FORT

Tecnologías de Ruteo
para una Internet Libre y Abierta

Seguridad en el ruteo de América Latina y el Caribe

NIC MÉXICO

lacnic

Tabla de contenido

Agradecimientos

Redacción:
Augusto Luciano Mathurin

Dirección:
Carolina Caeiro
Guillermo Cicileo

Revisión:
Carlos Martinez-Cagnazzo
Raúl Ramirez Castañeda

Edición de estilo:
María Eugenia Martínez

Edición gráfica:
Martin Mañana

Traducción al inglés:
Justina Díaz Cornejo

Colaboración:
Andrei Robachevsky
Gerardo Pias
Mariela Rocha

Introducción

El enrutamiento es uno de los pocos componentes de la infraestructura de Internet que sigue siendo inseguro. Hoy en día es fácil secuestrar los sistemas de enrutamiento para bloquear sitios web, espiar a los usuarios y redirigir el tráfico a destinos falsos. Estas vulnerabilidades pueden afectar el libre flujo de información alrededor del mundo y amenazan la seguridad y la privacidad de los usuarios.

Los organismos de estandarización de Internet han luchado durante mucho tiempo para identificar estrategias que hagan que el enrutamiento sea más seguro. Para abordar y comprender esta problemática, tanto en el mundo como en nuestra región, se presenta este informe, que consta de tres partes:

- En primer lugar, se explica de forma introductoria cómo Internet puede ser foco de distintos ataques con naturalezas técnicas muy distintas, para luego pasar a los ataques en la infraestructura de ruteo que devienen en incidentes: *hijacks* y *leaks* en el protocolo BGP.
- Luego se realiza un exhaustivo análisis de datos de los incidentes registrados en los años 2017, 2018 y parte de 2019. Esto, con el objetivo de comprender —en base a estadísticas que pueden estudiarse por países— cómo ha ido evolucionando la seguridad de ruteo en los últimos años. Estas nos permiten tener una idea de cómo se encuentra nuestra región comparada con el resto del mundo y comprobar cómo, efectivamente, estos incidentes pueden afectar las libertades en Internet.
- Finalmente, se detallan las distintas medidas que los operadores de red pueden comenzar a implementar para mejorar el sistema de ruteo de Internet. Principalmente, la implementación de infraestructura de clave pública para la certificación de recursos (RPKI), que ha sido la iniciativa más exitosa para asegurar el enrutamiento BGP.

Este reporte forma parte de una campaña de despliegue de RPKI en América Latina y el Caribe, promovida por el proyecto FORT, una iniciativa conjunta de LACNIC y NIC.MX que busca aumentar la seguridad y la resiliencia de los sistemas de enrutamiento.

Qué está en juego

Sugerencia

Esta sección pretende ser una introducción a conceptos técnicos y temas que le dan contexto al reporte. Si usted tiene conocimientos de operador de red, puede pasar directamente a la sección «*Línea de tiempo de incidentes*».

Los llamados ciberataques ya no son una novedad. Pasamos de unos pocos incidentes ocupando titulares sorprendentes a que sean parte de nuestra rutina informativa y así nos enteramos del bloqueo, *data breach*, *malware* o ataque de la semana.

Algunos gobiernos buscan impedir que sus habitantes puedan comunicarse libremente por Internet,[1] ya sea por razones culturales, históricas, para evitar manifestaciones o incidentes organizados, para ocultar verdades incómodas o, simplemente, para mantener más controlada a la población en nombre de la seguridad y el bienestar social.

Asociaciones criminales se dedican a estafas masivas *online* e incluso organizaciones intentan sabotear a sus competidores. Pero, ¿cómo pueden realizarse *ataques* en Internet?

Para abordar esta pregunta, primero hay que pensar cuál es el objetivo del atacante o, en otras palabras, cuál es la cualidad de la información que se desea afectar. Es posible atacar la confidencialidad (lo que se traduce en ataques de espionaje), la disponibilidad (que se traduce en censura) o la integridad (lo que deviene en fraudes).

Una vez definido el objetivo, el *qué* atacar, se puede pasar a plantear la estrategia o el *cómo* y, como suele suceder, es posible llegar al mismo destino (cumplir el objetivo) por distintos caminos. La arquitectura de Internet es compleja, los tipos de ataques pueden hacerse en distintos niveles o capas y van evolucionando con el tiempo. A la par, las medidas de seguridad para mitigarlos van perfeccionándose.

Respecto a la censura, que es el objetivo más común, hay distintos tipos de estrategias técnicas para llevarla a cabo.[2] Las más conocidas son:

- Bloquear el acceso a determinadas direcciones IP. Por ejemplo, un ISP puede evitar que sus clientes accedan a cierto sitio, descartando todas las solicitudes que tengan como destino la dirección IP correspondiente a los servidores donde se aloja el portal a bloquear. Esta técnica también puede utilizarse desde el otro extremo, es decir, un servidor que rechace las

[1]<https://www.maketecheasier.com/internet-censorship-block-citizens-from-websites/>

[2]<http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/>

solicitudes provenientes de un conjunto de IP. Por ejemplo, las que pertenezcan a determinado país.

- Filtrar por DNS. En general, los ISP ofrecen su propio servidor de resolución de DNS, es decir, el servicio que traduce las URL o dominios (como podría ser www.lacnic.net) a una dirección IP (en el caso anterior, 200.3.14.184). Es posible bloquear los dominios pertenecientes a los sitios que deseen censurarse, y así los clientes no podrán llegar al destino deseado. Esta técnica puede evadirse fácilmente cambiando el servidor de resolución DNS del dispositivo, aunque al día de hoy la gran mayoría de consultas DNS no se realizan por un medio cifrado. Es decir, los proveedores también pueden establecer filtros aun cuando estas no se realicen a sus servidores DNS.
- Filtrado por URL. Cuando los clientes se conectan a Internet por medio de un servidor proxy, es posible filtrar las direcciones o URL de los sitios web que contengan ciertas palabras.
- La solución de «bajar la palanca» también es posible. Se trata de apagar los *routers* por *software* (mediante *malware*) o desconectarlos físicamente. Así es posible dejar a una población sin acceso a Internet o bajar de la red a un servidor.
- Remoción de contenido. A veces no es necesario censurar todo un portal web, sino obligarlo de alguna forma para que deje de mostrar cierto contenido. Esta técnica es la más utilizada a la hora de resolver ciertas disputas legales, como una violación de derechos de autor.
- Ataques de denegación de servicio. Otra forma de tirar abajo un servidor es saturarlo, direccionando hacia él una cantidad irracional de tráfico basura.

Esta lista no es exhaustiva. Simplemente intenta dar una noción de la diversidad de ataques que pueden existir. Este informe se concentra en los ataques que ocurren en otra parte de la infraestructura de Internet: la capa de ruteo.

Como una red vial, Internet tiene sus propias autopistas e intersecciones, que consisten de cables y *routers*. Así como al conducir utilizamos un sistema de asistencia de GPS para saber cómo llegar de un punto A a un punto B, pasando por todas las rutas y paradas necesarias, Internet utiliza su propio sistema de navegación llamado BGP (Border Gateway Protocol, en inglés), el cual hace posible que el tráfico de datos en la red llegue a su destino.

Como ha ocurrido con la mayoría de los protocolos de Internet, BGP fue ideado para un escenario muy distinto al actual, a finales de los años 80, cuando solo era necesario conectar un puñado de redes. En esos momentos, la seguridad no era un principio central a tener en cuenta, por lo que el protocolo se basó fuertemente en un juego de confianza entre las partes.

Hoy en día la realidad es otra. Con más de 92.000[3] sistemas autónomos registrados y formando parte de este sistema de navegación de Internet, ya no puede asumirse que todos sus participantes son confiables. Incluso ciertos actores pueden ser adversarios, como por ejemplo dos ISP que compiten ofreciendo sus servicios a la misma población. ¿Cómo puede este escenario perjudicar a los usuarios de Internet?

Continuando con la analogía de la red vial, si los cables son las carreteras, BGP sería el sistema de señalización vial, es decir, todos los carteles que indican qué bifurcación tomar en cada caso para llegar

[3] <https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html>

al destino deseado. El problema, y al mismo tiempo virtud, de Internet es que no hay un organismo central que lo gestione, entonces no es posible controlar quién pone los carteles en esta red vial ni que sus instrucciones sean auténticas. Este es el llamado juego de confianza BGP y así se puede explotar para provocar ataques, censurar y vigilar a los usuarios.

Cuando ingresamos a un sitio web, ambos extremos (nuestro dispositivo y el servidor que aloja el portal) poseen una dirección IP que permite identificarlos. Así, los paquetes de datos tienen un origen y un destino, pero ¿qué pasa en el camino?

En el sistema postal, las cartas no se envían directamente a destino, sino a intermediarios: las oficinas postales.[4] Al enviar una carta, esta va a la oficina postal asignada en nuestra ciudad y puede pasar por varias oficinas postales intermedias hasta llegar a la ciudad que la entregará en el domicilio que deseamos. En Internet, cuando enviamos paquetes de datos desde nuestro dispositivo hasta el extremo deseado, estos primero son enviados a lo que serían las oficinas postales en el correo físico: los sistemas autónomos.

Un sistema autónomo es una red o conjunto de redes administrada por una organización y que tiene una política de ruteo en común. Por lo general, los sistemas autónomos son ISP u organizaciones que conectan múltiples ISP. Así como los dispositivos conectados a Internet se identifican con una dirección IP, los sistemas autónomos se identifican con un número de 16 o 32 bits, el ASN (Autonomous System Number, en inglés).

Cada sistema autónomo anuncia los prefijos (conjuntos de direcciones) IP a los cuales está conectado y puede transmitir información; los otros sistemas autónomos pueden armar sus rutas en base a estos anuncios para lograr que los paquetes de información que transportan lleguen a su destino. Esto hace de BGP un protocolo potente y flexible, que permite que la interconexión de redes pueda actualizarse de forma dinámica, logrando un intercambio de rutas administrable y una rápida respuesta en el caso de que una ruta deje de estar disponible.

Pero, como hemos anotado, BGP no se diseñó con una perspectiva de seguridad y esto lo hace vulnerable a ciertos ataques. Un sistema autónomo puede anunciar rutas hacia un prefijo de direcciones IP que en realidad no controla y estos anuncios, en caso de no filtrarse, pueden esparcirse por toda la red. En ese caso, todo el tráfico destinado a esas direcciones IP sería encaminado a este sistema autónomo que realizó el anuncio fraudulento de rutas. Esto amenaza el libre desarrollo de Internet; pueden idearse estrategias para generar censura o vigilancia, complementarias a las que ya hemos desarrollado.

El caso de un incidente de ruteo en Internet más emblemático sucedió en 2008,[5] cuando el gobierno paquistaní ordenó bloquear el portal de videos Youtube. Cuando el ISP público de este país recibió esa orden, configuró su sistema autónomo para que las conexiones que tuvieran como destino las direcciones IP de Youtube fueran descartadas. Su objetivo era que las solicitudes locales al portal fueran enviadas a un «agujero negro», bloqueando así el acceso a la población paquistaní. Pero esos anuncios

[4] ‹https://www.cloudflare.com/learning/security/glossary/what-is-bgp/›

[5] ‹https://dyn.com/blog/pakistan-hijacks-youtube-1/›

fraudulentos de prefijos se filtraron afuera de Pakistán y se esparcieron por toda la red. De pronto, todas las solicitudes a Youtube fueron redirigidas a Pakistán Telecom, con lo que se bloqueó ese sitio a gran parte del mundo durante horas y se generaron estragos en el funcionamiento del ISP por la gran cantidad de tráfico recibido.

Pasaron más de diez años desde ese incidente. Si bien hoy Internet es más resiliente —gracias al aprendizaje que deja ese tipo de eventos— la infraestructura de ruteo sigue siendo objeto de intentos de ataques para coartar libertades o afectar servicios de sus usuarios.

Tipos de incidentes

Para comprender los distintos tipos de incidentes que pueden provocarse en la capa de ruteo de Internet, primero es necesario entender cómo funciona BGP de forma más detallada. Este protocolo establece la comunicación entre sistemas autónomos que se configuran para que anuncien y/o aprendan rutas, lo que permitirá que se alcancen los destinos. Para hacer más controlado el proceso de pasaje de rutas, existen medidas como la implementación de filtros o políticas.

No obstante, la confianza en Internet radica en que cada organización anuncie solo sus propios prefijos o los prefijos de las organizaciones a las que les da tránsito. Sin embargo, eso no está garantizado en BGP, sino que se basa en el buen trabajo que hagan los operadores de las diferentes redes.

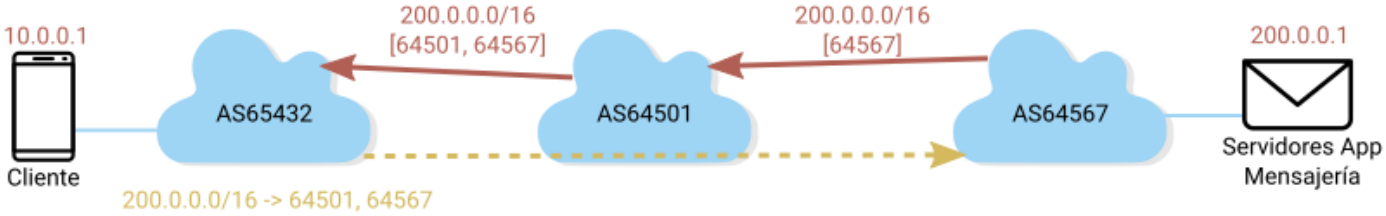
Ya sea de forma involuntaria o intencional, los dispositivos enrutadores pueden tener un comportamiento inesperado y anunciar un prefijo que no les corresponde anunciar. A esto se lo denomina *incidente de ruteo* y puede clasificarse en dos grandes tipos: *hijacks* y *leaks*.

Supongamos que queremos conectarnos a algún servicio de mensajería mediante una app. Tanto nuestro dispositivo móvil como los servidores de dicha app deben estar conectados a Internet y entre ambos extremos debe existir una ruta que permita establecer un flujo de información.

Ahora sabemos también que ambos extremos no estarán directamente conectados, sino que cada uno estará conectado a un sistema autónomo. Estos sistemas autónomos pertenecen a los ISP contratados por cada extremo para obtener conectividad. Para este caso, nuestro móvil tendrá asignada la dirección IP 10.0.0.1 y el ASN de nuestro proveedor será 65432, mientras que los servidores de la app estarán conectados mediante la dirección IP 200.0.0.1 y su sistema autónomo tendrá registrado el ASN 64567.

Cada sistema autónomo puede conectarse con otros sistemas autónomos; estos, a su vez, con otros y así sucesivamente. Supongamos que en este ejemplo solo existe una red intermedia.

¿Cómo logra encontrar a dónde enviar los paquetes de datos el AS65432, que es el que nos conecta para llegar a la dirección IP 200.0.0.1? Ahí es donde entra en juego el protocolo BGP. El AS64567, propietario de dicha dirección IP, anuncia que tiene el prefijo correspondiente. Así, el AS64501, que provee tránsito a los otros dos sistemas, anuncia la ruta 64501 64567 a nuestro AS65432 para llegar a la red 200.0.0.0/16.

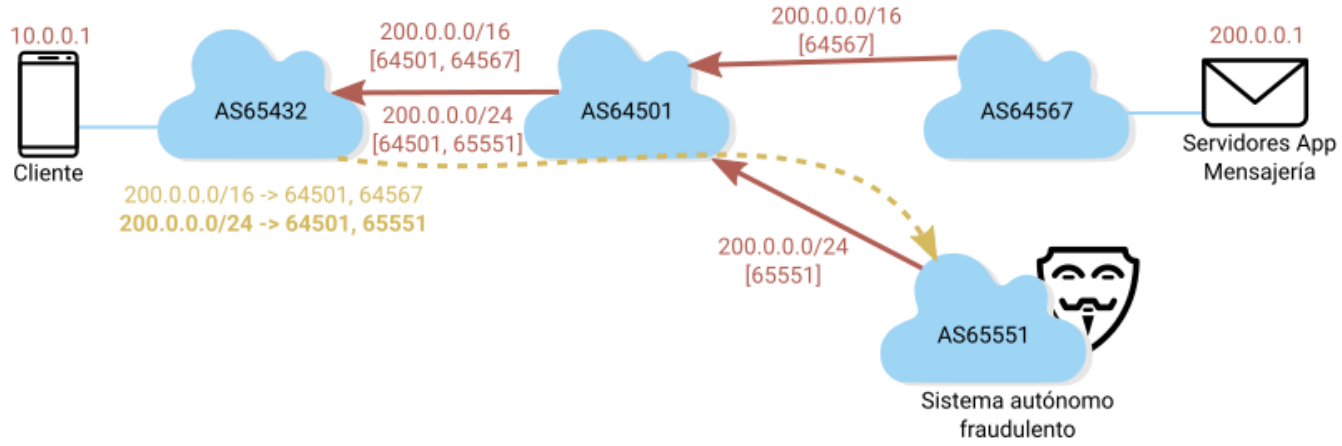


Así, cuando nuestro dispositivo quiere enviar información a la dirección 200.0.0.1, el AS65432 ya contará con la ruta adecuada para transmitir los datos desde nuestro móvil a los servidores de la app. De forma similar el AS64567 podrá obtener una ruta para llegar a nuestra dirección IP.

Secuestros de ruta (BGP *hijacks*)

Lo desarrollado anteriormente es un escenario donde no ocurren incidentes. Pero ¿qué pasa si agregamos un AS fraudulento que quiera provocar un *hijack* o secuestro de ruta? Se le llama «secuestro de ruta» a la acción de anunciar a Internet prefijos cuando no se está autorizado a hacerlo. Este anuncio indebido puede ser intencional o por error en la operación y logra propagarse porque ofrece una «mejor ruta». Es decir, el anuncio es de un prefijo más específico que el que anuncia el AS original o es un anuncio de una ruta más corta, exista o no.

Volviendo a nuestro ejemplo, supongamos que aparece un operador fraudulento que quiere bloquear el acceso a nuestra app. Entonces anuncia que posee un prefijo más específico que comprende la dirección 200.0.0.1 (en este caso 200.0.0.0/24).

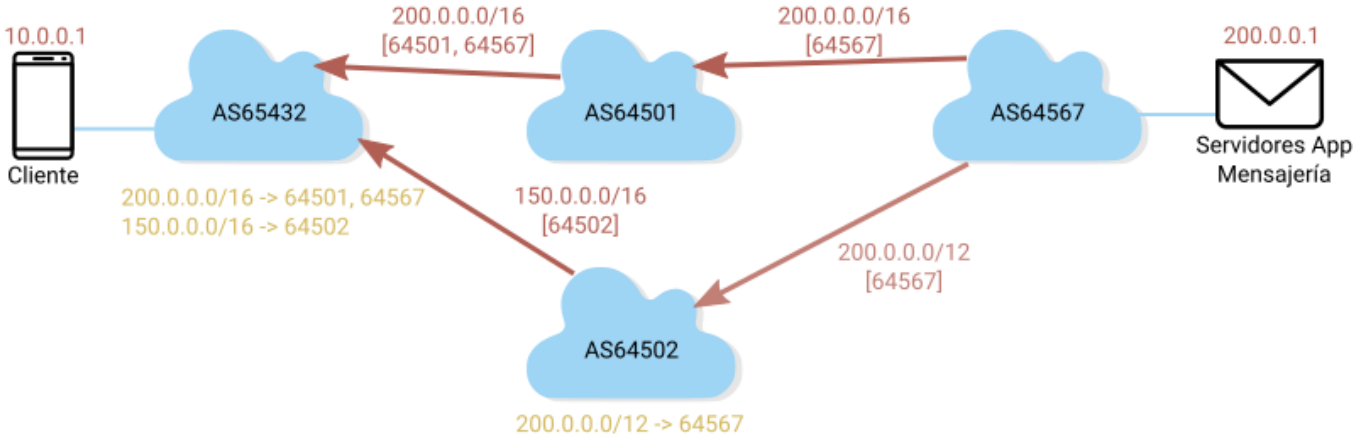


Entonces, al sistema autónomo que nos da conectividad le llegan dos rutas distintas para el mismo destino y termina eligiendo la más específica, es decir, la del AS fraudulento.

Fugas de ruta (BGP *leaks*)

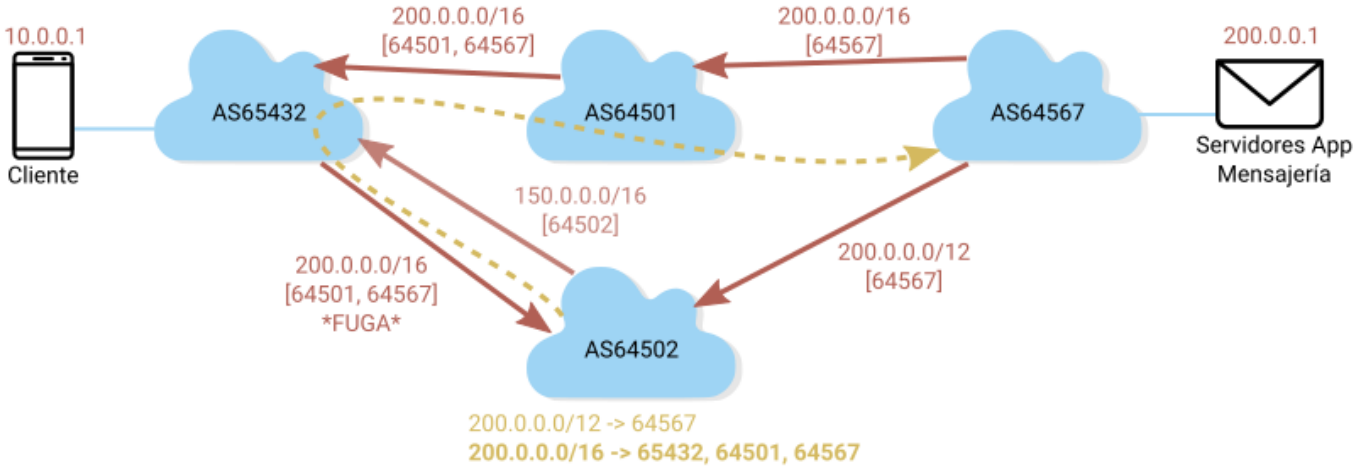
Otro tipo de incidente son las fugas o *leaks*. Cuando se propaga un anuncio de ruteo que supera su alcance deseado, es decir, que viola las políticas del sistema emisor, receptor o alguno de los que forman parte de la ruta, se produce una *fuga de ruta*.[6] Generalmente ocurre cuando un operador de red con más de un proveedor hacia arriba, de forma accidental, anuncia a uno de estos que posee una ruta hacia el destino a través de otro de los sistemas autónomos proveedores, transformando al operador inicial en un intermediario entre los dos proveedores de este.

Volviendo a nuestro ejemplo inicial, ahora supongamos que el AS65432, que nos brinda conectividad, cuenta con dos proveedores: el AS64501 que ya conocemos y el AS64502, que le permite llegar a la red 150.0.0.0/16. A su vez, este sistema autónomo está conectado con AS64567, aunque en principio es irrelevante para nuestro AS, ya que llega a ese destino por AS64501.



[6] RFC 7908

Pero, por algún error de configuración, el AS65432 anuncia la ruta con destino a 200.0.0.0/16 a AS64502. Esto no es un comportamiento esperado, porque nuestro AS es un cliente y no un proveedor de tránsito. El anuncio de ruteo supera su alcance deseado y se genera una fuga BGP. El AS64502 no filtra este anuncio y ahora cuenta con una ruta más específica para llegar a 200.0.0.1 (200.0.0.0/16 a través del AS65432, en contra de 200.0.0.0/12 a través de AS64567).



Sin importar que la ruta sea más larga, como el prefijo es más específico, el AS64502 comenzará a enviar flujos de datos hacia el AS65432, lo cual puede generar problemas de desempeño en la red e incluso cortes de servicio, tanto en el ISP, que nos brinda conectividad, como para los distintos clientes que quieran acceder a la app de mensajería.

Línea de tiempo de incidentes

Si bien todos los días ocurren anuncios incorrectos de BGP que generan pequeños incidentes, algunos de estos terminan generando estragos a nivel mundial durante tiempos considerables. A continuación se listan algunos de los incidentes que generaron noticias por su impacto.

Abril de 1997[7]

El incidente del AS 7007 fue una disrupción importante de Internet y el primer incidente de ruteo reportado globalmente por su impacto. El 25 de abril de 1997 empezó con un router operado por el sistema autónomo 7007 que anunció accidentalmente una parte sustancial de su tabla de ruteo a todo Internet y generó un «agujero negro» al redirigir el contenido a ninguna parte.

Febrero de 2008

El gobierno pakistaní intentó censurar Youtube mediante su ISP público actualizando las rutas BGP que llevaban al sitio. Estos anuncios, además, se elevaron a proveedores superiores y se esparcieron por todo Internet, provocando que todas las solicitudes a Youtube fueran enviadas a Pakistán Telecom, lo que bloqueó el acceso al portal en todo el mundo.

Noviembre de 2012[8]

Un error causado por una falla inesperada de hardware en equipos de Moratel (ASN 23947), un operador de Indonesia, provocó una fuga BGP y generó interrupciones y problemas para acceder a servicios de Google durante 27 minutos.

Noviembre de 2013[9]

Dyn Research presentó evidencias de que el tráfico de Internet perteneciente a instituciones financieras, gobiernos e ISP fue desviado en constantes ocasiones hacia lugares no autorizados. Se generaron sospechas de que ese tráfico haya podido ser monitoreado o modificado antes de llegar a su destino.

Agosto de 2013[10]

Durante seis días, el web host italiano Aruba S.p.A anunció de forma fraudulenta la posesión de 256 direcciones IP. Esto fue bajo la dirección del equipo de hacking y operaciones especiales de la policía militar italiana, con el fin de monitorear computadoras de distintos objetivos.

Septiembre de 2014[11]

Una compañía de hosting de Pensilvania, VolumeDrive (AS46664), generó una fuga de rutas que causó interrupciones de tráfico en lugares incluso lejanos a USA, como Pakistán o Bulgaria.

Marzo de 2017[12]

La SECW Telecom de Brasil anunció de forma fraudulenta prefijos de Cloudflare, Google y Banco Brazil, y generó algunos cortes de servicio en toda la región.

Abril de 2017[13]

Parte del tráfico de red perteneciente a Master Card, Visa y muchas otras compañías de servicios financieros, fue desviado a través de Rostelecom, un proveedor ruso. Durante varios minutos anunció fraudulentamente más de 50 prefijos que pertenecían a otros AS.

Agosto de 2017[14]

Google filtró accidentalmente prefijos que su AS obtuvo a partir de enlaces de peering, transformándose en un proveedor de tránsito. Esto causó interrupciones a gran escala en Internet. Los usuarios japoneses fueron los más afectados, con conexiones lentas o directamente interrumpidas a decenas de compañías de ese país.

Octubre de 2017[15]

Debido a una fuga BGP, el tráfico de múltiples CDN importantes fue desviado hacia Brasil. Esto provocó contratiempos para servicios como Google y Twitter, al menos durante 20 minutos.

Noviembre de 2017[16]

Una fuga de rutas de Level 3 generó degradación del servicio de Internet en América del Norte durante más de 90 minutos.

Diciembre de 2017[17]

Portales muy importantes como Google, Apple, Facebook, Microsoft y Twitch, entre otros, fueron desviados a un AS ruso que nunca antes había operado hasta el momento. Esto fue a causa de dos incidentes BGP que duraron unos pocos minutos.

Abril de 2018[18]

Un proveedor ruso anunció prefijos IP de forma fraudulenta, que en realidad pertenecían a los servidores de Route53 Amazon DNS. Esto le permitió a un grupo de hackers que un portal de criptomonedas fuera redirigido a un sitio falso que robaba las credenciales. Así, el grupo pudo robar aproximadamente 152.000 dólares en criptomonedas.

Julio de 2018[19]

En paralelo a distintas estrategias del gobierno iraní para censurar redes como Telegram e Instagram, el AS perteneciente a la compañía de telecomunicaciones pública iraní anunció de forma fraudulenta prefijos pertenecientes a otros ISP húngaros. Si bien estos incidentes tuvieron una escala muy pequeña, no se descarta que hayan sido intentos de provocar censura, explotando el sistema de ruteo BGP.

Enero de 2019[20]

En medio de protestas en Zimbabwe por subas en los combustibles, se acusó al gobierno de bloquear redes como Whatsapp y Facebook. En paralelo, se lo acusó de explotar también el ruteo BGP para generar apagones de Internet. Si bien no se encuentran incidentes registrados, sí hubo apagones de prefijos en esas fechas.

Junio de 2019[21]

Debido una fuga que Verizon no filtró, este gran proveedor de Internet estadounidense terminó redireccionando gran parte del tráfico a una pequeña compañía de Pensilvania. Esto provocó cortes y degradación del servicio para acceder a distintos sitios y servicios. Uno de los mayores afectados fue Cloudflare, lo que dejó aún más sitios de Internet caídos.

---

[7]‹https://www.bgp.us/case-studies/›
[8]‹https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/›
[9]‹https://arstechnica.com/information-technology/2015/07/hacking-team-orchestrated-brazen-bgp-hack-to-hijack-ips-it-didnt-own/›
[10]Ídem.
[11]‹https://dyn.com/blog/why-the-internet-broke-today/›
[12]‹https://twitter.com/bgpmon/status/846087079763177472›
[13]‹https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/›
[14]‹https://www.internetsociety.org/blog/2017/08/google-leaked-prefixes-knocked-japan-off-internet/›
[15]‹https://bgpmon.net/todays-bgp-leak-in-brazil/›
[16]‹https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/›
[17]‹https://www.internetsociety.org/blog/2017/12/another-bgp-routing-incident-highlights-internet-without-checkpoints/›
[18]‹https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/›
[19]‹https://blog.talosintelligence.com/2018/11/persian-stalker.html›
[20]‹https://www.thesouthafrican.com/news/zimbabwe-protest-mnangagwa-accused-blocking-whatsapp-facebook/›
[21]‹https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/›

Análisis de eventos

Los incidentes enumerados en la línea de tiempo de este informe son solo la punta del iceberg, son algunos de los eventos que mayor repercusión han tenido y que han afectado a gran cantidad de usuarios de Internet durante un tiempo considerable o en algún contexto social crítico. Pero la mayoría de incidentes, en general, pasan desapercibidos. En este informe analizaremos estos eventos en su totalidad, para poder conocer en qué estado se encuentra la seguridad del ruteo en el mundo y en nuestra región.

Metodología

Como hemos explicado, existen dos tipos de incidentes en BGP: fugas (*leaks*) y secuestros (*hijacks*) de rutas. En este informe analizaremos los eventos recolectados por el portal Bgpstream.com, que, además, registra otro tipo de evento: los apagones (*outages*), es decir, cuando un sistema autónomo deja de anunciar ciertos prefijos. De esta fuente se analizaron los eventos registrados en 2017, 2018 y parte de 2019.

En cada evento, los sistemas autónomos pueden estar involucrados de diferentes formas. En una fuga existe quien efectivamente *fuga* una ruta que no debe publicar (el responsable) y esa ruta es para llegar a un prefijo que pertenece a algún otro AS (el afectado o víctima). Además, la fuga se transmite a otros sistemas autónomos que por políticas pobres de filtrado aceptan dicha ruta (propagadores).

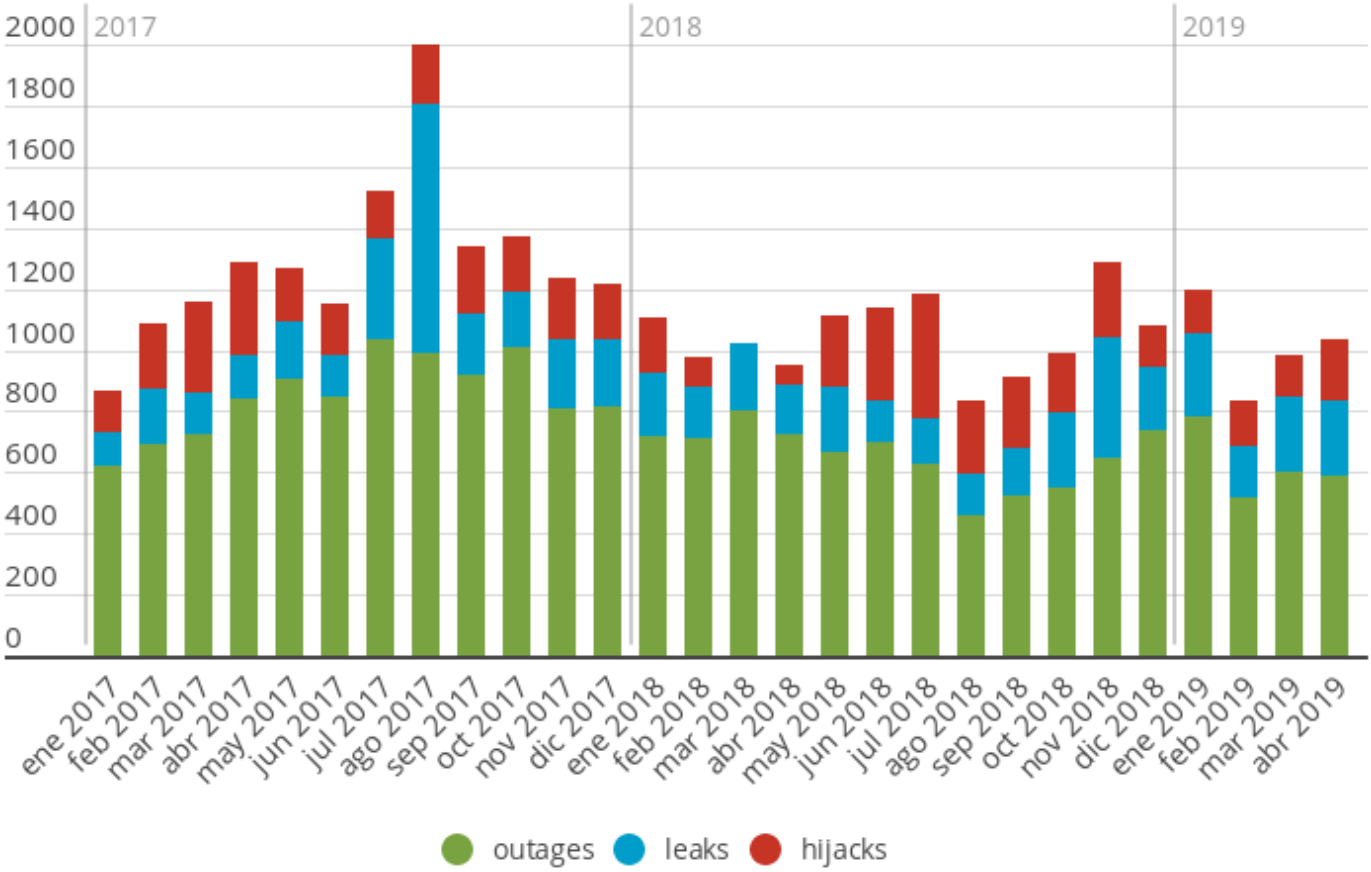
En un secuestro de rutas, se encuentra el AS que anuncia un prefijo de forma fraudulenta o que no le corresponde (responsable) y el AS que realmente posee dicho prefijo (víctima o afectado). En ambos casos también pueden registrarse los sistemas autónomos que observan dichos eventos, pero esta información no es analizada, ya que estos no están involucrados activamente en el incidente.

Para asociar los sistemas autónomos a territorios, en primera instancia, se toma la aproximación realizada por BGPSTREAM, que utiliza la base de datos MaxMind's GeoLite City. Si esa consulta no generó un resultado adecuado o no está realizada, se acude a asociarlo con el país que cada RIR asocia al registrarlo. Aunque no siempre sus prefijos terminen estando configurados en equipos radicados en dicho territorio, de todas formas es una buena aproximación utilizar dichos registros para asociar sistemas autónomos con países y, a partir de dicho vínculo, generar métricas a nivel geográfico.

Números en el mundo

Cada día las tablas BGP de decenas de miles de sistemas autónomos mutan y anuncian distintas rutas. En el gráfico 1 podemos observar la cantidad de incidentes ocurridos desde 2017 y hasta abril de 2019 que registró BGP Stream.

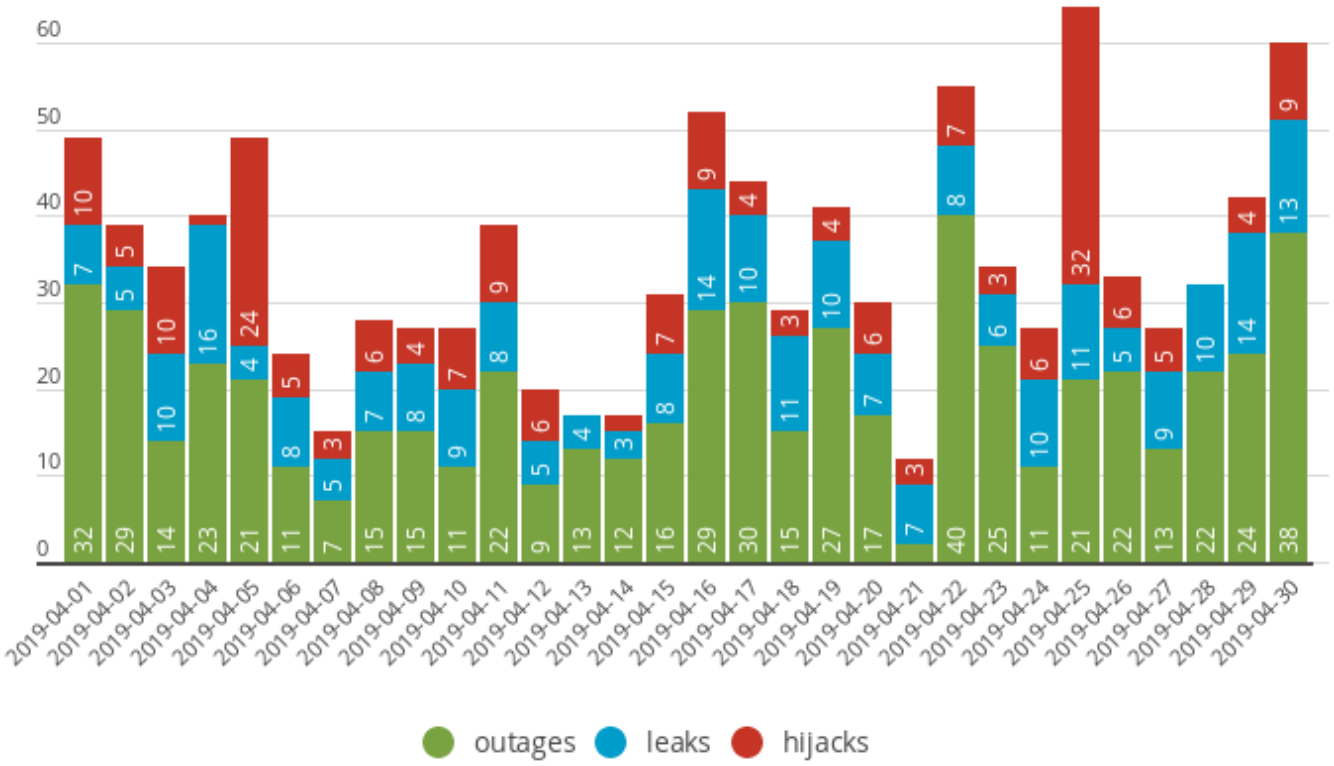
Gráfico 1: cantidad de incidentes ocurridos por mes en el mundo.



Fuentes: ‹https://bgpstream.com›

Es importante volver a destacar que un evento no representa necesariamente un ataque deliberado, ya que algunos anuncios pueden ser malinterpretados y generar falsos positivos o pueden deberse a errores de configuración (por lo tanto, no intencionales). Por otra parte, como mencionamos, todos los días ocurren incidentes BGP en la red, aunque no generen un gran impacto ni se transformen en noticia. Podemos observar esto visualizando, a modo de ejemplo, el mes de abril de 2019, con detalle día a día de los incidentes ocurridos.

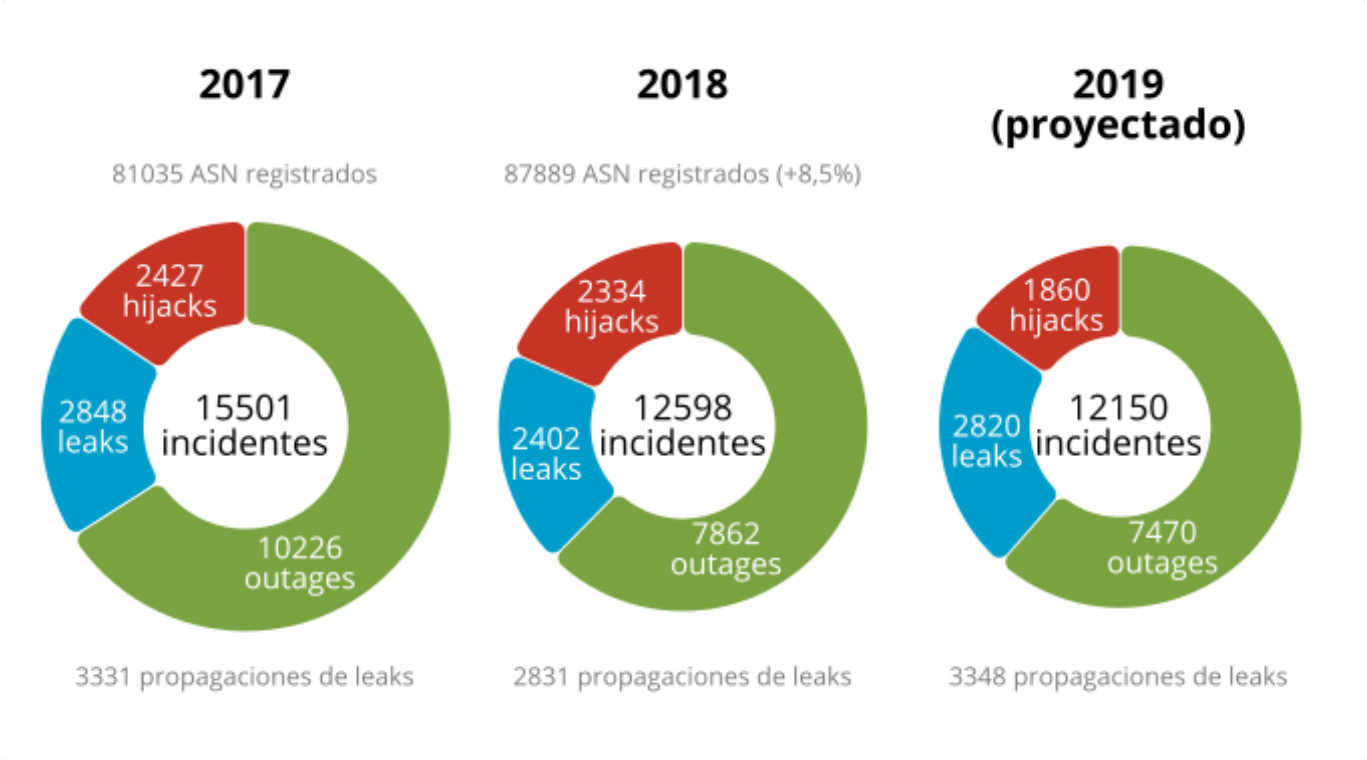
Gráfico 2: cantidad de incidentes ocurridos por día en el mundo en abril de 2019



Fuentes:‹https://bgpstream.com›

A simple vista puede parecer que la cantidad de incidentes ocurridos se mantiene constante, pero podemos notar una tendencia a la baja en el siguiente gráfico, donde se puede observar la cantidad de incidentes acumulados por año y clasificados según tipo (debajo de los *leaks* se especifica también la cantidad de propagaciones, es decir, cuando un sistema autónomo propaga una fuga por no implementar políticas de filtrado adecuadas).

Gráfico 3: cantidad de incidentes ocurridos cada año a nivel mundial



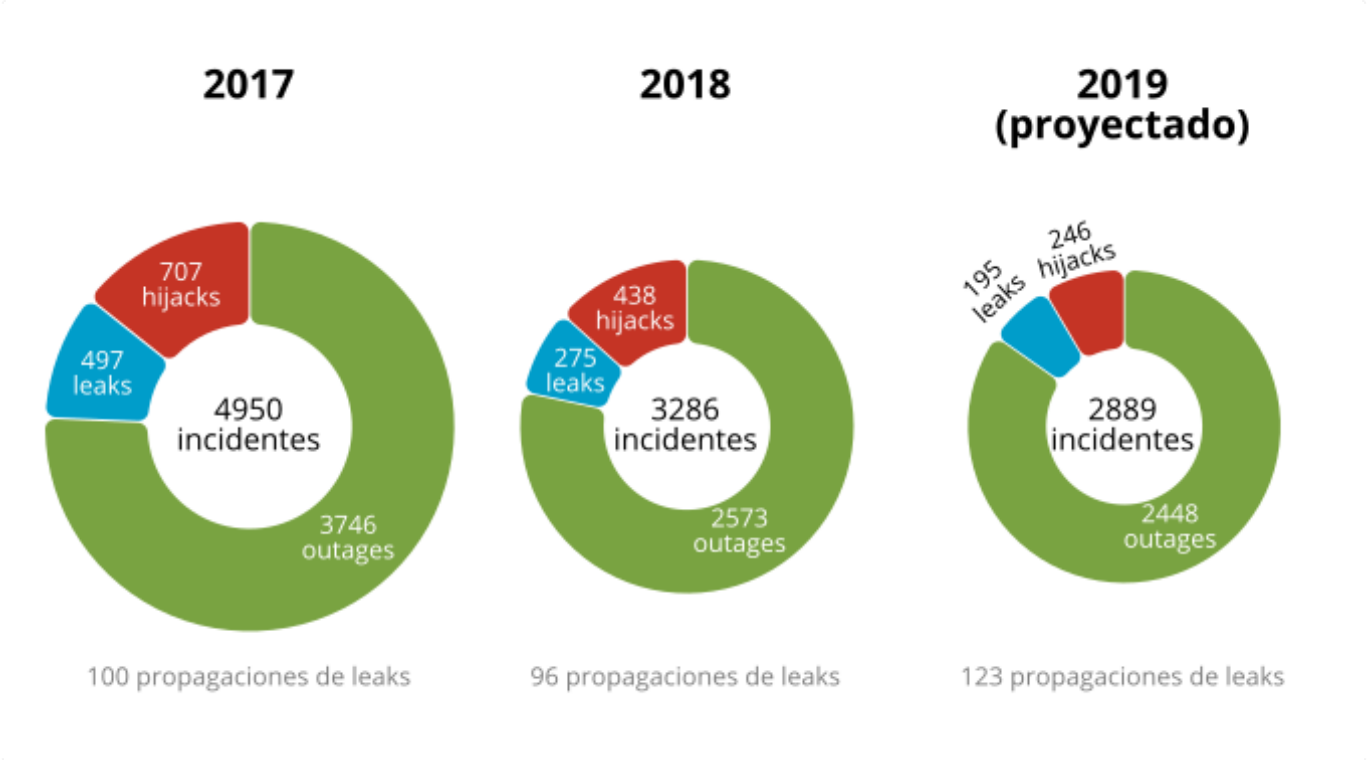
Nota: la proyección 2019 se realizó con base en los 4050 eventos registrados hasta abril de ese año.
Fuentes:‹https://bgpstream.com› ‹https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html›

Junto a la baja en números totales por año, debemos de tener en cuenta que cada vez más sistemas autónomos se registran y conectan a la red. El año 2017 cerró con 81.035 ASN registrados en el mundo, 2018 cerró con 87.889 ASN registrados. Se trata de un aumento de 8,5%, similar al que se prevé para 2019 (se espera que cierre con más de 94.000 ASN registrados).

Es decir, si bien la tendencia a la baja de incidentes año a año parece pequeña, considerando que la cantidad de sistemas autónomos ha aumentado, puede inferirse que esa mejora sí es considerable. Esto puede atribuirse a la adopción de nuevas medidas de filtrado en las tablas de ruteo BGP, como las propuestas por MANRS de Internet Society, iniciativa que se detallará más adelante. Entre ellas también puede mencionarse que existe una mayor cantidad de operadores implementando RPKI.

Si realizamos este mismo análisis acotando el estudio solo a los incidentes que involucran países de Latinoamérica y el Caribe, la mejora entre 2017 y 2018 es aún más pronunciada.

Gráfico 4: cantidad de incidentes ocurridos cada año en Latinoamérica y el Caribe.



Nota: La proyección 2019 se realizó con base en los 963 eventos registrados hasta abril de ese año.
Fuentes: ‹https://bgpstream.com› y ‹https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html›

En lo que respecta a sistemas autónomos puntuales, podemos también realizar un ranking en cada caso para conocer cuáles son los más involucrados en estos eventos.

Tabla 1: top 5 mundial (2017 y 2018) de sistemas autónomos que más fugas provocaron.

2017			2018		
ASN	**Detalle**	**leaks**	**ASN**	**Detalle**	**Leaks**
4258	atg-4258 - accretive networks, us	51	3910	centurylink-europe-legacy-qwest - centurylink Communications, LLC, US	337
393861	inova-primaryasn-01 - inova health system foundation, us	45	5391	T-ht croatian telecom inc., hr	134
7991	centurylink-legacy-savvis-asia-transit - centurylink communications, llc, us	40	58601	aamra-atl-bd aamra technologies limited, bd	115
24990	equinix-fr-asn equinix france autonomous system, fr	39	7991	Centurylink-legacy-savvis-asia-transit - centurylink Communications, llc, us	86
3908	centurylink-asia-legacy-qwest - centurylink communications, llc, us	29	39386	stc-igw-as, sa	45
37452	cb-nigeria, ng	29			
32787	prolexic-technologies-ddos-mitigation-network - akamai technologies, inc., us	29			

Fuentes: ‹https://bgpstream.com›

Tabla 2: top 5 mundial (2017 y 2018) de sistemas autónomos más afectados por fugas.

2017			2018		
ASN	Detalle	Leaks	ASN	Detalle	Leaks
27066	dnic-asblk-27032-27159 - dod Network Information center, US	15	18399	ytcl-as-ap yatanarpon teleport company limited, mm	21
63852	Fmg-mm myanmar net, mm	15	27066	dnic-asblk-27032-27159 - dod network information center, us	19
1541	dnic-asblk-01534-01546 - headquarters, usaisc, us	13	1541	dnic-asblk-01534-01546 - headquarters, usaisc, us	18
13896	Thinkingphones - fuze inc, us	12	59209	whil-bd walton hi-tech industries ltd, bd	15
38456	Speedcast-au speedcast australia pty limited, au	12	14210	edgecast-dca - mci communications services, inc. d/b/a verizon business, us	14

Fuentes:‹https://bgpstream.com›

Tabla 3: top 5 mundial (2017 y 2018) de sistemas autónomos que más *hijacks* provocaron.

2017			2018		
ASN	Detalle	Hijacks	ASN	Detalle	Hijacks
49291	interpro-as, ru	90	50607	epix-kgm, pl	158
198949	vs-as, il	53	37468	angola-cables, ao	131
263444	open x tecnologia ltda, br	50	198726	komdsl, de	75
39523	dv-link-as, ru	29	8859	osn bucher str. 78, de	37
27884	cablecolor s.a., hn	25	399261	bogon as - iana unallocated asn, zz	33

Fuentes:‹https://bgpstream.com›

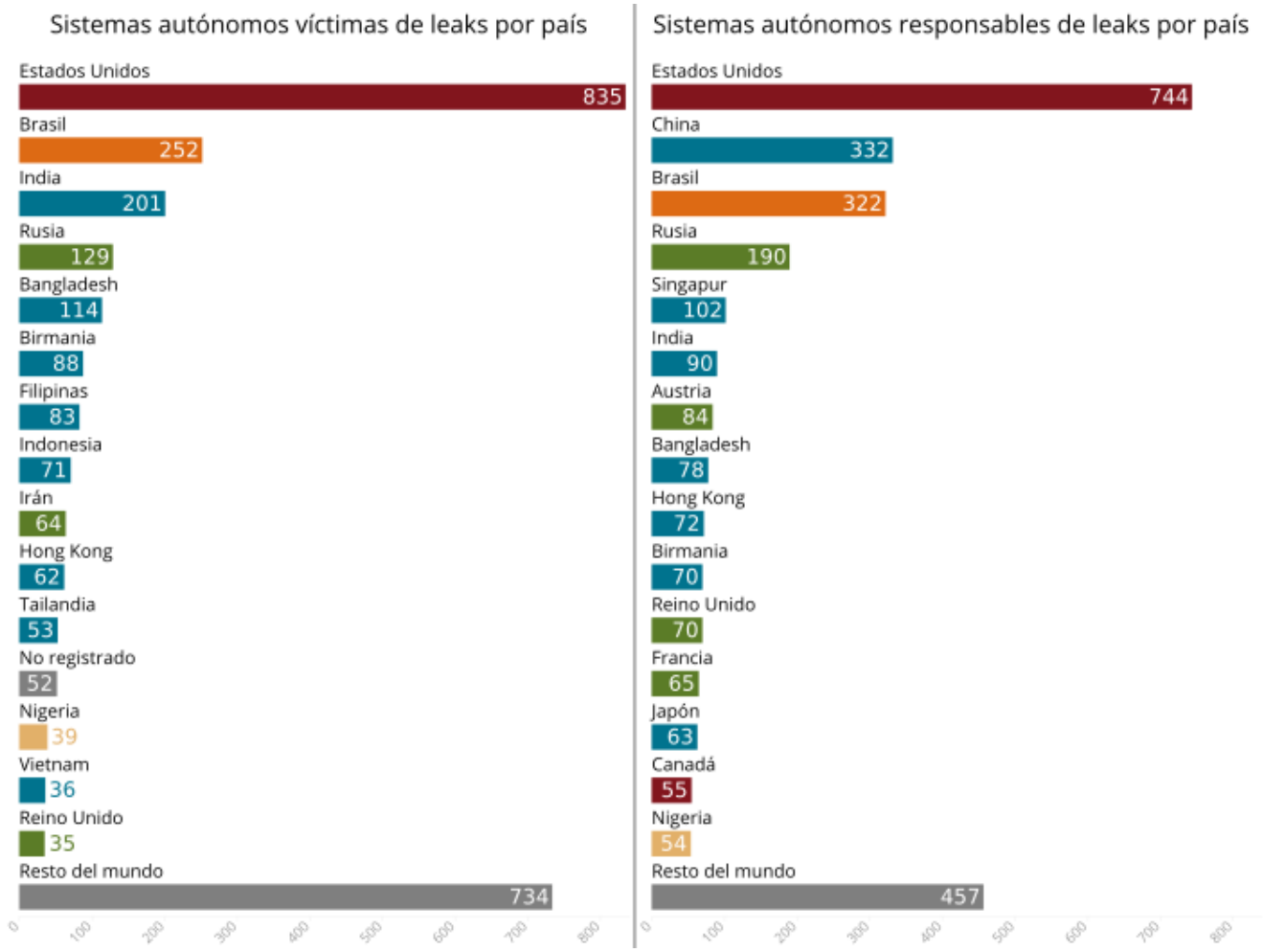
Tabla 4: top 5 mundial (2017 y 2018) de sistemas autónomos más afectados por *hijacks*.

2017			2018		
ASN	Detalle	Hijacks	ASN	Detalle	Hijacks
13489	epm telecomunicaciones s.a. e.s.p., co	233	14259	gtd internet s.a., cl	79
21928	t-mobile-as21928 - t-mobile usa, inc., us	17	35916	multa-asn1 - multacom corporation, us	15
35994	akamai-as - akamai technologies, inc., us	16	25577	c4l-as, gb	15
203661	william, gb	12	35994	akamai-as - akamai technologies, inc., us	14
1200	ams-ix1, nl	12	21928	t-mobile-as21928 - t-mobile usa, inc., us	14

Fuentes: ‹https://bgpstream.com›

Podemos observar que los sistemas autónomos provenientes de Estados Unidos predominan en las tablas. ¿Es esto una norma? ¿Cuáles son los países más involucrados en incidentes de ruteo? Para responder estas preguntas podemos analizar los datos agrupados por países. Comencemos analizando las fugas, o *leaks*, ocurridas en 2017.

Gráfico 5: BGP *leaks* en 2017 por países.

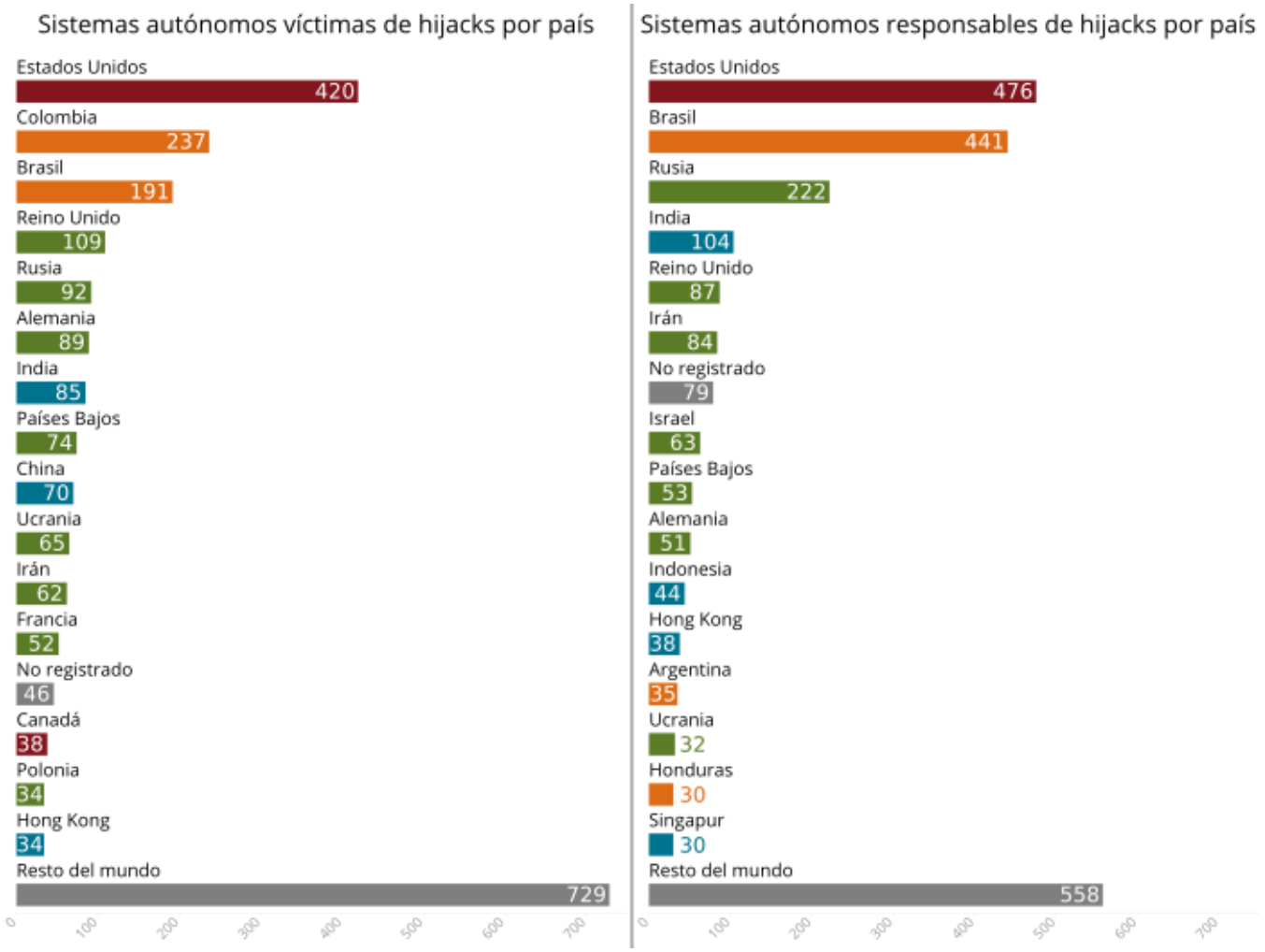


Fuentes: ‹https://bgpstream.com›

Así, en el gráfico 5, se acumula la cantidad de incidentes de acuerdo a los países de sus AS involucrados y cómo estos fueron parte de la fuga: siendo responsables, anunciando la ruta fuera de su alcance deseado o siendo víctimas cuyos prefijos IP fueron anunciados incorrectamente.

Como observamos, efectivamente existe un gran predominio de Estados Unidos en todos los casos, algo esperable, ya que ese país no solo posee un enorme número de proveedores de servicio, sino que también alberga a todas las compañías que juegan papeles importantes en el ecosistema de Internet. Respecto a Latinoamérica, solamente Brasil se encuentra en estos rankings, algo también esperable, ya que es el segundo país con mayor cantidad de sistemas autónomos conectados. ¿Y qué ocurre al analizar los secuestros de rutas o *hijacks*?

Gráfico 6: BGP hijacks en 2017 por países.



Fuentes: ‹https://bgpstream.com›

El gráfico 6 muestra que Brasil casi igualó a Estados Unidos en cantidad de sistemas autónomos responsables de *hijacks*. Según la línea de tiempo de este informe, 2017 fue un año en el que ocurrieron reiterados incidentes de ruteo en Brasil (esto mismo se refleja en las estadísticas cuantitativas). También entran en este ranking otros países de la región como Argentina y Honduras.

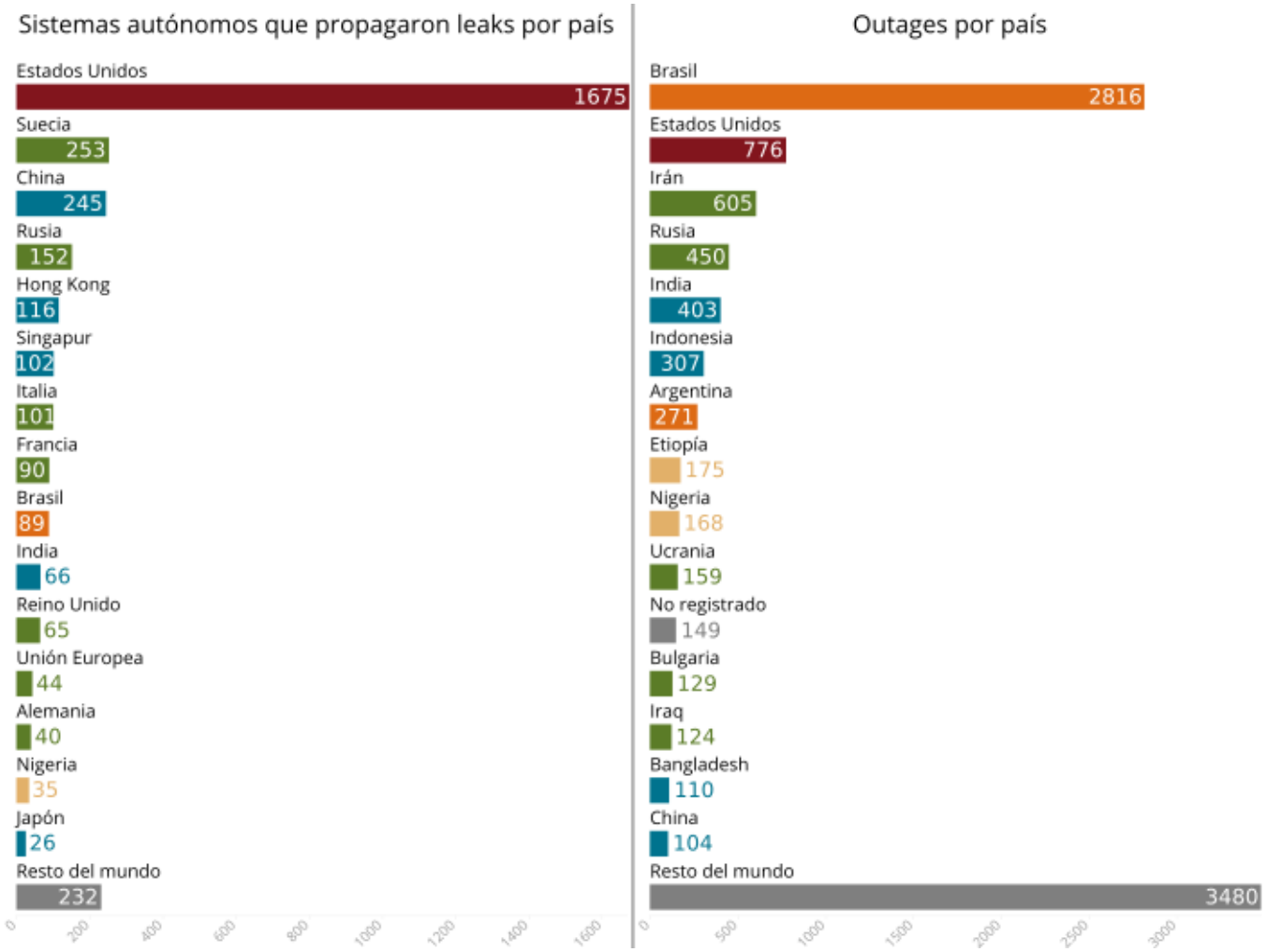
Llama la atención el puesto que ocupa Colombia, como el segundo país con mayor cantidad de sistemas autónomos en los cuales algunos de sus prefijos fueron anunciados fraudulentamente por otros. Si se observa el ranking discriminado por ASN, el AS13489 registrado en Colombia fue la mayor víctima de anuncio de prefijos fraudulentos ese año. Si analizamos los anuncios de dicho sistema autónomo ese año, podemos concluir que estos incidentes no son *hijacks* sino eventos producto de un error de configuración de ese AS.

Durante 2017, dicho sistema autónomo anunciaba ser el origen del prefijo IPv6 2800::/12. Este es el bloque asignado a LACNIC por IANA, es decir, el que se distribuye en prefijos más pequeños para todos los operadores de nuestra región que soliciten direcciones IPv6. Por alguna razón, probablemente una configuración inadecuada, el AS13489 estuvo anunciando dicho prefijo completo, junto con los que efectivamente posee. Esto generó que cada vez que otro operador de la región comenzaba a anunciar sus nuevos prefijos IPv6 mediante sus ASN, BGPSTREAM detectaba esto como un intento de *hijack* (recordemos que una forma de ganarle la ruta a un ASN es anunciando un prefijo más específico). Si bien

el tipo de incidente no es un secuestro de ruta, este evento demuestra el poco control que existe en BGP y cómo es sensible a errores de los operadores.

Por último, también podemos analizar del año 2017 otros dos datos que registra BGPSTREAM: los *outages* ocurridos (incidente que ocurre cuando un AS deja de anunciar prefijos IP que le pertenecen, haciéndolos inaccesibles) y las propagaciones de fugas BGP detectadas (cuando un AS recibe una ruta producto de un *leak* y, por no contar con reglas de filtrado adecuadas, este la continúa propagando a otros sistemas autónomos).

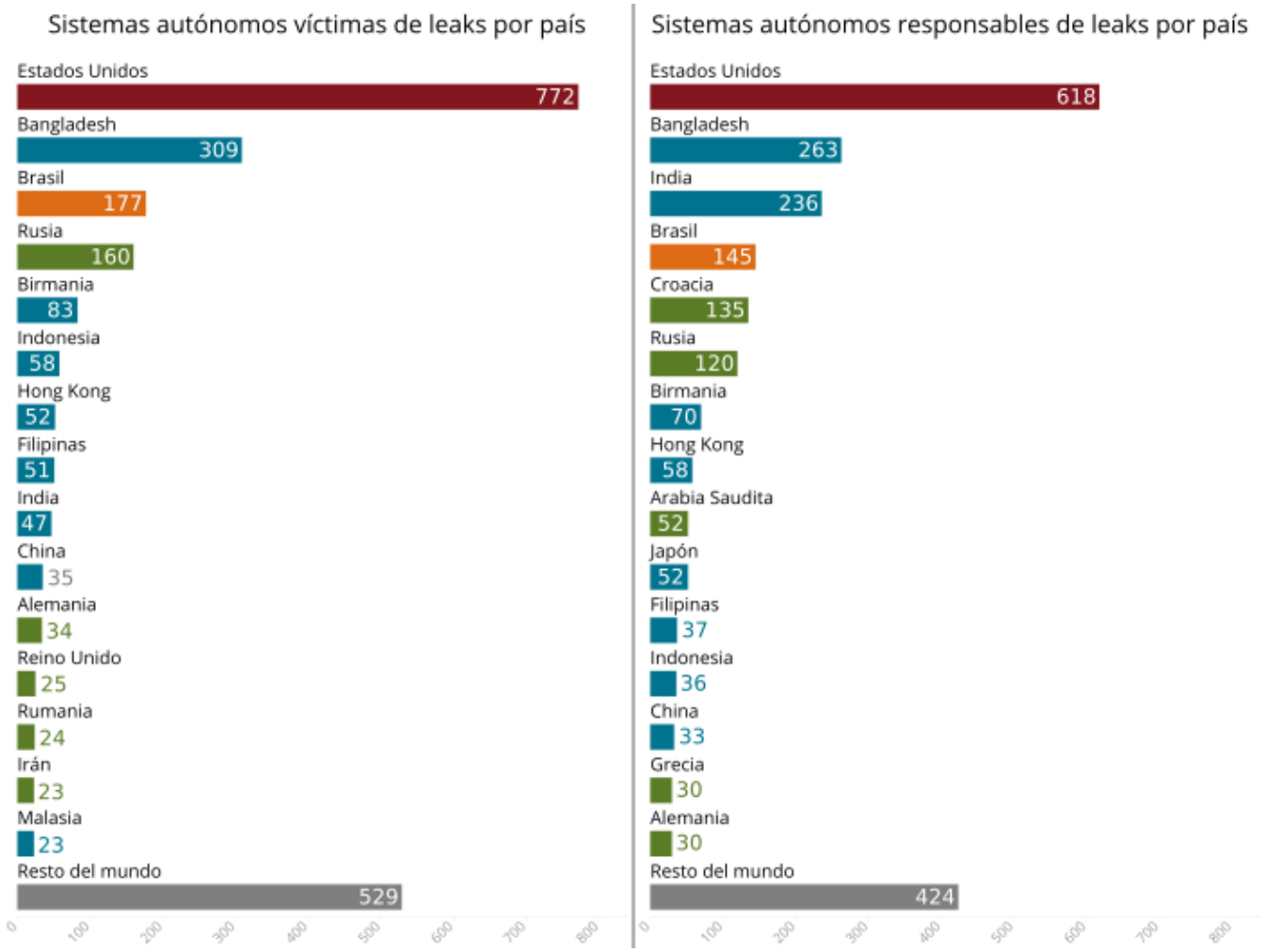
Gráfico 7: *outages* y propagación de BGP *leaks* en 2017 por países.



Fuentes:‹https://bgpstream.com›

Así, el gráfico 7 muestra cómo Estados Unidos tiene un problema no resuelto en cuanto a propagación de *leaks.* Ese país produjo más de la mitad de *leaks* en 2017. Por otra parte, se ve la cantidad excesiva de *outages* ocurridos en Brasil ese año. ¿Y qué ocurrió en 2018?

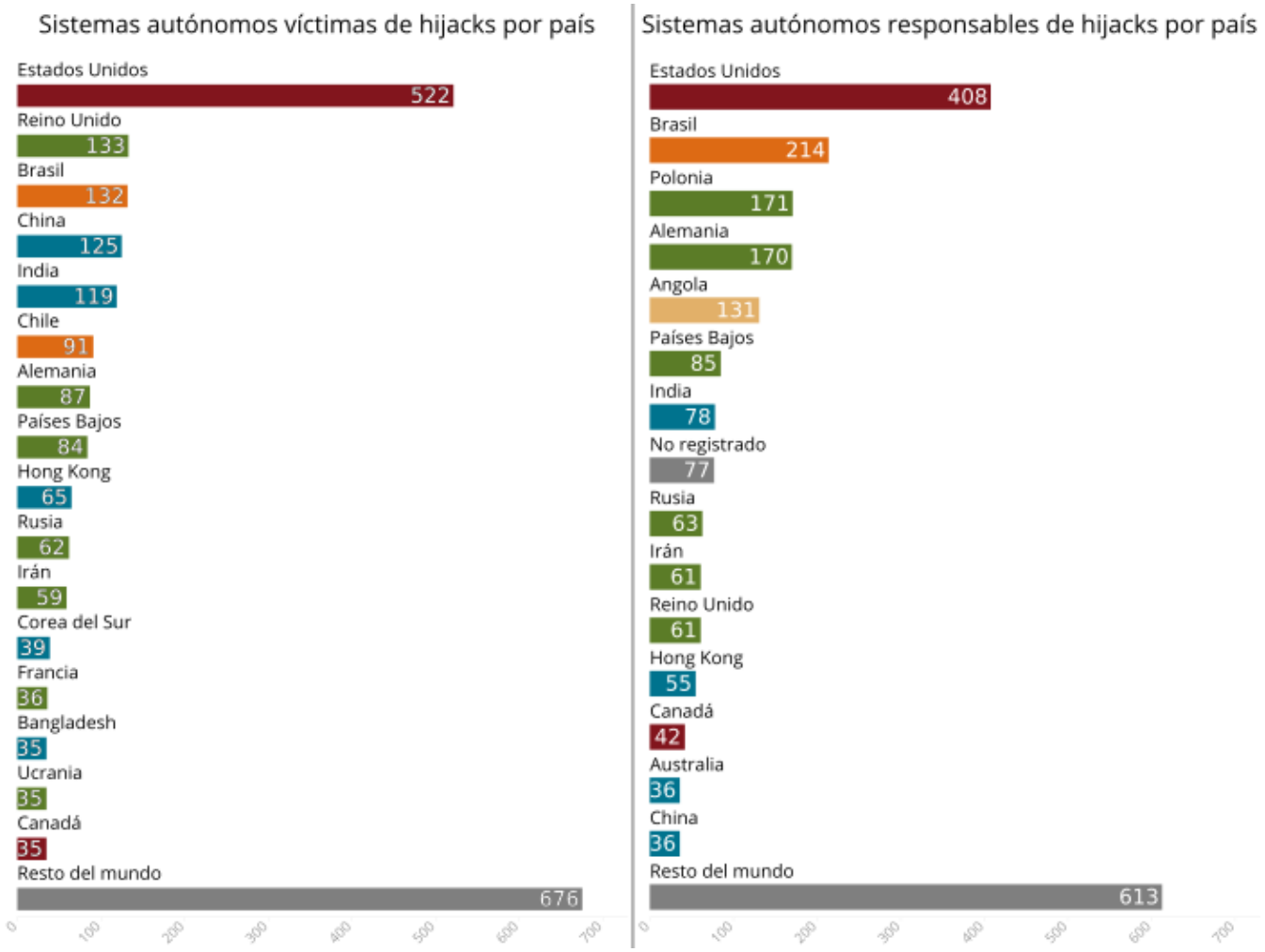
Gráfico 8: BGP *leaks* en 2018 por países.



Fuentes: ‹https://bgpstream.com›

El gráfico 8 nos permite observar cómo la cantidad de incidentes ha caído a nivel general, salvo algunos casos puntuales como Bangladesh. Estados Unidos sigue siendo el primer país en cuanto a cantidad de fugas. Por su parte, Brasil, si bien sigue siendo de los primeros, ha bajado un puesto en ambos rankings. Los países de la región de Asia y el Pacífico continúan predominando.

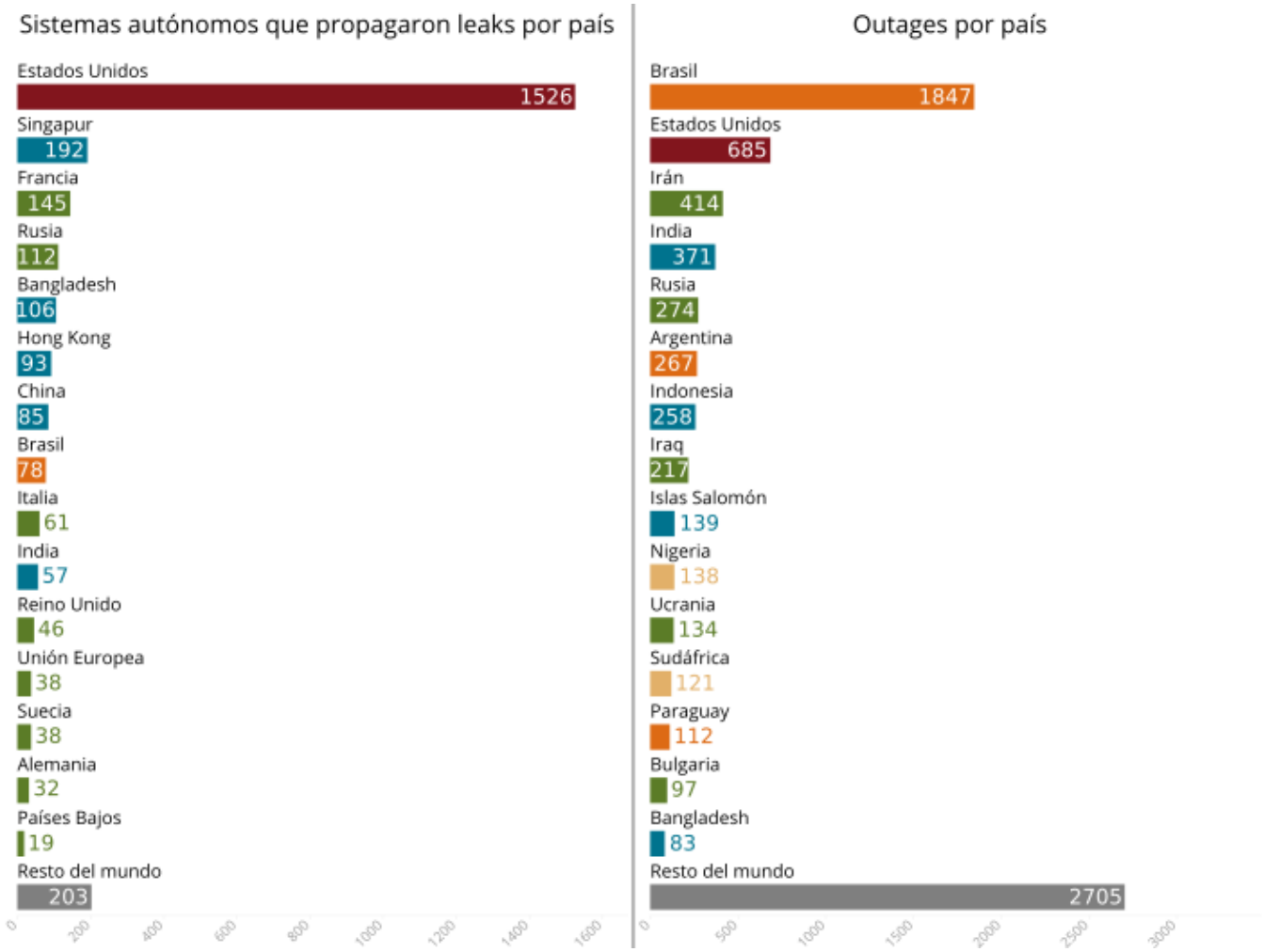
Gráfico 9: BGP *hijacks* en 2018 por países.



Fuentes: ‹https://bgpstream.com›

El gráfico 9 indica que tampoco existe mucha diferencia en lo que respecta a *hijacks*. Podemos destacar que Brasil, aunque siga conservando su segundo puesto como país con más sistemas autónomos que anunciaron prefijos de forma fraudulenta, en términos relativos bajó a la mitad la cantidad de incidentes (de 18,27% a 9.16%). Este año, además, no aparece ningún otro país de Latinoamérica entre los 15 con mayor cantidad de incidentes. Finalmente, podemos analizar los *outages* y propagación de *leaks* de 2018.

Gráfico 10: *outages* y propagación de BGP leaks en 2018 por países.



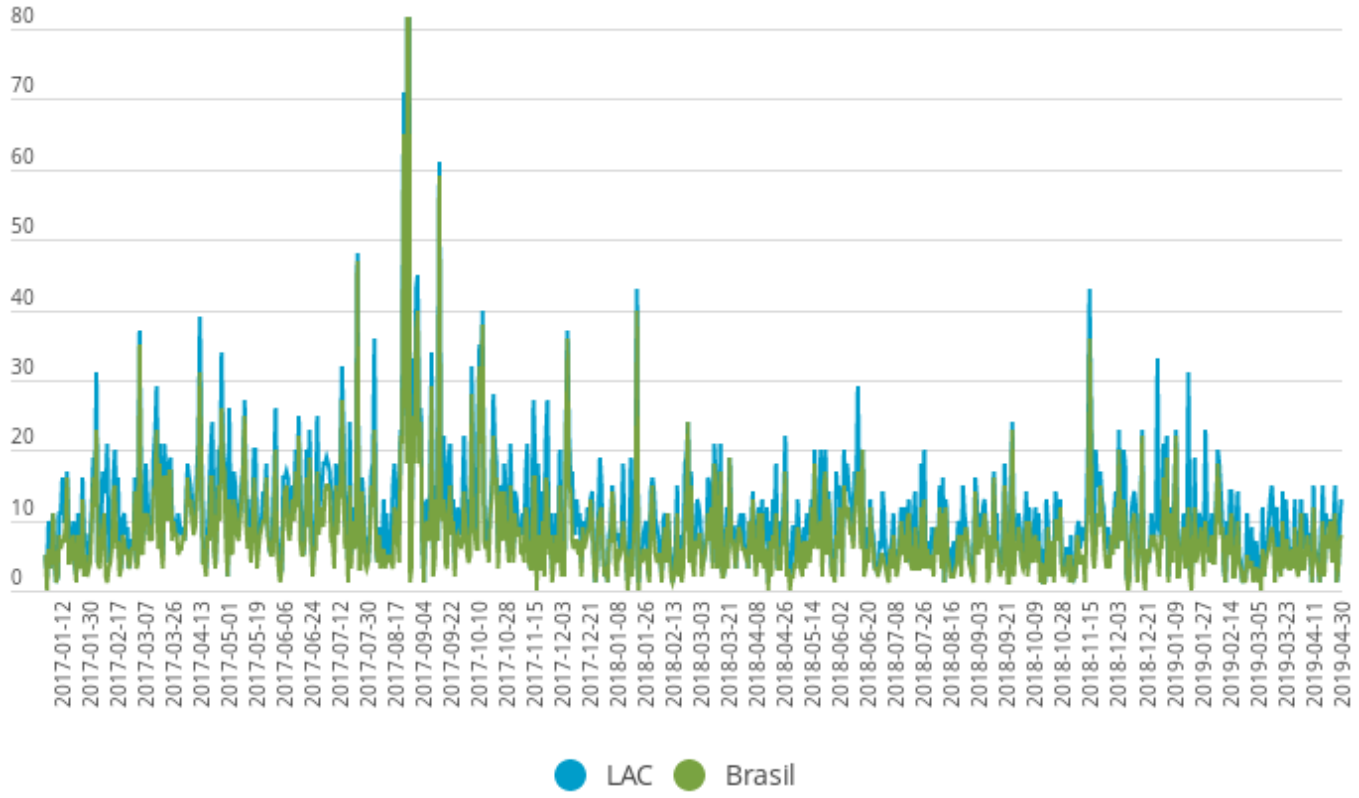
Fuentes:‹https://bgpstream.com›

El gráfico 10 no muestra grandes cambios en 2018 en lo que respecta a *outages* y propagación de fugas. Si bien Brasil redujo a casi la mitad la cantidad de *outages,* sigue siendo el primer país. Este año incluso aparecen en el ranking otros países de nuestra región como Argentina y Paraguay.

Números en la región

Es importante que hagamos un análisis análogo de los países de Latinoamérica y el Caribe para comprender cómo se encuentra la región en comparación con el mundo. Aquí debemos considerar una particularidad: la magnitud de Brasil. Al evaluar los números en todo el mundo se puede observar cómo Brasil siempre está presente entre los primeros cinco países con sistemas autónomos involucrados en distintos incidentes de ruteo. Sumado a esto, de los 4950 incidentes BGP ocurridos en Latinoamérica y el Caribe en 2017, 3768 involucran a algún ASN de Brasil (un 76,1%). En 2018, Brasil está involucrado en 2363 de los 3286 incidentes ocurridos en la región (un 71,9%).

Gráfico 11: incidentes ocurridos en Latinoamérica y el Caribe vs. incidentes ocurridos en Brasil.



Fuentes: ‹https://bgpstream.com›

La línea que indica los eventos ocurridos en toda Latinoamérica se ubica apenas por encima de la línea que representa los eventos ocurridos solamente en Brasil. Esto implica que los eventos que ocurren en otros países de la región quedan eclipsados frente a la gran actividad que comprende un solo país.

Eventos acumulados por país

Si bien Brasil termina moldeando las estadísticas generales al pensar toda la región, no deja de tener valor analizar otros países latinoamericanos de forma individual. Así, para obtener un rápido vistazo del estado de ruteo en cada uno, presentamos en la tabla 5 un listado de eventos acumulados por país, ocurridos en 2017:

Tabla 5: cantidad de incidentes ocurridos por país en Latinoamérica y el Caribe (2017).

País / Región		Leaks (r)	Leaks (v)	Leaks (a)	Hijacks (r)	Hijacks (v)	Total	ASNs	Total/ASNs
AR	Argentina	0	11	0	35	18	64	600	0.11
BZ	Belice	0	0	0	2	2	4	10	0.4
BO	Bolivia	0	3	0	3	2	8	25	0.32
BR	Brasil	322	252	89	441	191	1295	4939	0.26
CL	Chile	1	1	1	4	30	37	176	0.21
CO	Colombia	0	2	7	9	237	255	114	2.24
CR	Costa Rica	6	8	0	2	5	21	58	0.36
EC	Ecuador	2	3	2	7	8	22	67	0.33
GT	Guatemala	0	2	0	4	9	15	33	0.45
HN	Honduras	0	0	0	30	5	35	59	0.59
JM	Jamaica	0	0	0	5	0	5	8	0.63
MX	México	4	9	1	1	4	19	233	0.08
NI	Nicaragua	0	1	0	5	4	10	21	0.48
PA	Panamá	0	2	0	3	2	7	77	0.09
PE	Perú	0	0	0	2	4	6	28	0.21
PR	Puerto Rico	5	4	0	5	0	14	48	0.29
BL	San Bartolomé	0	1	0	1	0	2	3	0.67
MF	San Martín (FR)	0	1	0	3	0	4	3	1.33
TT	Trinidad y Tobago	0	1	0	2	1	4	13	0.31
VI	Islas Vírgenes (US)	0	2	0	1	2	5	6	0.83
VE	Venezuela	6	12	0	1	1	20	53	0.38
	Resto de países LAC	3	4	0	5	6	18	190	0.09
	Total LAC	349	319	100	571	531	1870	6764	0.28
	Total mundial	2848	2848	3331	2427	2427	13881	80866	0.17
US	Estados Unidos	744	835	1675	476	420	4150	16379	0.25

Fuentes: ‹https://bgpstream.com› ripe ncc

Referencias:

- *Leaks* (r): cantidad de sistemas autónomos que provocaron una fuga.
- *Leaks* (v): cantidad de sistemas autónomos cuyos prefijos fueron fugados por otro AS.
- *Leaks* (a): cantidad de sistemas autónomos que aceptaron una fuga.
- *Hijacks* (r): cantidad de sistemas autónomos que anunciaron un prefijo de forma fraudulenta.
- *Hijacks* (v) cantidad de sistemas autónomos que fueron víctimas de un *hijack*.
- Total: suma de los eventos contabilizados.
- ASN: cantidad de ASN que el país tuvo activos a fin de año. Fuente: ‹https://stat.ripe.net/›
- Total/ASN: división resultante de ambos valores.

En esta tabla se comprenden los países en los que ocurrieron al menos cinco incidentes en 2017 o en 2018. Los demás se agrupan como «Otros países de LAC» y comprenden: Anguilla, Antigua y Barbuda, Aruba, Bahamas, Barbados, Bonaire, San Eustaquio y Saba, Isla Bouvet, Islas Vírgenes Británicas, Islas Caimán, Cuba, Curaçao, Dominica, República Dominicana, El Salvador, Islas Malvinas, Guyana Francesa, Granada, Guadalupe, Guyana, Haití, Martinica, Montserrat, Paraguay, Saint Kitts y Nevis, Santa Lucía, San Vicente y las Granadinas, San Martín (parte holandés), Islas Sandwich y Georgia del Sur, Suriname, Islas Turcas y Caicos, y Uruguay. Para fines comparativos, se incluye también toda Latinoamérica agrupada, todo el mundo y Estados Unidos.

Comparar el número absoluto de cantidad de eventos no es muy enriquecedor, ya que los países presentan distintos tamaños en múltiples sentidos: territorio, población, usuarios conectados, sistemas autónomos radicados. Es por eso que —en busca de una métrica más armonizada— se incluye en la tabla la cantidad de sistemas autónomos que posee cada país, así luego puede dividirse la cantidad de incidentes ocurridos por ese valor, obteniendo valores que podrían compararse. Además, ese valor puede compararse año por año. A continuación se muestra una tabla con los mismos valores para 2018:

Tabla 6: cantidad de incidentes ocurridos por país en Latinoamérica y el Caribe (2018).

País / Región		Leaks (r)	Leaks (v)	Leaks (a)	Hijacks (r)	Hijacks (v)	Total	ASNs	Total/ASNs
AR	Argentina	1	8	1	21	18	49	718	0.07 (-0.04)
BZ	Belice	1	2	0	2	1	6	17	0.35 (-0.05)
BO	Bolivia	0	0	0	1	0	1	30	0.03 (-0.29)
BR	Brasil	145	177	78	214	132	746	5942	0.13 (-0.13)
CL	Chile	0	2	0	10	91	103	219	0.47 (0.26)
CO	Colombia	17	3	0	15	8	43	127	0.34 (-1.9)
CR	Costa Rica	6	7	0	3	3	19	67	0.28 (-0.08)
EC	Ecuador	0	1	0	7	7	15	90	0.17 (-0.16)
GT	Guatemala	0	0	1	0	8	9	36	0.25 (-0.2)
HN	Honduras	0	0	0	9	8	17	62	0.27 (-0.32)
JM	Jamaica	0	0	0	2	1	3	8	0.38 (-0.25)

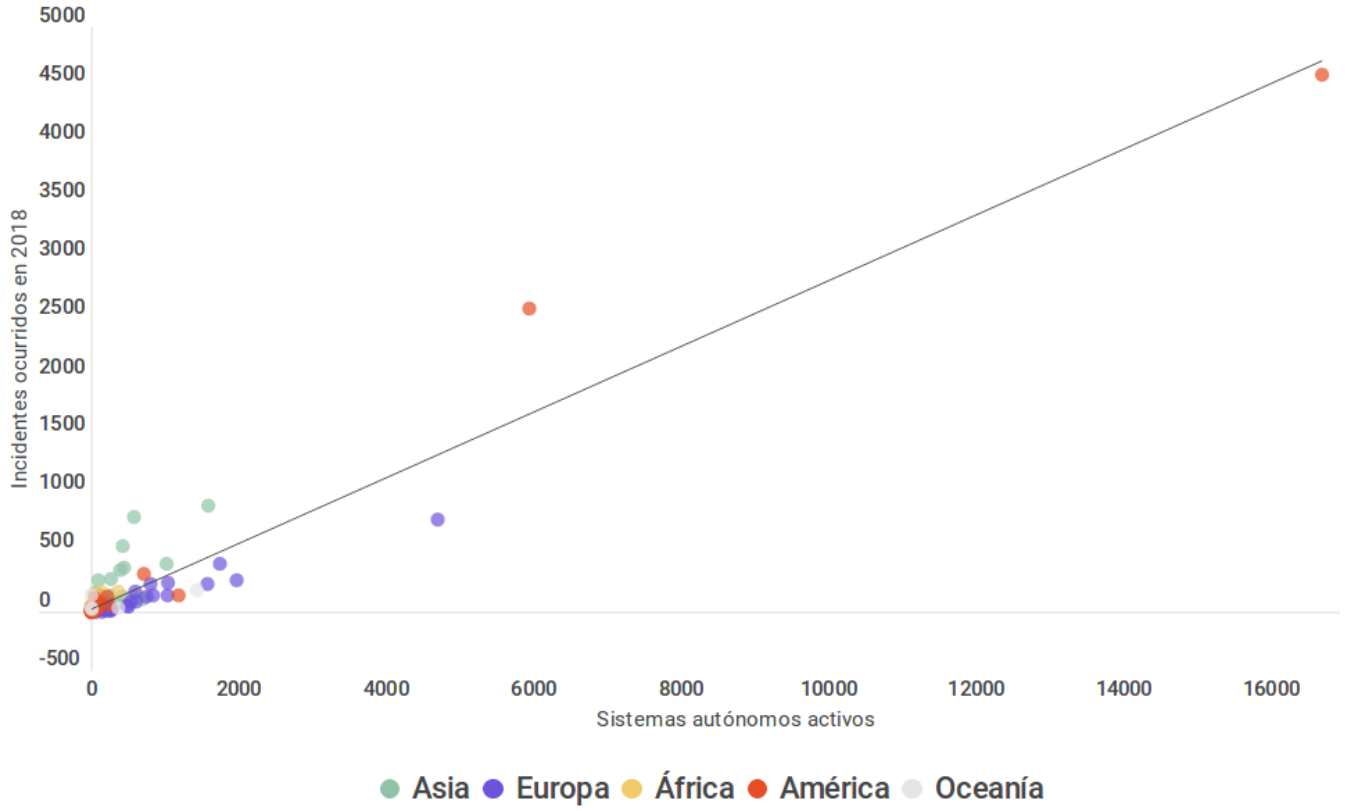
MX	México	3	3	2	4	4	16	250	0.06 (-0.02)
NI	Nicaragua	0	0	0	6	0	6	21	0.29 (-0.19)
PA	Panamá	2	3	14	8	3	30	76	0.39 (+0.3)
PE	Perú	0	0	0	4	3	7	31	0.23 (+0.02)
PR	Puerto Rico	0	1	0	4	3	8	49	0.16 (-0.13)
BL	San Bartolomé	0	5	0	0	0	5	3	1.67 (+1)
MF	San Martín (FR)	0	0	0	0	0	0	4	0 (-1.33)
TT	Trinidad y Tobago	0	2	0	2	1	5	14	0.36 (+0.05)
VI	Islas Vírgenes (US)	0	0	0	0	1	1	6	0.17 (-0.66)
VE	Venezuela	0	1	0	2	1	4	54	0.07 (-0.31)
	Resto de países LAC	0	3	0	6	8	17	219	0.08 (-0.01)
	Total LAC	175	218	96	320	301	1110	8043	0.14 (-0.14)
	Total mundial	2402	2402	2831	2335	2335	12305	87853	0.14 (-0.03)
US	Estados Unidos	681	772	1526	408	522	3909	16689	0.23 (-0.02)

Fuentes:‹https://bgpstream.com› ripe ncc

A simple vista observamos que la relación entre cantidad de incidentes y cantidad de sistemas autónomos disminuyó en la mayoría de los países de la región y también lo hizo en el mundo.

Esta métrica, que surge de dividir la suma de incidentes entre la cantidad de ASN activos por país, puede considerarse adecuada para comparar los distintos países dejando de lado sesgos por tamaño. Esto se puede comprobar si observamos la correlación entre ambos datos. Si se toman las estadísticas de 2018, resultan en un índice de correlación de 0.95, es decir, una fuerte correlación.

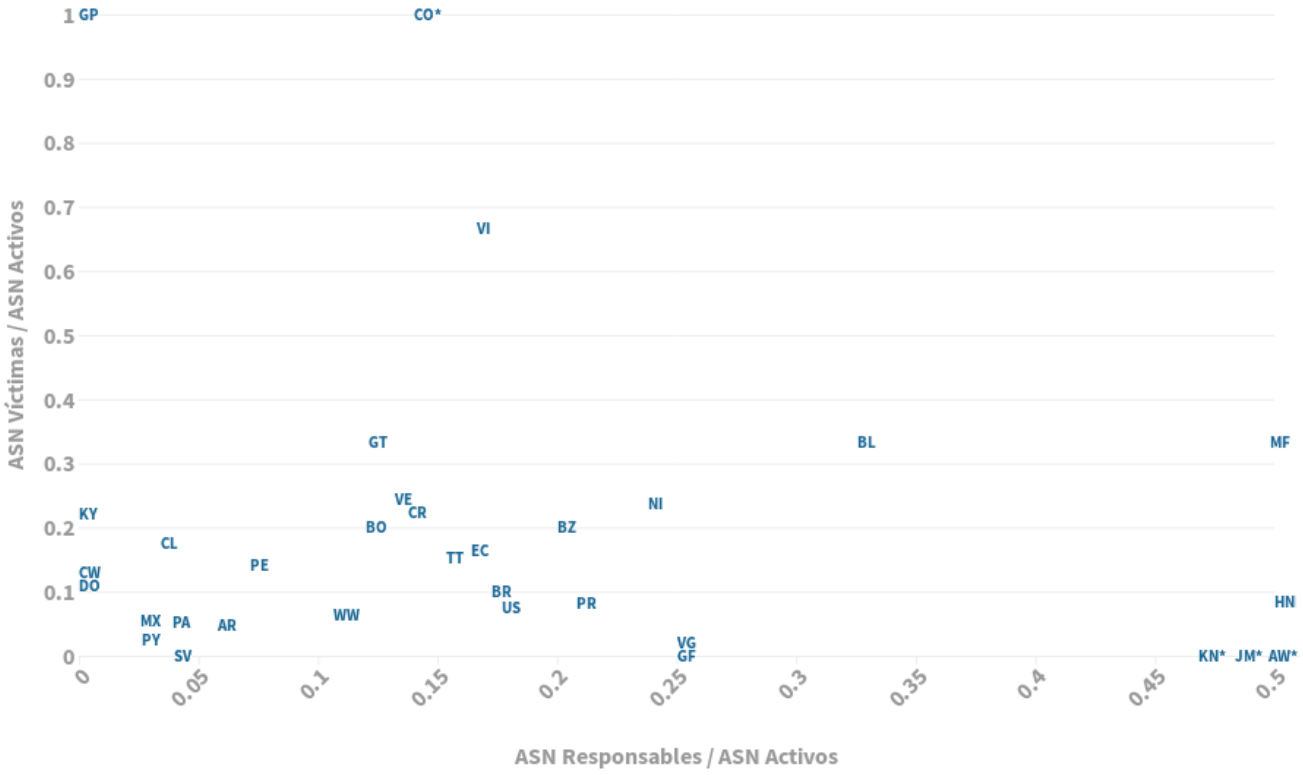
Gráfico 12: cantidad de incidentes ocurridos por país vs. cantidad de sistemas autónomos activos (2018).



Fuentes: ‹https://bgpstream.com› ripe ncc

Así también podemos realizar comparaciones entre países, como podemos observar en el siguiente gráfico, donde se comparan los distintos países de la región, sumado a Estados Unidos (US) y el total global (WW). Para realizar esta comparación se toma en el eje vertical una métrica que consiste en sumar por país los eventos en los que un sistema autónomo fue víctima (de un *hijack* o *leak*) dividido por la cantidad de ASN activos al final de ese año. En el eje horizontal se toma como métrica la cantidad de sistemas autónomos responsables de incidentes por país (*leaks* o propagación de estas y provocación de *hijacks*), dividida por la cantidad de sistemas autónomos activos al final del año.

Gráfico 13: Comparación de países de LAC en base a incidentes de 2017.



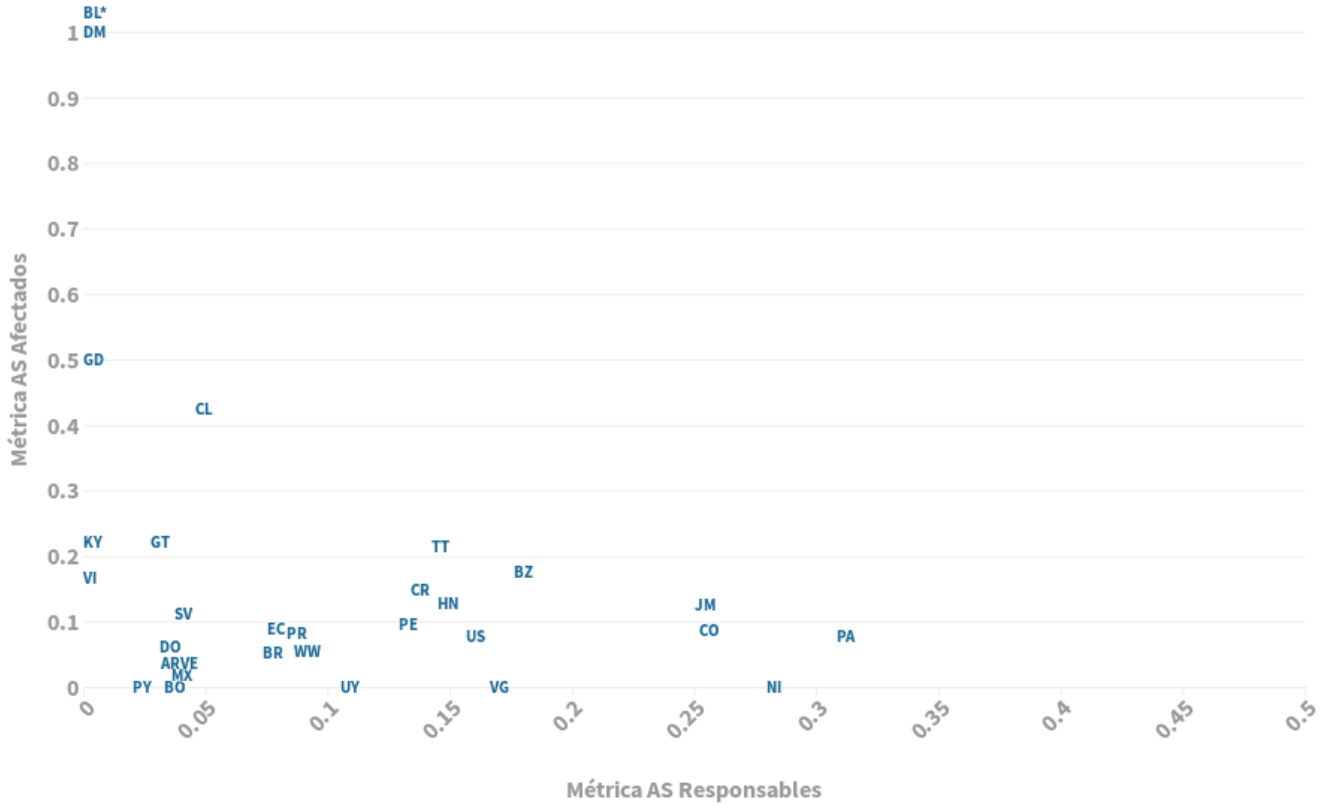
Fuentes:‹https://bgpstream.com› ripe ncc

Países fuera de los límites del gráfico:

- Colombia (CO): asn víctimas / asn activos: 2,1
- Saint Kitts y Nevis (KN): asn responsables / asn activos: 1
- Jamaica (JM): asn responsables / asn activos: 0,6
- Aruba (AW): asn responsables / asn activos: 3

Los países más cercanos al origen [0, 0] están mejor posicionados y tienen menor cantidad de sistemas autónomos protagonistas de incidentes de ruteo. Podemos ver que hay un clúster de países (Argentina, Chile, México, Panamá y Perú, entre otros) que está mejor que la media mundial. Brasil está en una situación muy similar a la de Estados Unidos. Luego, países de Centroamérica e islas del Caribe tuvieron una media de incidentes por ASN superior a las que tuvo el mundo.

Gráfico 14: comparación de países de LAC en base a incidentes de 2018.



Fuentes: ‹https://bgpstream.com› ripe ncc

Países fuera de los límites del gráfico:

- San Bartolomé (BL): ASN víctimas / ASN activos: 1,7

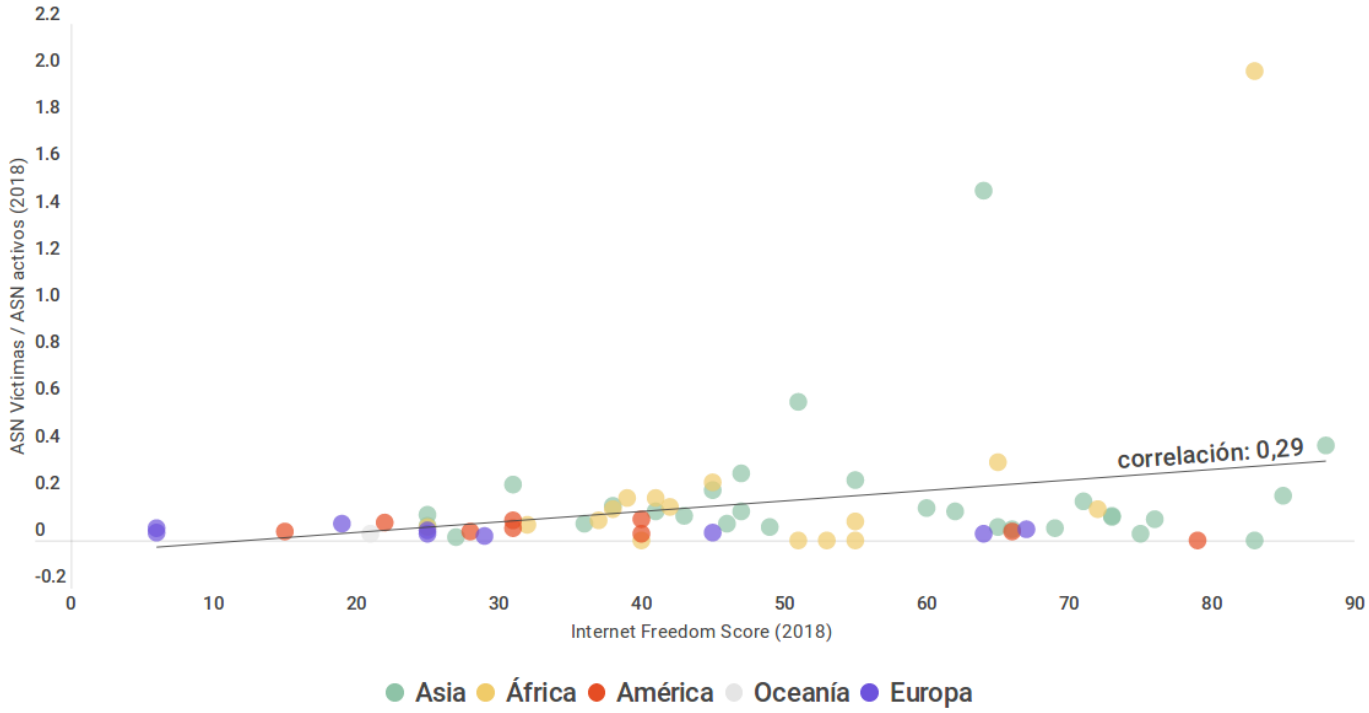
Notamos cómo en 2018 Brasil mejoró su situación sustancialmente y quedó incluso por debajo de la media mundial. En general, los países mejoraron sus estadísticas este año y se acercaron al origen en el gráfico, pero la mayoría de los países de Centroamérica aún siguen por encima de la media en cantidad de incidentes.

Además de utilizarse para comparar países entre sí o su evolución en los distintos años, esta métrica de suma de incidentes sobre cantidad de ASN activos por país puede utilizarse para buscar correlaciones con otras métricas e indicadores de los países. Por ejemplo, existe una ligera correlación entre la cantidad de ASN víctimas por país y el índice de libertad en Internet realizado por la organización Freedom House.[22] Este índice mide el nivel de libertad de Internet y medios digitales de cada país. Para eso se basa en preguntas metodológicas —desarrolladas en conjunto con expertos internacionales— que buscan determinar los principales asuntos que implican una Internet libre. La metodología incluye

[22] ‹https://freedomhouse.org/report/freedom-net/freedom-net-2018›

21 preguntas y cerca de 100 subpreguntas, divididas en tres categorías: obstáculos en el acceso, límites al contenido y violación a los derechos de los usuarios.

Gráfico 15: correlación entre ASN víctimas por país e índice de libertad en Internet.



Fuentes:‹https://bgpstream.com› / ripe ncc / ‹https://freedomhouse.org/report/countries-net-freedom-2018›

Aunque la correlación no sea muy fuerte, habiendo analizado casos puntuales como los desarrollados en este informe, podemos ver indicios de que, si Internet posee una infraestructura de ruteo débil, se transforma en un ambiente propicio para coartar libertades.

Rankings en Latinoamérica

Al igual que a nivel global, a continuación mostramos el top 5 de los sistemas autónomos más involucrados en incidentes de ruteo dentro de nuestra región.

Tabla 7: sistemas autónomos de LAC que más fugas provocaron.

2017			2018		
ASN	DETALLE	Leaks	ASN	Detalle	Leaks
266430	VICTOR.NET E LINK EVOLUTION TELECOM LTDA ME, BR	19	52654	BI-LINK TELECOM, BR	33
52866	IVELOZ TELECOM SERV. EM TELECOMUNICACOES LTDA, BR	16	61678	NETWAY INFORMATICA LTDA, BR	17
262740	VELOO NET LTDA, BR	10	263798	UFINET COLOMBIA, S. A., CO	12
16735	ALGAR TELECOM S/A, BR	6	61832	FORTEL FORTALEZA TELECOMUNICACOES LTDA, BR	8
27908	TRACITY INC., CR	6	52865	R. JOSE DA SILVA E CIA LTDA - ONDAÁGIL, BR	8
			28327	PS5 INTERNET, BR	8

Fuentes: ‹https://bgpstream.com›

Tabla 8: sistemas autónomos de LAC más afectados por fugas.

2017			2018		
ASN	Detalle	Leaks	ASN	Detalle	Leaks
263935	URUCUINET TELECOM E INFORMATICA LTDA - ME, BR	5	264043	SILFERNET COMÉRCIO E SERVIÇOS LTDA, BR	10
262961	INFOWEB SERVIÇOS E ENTRETENIMENTO LTDA - ME, BR	5	264070	FARIA & SCHIMITH LTDA - ME, BR	8
263859	PREFEITURA MUNICIPAL DE PARAUAPEBAS, BR	4	263085	VIA FIBRA NET TELECOM LTDA - ME, BR	7
52408	ITECH SOLUCIONES S.A, CR	4	21538	IGWAN-BL-AS - IGWAN.NET, BL	5
263580	EVEREST SOLUÇÕES EM TELECOMUNICAÇÕES LTDA, BR	4	52408	ITECH SOLUCIONES S.A, CR	5

Fuentes: ‹https://bgpstream.com›

Tabla 9: sistemas autónomos de LAC que más *hijacks* provocaron.

2017			2018		
ASN	Detalle	Hijacks	ASN	Detalle	Hijacks
263444	OPEN X TECNOLOGIA LTDA, BR	50	28140	MAXIWEB INTERNET PROVIDER, BR	21
27884	CABLECOLOR S.A., HN	25	267604	REACH TELECOM, BR	11
28229	HARDONLINE LTDA, BR	10	27884	CABLECOLOR S.A., HN	9
262725	RG SILVEIRA LTDA, BR	8	263459	INTERLINK COMUNICAÇÃO VIRTUAL LTDA ME, BR	7
264979	FRISIA COOPERATIVA AGROINDUSTRIAL, BR	6	262589	INTERNEXA BRASIL OPERADORA DE TELECOMUNICAÇÕES S.A, BR	6
			267286	DJG PROVEDOR E SERVICOS DE TELECOMUNICACOES, BR	6

Fuentes: ‹https://bgpstream.com›

Tabla 10: sistemas autónomos más afectados por *hijacks*.

2017			2018		
ASN	Detalle	Hijacks	ASN	Detalle	Hijacks
13489	EPM TELECOMUNICACIONES S.A. E.S.P., CO	233	14259	GTD INTERNET S.A., CL	79
61440	DIGITAL ENERGY TECHNOLOGIES CHILE SPA, CL	11	265791	COOPERATIVA ELÉCTRICA LIMITADA OBERÁ, AR	4
11993	BANCO DO BRASIL S.A., BR	5	266390	TAJO TECNOLOGIA LTDA, BR	4
52568	TOOLSNET TELECOMUNICACOES LTDA - ME, BR	4	61440	DIGITAL ENERGY TECHNOLOGIES CHILE SPA, CL	3
52850	M & M TELECOMUNICAÇÕES LTDA, BR	4	28646	CONFEDERAÇÃO INT. DAS COOP. LIGADAS AO SICREDI, BR	3
52768	ALSOL PROVEDOR DE INTERNET LTDA., BR	4			
262544	SULCOM INFORMÁTICA LTDA, BR	4			
27730	BBVA BANCO FRANCÉS SA, AR	4			

Fuentes: ‹https://bgpstream.com›

Estrategias de mitigación

Si bien BGP no fue diseñado considerando aspectos de seguridad, como se explicó antes, hoy en día no todo queda a la buena voluntad y confianza de los operadores de red. Con el tiempo se han implementado distintas estrategias para mitigar los efectos de los malos anuncios de ruteo.

En primer lugar, es importante el monitoreo constante. Un operador no puede controlar qué se está anunciando al otro lado de la red ni si sus prefijos están siendo correctamente direccionados, pero puede chequear lo que se está anunciado a través de servicios colectores de anuncios BGP en distintos puntos de la red. Así, los operadores pueden tomar medidas proactivas si ven que algunos de sus prefijos se están anunciando de forma incorrecta en algún punto. Por ejemplo, pueden contactar al proveedor que está generando dicho incidente.

Por otra parte, el filtrado de prefijos anunciados es otra medida clave. La mayoría de las redes solo deben aceptar anuncios de prefijos cuando es necesario, y anunciar sus prefijos a ciertos pares y no a todo Internet. Incluso es posible detectar los *hijacks* monitoreando indicios como cambios en la latencia, degradación del desempeño de la red o desvíos del tráfico de Internet.

Para evitar que todo dependa de la confianza en que los anuncios de prefijos que hace un sistema autónomo sean legítimos, se han creado bases de datos en las que puede registrarse esta información, delegando entonces esa confianza a estas entidades llamadas IRR (Internet Routing Registries). Allí los operadores pueden registrar sus ASN y los prefijos que anuncian, información que los demás operadores podrán consultar para luego filtrar los anuncios BGP y descartar los que no coincidan con datos de estos registros. De todas formas, la seguridad no está garantizada con los IRR: no existe un registro único, por lo que no todos los prefijos están registrados en un único lugar. Incluso pueden contener errores, es decir, que algunos registros son de mayor calidad que otros.[23]

[23] ‹https://blog.cloudflare.com/rpki/›

En el esfuerzo por confiar en los anuncios de direcciones que hacen los sistemas autónomos, empezó a utilizarse criptografía y se adoptaron estándares de infraestructura de clave pública. De forma exitosa, se resolvieron problemas de confianza en otras capas de Internet, como el TLS/SSL que cifra y autentifica las sesiones HTTP, por ejemplo.

Así, el sistema RPKI (Resource Public Key Infrastructure) permite asociar rangos de direcciones IP con números de sistemas autónomos mediante firmas digitales. Esta infraestructura está conformada por los cinco registros regionales de Internet (RIR): ARIN, RIPE NCC, APNIC, LACNIC y AFRINIC. Cada uno conforma una autoridad certificante raíz que emite los correspondientes certificados cuando asigna recursos.[24]

De forma resumida, cada operador puede generar una autorización de origen de ruta o ROA (Route Origination Authorization, en inglés) que asocia un ASN con el prefijo que puede anunciar, junto a una longitud máxima de prefijo posible, para evitar *hijacks* por anuncios más específicos. Estos ROA son firmados digitalmente por el propietario de ese espacio de direcciones IP, es decir, que solo podrán ser generados con el aval de algún RIR y por lo general tienen que renovarse cada año.

Los certificados y ROA se publican en algún repositorio público, donde puedan ser accedidos por los distintos operadores para la validación que les permita filtrar los anuncios BGP incorrectos. Es decir, anuncios originados por un ASN erróneo o más específicos de lo permitido, de acuerdo a las políticas que defina el propietario de cada bloque de direcciones IP.

Si bien esta tecnología está disponible para que todos los operadores la implementen, aún no está bien extendida. Al día de hoy, menos de un 20% de los anuncios BGP realizados en toda la red poseen su respectivo ROA que asegure su autenticidad.[25]

RPKI es una protección efectiva contra ataques como *hijacks* de sistemas autónomos, que anuncian fraudulentamente prefijos que no poseen, pero recordemos que en BGP no solo puede ser anunciado un origen falso sino también una ruta falsa. Una red maliciosa aún podría anunciar de forma fraudulenta una ruta con destino final al ASN que efectivamente está asociado al prefijo deseado por medio de un ROA. Con RPKI esto no se detectaría, ya que no se verifican todos los eslabones de cada ruta anunciada, sino solo el destino final. En respuesta a esto, se diseñó BGPSEC, un protocolo que asegura la legitimidad de las rutas de sistemas autónomos. Esta especificación plantea cambios importantes al protocolo BGP, lo que implica la necesidad de actualizar equipos de *hardware*, algo que hará aún más lenta su adopción.

[24] ‹https://www.noction.com/blog/rpki-overview›

[25] ‹https://observatory.manrs.org/›

Iniciativas

SIDR (The Secure Inter Domain Routing)

Esta iniciativa surgió en el ámbito del IETF 64 en 2005 y se estableció como grupo de trabajo en 2006. Su propósito es reducir la vulnerabilidades de los sistemas de ruteo interdominio. Puntualmente, intenta asegurar que los sistemas autónomos anuncien solo prefijos para los que están autorizados y validar la generación de rutas. Esto último fue base para la especificación de validación de rutas AS, que más tarde se transformó en BGPSEC.

SCION (Scalability, Control, and Isolation On Next-Generation Networks)[26]

Como se ha mencionado, BGP no fue diseñado con aspectos de seguridad en mente. Esto provocó que algunos grupos de investigación buscaran soluciones completamente disruptivas. SCION es una propuesta nacida en la Escuela Politécnica Federal de Zúrich y plantea una nueva arquitectura de Internet, partiendo de la base de que soluciones como BGPSEC atienden el problema de *hijacks* de ruteo, pero devienen en una solución que no escala correctamente y genera otros inconvenientes, como una convergencia más lenta. Entonces, proponen un diseño desde cero que dé una solución de fondo a los problemas.

SCION ya fue implementado y funciona actualmente en algunos ISP suizos, aunque lograr que todos los operadores migren a esta arquitectura parece algo muy poco probable en el corto y mediano plazo.

MANRS (Mutually Agreed Norms for Routing Security)

MANRS es una iniciativa global, impulsada por Internet Society, que provee soluciones para reducir las principales amenazas de ruteo. Su objetivo es dar soporte a dos tipos de actores: operadores de red (ISP) y puntos de intercambio de Internet (IXP). Promueve una serie de acciones que cada uno debe adoptar para poder ser parte de la iniciativa. En el caso de los ISP, estas son: filtrado, anti-spoofing, coordinación, y validación global. Mientras que para los IXP se fomentan las siguientes acciones: prevenir propagaciones, promover MANRS, proteger la plataforma de *peering*, facilitar la comunicación entre ISP y proveer herramientas de monitoreo.[27]

[26] ‹https://www.scion-architecture.net/›

[27] ‹https://www.manrs.org/›

Proyecto FORT

El proyecto FORT[28] es una iniciativa de LACNIC y NIC.MX sobre seguridad de ruteo para una Internet libre y abierta. Busca potenciar el despliegue de RPKI para aumentar la seguridad y la resiliencia de los sistemas de enrutamiento. RPKI es un protocolo que mitiga las vulnerabilidades de estos sistemas al facilitar el intercambio de información segura, de forma de prevenir secuestros de ruta. Paralelamente, FORT abre datos sobre incidentes de ruteo para exponer cómo las vulnerabilidades del sistema de ruteo afectan a los usuarios finales de Internet y su habilidad de disfrutar de una Internet abierta y libre.

FORT ofrece tres productos específicos:

- El presente reporte, que busca generar un diagnóstico sobre la cantidad de incidentes de ruteo que ocurren en la región y su impacto sobre usuarios finales.
- La herramienta Monitoreo FORT, que tiene por objeto estudiar incidentes de enrutamiento en la región y exponer secuestros intencionales. Esta herramienta puede ser consultada por tomadores de decisiones y operadores de la región.
- El Validador FORT, un validador de infraestructura de clave pública para recursos de numeración de Internet (RPKI). Este validador es de código abierto y fue diseñado y desarrollado buscando una eficiencia en el uso de recursos al ejecutarse.

[28] ‹https://fortproject.net/›

Conclusión

En los próximos años, más de cinco mil millones de personas estarán conectadas a Internet. Gran parte de estos nuevos usuarios, viven en sociedades altamente censuradas.[29] Si bien estas acciones de censura pueden realizarse mediante distintas estrategias técnicas y a distintos niveles de las capas de Internet, han existido innumerables casos en los que dichos ataques se realizan en la capa de ruteo. Esto es posible aprovechando las vulnerabilidades que el protocolo BGP no abordó en su diseño, porque fue pensado para una red muy distinta a la de hoy en día, en la que se podía confiar en el buen accionar de todos los operadores.

Actualmente, con más de 92.000 sistemas autónomos, es necesario implementar medidas de seguridad, ya que una infraestructura de ruteo vulnerable afecta la libertad en Internet. Esto se ha observado en incidentes que tuvieron repercusiones contundentes, como el *hijack* de 2008 en Pakistán o incluso casos en la región como los ocurridos en Brasil en 2017.

Considerando la cantidad de incidentes, puede notarse una tendencia a la baja desde el año 2018. A nivel global, se pasó de más de 15.000 incidentes en 2017 a menos de 13.000 el año pasado. En nuestra región esa baja es aún más pronunciada: de casi 5000 a un poco más de 3000. Esto puede adjudicarse al accionar de organizaciones como NIC.BR que han trabajado con los operadores de red para que tomen medidas en el filtrado de rutas y así mitigar los incidentes BGP.

En Brasil ocurren más del 70% de los incidentes de América Latina. Es el segundo país con más ASN registrados (el primero es Estados Unidos), por lo que gran parte de los números en la región dependen del buen trabajo de sus operadores de red. Pero no solo en este país la situación está mejorando, sino que la mayoría de los países de América Latina y el Caribe presentan una mejora con respecto a dos años atrás.

Aun así, esta reducción en la cantidad de incidentes en la región no significa que debemos confiarnos y asumir que el problema ya está resuelto. Sigue siendo necesario el compromiso de todas las partes para lograr una red segura y resiliente. Los gobiernos deben promover un espacio libre de censura y acompañar con políticas el despliegue de tecnologías que construyan una red segura y confiable, algo que solo es posible si contamos con una comunidad técnica activa, que trabaje en solucionar las vulnerabilidades de nuestros protocolos actuales, mediante estándares como BGPSEC y RPKI.

Además, es clave que la sociedad civil siga monitoreando y registrando las anomalías de conectividad que padecen distintas comunidades para hacer sus denuncias cuando corresponda. Todo este esfuerzo es en vano si los protagonistas de este asunto, es decir, los operadores de red de nuestra región, no continúan su trabajo para fortalecer el sistema de ruteo. Hoy cuentan con las herramientas para lograrlo: pueden generar los ROA de sus prefijos obtenidos a través del portal de LACNIC, realizar validación usando el Validador FORT y monitorear incidentes a través de la herramienta de monitoreo FORT.

[29] ‹https://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html›

Anexos

Cantidad de incidentes ocurridos por mes en el mundo

Fecha	Outages	Leaks	Hijacks
ene 2017	620	111	139
feb 2017	694	183	213
mar 2017	722	136	301
abr 2017	840	143	304
may 2017	907	189	170
jun 2017	850	133	167
jul 2017	1038	326	155
ago 2017	993	811	193
sep 2017	922	198	220
oct 2017	1011	177	184
nov 2017	812	225	199
dic 2017	817	216	182
ene 2018	718	210	181
feb 2018	711	168	98
mar 2018	804	218	0
abr 2018	724	165	63
may 2018	668	213	230
jun 2018	696	141	302
jul 2018	627	149	407
ago 2018	457	137	239
sep 2018	524	155	236
oct 2018	548	246	195
nov 2018	647	392	249
dic 2018	738	208	135
ene 2019	782	270	143
feb 2019	518	171	144
mar 2019	604	247	133
abr 2019	586	252	200

Estadísticas 2017

CC	País	outages	leaks (resp.)	leaks (vict.)	leaks (prop.)	hijacks (resp.)	hijacks (vict.)	ASNs activos
AD	Andorra	3	0	0	0	0	0	1
AE	Emiratos Árabes Unidos	18	0	1	5	2	5	57
AF	Afganistán	16	0	6	0	4	6	41
AL	Albania	9	1	6	1	0	0	53
AM	Armenia	32	0	4	0	1	0	56
AO	Angola	12	5	3	0	4	1	38
AR	Argentina	271	0	11	0	35	18	598
AS	Samoa Americana	0	0	0	0	0	2	1
AT	Austria	4	84	6	12	6	13	469
AU	Australia	28	17	31	2	24	26	1372
AW	Aruba	0	3	0	0	0	0	1
AZ	Azerbaiyán	75	0	1	1	1	1	43
BA	Bosnia y Herzegovina	12	3	2	0	0	3	31
BD	Bangladesh	110	78	114	10	17	23	438
BE	Bélgica	6	1	2	9	4	6	202
BF	Burkina Faso	34	1	5	0	0	1	8
BG	Bulgaria	129	1	5	1	22	21	561
BH	Bahrein	0	0	0	0	0	1	17
BI	Burundi	0	0	0	0	0	2	9
BJ	Benin	12	0	1	0	3	4	11
BL	San Bartolomé	0	0	1	0	1	0	3
BM	Bermuda	0	0	1	0	0	1	15
BN	Brunei Darussalam	8	0	0	0	0	0	6
BO	Bolivia	81	0	3	0	3	2	25
BR	Brasil	2816	322	252	89	441	191	4914
BS	Bahamas	1	0	0	0	0	0	6
BT	Bhután	1	0	1	0	0	0	6
BW	Botswana	19	0	1	0	1	2	17
BY	Belarús	41	0	2	0	7	0	92
BZ	Belice	1	0	0	0	2	2	10
CA	Canadá	24	55	21	14	22	38	1159
CD	República Democrática del Congo	0	3	9	0	4	6	16
CF	República Centroafricana	7	0	9	0	0	0	2
CG	Congo	50	0	0	0	1	1	10
CH	Suiza	9	16	10	6	7	16	593
CI	Côte d´Ivoire	7	10	2	0	3	0	12
CK	Islas Cook	56	0	1	0	0	0	1
CL	Chile	39	1	1	1	4	30	176
CM	Camerún	28	0	3	0	1	3	14
CN	China	104	332	18	245	17	70	364
CO	Colombia	28	0	2	7	9	237	114
CR	Costa Rica	12	6	8	0	2	5	58
CV	Cabo Verde	11	0	0	0	0	0	3
CW	Curaçao	0	0	0	0	0	2	16
CY	Chipre	2	0	1	0	1	2	58
CZ	Chequia	4	3	8	5	8	9	482
DE	Alemania	51	20	18	40	51	89	1637
DJ	Djibouti	16	0	0	0	0	0	2
DK	Dinamarca	0	0	0	0	3	5	264
DO	República Dominicana	47	0	2	0	0	1	26
DZ	Argelia	51	0	1	0	1	0	9

EC	Ecuador	33	2	3	2	7	8	67
EE	Estonia	1	0	2	0	1	3	78
EG	Egipto	55	0	4	0	1	2	57
ER	Eritrea	1	0	1	0	0	0	1
ES	España	58	4	6	4	22	32	677
ET	Etiopía	175	0	0	0	0	0	1
EU	Unión Europea	0	7	0	44	1	1	31
FI	Finlandia	1	0	0	0	3	7	215
FJ	Fiji	12	0	2	0	2	0	7
FK	Islas Malvinas	3	0	0	0	0	0	0
FR	Francia	28	65	11	90	19	52	978
GA	Gabón	22	3	13	0	0	0	11
GB	Reino Unido e Irlanda del Norte	43	70	35	65	87	109	1626
GE	Georgia	31	2	5	1	1	7	72
GF	Guayana Francesa	7	0	0	0	1	0	4
GH	Ghana	18	28	14	10	9	1	48
GI	Gibraltar	0	0	1	0	0	0	8
GM	Gambia	2	0	0	0	0	2	8
GP	Guadalupe	0	0	1	0	0	1	2
GQ	Guinea Ecuatorial	3	0	1	0	0	0	6
GR	Grecia	0	0	1	0	1	0	129
GT	Guatemala	2	0	2	0	4	9	33
GU	Guam	0	1	1	0	1	0	7
GY	Guyana	1	0	0	0	0	0	3
HK	Hong Kong	76	72	62	116	38	34	412
HN	Honduras	21	0	0	0	30	5	59
HR	Croacia	1	1	1	4	0	1	111
HT	Haití	6	0	0	0	0	0	6
HU	Hungría	3	3	0	5	1	3	190
ID	Indonesia	307	26	71	5	44	20	895
IE	Irlanda	2	0	1	0	2	10	154
IL	Israel	19	1	32	0	63	9	222
IM	Isla de Man	0	0	1	0	1	0	6
IN	India	403	90	201	66	104	85	1389
IO	Territorio Británico del Océano Índico	22	0	0	0	0	0	1
IQ	Iraq	124	5	17	2	10	13	82
IR	Irán	605	5	64	5	84	62	430
IS	Islandia	0	0	2	0	1	0	58
IT	Italia	41	2	9	101	8	22	781
JM	Jamaica	1	0	0	0	5	0	8
JO	Jordania	4	1	0	0	3	1	31
JP	Japón	6	63	3	26	4	26	574
KE	Kenya	61	10	7	1	1	3	69
KG	Kirguistán	28	1	1	1	0	0	27
KH	Camboya	5	2	12	0	1	0	55
KI	Kiribati	38	0	0	0	0	0	2
KM	Comoras	5	0	0	0	0	0	2
KN	Saint Kitts y Nevis	0	0	0	0	1	0	1
KP	Corea del Norte	10	0	0	0	1	0	1
KR	Corea del Sur	79	0	31	1	27	19	692
KW	Kuwait	19	1	1	0	1	1	57
KY	Islas Caimán	0	0	0	0	0	2	9
KZ	Kazajstán	22	16	12	12	9	12	91
LA	República Democrática Popular Lao	0	0	13	0	0	0	14
LB	Líbano	37	1	9	0	2	7	111

LK	Sri Lanka	3	4	6	0	1	1	13
LR	Liberia	1	0	0	0	0	0	8
LS	Lesotho	1	0	0	0	0	0	6
LT	Lituania	1	0	1	0	4	11	112
LU	Luxemburgo	3	0	0	0	2	1	71
LV	Letonia	3	3	1	0	2	10	217
LY	Libia	2	0	0	0	0	0	5
MA	Marruecos	7	0	3	3	0	0	10
MD	República de Moldova	6	0	3	0	16	20	107
ME	Montenegro	1	0	0	0	0	1	13
MF	San Martín (parte francesa)	0	0	1	0	3	0	3
MG	Madagascar	37	0	0	0	1	0	4
MH	Islas Marshall	4	0	0	0	0	0	1
MK	ex República Yugoslava de Macedonia	12	0	1	1	0	0	39
MM	Myanmar	4	70	88	4	1	1	36
MN	Mongolia	2	0	0	0	0	0	37
MO	Macao	0	0	6	0	0	0	6
MR	Mauritania	5	0	0	1	0	1	3
MT	Malta	5	0	0	0	0	1	27
MU	Mauricio	4	1	1	6	0	2	16
MV	Maldivas	6	0	1	0	0	2	8
MW	Malawi	15	1	2	0	0	1	8
MX	México	28	4	9	1	1	4	233
MY	Malasia	2	18	17	0	12	8	161
MZ	Mozambique	63	0	2	0	0	2	20
NA	Namibia	2	1	1	1	0	0	8
NC	Nueva Caledonia	2	0	2	0	0	0	8
NE	Níger	6	0	4	0	1	3	6
NF	Islas Norfolk	2	0	0	0	0	0	1
NG	Nigeria	168	54	39	35	6	4	133
NI	Nicaragua	66	0	1	0	5	4	21
NL	Países Bajos	24	19	18	6	53	74	741
NO	Noruega	4	2	1	16	4	14	261
NP	Nepal	14	6	6	0	3	0	56
NR	Nauru	1	0	0	0	0	0	2
NU	Niue	1	0	0	0	0	0	0
NZ	Nueva Zelandia	4	0	6	0	3	6	347
OM	Omán	9	0	2	0	0	0	10
PA	Panamá	42	0	2	0	3	2	77
PE	Perú	84	0	0	0	2	4	28
PF	Polinesia Francesa	8	0	0	0	0	0	3
PG	Papúa Nueva Guinea	101	5	5	0	0	0	11
PH	Filipinas	12	40	83	9	18	4	246
PK	Pakistán	74	1	5	0	0	3	101
PL	Polonia	20	6	12	1	18	34	1907
PR	Puerto Rico	32	5	4	0	5	0	48
PS	Estado de Palestina	44	0	13	0	3	4	39
PT	Portugal	2	0	2	3	6	1	75
PW	Palau	16	0	0	0	0	0	3
PY	Paraguay	65	0	1	0	1	0	38
QA	Qatar	0	0	0	1	0	0	9
RE	Reunión	1	0	0	0	0	0	3
RO	Rumania	63	19	19	6	11	10	1049
RS	Serbia	22	7	7	2	0	5	148
RU	Federación de Rusia	450	190	129	152	222	92	4594

RW	Rwanda	2	1	4	0	0	0	12
SA	Arabia Saudita	83	13	6	2	4	7	116
SB	Islas Salomón	57	0	3	0	0	0	4
SC	Seychelles	19	0	2	0	0	0	12
SD	Sudán	15	0	0	0	0	0	6
SE	Suecia	11	3	7	253	14	16	528
SG	Singapur	22	102	12	102	30	28	251
SH	Santa Elena	5	0	0	0	0	0	0
SI	Eslovenia	0	10	9	7	0	0	249
SK	Eslovaquia	1	1	1	1	0	0	139
SL	Sierra Leona	3	0	1	0	1	1	10
SO	Somalia	27	0	0	0	0	0	11
SR	Suriname	8	0	0	0	0	0	2
SS	Sudán del Sur	0	0	1	0	0	0	6
SV	El Salvador	16	0	0	0	1	0	25
SX	San Martín (parte holandés)	1	0	0	0	0	0	3
SY	República Árabe Siria	27	0	0	0	0	1	2
SZ	Suazilandia	5	0	0	0	0	0	7
TD	Chad	16	0	3	0	0	0	6
TG	Togo	19	0	0	0	0	0	3
TH	Tailandia	37	14	53	8	11	17	336
TJ	Tayikistán	8	1	0	0	2	1	7
TL	Timor-Leste	27	0	2	0	0	0	5
TM	Turkmenistán	7	1	1	0	0	0	3
TN	Túnez	60	0	0	0	0	0	12
TO	Tonga	0	0	0	0	0	2	3
TR	Turquía	91	7	12	2	10	19	408
TT	Trinidad y Tobago	14	0	1	0	2	1	13
TV	Tuvalu	1	0	0	0	0	0	1
TW	Taiwán	6	8	20	1	7	8	128
TZ	República Unida de Tanzanía	37	0	0	0	10	4	57
UA	Ucrania	159	14	33	2	32	65	1628
UG	Uganda	55	0	0	0	0	3	27
UM	Islas menores alejadas de Estados Unidos	1	0	0	0	0	0	0
US	Estados Unidos de América	776	744	835	1675	476	420	16380
UY	Uruguay	12	0	0	0	0	0	20
UZ	Uzbekistán	7	0	0	0	0	13	35
VE	Venezuela	5	6	12	0	1	1	52
VG	Islas Vírgenes Británicas	0	0	0	0	1	0	4
VI	Islas Vírgenes de los Estados Unidos	4	0	2	0	1	2	6
VN	Vietnam	27	19	36	7	8	8	224
VU	Vanuatu	4	0	0	0	0	0	8
WS	Samoa	7	0	1	0	0	0	4
YE	Yemen	3	0	1	0	0	0	2
ZA	Sudáfrica	87	4	4	14	11	18	311
ZM	Zambia	2	0	0	0	6	2	15
ZW	Zimbabwe	23	0	4	0	0	0	16
ZZ	No registrado	149	0	52	0	79	46	0

Estadísticas 2018

CC	País	outages	leaks (resp.)	leaks (vict.)	leaks (prop.)	hijacks (resp.)	hijacks (vict.)	ASNs activos
AD	Andorra	0	0	0	0	2	0	1
AE	Emiratos Árabes Unidos	9	0	0	0	2	3	59
AF	Afganistán	24	0	8	0	3	7	44
AL	Albania	12	0	2	0	1	2	57
AM	Armenia	3	5	0	1	0	1	62
AO	Angola	14	6	0	0	131	0	43
AQ	Antártida	1	0	0	0	0	0	0
AR	Argentina	267	1	8	1	21	18	716
AS	Samoa Americana	20	0	0	0	0	0	2
AT	Austria	3	7	9	9	7	12	491
AU	Australia	67	29	22	4	36	21	1437
AW	Aruba	1	0	0	0	0	0	1
AZ	Azerbaiyán	26	0	6	2	0	0	44
BA	Bosnia y Herzegovina	2	0	4	0	0	0	33
BD	Bangladesh	83	263	309	106	16	35	582
BE	Bélgica	7	0	8	5	10	10	212
BF	Burkina Faso	11	0	9	0	0	2	13
BG	Bulgaria	97	24	16	8	21	6	598
BH	Bahrein	0	3	2	0	0	1	18
BI	Burundi	0	0	0	0	0	2	9
BJ	Benin	12	7	0	0	0	0	12
BL	San Bartolomé	0	0	5	0	0	0	3
BM	Bermuda	0	0	0	0	0	2	14
BN	Brunei Darussalam	2	0	0	0	0	0	6
BO	Bolivia	38	0	0	0	1	0	30
BR	Brasil	1847	145	177	78	214	132	5941
BS	Bahamas	6	0	0	0	0	0	5
BW	Botswana	16	0	0	0	0	0	19
BY	Belarús	17	1	1	1	2	2	100
BZ	Belice	0	1	2	0	2	1	17
CA	Canadá	25	13	11	12	42	35	1188
CD	República Democrática del Congo	0	2	5	0	5	5	22
CF	República Centroafricana	2	0	0	0	0	0	2
CG	Congo	16	0	0	0	1	3	9
CH	Suiza	11	15	14	12	15	13	608
CI	Côte d´Ivoire	5	0	3	0	1	0	11
CK	Islas Cook	49	0	1	0	0	0	1
CL	Chile	22	0	2	0	10	91	220
CM	Camerún	38	0	3	0	1	0	15
CN	China	36	33	35	85	36	125	395
CO	Colombia	25	17	3	0	15	8	127
CR	Costa Rica	3	6	7	0	3	3	67
CU	Cuba	1	0	0	0	0	0	3
CV	Cabo Verde	1	0	0	0	0	0	3
CY	Chipre	18	1	5	0	3	4	61
CZ	Chequia	6	6	12	2	4	8	505
DE	Alemania	51	30	34	32	170	87	1746
DJ	Djibouti	6	6	0	0	20	0	2
DK	Dinamarca	4	0	1	0	1	3	272
DM	Dominica	0	0	2	0	0	0	2

DO	República Dominicana	28	0	0	0	1	2	32
DZ	Argelia	14	0	1	0	0	1	9
EC	Ecuador	16	0	1	0	7	7	89
EE	Estonia	7	0	0	0	2	5	96
EG	Egipto	24	0	4	0	0	4	59
ER	Eritrea	2	0	0	0	0	0	1
ES	España	56	2	4	4	34	30	753
ET	Etiopía	52	0	0	0	0	2	1
EU	Unión Europea	0	5	0	38	0	3	38
FI	Finlandia	0	4	4	4	3	7	230
FJ	Fiji	20	0	2	0	0	0	10
FK	Islas Malvinas	6	0	0	0	0	0	0
FM	Micronesia	0	0	0	0	0	1	4
FO	Islas Feroe	0	0	0	0	1	0	3
FR	Francia	23	20	10	145	15	36	1043
GA	Gabón	6	2	1	0	1	0	11
GB	Reino Unido e Irlanda del Norte	53	17	25	46	61	133	1683
GD	Granada	2	0	0	0	0	2	4
GE	Georgia	15	8	3	0	0	6	82
GF	Guayana Francesa	7	0	0	0	0	0	4
GH	Ghana	14	19	7	1	4	0	57
GL	Groenlandia	0	0	4	0	0	0	1
GM	Gambia	1	0	0	0	0	0	8
GN	Guinea	0	0	1	0	0	0	8
GQ	Guinea Ecuatorial	2	0	0	0	0	0	6
GR	Grecia	1	30	4	0	0	2	129
GS	Georgia e Islas Sandwich del Sur	1	0	0	0	0	0	0
GT	Guatemala	2	0	0	1	0	8	36
GU	Guam	1	1	0	0	0	0	8
GW	Guinea-Bissau	1	0	0	0	0	0	2
GY	Guyana	2	0	0	0	0	0	4
HK	Hong Kong	51	58	52	93	55	65	448
HN	Honduras	4	0	0	0	9	8	62
HR	Croacia	1	135	2	1	0	0	113
HT	Haití	10	0	0	0	0	0	8
HU	Hungría	3	0	0	0	0	4	195
ID	Indonesia	258	36	58	17	24	16	1024
IE	Irlanda	5	0	2	0	5	8	159
IL	Israel	20	0	15	0	24	10	230
IN	India	371	236	47	57	78	119	1589
IO	Territorio Británico del Océano Índico	6	0	0	0	0	0	1
IQ	Iraq	217	9	22	2	8	10	98
IR	Irán	414	3	23	3	61	59	429
IS	Islandia	0	0	1	0	0	1	62
IT	Italia	46	0	6	61	4	19	841
JE	Jersey	1	0	1	0	1	0	3
JM	Jamaica	0	0	0	0	2	1	8
JO	Jordania	7	22	2	0	0	0	34
JP	Japón	6	52	3	10	8	33	593
KE	Kenya	45	2	3	0	3	2	77
KG	Kirguistán	23	0	1	1	4	3	27
KH	Camboya	3	6	12	3	1	6	70
KI	Kiribati	48	0	0	0	0	0	2
KM	Comoras	21	0	0	0	0	0	2
KP	Corea del Norte	2	0	0	0	0	0	1

KR	Corea del Sur	38	3	10	3	17	39	700
KW	Kuwait	7	0	2	0	0	4	58
KY	Islas Caimán	0	0	0	0	0	2	9
KZ	Kazajstán	24	3	8	3	1	4	96
LA	República Democrática Popular Lao	0	2	2	0	0	0	16
LB	Líbano	31	0	5	0	4	10	120
LC	Santa Lucía	3	0	0	0	0	0	2
LI	Liechtenstein	0	1	2	0	0	1	21
LK	Sri Lanka	14	3	3	0	0	1	14
LR	Liberia	9	0	0	0	2	1	9
LS	Lesotho	1	0	0	0	0	0	6
LT	Lituania	5	1	4	1	3	6	123
LU	Luxemburgo	0	0	0	0	2	4	73
LV	Letonia	13	1	0	0	3	6	217
LY	Libia	2	0	0	0	0	0	5
MA	Marruecos	28	0	1	1	2	2	12
MD	República de Moldova	10	0	5	0	6	8	120
MF	San Martín (parte francesa)	1	0	0	0	0	0	4
MG	Madagascar	45	0	0	0	0	1	4
MK	ex República Yugoslava de Macedonia	1	0	0	0	0	1	43
ML	Malí	0	0	0	0	3	0	6
MM	Myanmar	1	70	83	6	2	2	57
MN	Mongolia	12	0	0	0	0	0	37
MO	Macao	0	0	2	0	0	0	7
MR	Mauritania	3	0	0	0	0	0	3
MT	Malta	7	0	0	0	0	1	28
MU	Mauricio	4	0	0	5	3	2	17
MV	Maldivas	21	0	0	0	0	0	10
MW	Malawi	9	0	2	0	0	0	11
MX	México	31	3	3	2	4	4	250
MY	Malasia	8	4	23	6	26	15	179
MZ	Mozambique	27	0	0	0	6	0	20
NA	Namibia	2	0	0	0	0	2	9
NE	Níger	22	0	2	0	0	1	6
NF	Islas Norfolk	29	0	1	0	0	0	1
NG	Nigeria	138	13	9	0	3	3	139
NI	Nicaragua	36	0	0	0	6	0	21
NL	Países Bajos	24	7	12	19	85	84	807
NO	Noruega	1	0	2	12	0	4	278
NP	Nepal	10	0	1	0	2	2	70
NR	Nauru	17	0	0	0	0	0	2
NU	Niue	1	0	0	0	0	0	0
NZ	Nueva Zelandia	9	1	11	0	4	8	370
OM	Omán	0	0	0	0	1	1	12
PA	Panamá	25	2	3	14	8	3	76
PE	Perú	9	0	0	0	4	3	30
PF	Polinesia Francesa	16	0	0	0	0	0	3
PG	Papúa Nueva Guinea	16	0	2	0	0	1	10
PH	Filipinas	9	37	51	2	31	9	250
PK	Pakistán	41	0	4	0	1	8	119
PL	Polonia	41	9	12	5	171	32	1974
PM	San Pedro y Miquelón	2	0	0	0	0	0	1
PR	Puerto Rico	11	0	1	0	4	3	49
PS	Estado de Palestina	28	0	4	0	1	2	40
PT	Portugal	0	0	0	8	22	8	84

PY	Paraguay	112	0	0	0	1	0	50
QA	Qatar	0	0	0	0	0	1	10
RO	Rumania	69	10	24	6	15	16	1037
RS	Serbia	34	0	2	0	4	1	151
RU	Federación de Rusia	274	120	160	112	63	62	4699
RW	Rwanda	0	0	1	0	0	0	12
SA	Arabia Saudita	10	52	9	3	1	4	123
SB	Islas Salomón	139	0	1	0	0	0	3
SC	Seychelles	12	0	1	0	0	0	11
SD	Sudán	36	0	2	0	0	0	6
SE	Suecia	18	7	4	38	7	6	539
SG	Singapur	33	12	9	192	9	24	269
SH	Santa Elena	18	0	0	0	0	0	0
SI	Eslovenia	0	4	4	2	1	0	251
SK	Eslovaquia	1	0	0	0	0	0	147
SL	Sierra Leona	2	0	0	0	0	0	13
SM	San Marino	3	0	0	0	0	0	6
SN	Senegal	0	0	0	0	0	1	6
SO	Somalia	1	0	0	0	0	0	12
SR	Suriname	14	0	0	0	0	0	3
SS	Sudán del Sur	0	0	2	0	0	1	6
ST	Santo Tomé y Príncipe	1	0	0	0	0	0	2
SV	El Salvador	7	0	1	0	1	2	27
SY	República Árabe Siria	26	0	0	0	0	0	2
SZ	Suazilandia	4	0	0	0	2	0	7
TD	Chad	6	0	0	0	0	0	8
TG	Togo	0	0	5	0	0	0	4
TH	Tailandia	25	14	10	4	5	10	351
TJ	Tayikistán	17	1	0	0	0	1	7
TL	Timor-Leste	9	0	3	0	0	0	6
TM	Turkmenistán	20	0	0	0	0	0	4
TN	Túnez	53	0	1	0	0	1	15
TR	Turquía	82	5	6	4	18	14	425
TT	Trinidad y Tobago	13	0	2	0	2	1	14
TW	Taiwán	9	3	8	3	6	14	141
TZ	República Unida de Tanzanía	19	1	4	0	4	5	60
UA	Ucrania	134	11	21	1	33	35	1578
UG	Uganda	6	0	1	0	0	4	28
UM	Islas menores alejadas de Estados Unidos	1	0	0	0	0	0	0
US	Estados Unidos de América	685	681	772	1526	408	522	16688
UY	Uruguay	4	0	0	0	2	0	19
UZ	Uzbekistán	11	0	0	0	0	1	36
VE	Venezuela	8	0	1	0	2	1	54
VG	Islas Vírgenes Británicas	0	0	0	0	1	0	6
VI	Islas Vírgenes de los Estados Unidos	11	0	0	0	0	1	6
VN	Vietnam	11	26	12	3	10	10	242
VU	Vanuatu	30	0	0	0	0	0	9
WF	Islas Wallis y Futuna	6	0	0	0	0	0	1
WS	Samoa	18	0	1	0	0	0	4
YE	Yemen	4	0	0	0	0	0	3
ZA	Sudáfrica	121	7	2	5	21	19	368
ZM	Zambia	2	0	1	0	2	1	14
ZW	Zimbabwe	19	0	0	0	0	0	18
ZZ	No registrado	60	0	15	0	77	33	0