede ayudar a QRadar a evitar las degradaciones de rendimiento en torno a las reglas, lo que hace que las reglas eludan la correlación de reglas. El resultado es que es posible que la posible actividad sospechosa no activará una notificación, lo que puede suponer que en el futuro se pierdan problemas relacionados con la seguridad.

Para obtener más información sobre cómo ajustar las reglas, consulte el documento *IBM QRadar Tuning Guide*.

### Ver las métricas de una regla

Puede ver las métricas de una regla en la página **Reglas**, cuando pasa el puntero del ratón sobre las barras coloreadas en la columna **Rendimiento** y en el cuadro de texto **Análisis de rendimiento**, que está en la esquina inferior derecha de la página **Reglas**. También puede ver las métricas de una regla en el **Asistente de reglas**, cuando edita una regla. La indicación de fecha y hora del recuadro de texto **Análisis de rendimiento** muestra cuándo se han actualizado las métricas de la regla. Para obtener más información acerca de cómo crear reglas, consulte el tema [Reglas](#).

En la pestaña **Actividad de red** o en la pestaña **Actividad de registro**, pulse **Reglas** para visualizar la página **Reglas**. Efectúe una doble pulsación en una regla para abrir el **Asistente de reglas**.

The screenshot displays the IBM QRadar Rules management interface. At the top, there are navigation tabs for 'Rules', 'Groups', 'Actions', and 'Revert Rule'. Below this is a search bar and a 'View the IBM App Exchange for more...' link. The main area contains a table of rules with columns for Performance, Rule Name, Group, Rule Category, Rule Type, Enabled, Response, Event/Flow Count, Offense Count, Origin, Creation Date, and Modification Date. The first rule, 'Local Mass Mailing Host Detected', is highlighted with a yellow border. Below the table, the 'Rule' details for the selected rule are shown, including its description and logic. A 'Notes' section provides additional context. On the right side, a 'Performance Analysis' panel is visible, showing capacity metrics and lowest capacity host details.

Performance	Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
Local Mass Mailing Host Detec...	Destination Asset Weight is High	Magnitude Adjust...	Custom Rule	Common	True	Dispatch New Event	0	0	System	Mar 10, 2010, 3:33...	Dec 5, 2018, 6:03...
Login Failures Followed By Su...	Authentication, Intr...		Custom Rule	Event	True	Dispatch New Event	1,312,281	1	System	Jun 29, 2010, 6:38...	Dec 5, 2018, 6:03...
Source Address is a Known Q...	Magnitude Adjust...		Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:41...	Dec 5, 2018, 6:03...
Source Address is a Bogon IP	Magnitude Adjust...		Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:44...	Dec 5, 2018, 6:03...
AssetExclusion: Exclude NetBI...	Asset Reconciliati...		Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 4:02...	Dec 5, 2018, 6:03...
Login Failures Followed By Su...	Authentication, Intr...		Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 13, 2010, 2:42...	Dec 5, 2018, 6:03...
AssetExclusion: Exclude DNS ...	Asset Reconciliati...		Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 3:58...	Dec 5, 2018, 6:03...
Source Asset Exists	Magnitude Adjust...		Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:25...	Dec 5, 2018, 6:03...
Chained Exploit Followed by S...	Intrusion Detection		Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 14, 2010, 6:10...	Dec 5, 2018, 6:03...
Excessive Firewall Denies fro...	Recon		Custom Rule	Event	True	Dispatch New Event	0	0	System	Nov 29, 2005, 8:11...	Dec 5, 2018, 6:03...
Multiple Exploit Types Against ...	Intrusion Detection		Custom Rule	Event	True	Dispatch New Event	0	0	System	Jun 22, 2006, 9:50...	Dec 5, 2018, 6:03...
Source Asset Weight is Medium	Magnitude Adjust...		Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:30...	Dec 5, 2018, 6:03...
Destination Asset Exists	Magnitude Adjust...		Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:26...	Dec 5, 2018, 6:03...
__genyrule1			Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:46...	Dec 6, 2018, 4:46...
__genyrule2			Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57...	Dec 6, 2018, 4:59...
__genyrule3			Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57...	Dec 6, 2018, 4:59...

**Rule**  
Apply Local Mass Mailing Host Detected on events which are detected by the Local system and NOT when an event matches any of the following BB-HostDefinition: Mail Servers, BB-HostReference: Mail Servers and when the event(s) were detected by one or more of Flow Classification Engine and when any of these BB-CategoryDefinition: Mail Policy Violation with the same source IP more than 20 times, across more than 1 destination IP within 1 minutes and when the event context is Local to Remote

**Notes**  
Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.

**Performance Analysis** 4 minutes ago  
Capacity  
Lowest: 1,099,840 EPS  
Average: 1,099,840 EPS  
Lowest Capacity Host Details  
Hostname: ip-125-89  
Appliance Type: 3199  
License EPS Capacity: 5,000 EPS  
Appliance Capacity: 30,000 EPS

Figura 14. Análisis de rendimiento en la página **Reglas**

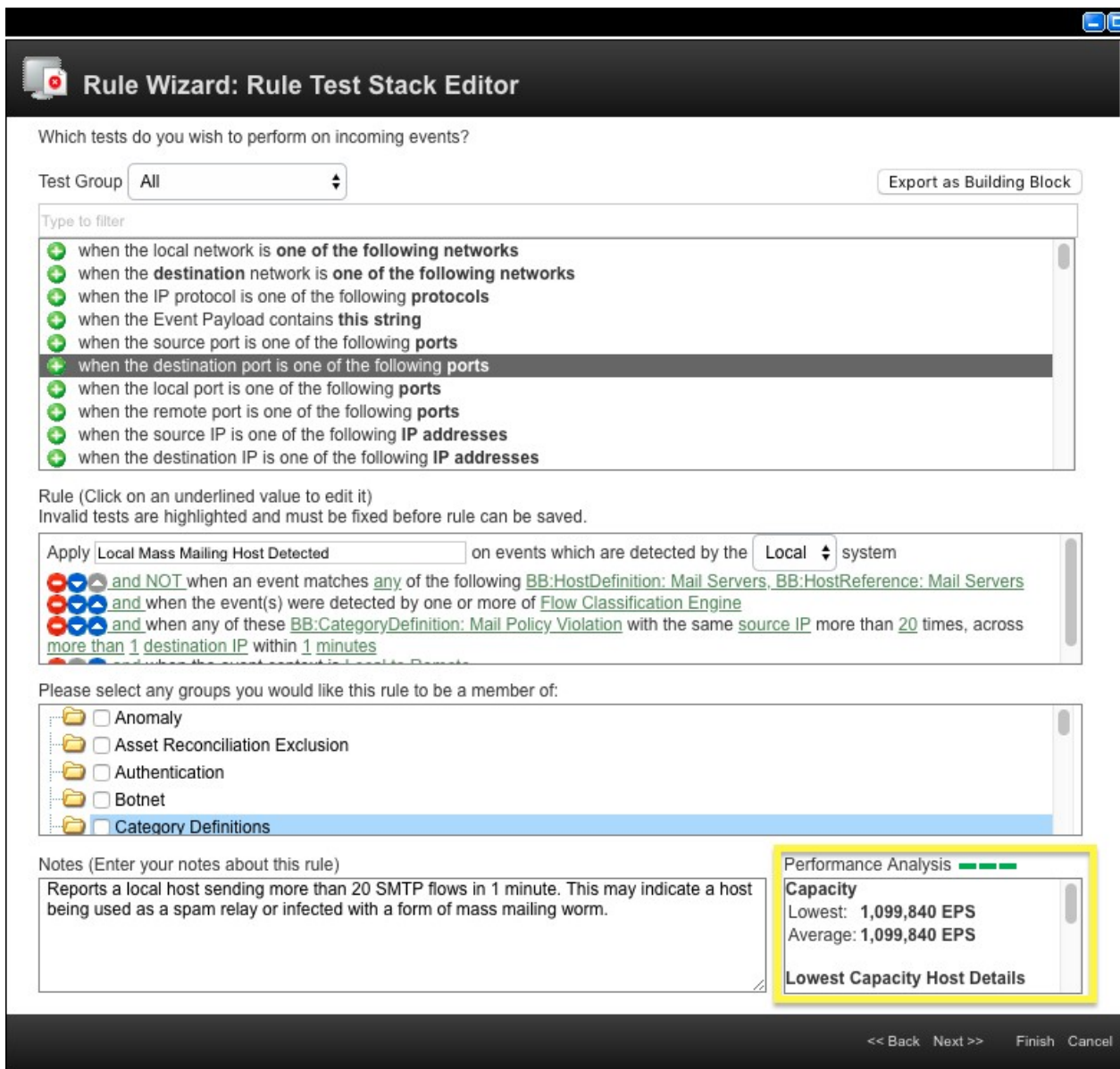


Figura 15. Análisis de rendimiento en el **Asistente de reglas**

### Colores y barras en la columna Rendimiento de la página Reglas

El número de barras que se muestra es una ayuda visual para los daltónicos.

#### Una barra roja

La regla es de bajo rendimiento y debe ser ajustada. El rendimiento de EPS/FPS de esta regla está por debajo del límite inferior. Abra la regla y ajuste las pruebas.

#### Dos barras naranjas

Es posible que la regla necesite algunos ajustes.

#### Tres barras verdes

La regla tiene un alto rendimiento, por encima del límite superior del umbral de EPS/FPS.

**Nota:** Los colores y el número de barras no se pueden cambiar. La definición de una regla que está bajo rendimiento es configurable por un administrador.

La imagen siguiente muestra los **Valores de regla personalizada** predeterminados en QRadar.

## Custom Rule Settings

Enable Performance Analysis	False	▼
Reset Metrics on Rule Change	True	▼
Performance Analysis Upper Limit	50,000	▲
Performance Analysis Lower Limit	12,500	▲

**Figura 16. Ajustes de regla personalizada**

Para obtener más información acerca de cómo ajustar las reglas, consulte el tema "Orden de pruebas de regla personalizada" en el documento *IBM QRadar Tuning Guide*.

### **Conceptos relacionados**

["Reglas"](#) en la página 183

Las reglas, a veces llamadas reglas de correlación, se aplican a los sucesos, flujos o delitos para buscar o detectar anomalías. Si se cumplen todas las condiciones de una prueba, la regla genera una respuesta.

---

## Capítulo 15. Correlación histórica

Utilice la correlación histórica para ejecutar sucesos y flujos pasados a través del motor de reglas personalizadas (CRE) para identificar amenazas o incidentes de seguridad que ya se han producido.

**Restricción:** No puede utilizar la correlación histórica en IBM QRadar Log Manager. Para obtener más información sobre las diferencias entre IBM QRadar SIEM y IBM QRadar Log Manager, consulte [Capítulo 2, “Prestaciones de su producto IBM QRadar”](#), en la página 3.

De forma predeterminada, un despliegue de IBM QRadar SIEM analiza la información que se recopila de los orígenes de registro y los orígenes de flujo en tiempo casi real. Con la correlación histórica, puede crear correlaciones por la hora de inicio o por la hora de dispositivo. La *hora de inicio* es la hora a la que el suceso se ha recibido en QRadar. La *hora de dispositivo* es la hora a la que se produjo el suceso en el dispositivo.

La correlación histórica puede resultar útil en las situaciones siguientes:

### **Análisis de datos en masa**

Si carga datos en masa en el despliegue de QRadar, puede utilizar la correlación histórica para correlacionar los datos contra los datos que se recopilaron en tiempo real. Por ejemplo, para evitar la degradación del rendimiento durante las horas de negocio normales, puede cargar sucesos de varios orígenes de registro cada día a media noche. Puede utilizar la correlación histórica para correlacionar los datos por hora de dispositivo para ver la secuencia de sucesos de red conforme se han producido en las últimas 24 horas.

### **Probar reglas nuevas**

Puede ejecutar la correlación histórica para probar reglas nuevas. Por ejemplo, uno de sus servidores ha sufrido recientemente un ataque de un programa malicioso nuevo para el cual no tiene reglas implementadas. Puede crear una regla para comprobar la existencia de ese programa malicioso. Después, puede utilizar la correlación histórica para comprobar la regla con datos históricos para ver si la regla desencadenaría una respuesta si estuviese implementada en el momento del ataque. De forma similar, puede utilizar la correlación histórica para determinar cuándo se ha producido el ataque o la frecuencia del ataque. Puede seguir ajustando la regla y después pasarla a un entorno de producción.

### **Volver a crear delitos que se habían perdido o depurado**

Si el sistema ha perdido delitos debido a un interrupción en la actividad o a cualquier otro motivo, puede volver a crear los delitos ejecutando la correlación histórica sobre los sucesos y los flujos que se recibieron durante ese tiempo.

### **Identificar hebras ocultas anteriormente**

Conforme se conoce información sobre las amenazas de seguridad más recientes, puede utilizar la correlación histórica para identificar sucesos de red que ya se han producido pero que no han desencadenado un suceso. Puede realizar pruebas rápidamente para amenazas que ya hayan comprometido el sistema o los datos de su organización.

---

## Visión general de la correlación histórica

Puede configurar un perfil de correlación histórica para especificar los datos históricos que desea analizar y el conjunto de reglas contra el que desea probar. Cuando se desencadena una regla, se crea un delito. Debe asignar el delito para la investigación y la corrección.

### **Selección de datos**

El perfil utiliza una búsqueda guardada para recopilar los datos históricos de sucesos y flujos a utilizar en la ejecución. Asegúrese de que el perfil de seguridad otorga permiso para ver los sucesos y los flujos que desea incluir en la correlación histórica ejecutada.

## Selección y manejo de reglas

La consola de QRadar procesa datos solo contra las reglas especificadas en el perfil de correlación.

Las reglas comunes prueban datos en sucesos y flujos. Debe tener permiso para ver sucesos y flujos para poder añadir reglas comunes al perfil. Cuando un usuario que carece de permiso para ver sucesos y flujos edita un perfil, las reglas comunes se eliminan automáticamente del perfil.

Puede incluir reglas inhabilitadas en un perfil de correlación histórica. Cuando se ejecuta el perfil, la regla inhabilitada se evalúa contra los sucesos y flujos entrantes. Si la regla se desencadena y la acción de regla es generar un delito, el delito se crea incluso aunque la regla esté inhabilitada. Para evitar la generación de distracciones innecesarias, las respuestas de regla, como por ejemplo la generación de informes y las notificaciones de correo se ignoran durante la correlación histórica.

Puesto que el proceso de correlación histórica se produce en una sola ubicación, las reglas que están incluidas en el perfil se tratan como reglas globales. El proceso no hace que una regla local se convierta en global, pero maneja la regla como si fuera global durante la ejecución de la correlación histórica. Algunas reglas, como por ejemplo las reglas con estados, podrían no desencadenar la misma respuesta que en una correlación normal que se ejecuta en un procesador de sucesos local. Por ejemplo, una regla con estados local que hace el seguimiento de cinco inicios de sesión fallidos en un periodo de cinco minutos con el mismo nombre de usuario se comporta de forma diferente en las ejecuciones de correlación normal e histórica. En una correlación normal, esta regla local mantiene un contador para el número de inicios de sesión fallidos que recibe cada procesador de sucesos local. En la correlación histórica, esta regla mantiene un solo contador para todo el sistema QRadar. En esta situación, se pueden crear delitos de forma diferente en comparación con una ejecución de correlación normal.

## Creación de delitos

Las ejecuciones de correlación histórica crean delitos solo cuando se desencadena una regla y la acción de regla específica que se debe crear un delito. Una correlación histórica no contribuye a un delito en tiempo real ni a un delito creado a partir de una correlación histórica anterior ejecutada, incluso cuando se utiliza el mismo perfil.

El número máximo de delitos que se pueden crear mediante una ejecución de correlación histórica es 100. La ejecución de correlación histórica se detiene cuando se alcanza el límite.

Puede ver delitos históricos en el panel de control **Supervisión de amenazas y seguridad** y en la pestaña **Delitos** al mismo tiempo que revisa los delitos en tiempo real.

## Creación de un perfil de correlación histórica

---

Puede crear un perfil de correlación histórica para volver a ejecutar sucesos y flujos pasados a través del motor de reglas personalizadas (CRE). El perfil incluye información sobre el conjunto de datos y las reglas a utilizar durante la ejecución.

**Restricción:** Puede crear perfiles históricos solamente en IBM QRadar SIEM. No puede crear perfiles históricos en IBM QRadar Log Manager.

### Antes de empezar

Las reglas comunes prueban datos en sucesos y flujos. Debe tener permiso para ver sucesos y flujos para poder añadir reglas comunes al perfil. Cuando un usuario que carece de permiso para ver sucesos y flujos edita un perfil, las reglas comunes se eliminan automáticamente del perfil.

### Acerca de esta tarea

Puede configurar un perfil para correlacionar por hora de inicio u hora de dispositivo. La *hora de inicio* es la hora a la que los sucesos llegan al recopilador de sucesos. La *hora de dispositivo* es la hora a la que se produjo el suceso en el dispositivo. Los sucesos se pueden correlacionar por hora de inicio o por hora de dispositivo. Los flujos se pueden correlacionar por hora de inicio únicamente.

Puede incluir reglas inhabilitadas en el perfil. Las reglas inhabilitadas se indican en la lista de reglas con **(Inhabilitado)** después del nombre de regla.

Una correlación histórica no contribuye a un delito en tiempo real ni a un delito creado a partir de una correlación histórica anterior ejecutada, incluso cuando se utiliza el mismo perfil.

### Procedimiento

1. Abra el cuadro de diálogo Correlación histórica.
  - En la pestaña **Actividad de registro**, pulse **Acciones > Correlación histórica**.
  - En la pestaña **Actividad de red**, pulse **Acciones > Correlación histórica**.
  - En la pestaña **Delitos**, pulse **Reglas > Acciones > Correlación histórica**.
2. Pulse **Añadir** y seleccione **Perfil de suceso** o **Perfil de flujo**.
3. Teclee un nombre para el perfil y seleccione una búsqueda guardada.  
Solo puede utilizar búsquedas guardadas no agregadas.
4. En la pestaña **Reglas**, seleccione las reglas a ejecutar contra los datos históricos y elija la hora de correlación.  
  
Si marca el recuadro de selección **Utilizar todas las reglas habilitadas**, no puede incluir reglas inhabilitadas en el perfil. Si desea incluir reglas habilitadas e inhabilitadas en el perfil, debe seleccionarlas individualmente de la lista de reglas y pulsar **Añadir seleccionado**.
5. En la pestaña **Planificar**, especifique el rango de horas para la búsqueda guardada y establezca los valores de planificación de perfil.
6. En la pestaña **Resumen**, revise la configuración y elija si desea ejecutar el perfil inmediatamente.
7. Pulse **Guardar**.  
  
El perfil se pone en cola para su proceso. Los perfiles en cola basados en una planificación tienen prioridad sobre las ejecuciones manuales.

## Visualización de la información sobre ejecuciones de correlación histórica

Puede ver el historial de un perfil de correlación histórica para ver información sobre ejecuciones pasadas del perfil. Puede ver la lista de delitos creados durante la ejecución y el catálogo de sucesos o flujos que coinciden con las reglas desencadenadas del perfil. Puede ver el historial de ejecuciones de correlaciones históricas en cola, en ejecución, completadas, completadas con errores y canceladas.

### Acerca de esta tarea

Se crea un catálogo de correlación histórica para cada regla desencadenada para cada dirección IP de origen exclusiva durante la ejecución, incluso si no se creó un delito. El catálogo contiene todos los sucesos o flujos que coinciden parcial o totalmente con la regla desencadenada.

No puede crear informes sobre datos de correlación histórica directamente desde QRadar. Si desea utilizar programas de terceros para crear informes, puede exportar los datos desde QRadar.

### Procedimiento

1. Abra el cuadro de diálogo Correlación histórica.
  - En la pestaña **Actividad de registro**, pulse **Acciones > Correlación histórica**.
  - En la pestaña **Actividad de red**, pulse **Acciones > Correlación histórica**.
  - En la pestaña **Delitos**, pulse **Reglas > Acciones > Correlación histórica**.
2. Seleccione un perfil y pulse **Ver historial**.
  - a) Si el estado de ejecución de correlación histórica es **Completado** y **Recuento de delitos** es 0, las reglas de perfil no han desencadenado delitos.

b) Si la ejecución de la correlación histórica ha creado delitos, en la columna **Recuento de delitos** pulse el enlace para ver una lista de los delitos que se han creado.

Si solo se ha creado un delito, se muestra el resumen de delitos.

3. En la columna **Catálogos**, pulse los enlaces para ver la lista de sucesos que coinciden completa o parcialmente con las reglas de perfil.

La columna **StartTime** en la lista de sucesos representa la hora en que QRadar ha recibido el suceso.

4. Pulse **Cerrar**.



## Capítulo 16. Integración de IBM X-Force

Los expertos de seguridad de IBM X-Force utilizan una serie de centros de datos internacionales para recopilar decenas de miles de ejemplos de programas maliciosos, para analizar páginas web y URLs y para ejecutar análisis para categorizar posibles direcciones IP y URLs maliciosos. Puede utilizar estos datos para identificar y remediar actividad no deseada en su entorno antes de que amenace la estabilidad de su red.

Por ejemplo, puede identificar y priorizar estos tipos de incidentes.

- Una serie de inicios de sesión intentados para un rango dinámico de direcciones IP
- Una conexión proxy anónima a un portal de Business Partner
- Una conexión entre un punto final interno y un mandato y control de botnet conocido
- Comunicación entre un punto final y un sitio distribución de programas maliciosos conocido

### X-Force datos en el panel de control

El widget **Internet Threat Information Center** del panel de control **Supervisión de amenazas y seguridad** utiliza datos de X-Force para proporcionarle avisos sobre problemas de seguridad, evaluaciones diarias sobre amenazas, noticias relacionadas con la seguridad y repositorios de amenazas.

El widget del panel de control utiliza un canal de información RSS para visualizar datos de X-Force en el widget del panel de control. QRadar Console debe tener acceso a internet para recibir datos del servidor de actualizaciones X-Force ([www.iss.net](http://www.iss.net)).

El panel de control utiliza cuatro imágenes de nivel de amenaza de AlertCon para proporcionar un indicador visual del nivel de amenaza actual.

*Tabla 40. Niveles de amenaza de AlertCon*

Nivel	Tipo	Descripción
1	Amenazas normales	Actividad ordinaria que compromete las redes no protegidas minutos u horas después de que QRadar se conecte a Internet.
2	Vigilancia aumentada	Vulnerabilidades o amenazas en línea para redes de sistemas que necesitan evaluación de vulnerabilidad y acciones correctoras.
3	Ataques centrados	Debilidades y vulnerabilidades específicas que son objeto de ataques de Internet y que necesitan una acción defensiva inmediata.
4	Amenazas catastróficas	Situaciones de seguridad críticas en una red que imponen una acción defensiva inmediata y centrada. Esta condición puede ser inminente o estar en curso.

Para obtener más información sobre el nivel de amenaza actual, pulse el enlace **Más información** para abrir la página **Actividad de amenaza actual** en el sitio web IBM X-Force Exchange.

Para ver un resumen de los avisos actuales, pulse el icono de flecha junto al aviso. Para investigar el aviso completo, pulse el enlace de aviso.

## Aplicación IBM Security Threat Content

---

La aplicación **IBM Security Threat Content** de IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub>) contiene reglas, bloques de construcción y propiedades personalizadas pensadas para su uso con X-Force.

Los datos de X-Force incluyen una lista de direcciones IP y URLs potencialmente maliciosos con una puntuación de amenaza correspondiente. Puede utilizar las reglas de X-Force para marcar automáticamente cualquier suceso de seguridad o cualesquiera datos de actividad de red que incluya las direcciones y para priorizar los incidentes antes de empezar a investigarlos.

La lista siguiente muestra ejemplos de los tipos de incidente que puede identificar mediante las reglas de X-Force:

- **when [IP de origen|destinationIP|anyIP] is part of any of the following [ubicaciones de red remota]**
- **when [esta propiedad de host] is categorized by X-Force as [Anonymization Servers|Botnet C&C|DynamicIPs|Malware|ScanningIPs|Spam] with confidence value [igual a] [esta cantidad]**
- **when [esta propiedad de URL] is categorized by X-Force as [Gambling|Auctions|Job Search|Alcohol|Social Networking|Dating]**

El administrador de QRadar debe instalar la aplicación **IBM Security Threat Content** para que las reglas aparezcan en el grupo **Amenazas** de la ventana **Lista de reglas**. Las reglas deben estar habilitadas para poder utilizarlas.

### Habilitación de reglas de X-Force en IBM QRadar

Al añadir la aplicación IBM Security Threat Content al sistema QRadar, se añaden reglas de X-Force a la **Lista de reglas**. Las reglas deben estar habilitadas para poder utilizarlas.

#### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas > Reglas**.
3. En el menú **Grupo**, pulse **Amenazas**.

La columna **Grupo** puede mostrar las reglas de legado y mejoradas. De forma predeterminada, las reglas de legado de X-Force están inhabilitadas. Sin embargo, puede ver las reglas de legado que están habilitadas. Utilice las reglas mejoradas más recientes en el grupo **Amenaza** y no las reglas de legado que utilizan las redes remotas.

4. Seleccione las reglas de **X-Force** en el grupo **Amenaza** y pulse **Acciones > Habilitar/inhabilitar**.

## Categorías de dirección IP y URL

---

X-Force Threat Intelligence categoriza la información de dirección IP y URL.

Las direcciones IP se agrupan en las categorías siguientes:

- Hosts de programas maliciosos
- Orígenes de correo no deseado
- Direcciones IP dinámicas
- Proxies anónimos
- Mandato y control de Botnet
- Exploración de direcciones IP

El canal de información de X-Force Threat Intelligence también categoriza direcciones URL. Por ejemplo, las direcciones URL pueden categorizarse como sitios de citas, apuestas o pornografía. Para ver la lista completa de categorías para la clasificación de URL, consulte el sitio web [IBM X-Force Exchange](https://exchange.xforce.ibmcloud.com/faq) (<https://exchange.xforce.ibmcloud.com/faq>).

## Búsqueda de información de direcciones IP y URL en X-Force Exchange

Utilice las opciones del menú contextual de IBM QRadar para buscar información sobre las direcciones IP y URL que se encuentra en IBM Security X-Force Exchange. Puede utilizar la información de las búsquedas, los delitos y las reglas de QRadar para investigar más o para añadir información sobre direcciones IP o URL a una recopilación de X-Force Exchange.

### Acerca de esta tarea

Puede proporcionar información pública o privada para hacer un seguimiento de los datos de las recopilaciones cuando investigue problemas de seguridad.

Una *recopilación* es un repositorio donde se almacena la información que se encuentra durante una investigación. Puede utilizar una recopilación para guardar informes, comentarios o cualquier otro contenido de X-Force Exchange. Un informe de X-Force Exchange contiene una versión del informe del momento en que se guardó y un enlace a la versión actual del informe. La recopilación contiene una sección que tiene un área de notas con estilo wiki en la que puede añadir comentarios que son relevantes para la recopilación.

Para obtener más información acerca de X-Force Exchange, consulte [X-Force Exchange](https://exchange.xforce.ibmcloud.com/) (https://exchange.xforce.ibmcloud.com/).

### Procedimiento

1. Para buscar una dirección IP en X-Force Exchange desde QRadar, siga estos pasos:
  - a) Seleccione la pestaña **Actividad de registro** o **Actividad de red**.
  - b) Pulse el botón derecho del ratón en la dirección IP que desea ver en X-Force Exchange y seleccione **Más opciones > Opciones de plugin > Búsqueda de X-Force Exchange** para abrir la interfaz de X-Force Exchange.
2. Para buscar un URL en X-Force Exchange desde QRadar, siga estos pasos:
  - a) Seleccione la pestaña **Delitos** o las ventanas de detalles de sucesos disponibles en **Delitos**.
  - b) Pulse el botón derecho del ratón en el URL que desea ver en X-Force Exchange y seleccione **Opciones de plugin > Búsqueda de X-Force Exchange** para abrir la interfaz de X-Force Exchange.

## Creación de una regla de categorización de URL para supervisar el acceso a determinados tipos de sitios web

Puede crear una regla que envíe una notificación de correo electrónico si los usuarios de la red interna acceden a direcciones de URL que están categorizadas como sitios web de apuestas.

### Antes de empezar

Para utilizar datos de X-Force en reglas, el administrador debe configurar QRadar para cargar datos de los servidores de X-Force.

Para crear una regla nueva, debe tener el permiso **Delitos > Mantener reglas personalizadas**.

### Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Acciones**, seleccione **Nueva regla de sucesos**.
4. Lea el texto introductorio en el asistente de reglas y pulse **Siguiente**.
5. Pulse **Sucesos** y pulse **Siguiente**.
6. En el recuadro de lista **Grupo de pruebas**, seleccione **X-Force Tests**.
7. Pulse el signo más (+) junto a la prueba **when URL (custom) is categorized by X-Force as one of the following categories**.

8. En el campo **especifique aquí el nombre de la regla** en el panel Regla, escriba un nombre exclusivo que desee asignar a esta regla.
9. En el recuadro de lista, seleccione **Local** o **Global**.
10. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.
  - a) Pulse **URL (personalizado)**.
  - b) Seleccione la propiedad de URL que contiene el URL que se ha extraído de la carga útil y pulse **Enviar**.
  - c) Pulse **una de las siguientes categorías**.
  - d) Seleccione **Gambling / Lottery** en las categorías de URL de X-Force, pulse **Añadir +** y pulse **Enviar**.
11. Para exportar la regla configurada como un componente básico para utilizarlo con otras reglas:
  - a) Pulse **Exportar como componente básico**.
  - b) Escriba un nombre exclusivo para este componente básico.
  - c) Pulse **Guardar**.
12. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla.
13. En el campo **Notas**, escriba una nota que desee incluir para esta regla y pulse **Siguiente**.
14. En la página **Respuestas de regla**, pulse **Correo electrónico** y escriba las direcciones de correo electrónico que recibirán la notificación.
15. Pulse **Siguiente**.
16. Si la regla es precisa, pulse **Finalizar**.

## Factor de confianza y reputación de dirección IP

---

Los datos de reputación de dirección IP se evalúan en función del tiempo que se ve y del volumen de mensajes o datos. X-Force categoriza los datos de reputación de dirección IP y asigna un factor de confianza de 0 a 100, donde 0 representa ninguna confianza y 100 representa la certeza. Por ejemplo, X-Force puede categorizar una dirección IP de origen como una IP de exploración con un factor de confianza de 75, que es un nivel de confianza moderadamente elevado.

### Determinación de un umbral

A modo de ejemplo, los mensajes de correo no deseado con una entrada de reputación de dirección IP de 0 indican que el tráfico de IP de origen no es correo no deseado mientras que una entrada de 100 indica que definitivamente se trata de tráfico de correo no deseado. Así, los valores inferiores a 50 indican menor probabilidad de que el mensaje sea correo no deseado y los valores superiores a 50 indican una mayor probabilidad de que el mensaje sea correo no deseado. Un valor de 50 o superior es el umbral para el que establecer una acción en una regla desencadenada.

Estas probabilidades están basadas en datos actuales basados en web que IBM Security X-Force Threat Intelligence recopila y analiza continuamente en todo el mundo, en centros de datos de X-Force. Conforme se recopilan los datos, el sistema valúa cuando correo no deseado se recibe de una dirección IP determinada o con qué frecuencia la dirección IP marcada está en la categoría de reputación de dirección IP. Cuantas más veces, mayor es la puntuación del sistema en el factor de confianza.

### Ajustar falsos positivos con el valor de factor de confianza

Utilice el factor de confianza para limitar el número de delitos creados por reglas desencadenadas. En función del nivel de protección que desea, puede ajustar los valores de confianza al nivel que mejor se ajuste a su entorno de red.

### Acerca de esta tarea

Cuando ajusta las reglas, considere una escala en la que 50 es el punto crítico. En activos de menor importancia, puede ponderar una regla de X-Force para que desencadene en un factor de confianza más elevado para categorías específicas, como por ejemplo correo no deseado. Por ejemplo, ajustar una regla a un factor de confianza de 75 significa que la regla se desencadena solo cuando X-Force ve una dirección IP con un factor de confianza igual o superior a 75. Este ajuste reduce el número de delitos generados en sistemas de prioridad más baja y activos no críticos. Sin embargo, un sistema importante o un activo de negocio crítico con un factor de confianza de 50 desencadena un delito en un nivel más bajo y reclama la atención sobre un problema más rápidamente.

Para la DMZ, elija un valor de confianza superior como ` por ejemplo 95% o superior. No es necesario investigar muchos delitos en este área. Con un nivel de confianza alto, es más probable que las direcciones IP coincidan con la categoría listada. Si hay un 95% de certidumbre de que un host esté proporcionando malware, debe saberlo.

Para áreas más seguras de la red, como por ejemplo una agrupación de servidores, baje el valor de confianza. Se identifican más amenazas potenciales y dedica menos esfuerzo a investigar porque la amenaza pertenece a un segmento de red específico.

Para un ajuste de falso positivo, gestione sus desencadenantes de regla por segmento. Busque en su infraestructura de red y decida qué activos necesitan un nivel de protección alto y qué activos no. Puede aplicar diferentes valores de confianza para los diferentes segmentos de red. Utilice los bloques básicos para agrupar las pruebas utilizada más habitualmente de modo que se puedan utilizar en reglas.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas > Reglas**.
3. Efectúe una doble pulsación sobre una regla para iniciar el asistente Regla.
4. En el recuadro de filtro, escriba lo siguiente:  
cuando esta propiedad de host está categorizada por X-Force como esta categoría con un valor de confianza igual a esta cantidad
5. Pulse el icono **Añadir prueba a regla (+)**.
6. En la sección Regla, pulse el enlace esta cantidad.
7. Especifique un valor de confianza.
8. Pulse **Enviar**.
9. Pulse **Finalizar** para salir del asistente Reglas.

## Buscar datos de IBM X-Force Exchange con criterios de búsqueda avanzados

Para consultas complejas, puede buscar y filtrar datos de X-Force Exchange mediante expresiones de Búsqueda avanzada.

### Acerca de esta tarea

Las búsquedas avanzadas devuelven datos de la pestaña **Actividad de registro** o **Actividad de red** en QRadar.

Las búsquedas de URL no se pueden devolver de la pestaña **Actividad de red** porque la información de URL la proporcionan los datos de suceso.

### Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas **Buscar**, seleccione **Búsqueda avanzada**.
3. Teclee una expresión de consulta de AQL.

**Nota:**

La tabla siguiente describe algunas expresiones de búsqueda comunes.

<i>Tabla 41. Expresiones de búsqueda avanzada de X-Force</i>	
<b>Descripción</b>	<b>Ejemplo</b>
Busca direcciones IP de origen cuyo factor de confianza es superior a 50.	<pre>select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)&gt;50</pre>
Búsquedas asociadas a un URL.	<pre>select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL</pre>
Búsquedas asociadas a una dirección IP de origen.	<pre>select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL</pre>

4. Pulse **Buscar**.

---

## Capítulo 17. Gestión de informes

Puede utilizar la pestaña **Informes** para crear, editar, distribuir y gestionar informes.

Unas opciones de creación de informes detalladas y flexibles satisfacen diversos estándares normativos como, por ejemplo, la conformidad con PCI.

Puede crear sus propios informes personalizados o utilizar informes predeterminados. Puede personalizar y cambiar el nombre de informes predeterminados y distribuirlos a otros usuarios.

La pestaña **Informes** puede necesitar un largo periodo de tiempo para renovarse si el sistema incluye muchos informes.

**Nota:** Si ejecuta Microsoft Exchange Server 5.5, es posible que aparezcan caracteres de tipos no disponibles en la línea del asunto de los informes enviados por correo electrónico. Para resolver este problema, descargue e instale el Service Pack 4 de Microsoft Exchange Server 5.5. Para obtener más información, póngase en contacto con el soporte de Microsoft.

### Consideraciones sobre el huso horario

Para asegurarse de que la característica de creación de informes utiliza la fecha y hora correctas para crear informes de datos, la sesión debe estar sincronizada con el huso horario.

Durante la instalación y configuración de los productos de QRadar, se configura el huso horario. Consulte con el administrador para asegurarse de que la sesión de QRadar está sincronizada con el huso horario.

### Permisos de la pestaña de informes

Los usuarios administrativos pueden ver todos los informes creados por otros usuarios.

Los usuarios no administrativos solo pueden ver los informes que ellos han creado o los informes compartidos por otros usuarios.

### Parámetros de la pestaña de informes

La pestaña **Informes** muestra una lista de informes personalizados y predeterminados.

En la pestaña **Informes**, puede ver información estadística acerca de la plantilla de informes, realizar acciones en las plantillas de informes, ver los informes generados y suprimir el contenido generado.

Si un informe no especifica una planificación de intervalo, debe generar manualmente el informe.

Puede pasar el puntero del ratón sobre cualquier informe para previsualizar un resumen de informe en una ayuda contextual. El resumen especifica la configuración del informe y el tipo de contenido que genera el informe.

---

## Diseño de informe

Un informe puede constar de varios elementos de datos y puede representar datos de red y de seguridad en diversos estilos, tales como tablas, gráficos de línea, gráficos circulares y gráficos de barras.

Al seleccionar el diseño de un informe, tenga en cuenta el tipo de informe que desea crear. Por ejemplo, no elija un contenedor de gráfico pequeño para un contenido de gráfico que muestra muchos objetos. Cada gráfico incluye una leyenda y una lista de redes de las que se deriva el contenido; elija un contenedor suficientemente grande para contener los datos. Para ver previamente cómo visualiza cada gráfico los datos, consulte Tipos de gráfico.

## Tipos de gráfico

Cuando se crea un informe, debe elegir un tipo de gráfico para cada gráfico que incluya en el informe. El tipo de gráfico determina cómo aparecen en el informe generado los datos y objetos de red. Puede utilizar cualquiera de los tipos de gráficos siguientes:

Tipo de gráfico	Descripción
Ninguno	Utilice esta opción si necesita un espacio en blanco en el informe. Si selecciona la opción Ninguno para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.
Vulnerabilidades de activos	Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM QRadar Vulnerability Manager.
Conexiones	Esta opción de gráfico solo se visualiza si ha adquirido IBM QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
Reglas de dispositivo	Esta opción de gráfico solo se visualiza si ha adquirido IBM QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
Objetos no utilizados de dispositivo	Esta opción de gráfico solo se visualiza si ha adquirido IBM QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación <i>IBM QRadar Risk Manager User Guide</i> .
Sucesos/Registros	Utilice este gráfico para ver información de suceso. Puede basar un gráfico en datos de búsquedas guardadas en la pestaña <b>Actividad de registro</b> . Puede configurar el gráfico para trazar datos durante un periodo de tiempo configurable para detectar tendencias de sucesos. Para obtener más información sobre las búsquedas guardadas, consulte <a href="#">Capítulo 12, “Búsquedas de sucesos y flujos”</a> , en la página 127.



Tabla 42. Tipos de gráfico (continuación)

Tipo de gráfico	Descripción
Orígenes de registro	Utilice este gráfico para exportar o informe sobre los orígenes de registro. Seleccione los orígenes de registro y los grupos de orígenes de registro que desea que aparezcan en el informe. Ordene los orígenes de registro por columnas de informe. Incluya orígenes de registro de los que no se ha informado durante un periodo de tiempo definido. Incluya orígenes de registro que se han creado en un periodo de tiempo especificado.
Flujos	Utilice este gráfico para ver información de flujo. Puede basar un gráfico en datos de búsquedas guardadas en la pestaña <b>Actividad de red</b> . Puede configurar el gráfico para trazar datos de flujo durante un periodo de tiempo configurable para detectar tendencias de flujo. Para obtener más información sobre las búsquedas guardadas, consulte Capítulo 12, “Búsquedas de sucesos y flujos”, en la página 127.
IP de destino principales	Utilice este gráfico para visualizar las direcciones IP de destino principales en las ubicaciones de red que seleccione.
Delitos principales	Utilice este gráfico para visualizar los delitos principales que se producen en el momento actual para las ubicaciones de red que seleccione.
Delitos a lo largo del tiempo	Utilice este gráfico para visualizar todos los delitos cuya hora de inicio está dentro de un intervalo de tiempo definido para las ubicaciones de red que seleccione.
IP de origen principales	Utilice este gráfico para visualizar y ordenar los principales orígenes de delito (direcciones IP) que atacan la red o los activos de la empresa.
Vulnerabilidades	La opción Vulnerabilidades solo se visualiza cuando se ha adquirido IBM QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación <i>Guía del usuario de IBM QRadar Vulnerability Manager</i> .

Tabla 43. Tipos de gráfico

Tipo de gráfico	Descripción
Ninguno	Utilice esta opción si necesita un espacio en blanco en el informe. Si selecciona la opción Ninguno para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.

Tabla 43. Tipos de gráfico (continuación)

Tipo de gráfico	Descripción
Vulnerabilidades de activos	Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM QRadar Vulnerability Manager.
Vulnerabilidades	La opción Vulnerabilidades solo se visualiza cuando se ha adquirido IBM QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación <i>Guía del usuario de IBM QRadar Vulnerability Manager</i> .

## Barra de herramientas de la pestaña de informes

Puede utilizar la barra de herramientas para realizar una serie de acciones en los informes.

La tabla siguiente identifica y describe las opciones de la barra de herramientas de Informes.

Tabla 44. Opciones de barra de herramientas de Informes

Opción	Descripción
Grupo	
Gestionar grupos	Pulse <b>Gestionar grupos</b> para gestionar <u>grupos de informes</u> . Mediante el uso de la característica <u>Gestionar grupos</u> , puede organizar los informes en grupos funcionales. Puede compartir los grupos de informes con otros usuarios.

Tabla 44. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Acciones	<p>Pulse <b>Acciones</b> para realizar las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• <b>Crear:</b> Seleccione esta opción para crear un informe nuevo.</li> <li>• <b>Editar:</b> Seleccione esta opción para editar el informe seleccionado. También puede efectuar una doble pulsación en un informe para editar el contenido.</li> <li>• <b>Duplicar:</b> Seleccione esta opción para <u>duplicar o renombrar</u> el informe seleccionado.</li> <li>• <b>Asignar grupos:</b> Seleccione esta opción para asignar el informe seleccionado a un <u>grupo de informes</u>.</li> <li>• <b>Compartir:</b> Seleccione esta opción para compartir el informe seleccionado con otros usuarios. Debe tener privilegios administrativos para <u>compartir informes</u>.</li> <li>• <b>Conmutar planificación:</b> Seleccione esta opción para conmutar el informe seleccionado al estado Activo o Inactivo.</li> <li>• <b>Ejecutar informe:</b> Seleccione esta opción para <u>generar el informe</u> seleccionado. Para generar varios informes, mantenga pulsada la tecla Control y pulse los informes que desea generar.</li> <li>• <b>Ejecutar informe para datos en bruto:</b> Seleccione esta opción para generar el informe seleccionado utilizando datos en bruto. Esta opción es útil si desea generar un informe antes de que estén disponibles los datos acumulados necesarios. Por ejemplo, si desea ejecutar un informe semanal antes de que haya transcurrido una semana completa desde que creó el informe, puede generar el informe utilizando esta opción.</li> <li>• <b>Suprimir informe:</b> Seleccione esta opción para suprimir el informe seleccionado. Para suprimir varios informes, mantenga pulsada la tecla Control y pulse los informes que desea suprimir.</li> <li>• <b>Suprimir contenido generado:</b> Seleccione esta opción para suprimir todo el contenido generado para las filas seleccionadas. Para suprimir varios informes generados, mantenga pulsada la tecla Control y pulse los informes generados que desea suprimir.</li> </ul>
Ocultar informes inactivos	<p>Seleccione este recuadro de selección para ocultar las plantillas de informes inactivos. La pestaña <b>Informes</b> se renueva automáticamente y muestra solo los informes de activos. Quite la marca del recuadro de selección para mostrar los informes inactivos ocultos.</p>

Tabla 44. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Buscar en informes	<p>Escriba los criterios de búsqueda en el campo <b>Buscar en informes</b> y pulse el icono <b>Buscar en informes</b>. Se ejecuta una búsqueda en los parámetros siguientes para determinar cuáles coinciden con los criterios especificados:</p> <ul style="list-style-type: none"> <li>• Título de informe</li> <li>• Descripción de informe</li> <li>• Grupo de informes</li> <li>• Grupos de informes</li> <li>• Nombre de usuario de autor de informes</li> </ul>

## Tipos de gráfico

Cada tipo de diagrama soporta varios tipos de gráfico que puede utilizar para visualizar datos.

Los archivos de configuración de red determinan los colores que los diagramas utilizan para representar el tráfico de red. Cada dirección IP se representa mediante un color exclusivo. La tabla siguiente proporciona ejemplos de cómo se utilizan los datos de red y de seguridad en los diagramas. La tabla describe los tipos de diagrama que están disponibles para cada tipo de gráfico.

Tabla 45. Tipos de gráfico

Tipo de gráfico	Tipos de diagrama disponibles
Línea	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• Conexiones</li> <li>• Vulnerabilidades</li> </ul>
Línea apilada	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• Conexiones</li> <li>• Vulnerabilidades</li> </ul>
Barra	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• Conexiones de vulnerabilidades de activos</li> <li>• Conexiones</li> <li>• Vulnerabilidades</li> </ul>
Barra horizontal	<ul style="list-style-type: none"> <li>• IP de origen principales</li> <li>• Delitos principales</li> <li>• Delitos a lo largo del tiempo</li> <li>• IP de destino principales</li> </ul>

Tabla 45. Tipos de gráfico (continuación)

Tipo de gráfico	Tipos de diagrama disponibles
Barra apilada	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• Conexiones</li> </ul>
Circular	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• Vulnerabilidades de activos</li> <li>• Conexiones</li> <li>• Vulnerabilidades</li> </ul>
Tabla	<ul style="list-style-type: none"> <li>• Sucesos/Registros</li> <li>• Flujos</li> <li>• IP de origen principales</li> <li>• Delitos principales</li> <li>• Delitos a lo largo del tiempo</li> <li>• IP de destino principales</li> <li>• Conexiones</li> <li>• Vulnerabilidades</li> </ul> <p>Para visualizar el contenido en una tabla, debe diseñar el informe con un contenedor de ancho de página completa.</p>
Tabla de agregación	<p>Disponible con el diagrama de Vulnerabilidades de activos.</p> <p>Para visualizar el contenido en una tabla, debe diseñar el informe con un contenedor de ancho de página completa.</p>

Están disponibles los siguientes tipos de gráfico para informes de QRadar Log Manager:

- Línea
- Línea apilada
- Barra
- Barra apilada
- Circular
- Tabla

**Nota:** Cuando crea informes de gráficos de barras y barras apiladas, la leyenda se presenta en formato fijo y las barras o las secciones de barras se representan por etiquetas codificadas por colores en la mayoría de los casos. Si selecciona el tiempo como el valor del eje x, puede crear intervalos de tiempo en el eje x.

## Creación de informes personalizados

Utilice el Asistente de informes para crear un nuevo informe y personalizarlo.

### Antes de empezar

Debe tener los permisos de red apropiados para compartir un informe generado con otros usuarios.

Para obtener más información sobre los permisos, consulte la publicación *Guía de administración de IBM QRadar*.

### Acerca de esta tarea

El Asistente de informes proporciona una guía paso a paso sobre cómo diseñar, planificar y generar informes.

El asistente utiliza los siguientes elementos clave para ayudarle a crear un informe:

- **Diseño:** Posición y tamaño de cada contenedor
- **Contenedor:** Marcador para el contenido presentado
- **Contenido:** Definición del gráfico que se coloca en el contenedor

Después de crear un informe que se genera semanal o mensualmente, debe transcurrir el tiempo planificado antes de que el informe generado devuelva resultados. Para un informe planificado, debe esperar el periodo de tiempo planificado para que se creen los resultados. Por ejemplo, una búsqueda semanal necesita siete días para crear los datos. Esta búsqueda devolverá resultados tras siete días.

Cuando especifique el formato de salida para el informe, tenga en cuenta que el tamaño de archivo de los informes generados puede tener de uno a dos megabytes, dependiendo del formato de salida seleccionado. El formato PDF es menor de tamaño y no utiliza una gran cantidad de espacio de almacenamiento de disco.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el cuadro de lista **Acciones**, seleccione **Crear**.
3. En la ventana **Bienvenido al Asistente de informes**, pulse **Siguiente**.
4. Seleccione una de las opciones siguientes:

Opción	Descripción
<b>Manualmente</b>	De forma predeterminada, el informe se genera una vez. Puede generar el informe con la frecuencia que desee.
<b>Cada hora</b>	Planifica que el informe se genere al final de cada hora. Se utilizan los datos de la hora anterior.  En los recuadros de lista, seleccione un intervalo de tiempo para empezar y finalizar el ciclo del informe. Se genera un informe para cada hora dentro de este intervalo de tiempo. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m. para los campos <b>Desde</b> y <b>Hasta</b> .
<b>Diariamente</b>	Planifica que el informe se genere al final de cada día. Se utilizan los datos del día anterior.  En los cuadros de lista, seleccione la hora y los días de la semana que desea que se ejecute el informe.
<b>Semanalmente</b>	Planifica que el informe se genere semanalmente utilizando los datos de la semana natural anterior, de lunes a domingo.  Seleccione el día que desea generar el informe. El valor predeterminado es Lunes. En el recuadro de lista, seleccione una hora para empezar el ciclo del informe. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.
<b>Mensualmente</b>	Planifica el informe para generar mensualmente utilizando los datos del mes natural anterior.

Opción	Descripción
	En el recuadro de lista, seleccione la fecha en la que desea generar el informe. El valor predeterminado es el primer día del mes. Seleccione una hora para empezar el ciclo del informe. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.

5. En el panel **Permitir que este informe se genere manualmente**, seleccione **Sí** o **No**.

6. Configure el diseño del informe:

- En el recuadro de lista **Orientación**, seleccione **Vertical** u **Horizontal** para la orientación de página.
- Seleccione una de las seis opciones de diseño que se muestran en el asistente de informes.
- Pulse **Siguiente**.

7. Especifique valores para los parámetros siguientes:

Parámetro	Valores
<b>Título de informe</b>	El título puede tener una longitud máxima de 100 caracteres. No utilice caracteres especiales.
<b>Logotipo</b>	En el recuadro de lista, seleccione un logotipo.
<b>Opciones de paginación</b>	En el recuadro de lista, seleccione la ubicación en el informe en la que se aparecerán los números de página. Puede optar por no mostrar números de página.
<b>Clasificación de informe</b>	Escriba una clasificación para este informe. Puede escribir un máximo de 75 caracteres. Puede utilizar espacios iniciales, caracteres especiales y caracteres de doble byte. La clasificación del informe se muestra en la cabecera y el pie de página del informe. Si lo desea, puede clasificar el informe como <b>confidencial</b> , <b>muy confidencial</b> , <b>sensible</b> o <b>interno</b> .

8. Configure cada contenedor en el informe:

- En el recuadro de lista **Tipo de gráfico**, seleccione un tipo de gráfico.
- En la ventana **Detalles de contenedor**, configure los parámetros de gráfico.

**Nota:** También puede crear búsquedas guardadas de activos. En el cuadro de lista **Buscar para utilizar**, seleccione la búsqueda guardada.

- Pulse **Guardar detalles de contenedor**.
- Si ha seleccionado más de un contenedor, repita los pasos del a al c.
- Pulse **Siguiente**.

9. Vea previamente la página **Vista previa del diseño** y, a continuación, pulse **Siguiente**.

10. Marque los recuadros de selección para los formatos de informe que desea generar y pulse **Siguiente**.

**Importante:** Extensible Markup Language solo está disponible para tablas.

11. Seleccione los canales de distribución para el informe y, a continuación, pulse **Siguiente**. Las opciones incluyen los siguientes canales de distribución:

Opción	Descripción
<b>Consola de informes</b>	Marque este recuadro de selección para enviar el informe generado a la pestaña <b>Informes</b> . <b>Consola de informes</b> es el canal de distribución predeterminado.
<b>Seleccione los usuarios que deben poder ver el informe generado.</b>	Esta opción se muestra después de seleccionar el recuadro de selección <b>Consola de informes</b> .

Opción	Descripción
	En la lista de usuarios, seleccione los usuarios a los que desea otorgar permiso para ver los informes generados.
<b>Seleccionar todos los usuarios</b>	Esta opción solo se visualiza después de seleccionar el recuadro de selección <b>Consola de informes</b> . Marque este recuadro de selección si desea otorgar permiso a todos los usuarios para ver los informes generados.  Debe tener permisos de red apropiados para compartir el informe generado con otros usuarios.
<b>Correo electrónico</b>	Marque este recuadro de selección si desea distribuir el informe generado por correo electrónico.
<b>Escriba la dirección o direcciones de correo electrónico de destino del informe:</b>	Esta opción solo se visualiza después de seleccionar el recuadro de selección <b>Correo electrónico</b> .  Escriba la dirección de correo electrónico para cada destinatario de informe generado; separe una lista de direcciones de correo electrónico con comas. El máximo de caracteres para este parámetro es de 255.  Los destinatarios de correo electrónico reciben este correo electrónico desde no_reply_reports@qradar.
<b>Incluir informe como archivo adjunto (solo no HTML)</b>	Esta opción solo se visualiza después de seleccionar el recuadro de selección <b>Correo electrónico</b> . Marque este recuadro de selección para enviar el informe generado como un archivo adjunto.
<b>Incluir enlace a consola de informes</b>	Esta opción solo se visualiza después de seleccionar el recuadro de selección <b>Correo electrónico</b> . Marque este recuadro de selección para incluir un enlace a la Consola de informes en el correo electrónico.

12. En la página **Se está terminando**, entre valores para los parámetros siguientes.

Opción	Descripción
<b>Descripción de informe</b>	Escriba una descripción para este informe. La descripción se visualiza en la página <b>Resumen de informe</b> y en el correo electrónico de distribución de informes generados.
<b>Seleccione los grupos a los que deba pertenecer este informe</b>	Seleccione los grupos a los que desea asignar este informe. Para obtener más información sobre grupos, consulte <a href="#">Grupos de informes</a> .
<b>¿Desea ejecutar el informe ahora?</b>	Marque este recuadro de selección si desea generar el informe cuando se complete el asistente. De manera predeterminada, el recuadro de selección aparece seleccionado.

13. Pulse **Siguiente** para ver el resumen de informe.

14. En la página **Resumen de informe**, seleccione las pestañas disponibles en el informe de resumen para previsualizar la configuración de informe.

## Resultados

El informe se genera inmediatamente. Si ha borrado el recuadro de selección **¿Desea ejecutar el informe ahora?** en la página final del asistente, el informe se guarda y se genera a la hora planificada. El título de informe es el título predeterminado para el informe generado. Si reconfigura un informe para entrar título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.



## Información relacionada

[Creación de informes en QRadar SIEM](#)

## Edición de un informe

---

Utilizando el asistente de informes, puede editar cualquier informe personalizado o predeterminado para cambiarlo.

### Acerca de esta tarea

Puede utilizar o personalizar un número significativo de informes predeterminados. La pestaña **Informes** predeterminada visualiza la lista de informes. Cada informe captura y visualiza los datos existentes.

**Nota:** Cuando personaliza un informe planificado para que se genere manualmente, seleccione el intervalo de tiempo **Fecha de finalización** antes de seleccionar el valor de **Fecha de inicio**.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Efectúe una doble pulsación en el informe que desea personalizar.
3. En el asistente de informes, cambie los parámetros para personalizar el informe para generar el contenido que necesita.

### Resultados

Si reconfigura un informe para entrar título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.

## Visualización de informes generados

---

En la pestaña **Informes**, se visualiza un icono en la columna **Formatos** si un informe ha generado contenido. Puede pulsar el icono para ver el informe.

### Acerca de esta tarea

Cuando un informe ha generado contenido, la columna **Informes generados** visualiza un recuadro de lista. El recuadro de lista muestra todo el contenido generado, que se organiza por la indicación de fecha y hora del informe. Los informes más recientes se muestran en la parte superior de la lista. Si un informe no tiene ningún contenido generado, se visualiza el valor **Ninguno** en la columna **Informes generados**.

Los iconos que representan el formato del informe generado se visualizan en la columna **Formatos**.

Los informes pueden generarse en los formatos PDF, HTML, XML y XLS.

**Nota:** Los formatos XML y XLS solo están disponibles para los informes que utilizan un formato de tabla de un solo gráfico (vertical u horizontal).

Puede ver solo los informes a los que se le ha dado acceso desde el administrador. Los usuarios administrativos pueden acceder a todos los informes.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el recuadro de lista de la columna **Informes generados**, seleccione la indicación de fecha y hora del informe desea ver.
3. Pulse el icono correspondiente al formato que desea ver.

## Supresión de contenido generado

---

Cuando suprime el contenido generado, todos los informes que se han generado a partir de la plantilla de informe se suprimen, pero la plantilla de informe se conserva.

### Procedimiento

1. Pulse la pestaña **Informe**.
2. Seleccione los informes para los que desea suprimir el contenido generado.
3. En el recuadro de lista **Acciones**, pulse **Suprimir contenido generado**.

## Generación manual de un informe

---

Un informe puede configurarse para que se genere automáticamente, sin embargo, el usuario puede generar manualmente un informe en cualquier momento.

### Acerca de esta tarea

Mientras se genera un informe, la columna Próxima hora de ejecución visualiza uno de los tres mensajes siguientes:

- **Generando:** El informe se está generando.
- **En cola (posición en la cola):** El informe se pone en cola para generarse. El mensaje indica la posición en la que está el informe en la cola. Por ejemplo, 1 de 3.
- **(x hora(s) x min(s) y seg(s)):** Está planificado que el informe se ejecute. El mensaje es un temporizador de cuenta atrás que especifica cuándo se ejecutará el informe la próxima vez.

Puede seleccionar el icono **Renovar** para renovar la vista, incluida la información de la columna **Próxima hora de ejecución**.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea generar.
3. Pulse **Ejecutar informe**.

### Qué hacer a continuación

Una vez que se ha generado el informe, puede [ver el informe generado](#) desde la columna Informes generados.

## Duplicación de un informe

---

Para crear un informe que se parezca detenidamente a un informe existente, puede duplicar el informe que desea modelar y, a continuación, personalizarlo.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea duplicar.
3. En el recuadro de lista **Acciones**, pulse **Duplicar**.
4. Escriba un nuevo nombre, sin espacios, para el informe.

### Qué hacer a continuación

Puede [personalizar](#) el informe duplicado.

## Compartición de un informe

---

Puede compartir informes con otros usuarios. Cuando se comparte un informe, se proporciona una copia del informe seleccionado a otro usuario para editarlo o planificarlo.

### Acerca de esta tarea

Las actualizaciones que el usuario realiza en un informe compartido no afectan a la versión original del informe.

Debe tener privilegios administrativos para compartir informes. Además, para que un usuario nuevo vea y acceda a los informes, un usuario administrativo debe compartir todos los informes necesarios con el nuevo usuario.

Solo puede compartir el informe con los usuarios que tienen el acceso adecuado.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione los informes que desea compartir.
3. En el recuadro de lista **Acciones**, pulse **Compartir**.
4. En la lista de usuarios, seleccione los usuarios con los que desea compartir este informe.

## Creación de marca de informes

---

Para marcar de informes, puede importar logotipos e imágenes específicas. Para marcar informes con logotipos personalizados, debe cargar y configurar los logotipos antes de empezar a utilizar el asistente de informes.

### Antes de empezar

Asegúrese de que el gráfico que desea utilizar tiene 144 x 50 píxeles con un fondo en blanco.

Para asegurarse de que el navegador visualice el nuevo logotipo, borre la caché de navegador.

### Acerca de esta tarea

La creación de marcas de informe es beneficiosa para la empresa cuando se soporta más de un logotipo. Cuando se carga una imagen, esta imagen se guarda de forma automática en formato PNG (Portable Network Graphic).

Cuando se carga una nueva imagen y se establece la imagen como valor predeterminado, la nueva imagen predeterminada no se aplica a los informes que se han generado anteriormente. Para actualizar el logotipo en informes generados previamente es necesario generar manualmente contenido nuevo desde el informe.

Si carga una imagen que tiene una longitud mayor que la que puede soportar la cabecera del informe, la imagen se redimensiona automáticamente para ajustarse a la cabecera; esto tiene aproximadamente una altura de 50 píxeles.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el menú de navegación, pulse **Creación de una identidad visual**.
3. Pulse **Examinar** para examinar los archivos que están ubicados en el sistema.
4. Seleccione el archivo que contiene el logotipo que desea cargar. Pulse **Abrir**.
5. Pulse **Cargar imagen**.

6. Seleccione el logotipo que desea utilizar como valor predeterminado y pulse **Establecer imagen predeterminada**.

## Grupos de informes

---

Los informes pueden ordenarse en grupos funcionales. Si se categorizan los informes por grupos, puede organizar y buscar informes de forma eficiente.

Por ejemplo, puede ver todos los informes relacionados con la conformidad con el estándar PCIDSS (Payment Card Industry Data Security Standard).

De forma predeterminada, la pestaña **Informes** muestra la lista de todos los informes, sin embargo, puede categorizar los informes en grupos tales como:

- Conformidad
- Ejecutivo
- Orígenes de registro
- Gestión de red
- Seguridad
- VoIP
- Otros

Cuando se crea un informe nuevo, se puede asignar el informe a un grupo existente o crear un grupo nuevo. Debe tener acceso administrativo para crear, editar o suprimir grupos.

Para obtener más información sobre los roles de usuario, consulte la publicación *Guía de administración de IBM QRadar*.

### Creación de un grupo de informes

Puede crear grupos nuevos.

#### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. Utilizando el árbol de navegación, seleccione el grupo en el que desea crear un nuevo grupo.
4. Pulse **Grupo nuevo**.
5. Escriba valores para los parámetros siguientes:
  - **Nombre:** Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
  - **Descripción:** Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
6. Pulse **Aceptar**.
7. Para cambiar la ubicación del nuevo grupo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.
8. Cierre la ventana **Grupos de informes**.

### Edición de un grupo

Puede editar un grupo de informes para cambiar el nombre o la descripción.

#### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.

3. En el árbol de navegación, seleccione el grupo que desea editar.
4. Pulse **Editar**.
5. Actualice los valores de los parámetros, según sea necesario:
  - **Nombre:** Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
  - **Descripción:** Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud. Este campo es opcional.
6. Pulse **Aceptar**.
7. Cierre la ventana **Grupos de informes**.

## Compartición de grupos de informes

Puede compartir los grupos de informes con otros usuarios.

### Antes de empezar

Debe tener permisos administrativos para compartir un grupo de informes con otros usuarios.

Para obtener más información sobre los permisos, consulte la publicación *Guía de administración de IBM QRadar*.

No puede utilizar la herramienta de gestión de contenido (CMT) para compartir grupos de informes.

Para obtener más información sobre la herramienta CMT, consulte la publicación *Guía de administración de IBM QRadar*.

### Acerca de esta tarea

En la ventana **Grupos de informes**, los usuarios compartidos pueden ver el grupo de informes en la lista de informes.

Para ver un informe generado, el usuario debe tener permiso para ver el informe.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. En la ventana **Informes**, pulse **Gestionar grupos**.
3. En la ventana **Grupos de informes**, seleccione el grupo de informes que desea compartir y pulse **Compartir**.
4. En la ventana **Opciones para compartir**, seleccione una de las opciones siguientes.

Opción	Descripción
<b>Valor predeterminado (heredar del padre)</b>	El grupo de informes no está compartido. Todos los grupos de informes copiados o todos los informes generados permanecen en la lista de informes del usuario. A cada informe del grupo se le asignan todas las opciones de compartición de informe padre que se hayan configurado.
<b>Compartir con todos</b>	El grupo de informes se comparte con todos los usuarios.
<b>Compartir con usuarios que coinciden con los criterios siguientes...</b>	El grupo de informes se comparte con usuarios determinados. <b>Roles de usuario</b> Efectúe una selección de la lista de roles de usuario y pulse el icono añadir (+).

Opción	Descripción
	<b>Perfiles de seguridad</b> Efectúe una selección de la lista de perfiles de seguridad y pulse el icono añadir (+).

5. Pulse **Guardar**.

### Resultados

En la ventana **Grupos de informes**, los usuarios compartidos ven el grupo de informes en la lista de informes. Los informes generados muestran el contenido en función del valor del perfil de seguridad.

### Tareas relacionadas

“Creación de informes personalizados” en la página 219

Utilice el Asistente de informes para crear un nuevo informe y personalizarlo.

## Asignar un informe a un grupo

Puede utilizar la opción **Asignar grupos** para asignar un informe a otro grupo.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea asignar a un grupo.
3. En el recuadro de lista **Acciones**, seleccione **Asignar grupos**.
4. En la lista **Grupos de elementos**, seleccione el recuadro de selección del grupo que desee asignar a este informe.
5. Pulse **Asignar grupos**.

## Copia de un informe en otro grupo

Utilice el icono **Copiar** para copiar un informe en uno o más grupos de informes.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, seleccione el informe que desea copiar.
4. Pulse **Copiar**.
5. Seleccione el grupo o los grupos en los que desea copiar el informe.
6. Pulse **Asignar grupos**.
7. Cierre la ventana **Grupos de informes**.

## Eliminación de un informe

Utilice el icono **Eliminar** para eliminar un informe de un grupo.

### Acerca de esta tarea

Cuando se elimina un informe de un grupo, el informe sigue existiendo en la pestaña **Informes**. El informe no se elimina del sistema.

### Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, vaya a la carpeta que contiene el informe que desea eliminar.
4. En la lista de grupos, seleccione el informe que desea eliminar.

5. Pulse **Eliminar**.
6. Pulse **Aceptar**.
7. Cierre la ventana **Grupos de informes**.





## Avisos

---

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Pero corresponde al usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 EE.UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se realizan cambios en la información incluida en este documento; estos cambios se incorporarán en las nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan solo para la comodidad del usuario y no constituyen un aval de estos sitios web. Los materiales de estos sitios web no forman parte de los materiales de IBM para este producto, y el uso que se haga de estos sitios web será responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione de cualquier modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los licenciarios de este programa que deseen obtener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, se deben poner en contacto con:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119

Armonk, NY 10504-1785  
EE.UU.

Esta información puede estar disponible, de acuerdo con los términos y condiciones apropiados, incluido en algunos casos el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento y los ejemplos de clientes citados se presentan solamente a efectos ilustrativos. Los resultados de rendimiento reales pueden variar en función de las configuraciones y las condiciones operativas específicas.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las consultas acerca de prestaciones de productos que no son de IBM se deben dirigir a los proveedores de esos productos.

Las declaraciones relativas a la dirección o intenciones futuras de IBM pueden cambiar o ser retiradas sin previo aviso, y solo representan propósitos y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres reales de personas o empresas es pura coincidencia.

## Marcas registradas

---

IBM, el logotipo de IBM e [ibm.com](http://ibm.com) son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o de sus filiales.



Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

## Términos y condiciones de la documentación de producto

---

Se otorga permiso para el uso de estas publicaciones si se cumplen estos términos y condiciones.

### Aplicabilidad

Estos términos y condiciones se añaden a los términos de uso del sitio web de IBM.

## Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre que se conserven todos los avisos sobre derechos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni de partes de las mismas, ni reproducirlas, distribuirlas o visualizarlas, sin el consentimiento expreso de IBM.

## Uso comercial

Puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de la empresa a condición de que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni de partes de las mismas, ni reproducirlas, distribuirlas o visualizarlas fuera de la empresa, sin el consentimiento expreso de IBM.

## Derechos

Salvo lo aquí permitido de forma expresa, no se conceden otros permisos, licencias o derechos, ni implícitos ni explícitos, para las publicaciones o cualquier información, datos software u otra propiedad intelectual que en ellas se incluya.

IBM se reserva el derecho de retirar los permisos que se hayan proporcionado siempre que, bajo su discreción, el uso de las publicaciones sea perjudicial para sus intereses o, según determine IBM, no se estén siguiendo adecuadamente las instrucciones detalladas anteriormente.

No se puede descargar, exportar o reexportar si no es en total cumplimiento con todas las leyes y reglamentos aplicables, incluidas las leyes y reglamentos de los EE.UU. en materia de exportación.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPLÍCITAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO INFRACCIÓN Y ADECUACIÓN A UN FIN DETERMINADO.

## Declaración de privacidad en línea de IBM

---

Los productos de software de IBM, incluido el software ofrecido como soluciones de servicio (“Ofertas de software”), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se describe información específica sobre la utilización de cookies por parte de esta oferta.

Dependiendo de las configuraciones desplegadas, esta oferta de software puede utilizar cookies de sesión que recogen el ID de sesión de cada usuario con fines de gestión y autenticación de sesiones. Estos cookies se pueden inhabilitar, pero si se inhabilitan también se pierde la función que los cookies hacen posible.

Si las configuraciones desplegadas para esta oferta de software le proporcionan como cliente la capacidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, incluido cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías, incluidas las cookies, para estos fines, consulte la política de privacidad de IBM en <http://www.ibm.com/privacy> y la declaración de privacidad en línea de IBM en <http://www.ibm.com/privacy/details/>, la sección titulada “Cookies, Web Beacons and Other Technologies”.

## Reglamento general de protección de datos

---

Los clientes son responsables de garantizar que cumplen diversas normativas y leyes, incluido el Reglamento general de protección de datos de la Unión Europea. Los clientes son los únicos responsables de obtener asesoramiento legal competente respecto a la identificación y la interpretación de cualquier normativa y ley que pueda afectar a los negocios de los clientes y a cualquier acción que los clientes puedan deber emprender para cumplir con dichas normativas y leyes. Los productos, los servicios y otras prestaciones descritas en este documento no son adecuados para todas las situaciones de los clientes y su disponibilidad puede estar restringida. IBM no proporciona asesoramiento legal, contable ni de auditoría ni garantiza que sus servicios o productos vayan a garantizar que los clientes cumplan cualquier normativa o ley.

Puede obtener más información sobre la preparación para el cumplimiento del Reglamento general de protección de datos de IBM, así como de nuestras prestaciones y ofertas en relación con el Reglamento general de protección de datos aquí: <https://ibm.com/gdpr>

# Glosario

---

Este glosario incluye términos y definiciones para productos y software de IBM QRadar SIEM.

En este glosario se utilizan las siguientes referencias cruzadas:

- Véase le remite de un término no preferido al término preferido o de un acrónimo o abreviatura a la forma completa.
- Véase *también* le remite a un término relacionado u opuesto.

Para otros términos y definiciones, consulte el [sitio web de terminología de IBM](#) (se abre en una ventana nueva).

## A

---

### **acumulador**

Registro en el que un operando de una operación se puede almacenar y posteriormente sustituir por el resultado de esa operación.

### **sistema activo**

En un clúster de alta disponibilidad (HA), sistema que tiene todos los servicios en ejecución.

### **Protocolo de resolución de direcciones (ARP)**

Protocolo que correlaciona dinámicamente una dirección IP con una dirección de adaptador de red en una red de área local.

### **compartimiento administrativo**

Recurso de red que se oculta a los usuarios sin privilegios administrativos. Los compartimientos administrativos proporcionan a los administradores acceso a todos los recursos en un sistema de red.

### **anomalía**

Desviación del comportamiento esperado de la red.

### **firma de aplicación**

Conjunto exclusivo de características que se derivan mediante el examen de la carga útil de paquete y, a continuación, se utilizan para identificar una aplicación específica.

### **ARP**

Véase [Protocolo de resolución de direcciones](#).

### **Redirección de ARP**

Método ARP para notificar al host si existe un problema en una red.

### **ASN**

Véase [número de sistema autónomo](#).

### **activo**

Objeto gestionable que se despliega o se tiene previsto desplegar en un entorno operativo.

### **número de sistema autónomo (ASN)**

En TCP/IP, número asignado a un sistema autónomo por la misma autoridad central que asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automáticos distingan los sistemas autónomos.

## B

---

### **comportamiento**

Efectos observables de una operación o suceso, incluidos los resultados.

### **interfaz vinculada**

Véase [agregación de enlaces](#).

**ráfaga**

Incremento brusco repentino en la tasa de sucesos o flujos entrantes de modo que se supera el límite de la tasa de sucesos o flujos con licencia.

**C**

---

**CIDR**

Véase [Classless Inter-Domain Routing](#).

**Classless Inter-Domain Routing (CIDR)**

Método para añadir direcciones de Protocolo Internet (IP) de clase C. Las direcciones se proporcionan a los proveedores de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y hacen que haya más direcciones IP disponibles en las organizaciones.

**cliente**

Programa de software o sistema que solicita servicios de un servidor.

**dirección IP virtual de clúster**

Dirección IP que se comparte entre el host primario o secundario y el clúster de alta disponibilidad.

**intervalo de fusión**

Intervalo en el que se empaquetan los sucesos. El empaquetado de sucesos se produce a intervalos de 10 segundos y empieza con el primer suceso que no coincide con ningún suceso de fusión simultánea. En el intervalo de fusión, los tres primeros sucesos coincidentes se empaquetan y envían al procesador de sucesos.

**Common Vulnerability Scoring System (CVSS)**

Sistema de puntuación mediante el cual se mide la gravedad de una vulnerabilidad.

**consola**

Estación de pantalla en la que un operador puede controlar y observar el funcionamiento del sistema.

**captura de contenido**

Proceso que captura una cantidad configurable de carga útil y, a continuación, almacena los datos en un registro de flujo.

**credencial**

Conjunto de información que otorga a un usuario o proceso determinados derechos de acceso.

**credibilidad**

Calificación numérica entre 0 y 10 que se utiliza para determinar la integridad de un suceso o un delito. La credibilidad aumenta a medida que varios orígenes informan el mismo suceso o delito.

**CVSS**

Véase [Common Vulnerability Scoring System](#).

**D**

---

**objeto de hoja de base de datos**

Nodo u objeto de terminal en una jerarquía de base de datos.

**punto de datos**

Valor calculado de una medida en un punto en el tiempo.

**Módulo de soporte de dispositivo (DSM)**

Archivo de configuración que analiza los sucesos recibidos de varios orígenes de registro y los convierte a un formato de taxonomía estándar que puede visualizarse como salida.

**DHCP**

Véase [Protocolo de configuración dinámica de hosts](#).

**DNS**

Véase [Sistema de nombres de dominio](#).

**Sistema de nombres de dominio (DNS)**

Sistema de base de datos distribuida que correlaciona nombres de dominio con direcciones IP.

**DSM**

Véase [Módulo de soporte de dispositivos](#).

**flujo duplicado**

Varias instancias de la misma transmisión de datos recibida de orígenes de flujo diferentes.

**Protocolo de configuración dinámica de hosts (DHCP)**

Protocolo de comunicación que se utiliza para gestionar de forma central información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a sistemas de una red.

---

**E****cifrado**

En seguridad de sistemas, proceso de transformación de datos a un formato ininteligible de manera que los datos originales no se puedan obtener o solo se puedan obtener utilizando un proceso de decodificación.

**punto final**

Dirección de una API o un servicio en un entorno. Una API expone un punto final y al mismo tiempo invoca los puntos finales de otros servicios.

**dispositivo de exploración externa**

Máquina que está conectada a la red para recopilar información de vulnerabilidad sobre los activos de la red.

---

**F****falso positivo**

Un suceso o flujo que el usuario puede decidir que no debe crear un delito, o un delito que el usuario decide que no es un incidente de seguridad.

**flujo**

Transmisión única de datos que pasan a través de un enlace durante una conversación.

**registro de flujo**

Colección de registros de flujo.

**orígenes de flujo**

Origen del que se captura el flujo. Un origen de flujo se clasifica como interno cuando el flujo procede del hardware instalado en un host gestionado o se clasifica como externo cuando el flujo se envía a un recopilador de flujo.

**destino de reenvío**

Uno o varios sistemas de proveedores que reciben datos en bruto y normalizados de orígenes de registro y orígenes de flujo.

**FQDN**

Véase [nombre de dominio completo](#).

**FQNN**

Véase [nombre de red completo](#).

**nombre de dominio completo (FQDN)**

En comunicaciones de Internet, nombre de un sistema host que incluye todos los subnombres del nombre de dominio. Un ejemplo de nombre de dominio completo es rchland.vnet.ibm.com.

**nombre de red completo (FQNN)**

En una jerarquía de red, nombre de un objeto que incluye todos los departamentos. Un ejemplo de un nombre de red completo es CompanyA.Department.Marketing.

## G

---

### **pasarela**

Dispositivo o programa utilizado para conectar redes o sistemas con diferentes arquitecturas de red.

## H

---

### **HA**

Véase [alta disponibilidad](#).

### **clúster de alta disponibilidad**

Configuración de alta disponibilidad que consta de un servidor primario y un servidor secundario.

### **código de autenticación de mensaje basado en hash (HMAC)**

Código criptográfico que utiliza una función hash críptica y una clave secreta.

### **alta disponibilidad (HA)**

Relativo a un sistema en clúster que se vuelve a configurar cuando se producen anomalías de nodo o daemon para que las cargas de trabajo se puedan redistribuir en los nodos restantes del clúster.

### **HMAC**

Véase [Código de autenticación de mensaje basado en hash](#).

### **contexto de host**

Servicio que supervisa los componentes para asegurarse de que cada componente está funcionando como se esperaba.

## I

---

### **ICMP**

Véase [protocolo de mensajes de control de Internet](#).

### **identidad**

Colección de atributos de un origen de datos que representan una persona, una organización, un lugar o un elemento.

### **IDS**

Véase [sistema de detección de intrusiones](#).

### **Protocolo de mensajes de control de Internet (ICMP)**

Protocolo de Internet utilizado por una pasarela para comunicarse con un host de origen, por ejemplo, para informar de un error en un datagrama.

### **Protocolo de Internet (IP)**

Protocolo que direcciona los datos a través de una red o de redes interconectadas. Este protocolo actúa como intermediario entre las capas de protocolo más altas y la red física. Véase también [Protocolo de control de transmisiones](#).

### **proveedor de servicios de Internet (ISP)**

Organización que proporciona acceso a Internet.

### **sistema de detección de intrusiones (IDS)**

Software que detecta los intentos o los ataques satisfactorios en los recursos supervisados que forman parte de una red o un sistema host.

### **sistema de prevención de intrusiones (IPS)**

Sistema que intenta denegar la actividad potencialmente maliciosa. Los mecanismos de denegación pueden implicar el filtrado, seguimiento o establecimiento de límites de velocidad.

### **IP**

Véase [Protocolo Internet](#).



**multidifusión IP**

Transmisión de un datagrama de Protocolo Internet (IP) para establecer un conjunto de sistemas que forman un grupo de multidifusión único.

**IPS**

Véase sistema de prevención de intrusiones.

**ISP**

Véase proveedor de servicios de Internet.

## K

---

**archivo de claves**

En seguridad de sistemas, archivo que contiene claves públicas, claves privadas, raíces de confianza y certificados.

## L

---

**L2L**

Véase Local a local.

**L2R**

Véase Local a remoto.

**LAN**

Véase red de área local.

**LDAP**

Véase Lightweight Directory Access Protocol.

**hoja**

En un árbol, entrada o nodo que no tiene hijos.

**Lightweight Directory Access Protocol (LDAP)**

Protocolo abierto que utiliza TCP/IP para proporcionar acceso a directorios que soportan un modelo X.500, y que no está sujeto a los requisitos de recursos del protocolo de acceso a directorios (DAP) X.500 más complejo. Por ejemplo, se puede utilizar LDAP para localizar personas, organizaciones y otros recursos en un directorio de Internet o de intranet.

**agregación de enlaces**

Agrupación de tarjetas de interfaz de red física, como cables o puertos, en una única interfaz de red lógica. La agregación de enlaces se utiliza para aumentar el ancho de banda y la disponibilidad de red.

**exploración en tiempo real**

Exploración de vulnerabilidad que genera datos de informe a partir de los resultados de exploración basándose en el nombre de sesión.

**red de área local (LAN)**

Red que conecta varios dispositivos en un área limitada (como un único edificio o campus) y que se puede conectar a una red más grande.

**Local a local (L2L)**

Relativo al tráfico interno de una red local a otra red local.

**Local a remoto (L2R)**

Relativo al tráfico interno de una red local a otra red remota.

**origen de registro**

Equipo de seguridad o equipo de red desde el que se origina un registro de sucesos.

**extensión de origen de registro**

Archivo XML que incluye todos los patrones de expresión regular necesarios para identificar y categorizar sucesos de la carga útil de sucesos.

## M

---

### **magistrado**

Componente interno que analiza el tráfico de red y los sucesos de seguridad respecto a las reglas personalizadas definidas.

### **magnitud**

Medida de la importancia relativa de un determinado delito. Magnitud es un valor ponderado calculado a partir de pertinencia, gravedad y credibilidad.

## N

---

### **NAT**

Véase [conversión de direcciones de red](#).

### **NetFlow**

Protocolo de red Cisco que supervisa datos de flujo de tráfico de red. Los datos de NetFlow incluyen la información de cliente y servidor, los puertos que se utilizan y el número de bytes y paquetes que fluyen a través de los conmutadores y direccionadores conectados a una red. Los datos se envían a recopiladores de NetFlow donde se realiza el análisis de datos.

### **conversión de direcciones de red (NAT)**

En un cortafuegos, conversión de las direcciones seguras del protocolo de Internet (IP) en direcciones registradas externas. Esto permite las comunicaciones con redes externas pero enmascara las direcciones IP que se utilizan dentro del cortafuegos.

### **jerarquía de red**

Tipo de contenedor que es una colección jerárquica de objetos de red.

### **capa de red**

En la arquitectura OSI, capa que proporciona servicios para establecer una vía de acceso entre sistemas abiertos con una calidad de servicio predecible.

### **objeto de red**

Componente de una jerarquía de red.

## O

---

### **delito**

Mensaje enviado o suceso generado en respuesta a una condición supervisada. Por ejemplo, un delito proporcionará información sobre si una política se ha incumplido o la red está bajo ataque.

### **origen externo**

Dispositivo que está fuera del sitio primario que reenvía datos normalizados a un recopilador de sucesos.

### **destino externo**

Dispositivo que está fuera del sitio primario que recibe el flujo de sucesos o datos de un recopilador de sucesos.

### **Open Source Vulnerability Database (OSVDB)**

Creado por la comunidad de seguridad de red para la comunidad de seguridad de red, base de datos de código abierto que proporciona información técnica sobre las vulnerabilidades de seguridad de la red.

### **interconexión de sistemas abiertos (OSI)**

Interconexión de sistemas abiertos de acuerdo con los estándares de la ISO (International Organization for Standardization) para el intercambio de información.

### **OSI**

Véase [interconexión de sistemas abiertos](#).

## OSVDB

Véase [Open Source Vulnerability Database](#).

## P

---

### orden de análisis

Una definición de origen de registro en la que el usuario puede definir el orden de importancia para los orígenes de registro que comparten una dirección IP o un nombre de host comunes.

### datos de carga útil

Datos de aplicación contenidos en un flujo de IP, excluyendo la cabecera y la información administrativa.

### host primario de alta disponibilidad

Sistema principal que está conectado al clúster de alta disponibilidad.

### protocolo

Conjunto de reglas que controlan la comunicación y la transferencia de datos entre dos o varios dispositivos o sistemas en una red de comunicaciones.

## Q

---

### Correlación de QID

Taxonomía que identifica cada suceso exclusivo y correlaciona los sucesos con categorías de bajo nivel y alto nivel para determinar cómo se debe correlacionar y organizar un suceso.

## R

---

### R2L

Véase [Remoto a local](#).

### R2R

Véase [Remoto a remoto](#).

### recon

Véase [reconocimiento](#).

### reconocimiento (recon)

Método mediante el cual se recopila información que pertenece a la identidad de los recursos de red. Se utilizan técnicas de exploración de red y otras para compilar una lista de sucesos de recursos de red a los que entonces se les asigna un nivel de gravedad.

### correlación de referencia

Registro de datos de la correlación directa de una clave con un valor, por ejemplo un nombre de usuario con un ID global.

### correlación de referencia de correlaciones

Registro de datos de dos claves correlacionadas con muchos valores. Por ejemplo, la correlación de los bytes totales de una aplicación con una IP de origen.

### correlación de referencia de conjuntos

Registro de datos de una clave correlacionada con muchos valores. Por ejemplo, la correlación de una lista de usuarios privilegiados con un host.

### conjunto de referencia

Lista de elementos únicos que se derivan de sucesos o flujos en una red. Por ejemplo, una lista de direcciones IP o una lista de nombres de usuario.

### tabla de referencia

Tabla donde el registro de datos correlaciona claves que tienen un tipo asignado con otras claves, que a continuación se correlacionan con un único valor.

**temporizador de renovación**

Dispositivo interno que se desencadena manual o automáticamente a intervalos temporizados que actualiza los datos de actividad de red actuales.

**pertinencia**

Medida de impacto relativo de un suceso, una categoría o un delito en la red.

**Remoto a local (R2L)**

Tráfico externo desde una red remota a una red local.

**Remoto a remoto (R2R)**

Tráfico externo desde una red remota a otra red remota.

**informe**

En gestión de consultas, datos formateados que se obtienen al ejecutar una consulta y aplicarle un formato.

**intervalo de informe**

Intervalo de tiempo configurable al final del cual el procesador de sucesos debe enviar todos los datos de sucesos y flujos capturados a la consola.

**regla de direccionamiento**

Condición en la que, cuando los datos de sucesos satisfacen sus criterios, se ejecutan un conjunto de condiciones y el direccionamiento consecuente.

**regla**

Conjunto de sentencias condicionales que permiten a los sistemas identificar relaciones y ejecutar respuestas automáticas como corresponda.

## S

---

**explorador**

Programa de seguridad automático que busca vulnerabilidades de software dentro de las aplicaciones web.

**host secundario de alta disponibilidad**

Sistema en espera que está conectado al clúster de alta disponibilidad. El host secundario de alta disponibilidad asume la responsabilidad del host primario de alta disponibilidad si el host primario de alta disponibilidad falla.

**gravedad**

Medida de la amenaza relativa que un origen plantea en un destino.

**Protocolo simple de gestión de red (SNMP)**

Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. La información sobre dispositivos gestionados se define y almacena en una MIB (Management Information Base - Base de información de gestión).

**SNMP**

Véase [Protocolo simple de gestión de red](#).

**SOAP**

Protocolo ligero basado en XML para intercambiar información en un entorno distribuido descentralizado. Se puede utilizar SOAP para consultar y devolver información e invocar servicios en Internet.

**sistema en espera**

Sistema que se activa automáticamente cuando el sistema activo falla. Si se ha habilitado la replicación de disco, replica los datos del sistema activo.

**subred**

Véase [subred](#).

**máscara de subred**

Para la gestión de subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte de host de una dirección IP.

**subred**

Red que se divide en subgrupos independientes más pequeños, que siguen estando interconectados.

**sub-búsqueda**

Función que permite realizar una consulta de búsqueda en un conjunto de resultados de búsqueda completada.

**superflujó**

Flujo único que consta de varios flujos con propiedades similares con el fin de aumentar la capacidad de proceso reduciendo las restricciones de almacenamiento.

**vista de sistema**

Representación visual de hosts primarios y gestionados que componen un sistema.

## T

---

**TCP**

Véase [Protocolo de control de transmisiones](#).

**Protocolo de control de transmisiones (TCP)**

Protocolo de comunicación utilizado en Internet y en cualquier red que cumple los estándares de IETF (Internet Engineering Task Force) para el protocolo entre redes. TCP proporciona un protocolo fiable de host a host en las redes de comunicaciones de conmutación de paquetes y en los sistemas interconectados de dichas redes. Véase también [Protocolo Internet](#).

**archivo de almacén de confianza**

Archivo de base de datos de claves que contiene las claves públicas para una entidad de confianza.

## V

---

**violación**

Acto que ignora o contraviene la política corporativa.

**vulnerabilidad**

Exposición de seguridad en un sistema operativo, software de sistema o componente de software de aplicación.

## W

---

**servidor whois**

Servidor que se utiliza para recuperar información sobre un recurso de Internet registrado, por ejemplo nombres de dominio y asignaciones de dirección IP.



# Índice

## Caracteres Especiales

último minuto (renovación automática) [12](#)

### A

acciones sobre un delito [45](#)  
actividad de red [12](#), [19](#), [27](#), [31](#), [87](#), [88](#), [123](#), [133](#), [166–170](#)  
actividad de red, pestaña [87](#), [91](#), [93](#)  
Actividad de red, pestaña [8](#), [88](#)  
actividad de registro  
    criterios de búsqueda [133](#)  
    visión general [59](#)  
actividad de registro, pestaña [127](#)  
activos [9](#)  
actualizar detalles de usuario [15](#)  
ajustar falsos positivos [82](#)  
Ajustar falsos positivos [91](#)  
amenaza [17](#)  
añadir activo [110](#)  
añadir elemento [19](#)  
añadir elemento de panel de control [19](#)  
añadir elementos [31](#)  
añadir elementos de búsqueda de flujo [31](#)  
añadir elementos de suceso [31](#)  
añadir filtro [166](#)  
aplicación [17](#)  
asistente de reglas personalizadas [11](#)  
Asistente de reglas personalizadas [26](#)

### B

barra de estado [64](#)  
barra de herramientas [59](#)  
barra de herramientas de detalles de suceso [80](#)  
buscar  
    copiar en un grupo [170](#)  
buscar delitos [159](#), [161](#), [163](#)  
búsqueda de perfiles de activo [114](#)  
búsqueda planificada  
    buscar [134](#)  
    búsqueda guardada [134](#)  
    sucesos [134](#)  
Búsquedas de delitos [152](#)  
búsquedas de flujos [19](#)  
búsquedas de sucesos y flujos [127](#)

### C

canal de información X-Force Threat Intelligence  
    ejemplo [209](#)  
cancelar una búsqueda [167](#)  
carga masiva  
    analiza sucesos y flujos [203](#)  
    correlación histórica [203](#)  
centro de información de amenazas de Internet [27](#)

cerrar delitos [46](#)  
columna Datos de PCAP [83](#), [85](#)  
compartir grupos de informes [227](#)  
compartir informes [225](#)  
configuración de actividad de red [28](#)  
configuración de actividad de registro [28](#)  
configuración de conexiones [28](#)  
configuración de elementos de panel de control [28](#)  
controles [11](#)  
copiar búsqueda guardada [117](#), [170](#)  
correlación histórica  
    crear un perfil [204](#)  
    delitos [205](#)  
    hora de dispositivo [203](#)  
    hora de inicio [203](#)  
    información sobre ejecuciones pasadas [205](#)  
    manejo de reglas [203](#)  
correlacionar suceso [82](#)  
creación de un grupo de búsqueda nuevo [169](#)  
crear grupos de búsqueda [168](#)  
crear informes [10](#)  
crear nuevo grupo de búsqueda [117](#)  
credibilidad [37](#)  
criterios de búsqueda  
    guardada disponible [166](#)  
    guardar [133](#)  
    pestaña Actividad de registro [166](#)  
    suprimir [166](#)  
criterios de búsqueda guardados [19](#)  
cuadro de lista Visualizar [70](#), [88](#)  
cumplimiento de normativas [17](#)

### D

datos de configuración [11](#)  
datos de Packet Capture (PCAP) [83](#)  
datos de PCAP [83](#), [84](#)  
datos de suceso en bruto [68](#)  
datos de suceso sin analizar [68](#)  
delito  
    investigaciones [37](#)  
    magnitud [37](#)  
delitos  
    asignar a usuarios [47](#)  
    correlación histórica [205](#)  
delitos actualizados [22](#)  
descargar archivo de datos de PCAP [84](#)  
descargar archivo de PCAP [85](#)  
desconectar un elemento de panel de control [29](#)  
descripción de suceso [75](#)  
desproteger delitos [36](#)  
detalles de flujo [88](#)  
detalles de suceso [80](#)  
detalles de suceso único [75](#)  
detalles de vulnerabilidad [119](#)  
Diseño de informe [213](#)  
dispositivo [11](#)

Distintivo [26](#)  
distribuir informes [10](#)  
Duplicar un informe [224](#)

## E

editar activo [110](#)  
editar grupo de búsqueda [117](#)  
Editar un grupo [226](#)  
editar un grupo de búsqueda [169](#)  
elemento de panel de control [30](#)  
elemento de panel de control Notificación del sistema [26](#)  
elemento de panel de control personalizado [19](#)  
elemento de panel de control Resumen del sistema [22](#)  
elementos de delito [20](#)  
elementos de la búsqueda de conexiones [22](#)  
elementos de panel de control Actividad de registro [21](#)  
elementos de visualización [25](#)  
elementos del panel de control de delitos [20](#)  
eliminar búsqueda guardada [118](#)  
eliminar búsqueda guardada de un grupo [170](#)  
eliminar elemento de panel de control [29](#)  
eliminar grupo [118](#), [170](#)  
especificar el número de objetos de datos para ver [28](#)  
especificar tipo de gráfico [28](#)  
excluye la opción [36](#)  
exploradores de terceros [107](#)  
exportación de activos [119](#)  
exportación de sucesos [85](#)  
exportar a CSV [93](#)  
exportar a XML [93](#)  
exportar delitos [47](#)  
Exportar flujos [93](#)  
exportar perfil de activo [118](#)

## F

falso positivo [82](#), [91](#)  
falsos positivos [107](#)  
filtro rápido [127](#)  
flujos [22](#), [127](#), [134](#)  
flujos normalizados [87](#), [88](#)  
funciones de barra de herramientas de detalles de suceso [80](#)

## G

generar un informe manualmente [224](#)  
gestión de delitos [33](#)  
gestión de panel de control [17](#)  
gestión de riesgos  
    supervisar cambio de riesgo [25](#)  
    supervisar cumplimiento de políticas [23](#)  
Gestionar grupos [117](#)  
gestionar grupos de búsqueda [163](#), [168](#)  
gestionar informes [10](#), [216](#)  
gestionar resultados de búsqueda [167](#), [168](#)  
glosario [235](#)  
gráfico de serie temporal [123](#)  
gravedad [37](#)  
grupo  
    eliminar [170](#)  
grupo de búsqueda

grupo de búsqueda (*continuación*)  
    crear [169](#)  
    editar [169](#)  
grupo de búsqueda de delitos [169](#)  
grupo de búsqueda de flujos [168](#), [169](#)  
grupo de búsqueda de sucesos [168](#), [169](#)  
grupos de búsqueda  
    gestionar [168](#)  
    ver [168](#)  
grupos de búsqueda de activos [116](#)  
grupos de informes [227](#)  
guardar criterios [115](#), [163](#)  
guardar criterios de búsqueda [163](#)  
guardar criterios de búsqueda de activos [115](#)  
guardar criterios de búsquedas de flujo y suceso [64](#)

## H

hora de consola [15](#)  
hora de dispositivo [203](#)  
hora de inicio [203](#)  
hora del sistema [15](#)  
hosts [9](#)

## I

IBM Security QRadar Risk Manager [11](#)  
icono Eliminar [118](#)  
imagen  
    cargar [225](#)  
    informes  
        marcas [225](#)  
importar activos [118](#)  
importar perfil de activo [118](#)  
información de usuario [15](#)  
informe  
    editar [223](#)  
informes  
    correlación histórica [205](#)  
    ver [223](#)  
informes personalizados [219](#)  
interfaz de usuario [6](#)  
investigar actividad de registro [59](#)  
investigar delito [6](#)  
investigar delitos [37](#)  
investigar flujos [8](#)  
investigar registros de sucesos [7](#)  
investigar sucesos [21](#)

## L

leyendas de gráficos [124](#)  
lista de sucesos [75](#)

## M

magnitud [37](#)  
mensaje de notificación [26](#)  
menú Mensajes [11](#)  
menú que aparece al pulsar el botón derecho del ratón [63](#)  
modalidad continua [87](#)  
modificación de correlación de sucesos [82](#)  
modo de documento



modo de documento (*continuación*)  
  explorador web de Internet Explorer [5](#)  
modo de explorador  
  explorador web de Internet Explorer [5](#)  
mostrar panel de control [27](#), [29](#), [30](#)

## N

nivel de peligro actual [27](#)  
nivel de peligro en Internet [27](#)  
notificación del sistema [30](#)  
notificaciones del sistema [11](#)  
nueva búsqueda [117](#)

## O

objetos de gráfico [124](#)  
ocultar delito [45](#)  
opciones de sucesos agrupados [70](#)  
organizar los elementos de panel de control [17](#)  
origen de registro [68](#)

## P

página de búsqueda de activo [114](#)  
página de detalles de suceso [75](#)  
página IP de origen [159](#)  
página Perfil de activo [119](#)  
página Por IP de destino [161](#)  
página Por red [163](#)  
panel de control [31](#)  
panel de control de gestor de riesgos  
  crear [25](#)  
panel de control de supervisión de riesgos [22](#)  
panel de control Gestión de vulnerabilidades [25](#)  
panel de control nuevo [27](#)  
panel de control personalizado [19](#), [22](#), [27](#)  
Panel de control, panel [20](#)  
panel de control, pestaña [17](#), [27](#)  
paneles de control de supervisión se riesgos  
  crear [23](#)  
parámetros de sucesos agrupados [70](#)  
perfil de activo [108](#), [110](#)  
perfiles de activo [107](#), [115](#), [116](#), [118](#), [119](#)  
Perfiles de activo [117](#)  
pertinencia [37](#)  
pestaña Actividad de red [127](#)  
pestaña Actividad de registro [7](#), [59](#), [63–65](#), [68](#), [70](#), [81](#), [83](#),  
[85](#), [127](#)  
pestaña Activo [107](#), [116](#)  
pestaña Activos [9](#), [108](#), [110](#), [116–118](#)  
Pestaña de actividad de red [87](#)  
pestaña Delito [159](#), [161](#), [163](#)  
pestaña Delitos [6](#), [36](#), [45–47](#), [163](#)  
pestaña Informe [216](#)  
pestaña Informes [10](#)  
pestaña Panel de control [6](#), [11](#), [17](#), [21](#), [22](#), [29](#), [30](#)  
pestaña predeterminada [6](#)  
pestaña Riesgos [22](#)  
pestañas [6](#)  
pestañas de interfaz de usuario [6](#), [11](#)  
poner datos en pausa [12](#)  
Procesador de flujos [87](#)

propiedad  
  modificación de personalizado [175](#)  
proteger delitos [36](#)  
prueba de regla [203](#)

## Q

QFlow Collector [87](#)  
QID [82](#)  
QRadar Vulnerability Manager [107](#)

## R

realizar una sub-búsqueda [166](#)  
red [17](#)  
registros de desbordamiento [87](#)  
regla de detección de anomalías [193](#)  
Regla de detección de anomalías, asistente [193](#)  
reglas [184](#), [190](#)  
reglas personalizadas  
  crear [185](#)  
renombrar panel de control [30](#)  
renovar datos [12](#)  
reproducir datos [12](#)  
resultados de búsqueda  
  cancelar [167](#)  
  gestionar [167](#)  
  suprimir [168](#)  
resultados de procesador de sucesos [64](#)  
resumen de actividad dentro de las últimas 24 horas [22](#)  
retención de delitos [36](#)

## S

seguridad [17](#)  
servidores [9](#)  
sistema [17](#)  
sucesos [22](#), [81](#), [127](#)  
sucesos de modalidad continua [64](#)  
sucesos normalizados [65](#)  
supervisar actividad de red [87](#)  
supervisar delitos [45](#)  
supervisar sucesos [21](#)  
supresión de activos [118](#)  
supresión de una búsqueda [168](#)  
suprimir panel de control [30](#)  
suprimir perfil de activo [118](#)

## T

tiempo real [64](#)  
tiempo real (modalidad continua) [12](#)  
tipos de gráfico [214](#), [218](#)

## V

varios paneles de control [17](#)  
ventana Grupos de búsqueda [168](#)  
ver datos de PCAP [84](#)  
ver delitos asociados con sucesos [81](#)  
Ver flujos agrupados [88](#)  
ver flujos continuos [87](#)  
ver mensajes [11](#)

ver notificaciones del sistema [30](#)  
ver perfil de activo [108](#)  
ver sucesos agrupados [70](#)  
visión general de gráficos [123](#)  
visualización de grupos de búsqueda [116](#), [168](#)  
visualización de sucesos en modalidad continua [64](#)  
visualizar en una ventana nueva [29](#)  
vulnerabilidades [107](#)  
vulnerabilidades de activo [119](#)



