LAC-IX
LATIN AMERICA AND CARIBBEAN IXPs

MEJORES PRÁCTICAS RTBH EN LOS IXP

Versión: 2.1
Fecha: Septiembre 2026
Audiencia: Miembros de Internet Exchange Points en LAC

1. Alcance y audiencia

1.1 Audiencia

Esta guía está dirigida a **operadores de Puntos de Intercambio de Tráfico (IXP)** que evalúan, implementan u operan un servicio de blackholing sobre su plataforma.

Los requisitos que recaen sobre los participantes conectados al IXP se tratan en el **Anexo A**, redactado como material que el operador del IXP puede adaptar y entregar directamente a sus miembros. La separación entre lo que hace el IXP y lo que debe hacer el participante se detalla en la sección 3.

1.2 Qué cubre

El diseño, la implementación y la operación de un servicio de blackholing en un IXP: señalización por BGP entre un participante bajo ataque, el route server del IXP y el resto de los participantes, y el descarte del tráfico resultante.

1.3 Qué no cubre

- Blackholing dentro de un mismo Sistema Autónomo (el modelo de RFC 5635, con router de disparo, sesiones iBGP y routers de borde bajo control de un solo operador). Es una técnica válida y complementaria, pero es una decisión interna de cada red y no involucra al IXP.
- Blackholing basado en origen con uRPF. No se distribuye a través de un route server y no forma parte del modelo de servicio de un IXP.
    - Servicios de mitigación gestionada o scrubbing.
    - BGP Flowspec, que se aborda únicamente como técnica complementaria (sección 11).

1.4 Naturaleza del documento

Todo el contenido tiene carácter de recomendación. No establece obligaciones ni condiciones de asociación. Las listas de verificación incluyen una columna de criticidad orientativa:

- **Crítico** — su ausencia genera un riesgo de seguridad o deja el servicio inoperante.
- **Recomendado** — mejora significativamente la eficacia o la usabilidad.
- **Opcional** — aporta valor según el contexto y la escala del IXP.

1.5 Convenciones

Las direcciones y números de sistema autónomo de los ejemplos provienen de los rangos reservados para documentación: 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24 (RFC 5737), 2001:db8::/32 (RFC 3849) y AS64496–AS64511 (RFC 5398). Deben sustituirse por los valores reales de cada IXP.

1.5 Relación con RFC 7999

RFC 7999, BLACKHOLE Community, es el documento de referencia principal de esta guía. Define la comunidad bien conocida que se utiliza para señalizar blackholing, y sus recomendaciones operativas y consideraciones de seguridad son la base de las secciones 4, 5 y 6. Toda implementación descrita aquí parte de ese documento.

Correspondencia entre RFC 7999 y esta guía:

RFC 7999	Contenido	Sección de esta guía
§2	Definición de la comunidad y su semántica	4.1
§3.1	Anuncio de prefijos con la comunidad adjunta; decisión de honrarla o ignorarla	4.1, 2.1, A.3
§3.2	Alcance local del blackhole; uso de NO_EXPORT o NO_ADVERTISE	4.5, A.2
§3.3	Longitud del prefijo; condiciones de aceptación; convivencia con validación de origen; separación respecto de Flowspec; conservación de registros	5.1, 6.1, 6.2, 11.2, 10.3
§4	Comportamiento por defecto de los equipos: no descartar sin configuración explícita	2.1, 3

RFC 7999	Contenido	Sección de esta guía
§5	Codepoint registrado en IANA	4.1
§6	Consideraciones de seguridad; verificación de que el vecino está autorizado	6.1, 6.3

Lo que RFC 7999 no cubre y esta guía sí. El documento es de carácter informativo y describe la señalización entre vecinos BGP, no la operación de un servicio en un IXP. Los siguientes elementos son práctica operativa construida sobre esa base y no se derivan del texto de la RFC:

- la reescritura del atributo NEXT_HOP por parte del route server (sección 5.2);
- los umbrales de longitud de prefijo diferenciados aplicados en el route server (sección 5.1);
- el plano de datos del IXP, ya sea con ACL de capa 2 o con servidor sumidero (sección 7);
- el control selectivo de redistribución por peer (sección 4.4);
- la arquitectura de la sesión BGP y las prácticas de publicación, prueba y operación del servicio (secciones 8 a 10).

Esa brecha es, precisamente, la razón de existir de este documento: aplicar RFC 7999 al entorno particular de un Punto de Intercambio de Tráfico.

2. Modelo de referencia

2.1 El blackholing en un IXP no es blackholing dentro de un AS

La confusión más frecuente al abordar este tema consiste en trasladar el modelo pensado para una red operada por una sola organización a un entorno donde ninguna parte controla los equipos de las demás.

Elemento	Dentro de un mismo AS	En un IXP
Quién dispara	Un router de disparo del propio operador	El router de borde del participante afectado
Señalización	iBGP interno	eBGP hacia el route server del IXP
Quién distribuye	Reflectores de ruta internos	El route server del IXP
Quién decide honrar la señal	El propio operador	Cada participante receptor, según su política
Dónde se descarta el tráfico	Interfaces de descarte propias	Plataforma del IXP, o borde del participante emisor
Confianza	Implícita	Debe construirse mediante validación
Alcance del efecto	Completo dentro del AS	Solo el tráfico que atraviesa el IX

La consecuencia operativa central: el IXP no descarta tráfico por decisión propia y no puede garantizar que un blackhole surta efecto. Su rol es validar y señalizar de forma confiable, y ofrecer un punto de descarte eficiente. La eficacia final depende de que los participantes receptores hayan configurado su política de importación.

2.2 Flujo de señalización

1. El participante afectado (AS64511) detecta un ataque volumétrico contra una dirección dentro de su prefijo 203.0.113.0/24.
2. Anuncia 203.0.113.10/32 a los route servers del IXP con la comunidad **BLACKHOLE (65535:666)** adjunta.
3. El route server verifica que el participante está autorizado a anunciar un prefijo que cubre esa dirección (sección 6) y que el anuncio cumple los umbrales de longitud aplicables a blackholes (sección 5).
4. El route server reescribe el **NEXT_HOP** hacia la dirección de blackhole del IXP y redistribuye el prefijo, opcionalmente restringido a un subconjunto de participantes (sección 4.4).
5. Cada participante receptor decide si acepta el prefijo, según su política de importación.
6. Los que lo aceptan resuelven la dirección MAC del next-hop de blackhole por ARP o NDP y encaminan hacia ella el tráfico destinado a 203.0.113.10.
7. El IXP descarta esas tramas en ingreso mediante una ACL de capa 2, o bien el participante las descarta localmente antes de que entren al IXP

3. Separación de responsabilidades

Esta tabla es la referencia para resolver cualquier ambigüedad sobre quién ejecuta qué. Ninguna de las dos columnas puede suplir a la otra.

Función	Responsable	Nota
Definir y publicar la comunidad de disparo	**IXP**	Se recomienda la comunidad estándar de RFC 7999
Detectar el ataque	**Participante**	El IXP no monitorea el tráfico del participante
Originar el anuncio de blackhole	**Participante**	Con la comunidad adjunta y el prefijo más específico posible
Permitir el más-específico en la política de salida propia	**Participante**	Punto de falla frecuente
Validar la autorización sobre el prefijo	**IXP**	El participante no puede autovalidarse
Aplicar los umbrales de longitud diferenciados	**IXP**	Solo en presencia de la comunidad
Reescribir el NEXT_HOP	**IXP**	Excepción deliberada al comportamiento normal del route server
Marcar el blackhole como validado	**IXP**	Permite al participante confiar en la marca del route server
Redistribuir la señal	**IXP**	Con control selectivo por peer si se ofrece
Aceptar la señal en la política de importación	**Participante**	**El IXP no puede hacerlo ni forzarlo**

Función	Responsable	Nota
Descartar el tráfico en la plataforma	**IXP**	ACL de capa 2 o sumidero
Descartar el tráfico en el borde propio	**Participante**	Opción alternativa, más eficiente para el participante
No propagar el blackhole fuera del AS	**Participante**	El IXP puede asistir agregando NO_EXPORT
Retirar el blackhole al terminar el ataque	**Participante**	El IXP puede expirar anuncios obsoletos
Proteger la infraestructura del IXP	**IXP**	Lista de prefijos que nunca se blackholean
Publicar documentación y procedimiento de prueba	**IXP**	
Ejecutar la prueba de verificación	**Participante**	Sobre el prefijo de prueba que provee el IXP
Registrar y auditar los eventos	**IXP y Participante**	Cada uno en su ámbito

3.1 El límite de responsabilidad del IXP

Se recomienda que el IXP declare explícitamente, en su documentación de servicio, que:

- el servicio consiste en validar, señalizar y ofrecer un punto de descarte;
- la eficacia depende de la configuración de terceros que el IXP no controla;
- el IXP no ofrece garantía de que un blackhole sea honrado por todos los participantes;
- el servicio no protege contra tráfico que no atraviesa el IXP.

Sin esta declaración, un servicio de blackholing genera expectativas que el IXP no está en condiciones de cumplir.

4. Señalización: comunidades BGP

4.1 Comunidad de disparo

Se recomienda soportar la comunidad bien conocida BLACKHOLE, definida en RFC 7999:

- Notación estándar: 65535:666
- Valor: 0xFFFF029A

Un IXP puede además aceptar una comunidad propia con la forma rs-asn:666 como alias, pero no se recomienda exigirla como única forma de señalización. El propósito de RFC 7999 es que un operador presente en varios IXP no deba aprender un mecanismo distinto en cada uno.

4.2 Comunidades large

Una fracción creciente de los participantes opera con ASN de 32 bits, que no puede representarse en una comunidad estándar de 16+16 bits. Se recomienda publicar equivalentes en *large communities* (RFC 8092) para todas las funciones de control, incluida la de blackholing y las de control de redistribución, y advertir a los participantes que no mezclen ambos formatos en un mismo anuncio.

4.3 Comunidad de confirmación

Se recomienda marcar con una comunidad propia los prefijos que efectivamente fueron aceptados y procesados como blackhole. Esto permite:

- distinguir un blackhole validado por el IXP de una comunidad que simplemente viajó adjunta al anuncio;
- que los participantes construyan su política de importación confiando en la marca del route server en lugar de en la comunidad de origen, lo que reduce la superficie de error.

4.4 Control selectivo de redistribución

Esta es la respuesta práctica al daño colateral y conviene documentarla de forma destacada.

Las comunidades de control de redistribución del route server (0:peer-as, rs-asn:peer-as y sus equivalentes large) son combinables con la comunidad BLACKHOLE. Un participante puede así descartar el tráfico proveniente únicamente de los sistemas autónomos que están originando el ataque, y mantener alcanzable el prefijo desde los peers que envían tráfico legítimo.

Ejemplo, con route server en AS64500, para anunciar el blackhole a todos los peers excepto AS64504:

65535:666 64500:64500 0:64504

Un servicio de blackholing que no soporte esta combinación pierde su principal ventaja frente al blackholing contratado con un proveedor de tránsito, donde esta granularidad no existe.

4.5 Alcance local del blackhole

RFC 7999 recomienda que el receptor de un anuncio con la comunidad BLACKHOLE agregue NO_EXPORT (65535:65281) o NO_ADVERTISE para impedir la propagación fuera del AS local. Se recomienda que el route server agregue NO_EXPORT a los blackholes antes de reanunciarlos.

Nota: existe consenso en la comunidad de IXP en que las comunidades bien conocidas de RFC 1997 deberían pasar a través del route server sin ser interpretadas. La adición de NO_EXPORT a los blackholes es una excepción deliberada, justificada por el riesgo de fuga de más-específicos, y conviene documentarla como tal.

5. Filtrado en el route server

5.1 Umbrales de longitud de prefijo

Se recomienda aplicar dos conjuntos de umbrales según la presencia de la comunidad BLACKHOLE:

Caso	IPv4	IPv6
Anuncio normal	/8 a /24	/19 a /48
Con comunidad BLACKHOLE presente	/8 a /32	/19 a /128

La excepción de longitud debe aplicarse únicamente en presencia de la comunidad. Un más-específico sin ella se rechaza con la regla normal.

RFC 7999 es explícito en que el prefijo de blackhole conviene que sea lo más específico posible, típicamente /32 o /128, precisamente para acotar el daño colateral. Un IXP que solo acepte blackholes hasta /24 obliga a sus participantes a apagar 256 direcciones para proteger una.

Se recomienda que el route server reescriba el atributo NEXT_HOP de los prefijos de blackhole hacia la dirección de blackhole correspondiente a esa LAN de peering y familia de direcciones.

Esto constituye una desviación deliberada del comportamiento descrito en RFC 7947, según el cual el route server no modifica el NEXT_HOP. Es la excepción que hace posible el servicio, y conviene documentarla públicamente para que los participantes no la interpreten como una manipulación indebida del next-hop.

La verificación normal de next-hop (rechazar anuncios cuyo next-hop no coincida con la dirección del peer) debe mantenerse para todos los prefijos que no sean blackholes.

5.3 Orden de evaluación sugerido

```
1. Bogons y martians          -> rechazar
2. Sanidad de AS_PATH (1 a 64 ASN)     -> rechazar si falla
3. Primer ASN del AS_PATH = ASN del peer  -> rechazar si falla
4. Prefijo de infraestructura protegida  -> rechazar   (6.3)
5. ¿Lleva la comunidad BLACKHOLE?
 5a. SI -> umbral extendido /32 o /128          (5.1)
        -> autorización sobre el prefijo cubriente      (6.1)
        -> validación RPKI laxa             (6.2)
        -> marcar con la comunidad de confirmación      (4.3)
        -> reescribir NEXT_HOP              (5.2)
        -> agregar NO_EXPORT                (4.5)
 5b. NO -> umbral normal /24 o /48
        -> verificación de next-hop
        -> filtrado IRRDB y validación RPKI estricta
6. Aplicar comunidades de control de redistribución       (4.4)
```

5.4 Advertencia sobre plantillas de configuración por defecto

Las herramientas de generación automática de configuración de route servers de uso extendido producen, en su configuración estándar, filtros que **descartan los prefijos más específicos que /24 y /48 como primer paso del algoritmo,** antes de cualquier otra evaluación, y no contemplan la comunidad BLACKHOLE ni la reescritura del NEXT_HOP.

Un IXP que anuncie un servicio de blackholing sin modificar esos filtros verá los anuncios descartados de forma silenciosa, sin ningún mensaje de error para el participante. Se recomienda verificar este punto en laboratorio antes de publicar el servicio.

6. Validación y autorización

Esta es la sección de seguridad del servicio. Sin ella, cualquier participante puede dejar inalcanzable a cualquier otro.

6.1 Autorización sobre el prefijo cubriente

RFC 7999 establece dos condiciones para aceptar y honrar un anuncio con la comunidad BLACKHOLE, y recomienda aplicar las mismas condiciones en topologías con route server:

1. el prefijo anunciado debe estar cubierto por un prefijo igual o más corto que la red vecina esté autorizada a anunciar;
2. la parte receptora debe haber acordado honrar la comunidad en esa sesión BGP.

En la práctica del route server esto significa que, para cada participante, el conjunto de prefijos autorizados se construye desde su AS-SET en los registros de enrutamiento y desde sus ROA, y que para los blackholes ese conjunto se expande para admitir cualquier más-específico contenido en él. Un participante autorizado a anunciar 203.0.113.0/24 puede blackholear 203.0.113.10/32, y ninguna dirección fuera de ese /24.

No se recomienda aceptar un blackhole cuyo prefijo cubriente no esté en el conjunto autorizado del participante que lo anuncia.

6.2 Validación RPKI: laxa sobre blackholes

Este punto se implementa mal con frecuencia y tiene consecuencias severas.

El problema. RFC 9319 (BCP 185) recomienda ROA mínimos y desaconseja el uso del atributo maxLength. Bajo un ROA mínimo para 203.0.113.0/24, un anuncio de 203.0.113.10/32 resulta RPKI Invalid. Una validación de origen estricta rechaza, por tanto, todos los blackholes legítimos.

La solución equivocada. Emitir ROA con maxLength /32 o /128 para que los blackholes validen. RFC 9319 desaconseja explícitamente esa práctica: amplía la superficie de ataque a secuestros de sub-prefijo con origen falsificado. No conviene recomendarla a los participantes.

El criterio de RFC 7999. El documento indica que el operador debe asegurarse de que las técnicas de validación de origen no bloqueen inadvertidamente anuncios legítimos que llevan la comunidad BLACKHOLE. Es la única cláusula que resuelve el conflicto entre ambos marcos.

La política sugerida:

Tipo de ruta	**Validación RPKI**
Blackhole (comunidad BLACKHOLE presente)	**Laxa:** se honra el ASN de origen del ROA, se ignora el atributo maxLength
Cualquier otra ruta	Estricta: origen y maxLength

Nota de implementación. Las funciones de validación disponibles en los demonios de enrutamiento de uso común honran el atributo maxLength y devuelven Invalid para el /32. Mientras no exista una primitiva de validación laxa, se recomienda que el control primario de autorización sobre blackholes sea el conjunto de prefijos autorizados descrito en 6.1, con la validación RPKI aplicada sobre el prefijo cubriente durante la generación de ese conjunto, y no sobre el /32 en tiempo de anuncio.

6.3 Prefijos de infraestructura protegida

Se recomienda rechazar anuncios de blackhole que cubran, total o parcialmente:

- la LAN de peering del IXP;
- las direcciones de route servers, colectores de rutas, servidores AS112, NTP, DNS y demás infraestructura de servicio;
- los prefijos de gestión del IXP.

Sin esta lista de denegación, un error de configuración de un solo participante puede afectar la plataforma completa.

6.4 Límites y expiración

- Se recomienda aplicar un límite específico a la cantidad de prefijos de blackhole aceptados por participante, independiente del límite general de prefijos. Un valor del orden de decenas a bajas centenas resulta adecuado en la mayoría de los casos.

- Se recomienda implementar expiración automática de los blackholes que superen un tiempo definido sin ser reafirmados, o al menos generar alertas sobre ellos. Los blackholes que permanecen activos sin actividad de plano de datos que los justifique son un fenómeno documentado y dejan servicios inalcanzables de forma indefinida.

7. Plano de datos

7.1 Modelo A — Dirección de blackhole con MAC de descarte y ACL de capa 2

1. El IXP define una dirección de blackhole next-hop por LAN de peering y por familia de direcciones, dentro del rango de la LAN de peering.
2. El IXP responde ARP y NDP para esa dirección con una dirección MAC dedicada y reservada.
3. Todos los puertos de participante llevan una ACL de capa 2 aplicada en ingreso, que descarta las tramas cuya MAC de destino sea la del blackhole next-hop.

Ventaja decisiva: el tráfico se descarta en el puerto de ingreso y no atraviesa el fabric del IXP, por lo que no consume capacidad de los enlaces internos ni de los troncales entre sitios.

Convención de direccionamiento MAC: es práctica frecuente en la industria utilizar direcciones fácilmente reconocibles del patrón DE:AD:BE:EF:66:xx, lo que facilita el diagnóstico. La dirección elegida debe estar fuera de cualquier rango en uso por participantes.

7.2 Modelo B — Servidor sumidero

La dirección de blackhole se asigna a un servidor conectado a la plataforma, que recibe y descarta el tráfico.
Ventaja: no requiere ACL de capa 2 en hardware. Desventaja: el tráfico atraviesa el fabric hasta llegar al sumidero, de modo que un ataque de decenas de Gbps puede congestionar enlaces internos y el propio puerto del sumidero.

7.3 Comparación

Criterio	Modelo A (ACL de capa 2)	Modelo B (sumidero)
Consumo de fabric	Ninguno	Igual al volumen del ataque
Requisito de hardware	ACL de MAC en hardware en todos los puertos	Ninguno
Escalabilidad ante ataques grandes	Alta	Limitada por el enlace del sumidero
Complejidad de aprovisionamiento	Media (ACL en cada puerto nuevo)	Baja
Visibilidad del tráfico descartado	Contadores de ACL	Captura completa posible

Se recomienda el Modelo A. Si la plataforma no dispone de ACL de MAC en hardware, o el número de entradas disponibles es insuficiente, el Modelo B es una alternativa viable, documentando explícitamente el límite de capacidad del sumidero.

7.4 Descarte en el borde del participante

Un participante puede optar por instalar el prefijo de blackhole con un next-hop de descarte local, en lugar de encaminarlo hacia la dirección de blackhole del IXP. Es la opción más eficiente desde su perspectiva, porque el tráfico ni siquiera egresa hacia su puerto del IXP. Se recomienda presentar ambas opciones en la documentación al participante y no imponer una.

8. Arquitectura de la sesión BGP

Opción	Ventajas	Desventajas
Integrada en los route servers de peering	Sin sesiones adicionales; adopción inmediata	El participante debe distinguir blackholes dentro del flujo general de rutas
Dedicada: sesión BGP separada que solo anuncia blackholes	La política de importación del participante se reduce a aceptar /32 y /128 desde ese peer; menor riesgo de error	Requiere que cada participante configure una sesión adicional

Ambas pueden coexistir. La opción dedicada reduce de forma significativa la barrera de adopción del lado receptor, que es el cuello de botella real de la eficacia del servicio.

9. Publicación del servicio

Se recomienda publicar, en documentación accesible sin autenticación:

1. la existencia del servicio y si es de adhesión voluntaria;
2. la comunidad de disparo y su equivalente en formato large;
3. la comunidad de confirmación, si se utiliza;
4. las comunidades de control de redistribución y ejemplos de combinación con la comunidad de blackholing;
5. las direcciones IPv4 e IPv6 de blackhole, por LAN de peering;
6. la dirección MAC asociada;
7. los umbrales de longitud de prefijo aceptados, en formato de tabla;
8. la política de validación RPKI y de registros de enrutamiento aplicada a blackholes;
9. la lista de prefijos de infraestructura que nunca se aceptarán como blackhole;
10. el límite de prefijos de blackhole por participante y la política de expiración;
11. un prefijo de prueba y el procedimiento de verificación;
12. ejemplos de configuración para las plataformas de uso más extendido entre los participantes;
13. la declaración de límite de responsabilidad de la sección 3.1;
14. la política de uso aceptable.
15.

Se recomienda ofrecer el servicio sin costo adicional. Es higiene de la plataforma, no un producto diferenciado.

10. Operación

10.1 Prueba y verificación

Se recomienda reservar una dirección de prueba dentro del propio espacio del IXP y publicar un procedimiento que permita a un participante verificar, sin coordinación previa:

1. que su anuncio de blackhole es aceptado por el route server;
2. que el NEXT_HOP fue reescrito;
3. que el prefijo es redistribuido a los demás participantes;
4. que el tráfico hacia la dirección de prueba efectivamente se descarta.

Sin un procedimiento de prueba, el participante descubre que el servicio no funciona durante un incidente.

10.2 Visibilidad

- El looking glass debería mostrar los prefijos de blackhole activos y permitir a cada participante ver cuáles de sus anuncios fueron aceptados o rechazados, y por qué regla.
- Conviene publicar contadores agregados del servicio.

La métrica más útil, y la que rara vez se publica, es el porcentaje de participantes que aceptan blackholes. Es el indicador directo de la eficacia real del servicio y el insumo para las campañas de adopción.

10.3 Registro y auditoría

RFC 7999 alienta a conservar los mensajes BGP que llevan la comunidad BLACKHOLE para análisis de largo plazo y auditoría interna. Se recomienda registrar, como mínimo: marca temporal, ASN que dispara, prefijo, comunidades adjuntas y resultado de la validación.

10.4 Política de uso aceptable

El blackholing es una capacidad de denegación de alcance. Existen usos documentados que se apartan de la mitigación de DDoS, entre ellos la protección frente a ocupación de prefijos no anunciados, el bloqueo de contenido y la censura.

Se recomienda establecer y publicar que el servicio se ofrece exclusivamente para que un participante proteja su propia infraestructura, que solo puede aplicarse a direcciones que el participante está autorizado a anunciar, y cuál es el procedimiento ante un uso indebido.

11. Límites del servicio y técnicas complementarias

11.1 Límites inherentes

Conviene comunicarlos de forma explícita a los participantes.

- **Solo afecta al tráfico que atraviesa el IXP.** El tráfico de ataque que llega por tránsito o por interconexiones privadas no se ve afectado. El blackholing en el IXP se complementa con el blackholing del proveedor de tránsito.
- **Depende de la cooperación de terceros.** Mediciones publicadas sobre plataformas de gran porte encontraron que los blackholes anunciados como /32 lograron tasas medias de descarte cercanas al 50%, pese a que los /32 representaban la enorme mayoría del tráfico que debía descartarse. La causa dominante fue que los participantes receptores no aceptan prefijos más específicos que /24.
- **Completa el ataque respecto del destino.** El servicio atacado queda inalcanzable. El blackholing protege el enlace, el router y el resto de la red, no al servicio bajo ataque.
- **No distingue capa 4.** La granularidad disponible es por prefijo y por peer, no por puerto ni por protocolo.
- **No es adecuado contra ataques de aplicación de bajo volumen.**

11.2 Filtrado de grano fino

El blackholing descarta todo el tráfico dirigido a una dirección. Las mediciones disponibles indican que una amplia mayoría de los ataques volumétricos mitigados por esta vía utiliza un número muy reducido de vectores, identificables por el puerto de origen de la aplicación abusada. Un filtro por puerto elimina la mayor parte del daño colateral.

BGP Flowspec (RFC 8955 y RFC 8956) permite señalizar ese tipo de filtro. Dos advertencias:

- RFC 7999 indica expresamente que la comunidad BLACKHOLE no está pensada para usarse con NLRI de Flowspec. Son mecanismos separados y no deben mezclarse en la señalización.
- Flowspec en un IXP arrastra el mismo problema de cooperación que el blackholing: requiere que los participantes receptores lo acepten e implementen.

Existen aproximaciones de blackholing de grano fino en las que el filtro se aplica en la propia plataforma del IXP, sin requerir cooperación de los participantes. Es una línea de evolución razonable una vez que el servicio básico esté consolidado y medido, y no antes.

12. Lista de verificación para el operador del IXP

#	Elemento	Criticidad	Sección
1	Acepta la comunidad estándar de RFC 7999	Crítico	4.1
2	Publica equivalente en formato large	Recomendado	4.2
3	Umbrales extendidos a /32 y /128 solo con la comunidad presente	Crítico	5.1
4	Reescribe el NEXT_HOP hacia una dirección de blackhole documentada	Crítico	5.2
5	Valida que el prefijo esté cubierto por espacio autorizado del participante	**Crítico**	6.1
6	Mantiene lista de prefijos de infraestructura protegida	**Crítico**	6.3
7	Aplica validación RPKI laxa a blackholes y estricta al resto	Crítico	6.2
8	Agrega NO_EXPORT a los blackholes reanunciados	Recomendado	4.5
9	Paridad funcional entre IPv4 e IPv6	Crítico	5.1
10	Descarta en ingreso mediante ACL de capa 2	Recomendado	7.1
11	Marca los blackholes validados con una comunidad de confirmación	Recomendado	4.3
12	Soporta control selectivo de redistribución por peer	Recomendado	4.4
13	Aplica límite de prefijos de blackhole por participante	Recomendado	6.4
14	Implementa expiración o alerta de blackholes obsoletos	Recomendado	6.4

#	Elemento	Criticidad	Sección
15	Publica documentación completa del servicio	Crítico	9
16	Publica declaración de límite de responsabilidad	Recomendado	3.1
17	Ofrece prefijo de prueba y procedimiento de verificación	Recomendado	10.1
18	Expone los blackholes activos en el looking glass	Recomendado	10.2
19	Registra los eventos de blackholing para auditoría	Recomendado	10.3
20	Publica política de uso aceptable	Recomendado	10.4
21	Ofrece sesión BGP dedicada para blackholes	Opcional	8
22	Publica el porcentaje de participantes que aceptan blackholes	Opcional	10.2

13. Configuración de referencia del route server

Ejemplo en BIRD 2. Los valores son de documentación y deben sustituirse.

```
ASN del route server   : 64500
 ASN del participante   : 64511
 LAN de peering IPv4    : 198.51.100.0/24
 LAN de peering IPv6    : 2001:db8:1::/64
 Blackhole next-hop IPv4  : 198.51.100.66
 Blackhole next-hop IPv6  : 2001:db8:1::66
 Prefijo del participante  : 203.0.113.0/24
# ---------- Objetos comunes ----------
 define BLACKHOLE_COMM = (65535, 666);
 define NO_EXPORT_COMM = (65535, 65281);
 define BH_CONFIRMED = (64500, 666);

 define BH_NEXTHOP_V4 = 198.51.100.66;
 define BH_NEXTHOP_V6 = 2001:db8:1::66;

 # Umbrales de longitud
 define PL_RS_NORMAL_V4 = [ 0.0.0.0/0{8,24} ];
 define PL_RS_BH_V4  = [ 0.0.0.0/0{8,32} ];

 # Infraestructura que nunca puede blackholearse
 define PL_RS_PROTECTED_V4 = [ 198.51.100.0/24+ ];
 define PL_RS_PROTECTED_V6 = [ 2001:db8:1::/64+ ];

 # Conjunto autorizado del participante, generado desde IRR y RPKI.
 # El sufijo '+' habilita cualquier mas-especifico, solo para blackholes.
 define PL_AS64511_V4 = [ 203.0.113.0/24 ];
 define PL_AS64511_BH_V4 = [ 203.0.113.0/24+ ];

 function is_blackhole() {
    return BLACKHOLE_COMM ~ bgp_community;
 }

 # ---------- Import desde el participante (IPv4) ----------
 filter f_rs_in_as64511_v4 {
  # Infraestructura del IXP: nunca
    if net ~ PL_RS_PROTECTED_V4 then reject;

    if is_blackhole() then {
       # Umbral extendido, solo para blackholes
       if ! (net ~ PL_RS_BH_V4) then reject;
```

```
# Cubierto por espacio autorizado del participante
      if ! (net ~ PL_AS64511_BH_V4) then reject;

      # Marca de confirmacion
      bgp_community.add(BH_CONFIRMED);
      accept;
}

# Ruta normal
   if ! (net ~ PL_RS_NORMAL_V4) then reject;
   if from != bgp_next_hop then reject;    # anti next-hop hijacking
   if ! (net ~ PL_AS64511_V4) then reject;
# ... filtrado IRRDB y validacion RPKI estricta habituales ...
   accept;
}

# ---------- Export hacia los participantes (IPv4) ----------
filter f_rs_out_v4 {
   if BH_CONFIRMED ~ bgp_community then {
      bgp_next_hop = BH_NEXTHOP_V4;      # excepcion a RFC 7947
      bgp_community.add(NO_EXPORT_COMM);
}
# ... comunidades de control de redistribucion ...
   accept;
}
```

Para IPv6, replicar cada objeto sustituyendo el sufijo _V4 por _V6, con [::/0{19,48}] para rutas normales y [::/0{19,128}] para blackholes.

La convención de nomenclatura usada aquí (PL_ para conjuntos de prefijos, f_rs_in_ y f_rs_out_ para filtros) es la misma que la del Anexo A.7.1, con el prefijo rs_ para distinguir los objetos del route server de los del participante.

Verificación previa a producción. Se recomienda validar en laboratorio, como mínimo, que un /32 con la comunidad es aceptado y reescrito; que un /32 sin la comunidad es rechazado; que un /32 fuera del espacio autorizado del participante es rechazado; y que un /32 que cubre infraestructura del IXP es rechazado.

14. Errores comunes

#	Error	Responsable	Síntoma	Sección
1	El route server filtra más-específicos antes de evaluar la comunidad	IXP	El anuncio se descarta sin mensaje; el participante concluye que el servicio no existe	5.3, 5.4
2	Validación RPKI estricta aplicada a blackholes	IXP	Todos los blackholes resultan Invalid y se rechazan	6.2
3	No se reescribe el NEXT_HOP	IXP	El prefijo se propaga con el next-hop del atacado, que se congestiona igual	5.2
4	Sin lista de prefijos de infraestructura protegida	IXP	Un error de un participante puede afectar la plataforma	6.3
5	Sin validación de autorización sobre el prefijo cubriente	IXP	Un participante puede dejar inalcanzable a otro	6.1
6	Servicio implementado solo en IPv4	IXP	Los ataques sobre IPv6 quedan sin mitigación	5.1
7	Sin procedimiento de prueba publicado	IXP	El fallo se descubre durante el incidente	10.1
8	La política de salida del participante corta en /24	Participante	El más-específico nunca sale de su route	Anexo A
9	El participante no configura la política de importación	Participante	El servicio parece funcionar pero el tráfico sigue llegando	Anexo A
10	El blackhole se propaga hacia el tránsito del participante	Participante	Más-específico global no deseado	Anexo A
11	Blackholes olvidados sin retirar	Participante	Servicio propio inalcanzable de forma indefinida, sin alarma	6.4

#	Error	Responsable	Síntoma	Sección
12	Se anuncia un /24 en lugar de un /32	Participante	256 direcciones apagadas para proteger una	5.1
13	Validación RPKI estricta aplicada a blackholes	Participante	El servicio funciona, pero se abre superficie a secuestro de sub-prefijo	Anexo A

15. Glosario

Blackholing — Descarte deliberado del tráfico dirigido a un prefijo, señalizado mediante BGP.

Blackhole next-hop — Dirección IP definida por el IXP hacia la cual el route server reescribe el NEXT_HOP de los prefijos de blackhole.

BLACKHOLE (comunidad) — Comunidad BGP bien conocida 65535:666 (0xFFFF029A), definida en RFC 7999.

Daño colateral — Tráfico legítimo descartado junto con el tráfico de ataque, consecuencia de la granularidad por prefijo.

IRR / AS-SET — Registros de enrutamiento donde un operador declara el conjunto de prefijos y ASN que está autorizado a anunciar.

maxLength — Atributo de un ROA que autoriza más-específicos hasta cierta longitud. RFC 9319 desaconseja su uso.

Prefijo cubriente — Prefijo igual o más corto que contiene al prefijo de blackhole y que el participante está autorizado a anunciar.

Route server — Sistema del IXP que mantiene sesiones BGP con los participantes y redistribuye rutas entre ellos, sin participar del reenvío de paquetes.

ROV (Route Origin Validation) — Validación del ASN de origen de un anuncio contra los ROA de RPKI (RFC 6811).

RTBH (Remotely Triggered Black Hole) — Denominación tradicional del blackholing señalizado por BGP. RFC 9319 usa el término RTDR (Remotely Triggered Discard Route).

16. Referencias

Referencia principal

- RFC 7999 — *BLACKHOLE Community*. Define la comunidad de señalización y las recomendaciones operativas y de seguridad sobre las que se apoya toda esta guía. Ver la correspondencia sección por sección en 1.6.

Referencias complementarias

Citadas por RFC 7999 o necesarias para su aplicación en un IXP:

- RFC 1997 — BGP Communities Attribute (define NO_EXPORT y NO_ADVERTISE)
- RFC 4271 — A Border Gateway Protocol 4 (BGP-4)
- RFC 6811 — BGP Prefix Origin Validation
- RFC 7454 (BCP 194) — BGP Operations and Security (filtrado estricto referido por RFC 7999)
- RFC 7606 — Revised Error Handling for BGP UPDATE Messages
- RFC 7947 — Internet Exchange BGP Route Server
- RFC 7948 — Internet Exchange BGP Route Server Operations
- RFC 8092 / RFC 8195 — BGP Large Communities y su uso
- RFC 9319 (BCP 185) — The Use of maxLength in the RPKI

Referencias de contexto

Mencionadas para delimitar el alcance, no aplicadas en esta guía:

- RFC 5635 — Remote Triggered Black Hole Filtering with uRPF (modelo dentro de un mismo AS; ver 1.3)
- RFC 8955 / RFC 8956 — Dissemination of Flow Specification Rules, IPv4 e IPv6 (técnica complementaria; ver 11.2)

Investigación aplicada

- *Blackholing at IXPs: On the Effectiveness of DDoS Mitigation in the Wild* (PAM 2016)
- *Stellar: Network Attack Mitigation using Advanced Blackholing* (CoNEXT 2018)
- *Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs* (IMC 2019)
- *A Tale of Two Synergies: Uncovering RPKI Practices for RTBH at IXPs* (PAM 2024)

Documentos previos de LAC-IX

- *Mejores Prácticas BGP para Participantes de IXP* — Grupo Técnico de LAC-IX

Anexo A — Material para participantes

Este anexo está redactado para ser adaptado y entregado por el IXP a sus participantes. Contiene únicamente lo que el participante debe hacer; todo lo referido a la plataforma del IXP queda fuera.

A.1 Qué necesita saber antes de empezar

- El blackholing en el IXP afecta únicamente al tráfico que llega por el IXP. Conviene combinarlo con las comunidades de blackholing del proveedor de tránsito.
- Aceptar blackholes de otros participantes es lo que hace funcionar el servicio para todos. Es recíproco: si la mayoría no acepta, el servicio no sirve para nadie, incluido quien lo dispara.
- Ambos sentidos, recepción y disparo, se configuran antes de necesitarlos. No es algo que se pueda configurar durante un incidente.

A.2 Recibir blackholes

Es la parte que la mayoría de los participantes no configura, y la razón principal de la baja eficacia medida del mecanismo.

Política de importación. La política hacia los route servers del IXP normalmente rechaza prefijos más específicos que /24 y /48. Se agrega una excepción ubicada antes de esa regla:

- aceptar prefijos de hasta /32 en IPv4 y /128 en IPv6 únicamente si llevan la comunidad de blackholing, o la comunidad de confirmación del IXP;
- seguir rechazando cualquier otro más-específico.

Si el IXP ofrece una sesión dedicada a blackholes, la política se reduce a aceptar /32 y /128 exclusivamente desde ese peer.

Qué hacer con el prefijo aceptado. Dos opciones:

- *Encaminar hacia la dirección de blackhole del IXP*. No requiere acción adicional: el next-hop viene reescrito y el IXP descarta las tramas. El tráfico egresa por el puerto del IXP.
- *Descartar localmente (más eficiente).* Reescribir el next-hop hacia una dirección propia enrutada a una interfaz de descarte. El tráfico muere en la red propia y no consume el puerto del IXP.

Protecciones.

- No propagar los prefijos de blackhole recibidos hacia proveedores de tránsito, clientes ni otros peers.
- Verificar que NO_EXPORT esté presente y sea respetada por la plataforma.
- Aplicar un límite de prefijos específico para blackholes.
- No aceptar blackholes que cubran direcciones propias críticas: LAN de peering, resolvers, servidores de nombres autoritativos.

A.3 Disparar un blackhole

1. Originar el prefijo más específico posible: /32 en IPv4, /128 en IPv6. Anunciar un /24 completo para proteger una dirección multiplica el daño colateral.
2. Adjuntar la comunidad de blackholing del IXP, o su equivalente large si el ASN es de 32 bits.
3. **Verificar que la política de salida propia permite anunciar ese más-específico.** La lista de prefijos de salida hacia el IXP casi con seguridad termina en le 24. Es el error de configuración más frecuente del lado del disparador, y hace que el anuncio nunca salga del router.
4. Considerar el uso de las comunidades de control del IXP para anunciar el blackhole solo a los sistemas autónomos que originan el ataque, preservando el alcance desde el resto.
5. Confirmar en el *looking glass* del IXP que el prefijo fue aceptado y que el NEXT_HOP fue reescrito.

A.4 Higiene operativa

- Retirar el blackhole cuando el ataque termine. Verificar si continúa requiere retirar el anuncio y observar, por lo que es habitual anunciar y retirar de forma repetida.

- Revisar periódicamente los blackholes propios activos. Uno olvidado deja un servicio inalcanzable de forma indefinida y sin síntoma evidente.
- Documentar internamente cada disparo: quién, cuándo, qué prefijo y por qué.

A.5 ROA y maxLength

- Emitir ROA mínimos, sin usar el atributo maxLength, conforme a RFC 9319.
- No emitir ROA con maxLength /32 o /128 para "habilitar" los blackholes propios. Esa práctica expone a secuestros de sub-prefijo con origen falsificado.
- La compatibilidad entre RPKI y blackholing es responsabilidad del route server del IXP, no del participante mediante ROA no mínimos.
- Las redes que aplican validación estricta en Internet rechazarán los más-específicos de blackhole. Es una razón adicional para no propagarlos fuera del IXP.

A.6 Lista de verificación para el participante

#	Elemento	Criticidad
1	Acepta /32 y /128 con la comunidad de blackholing desde los route servers	Crítico
2	La política de salida permite originar el más-específico de blackhole	Crítico
3	No propaga blackholes recibidos fuera del AS propio	Crítico
4	Puede originar blackholes en IPv4 e IPv6	Crítico
5	Emite ROA mínimos, sin maxLength inflado	Recomendado
6	Protege sus direcciones críticas frente a blackholes recibidos	Recomendado
7	Tiene procedimiento documentado de disparo y retiro	Recomendado
8	Ejecutó la prueba de verificación del IXP	Recomendado

A.7 Configuraciones de referencia

Valores de documentación, a sustituir por los del IXP y del participante correspondientes.

```
Route server del IXP (IPv4)     : 198.51.100.250
 Blackhole next-hop del IXP     : 198.51.100.66
 ASN del route server del IXP : 64500
 ASN propio                     : 64511
 Prefijo propio                 : 203.0.113.0/24
 Destino bajo ataque            : 203.0.113.10
 Descarte local propio          : 192.0.2.1 (usar espacio propio no anunciado)
 Marca de ruta de blackhole     : tag 666
```

A.7.1 Convención de nomenclatura

Los ejemplos de recepción y de disparo de una misma plataforma están pensados para coexistir en el mismo router. Para que no colisionen, todos usan el siguiente esquema:

Elemento	Patrón	Ejemplos
Lista de prefijos entrantes, rutas normales	PL-IXP-IN-V4	PL-IXP-IN-V6
Lista de prefijos entrantes, rango de blackhole	PL-IXP-IN-BH-V4	PL-IXP-IN-BH-V6
Lista de prefijos salientes, rutas normales	PL-IXP-OUT-V4	PL-IXP-OUT-V6
Lista de prefijos salientes, rango de blackhole	PL-IXP-OUT-BH-V4	PL-IXP-OUT-BH-V6
Lista de comunidades	CL-BLACKHOLE	
Política de importación	RM-IXP-IN-V4	
Política de exportación	RM-IXP-OUT-V4	
Política de redistribución de blackholes	RM-IXP-REDIST-BH-V4	

Equivalencias por plataforma:

Concepto	Cisco IOS / Arista	Cisco IOS-XR	Juniper Junos	BIRD 2	MikroTik
Lista de prefijos	PL-...	PS-... (prefix-set)	route-filter en línea	define	parámetros de la regla
Lista de comunidades	CL-BLACKHOLE	CS-BLACKHOLE	community BLACKHOLE	define	valor literal
Política	RM-... (route-map)	RP-... (route-policy)	IXP-IN-V4 (policy-statement)	f_ixp_in_v4 (filter)	ixp-in-v4 (cadena)

Para IPv6, replicar cada objeto sustituyendo el sufijo -V4 por -V6, con los umbrales /48 y /128 en lugar de /24 y /32.

A.7.2 Cisco IOS / IOS-XE

```
! ---------- Objetos comunes ----------
 ip community-list standard CL-BLACKHOLE permit 65535:666
 !
 ip prefix-list PL-IXP-IN-V4  seq 5 permit 0.0.0.0/0 le 24
 ip prefix-list PL-IXP-IN-BH-V4 seq 5 permit 0.0.0.0/0 ge 25 le 32
 ip prefix-list PL-IXP-OUT-V4  seq 5 permit 203.0.113.0/24
 ip prefix-list PL-IXP-OUT-BH-V4 seq 5 permit 203.0.113.0/24 ge 25 le 32
 !
 ip route 192.0.2.1 255.255.255.255 Null0
 !
 ! ---------- Recepcion ----------
 route-map RM-IXP-IN-V4 permit 10
  description Blackhole valido: aceptar y descartar localmente
  match ip address prefix-list PL-IXP-IN-BH-V4
  match community CL-BLACKHOLE
  set ip next-hop 192.0.2.1
 !
 route-map RM-IXP-IN-V4 deny 20
  description Cualquier otro mas-especifico se rechaza
  match ip address prefix-list PL-IXP-IN-BH-V4
 !
 route-map RM-IXP-IN-V4 permit 30
  match ip address prefix-list PL-IXP-IN-V4
 !
```

```
! ---------- Disparo ----------
route-map RM-IXP-OUT-V4 permit 10
 description Blackholes propios
 match ip address prefix-list PL-IXP-OUT-BH-V4
 match tag 666
 set community 65535:666
!
route-map RM-IXP-OUT-V4 permit 20
 match ip address prefix-list PL-IXP-OUT-V4
!
! ---------- Sesion ----------
router bgp 64511
 address-family ipv4
  redistribute static route-map RM-IXP-OUT-V4
  neighbor 198.51.100.250 route-map RM-IXP-IN-V4 in
  neighbor 198.51.100.250 route-map RM-IXP-OUT-V4 out
!
! ---------- Activacion durante el ataque ----------
ip route 203.0.113.10 255.255.255.255 Null0 tag 666
!
! ---------- Retiro al finalizar ----------
no ip route 203.0.113.10 255.255.255.255 Null0 tag 666
```

Variantes:

- Para encaminar hacia la dirección de blackhole del IXP en lugar de descartar localmente, omitir set ip next-hop en RM-IXP-IN-V4 secuencia 10.
- Para anunciar el blackhole a todos los peers excepto AS64504, en RM-IXP-OUT-V4 secuencia 10: set community 65535:666 64500:64500 0:64504 additive.

A.7.3 Cisco IOS-XR

```
! ---------- Objetos comunes ----------
 community-set CS-BLACKHOLE
  65535:666
 end-set
 !
 prefix-set PS-IXP-IN-V4
  0.0.0.0/0 le 24
 end-set
 !
 prefix-set PS-IXP-IN-BH-V4
  0.0.0.0/0 ge 25 le 32
 end-set
 !
```

```
prefix-set PS-IXP-OUT-V4
  203.0.113.0/24
 end-set
 !
 prefix-set PS-IXP-OUT-BH-V4
  203.0.113.0/24 ge 25 le 32
 end-set
 !
 ! ---------- Recepcion ----------
 route-policy RP-IXP-IN-V4
  if destination in PS-IXP-IN-BH-V4 then
 if community matches-any CS-BLACKHOLE then
   set next-hop 192.0.2.1
   pass
 else
   drop
 endif
  elseif destination in PS-IXP-IN-V4 then
 pass
  else
 drop
  endif
end-policy
!
! ---------- Redistribucion de blackholes propios ----------
route-policy RP-IXP-REDIST-BH-V4
  if tag eq 666 then
 set community (65535:666)
 pass
  else
 drop
  endif
end-policy
!
! ---------- Disparo ----------
route-policy RP-IXP-OUT-V4
  if destination in PS-IXP-OUT-BH-V4 and community matches-any CS-BLACKHOLE then
 pass
  elseif destination in PS-IXP-OUT-V4 then
 pass
  else
 drop
  endif
end-policy
!
```

```
! ---------- Sesion ----------
router bgp 64511
 address-family ipv4 unicast
  redistribute static route-policy RP-IXP-REDIST-BH-V4
 !
 neighbor 198.51.100.250
  address-family ipv4 unicast
   route-policy RP-IXP-IN-V4 in
   route-policy RP-IXP-OUT-V4 out
!
router static
 address-family ipv4 unicast
  192.0.2.1/32 Null0
!
! ---------- Activacion durante el ataque ----------
router static
 address-family ipv4 unicast
  203.0.113.10/32 Null0 tag 666
```

A.7.4 Juniper Junos

```
policy-options {
 community BLACKHOLE members 65535:666;

 /* ---------- Recepcion ---------- */
 policy-statement IXP-IN-V4 {
    term blackhole-valido {
       from {
          community BLACKHOLE;
          route-filter 0.0.0.0/0 prefix-length-range /25-/32;
       }
       then {
          next-hop 192.0.2.1;
          accept;
       }
       }
    term rechazar-otros-especificos {
       from { route-filter 0.0.0.0/0 prefix-length-range /25-/32; }
       then reject;
    }
    term rutas-normales {
       from { route-filter 0.0.0.0/0 upto /24; }
       then accept;
    }
    then reject;
 }
```

```
/* ---------- Disparo ---------- */
  policy-statement IXP-OUT-V4 {
     term blackholes-propios {
        from {
           protocol static;
           tag 666;
           route-filter 203.0.113.0/24 prefix-length-range /25-/32;
        }
        then {
           community add BLACKHOLE;
           accept;
        }
     }
     term prefijos-propios {
        from { route-filter 203.0.113.0/24 exact; }
        then accept;
     }
     then reject;
  }
 }

  protocols {
   bgp {
     group IXP-RS {
        neighbor 198.51.100.250 {
           import IXP-IN-V4;
           export IXP-OUT-V4;
        }
     }
   }
 }
routing-options {
   static {
     route 192.0.2.1/32 discard;

     /* ---------- Activacion durante el ataque ---------- */
     route 203.0.113.10/32 {
        discard;
        tag 666;
     }
   }
 }
```

A.7.5 Arista EOS

```
! ---------- Objetos comunes ----------
 ip community-list CL-BLACKHOLE permit 65535:666
 !
 ip prefix-list PL-IXP-IN-V4  seq 10 permit 0.0.0.0/0 le 24
 ip prefix-list PL-IXP-IN-BH-V4 seq 10 permit 0.0.0.0/0 ge 25 le 32
 ip prefix-list PL-IXP-OUT-V4  seq 10 permit 203.0.113.0/24
 ip prefix-list PL-IXP-OUT-BH-V4 seq 10 permit 203.0.113.0/24 ge 25 le 32
 !
 ip route 192.0.2.1/32 Null0
 !
 ! ---------- Recepcion ----------
 route-map RM-IXP-IN-V4 permit 10
   description Blackhole valido: aceptar y descartar localmente
   match community CL-BLACKHOLE
   match ip address prefix-list PL-IXP-IN-BH-V4
   set ip next-hop 192.0.2.1
 !
 route-map RM-IXP-IN-V4 deny 20
   match ip address prefix-list PL-IXP-IN-BH-V4
 !
 route-map RM-IXP-IN-V4 permit 30
   match ip address prefix-list PL-IXP-IN-V4
 !
 ! ---------- Disparo ----------
 route-map RM-IXP-OUT-V4 permit 10
   description Blackholes propios
   match ip address prefix-list PL-IXP-OUT-BH-V4
   match tag 666
   set community 65535:666 additive
 !
 route-map RM-IXP-OUT-V4 permit 20
   match ip address prefix-list PL-IXP-OUT-V4
 !
 ! ---------- Sesion ----------
 router bgp 64511
   redistribute static route-map RM-IXP-OUT-V4
   neighbor 198.51.100.250 route-map RM-IXP-IN-V4 in
   neighbor 198.51.100.250 route-map RM-IXP-OUT-V4 out
 !
 ! ---------- Activacion durante el ataque ----------
 ip route 203.0.113.10/32 Null0 tag 666
```

A.7.6 BIRD 2

```
# ---------- Objetos comunes ----------
 define BLACKHOLE_COMM = (65535, 666);
 define LOCAL_DISCARD = 192.0.2.1;

 define PL_IXP_IN_V4  = [ 0.0.0.0/0{8,24} ];
 define PL_IXP_IN_BH_V4 = [ 0.0.0.0/0{25,32} ];
 define PL_IXP_OUT_V4  = [ 203.0.113.0/24 ];
 define PL_IXP_OUT_BH_V4 = [ 203.0.113.0/24{25,32} ];

 # ---------- Recepcion ----------
 filter f_ixp_in_v4 {
  if net ~ PL_IXP_IN_BH_V4 then {
     if ! (BLACKHOLE_COMM ~ bgp_community) then reject;
     dest = RTD_BLACKHOLE;    # descarte local
     accept;
  }
  if ! (net ~ PL_IXP_IN_V4) then reject;
  accept;
 }

 # ---------- Disparo ----------
 filter f_ixp_out_v4 {
  if BLACKHOLE_COMM ~ bgp_community then {
     if net ~ PL_IXP_OUT_BH_V4 then accept;
     reject;
  }
  if net ~ PL_IXP_OUT_V4 then accept;
  reject;
 }

 # ---------- Blackholes activos ----------
 protocol static st_ixp_bh_v4 {
  ipv4;
  route 203.0.113.10/32 blackhole {
     bgp_community.add(BLACKHOLE_COMM);
  };
 }

 # ---------- Sesion ----------
 protocol bgp ixp_rs_v4 {
  local as 64511;
  neighbor 198.51.100.250 as 64500;
  ipv4 {
     import filter f_ixp_in_v4;
     export filter f_ixp_out_v4;
  };
 }
```

Para encaminar hacia la dirección de blackhole del IXP en lugar de descartar localmente, omitir la asignación de dest en f_ixp_in_v4.

A.7.7 MikroTik RouterOS

La sintaxis de filtros de enrutamiento cambió de forma sustantiva entre RouterOS v6 y v7. El ejemplo corresponde a v6; verificar antes de aplicar en v7.

```
# ---------- Recepcion ----------
 /routing filter
 add chain=ixp-in-v4 bgp-communities=65535:666 prefix-length=25-32 \
  action=accept set-type=blackhole
 add chain=ixp-in-v4 prefix-length=25-32 action=discard
 add chain=ixp-in-v4 prefix-length=8-24 action=accept
 add chain=ixp-in-v4 action=discard

 # ---------- Disparo ----------
 add chain=ixp-out-v4 prefix=203.0.113.0/24 prefix-length=25-32 \
  action=accept set-bgp-communities=65535:666
 add chain=ixp-out-v4 prefix=203.0.113.0/24 prefix-length=24 action=accept
 add chain=ixp-out-v4 action=discard

 # ---------- Sesion ----------
 /routing bgp peer set [find remote-address=198.51.100.250] \
  in-filter=ixp-in-v4 out-filter=ixp-out-v4

 /routing bgp instance set default redistribute-static=yes

 # ---------- Activacion durante el ataque ----------
 /ip route add dst-address=203.0.113.10/32 type=blackhole comment="RTBH"

 # ---------- Retiro al finalizar ----------
 /ip route remove [find comment="RTBH"]
```

A.7.8 Verificación

```
! El anuncio salio del router propio
 show bgp ipv4 unicast neighbors 198.51.100.250 advertised-routes | include 203.0.113.10

 ! Un peer lo recibio con el next-hop reescrito
 show bgp ipv4 unicast 203.0.113.10/32
   -> next-hop debe ser la direccion de blackhole del IXP
   -> comunidades: 65535:666, la de confirmacion del IXP, y 65535:65281
```