CENTRO DE POSGRADOS

Tema:

PROPUESTA DE IMPLEMENTACION DE *MUTUALLY AGREED NORMS FOR ROUTING SECURITY* (MANRS) EN UN ISP

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Edison Xavier Ríos Verdezoto

Director:

Mg. Paúl Fernando Bernal Barzallo

Ambato – Ecuador

Octubre 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **EDISON XAVIER RÍOS VERDEZOTO**, con cédula de ciudadanía **0202135794**, autor del trabajo de graduación intitulado: "PROPUESTA DE IMPLEMENTACION DE *MUTUALLY AGREED NORMS FOR ROUTING SECURITY* (MANRS) EN UN ISP", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, octubre 2024

Edison Xavier Ríos Verdezoto

CC. 0202135794

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

PROPUESTA DE IMPLEMENTACION DE *MUTUALLY AGREED NORMS FOR ROUTING SECURITY* (MANRS) EN UN ISP

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Edison Xavier Ríos Verdezoto

Paúl Fernando Bernal Barzallo, Ing. Mg.
CC. 0602752339
CALIFICADOR

f. PAUL FERNANDO BERNAL BARZALLO

Verónica Maribel Pailiacho Mena, Ing. Mg.
CALIFICADOR

f. VERONICA MARIBEL PAILIACHO MENA

Diego Fernando Ávila Pesantez, Ing. Mg.
CALIFICADOR

f. DIEGO FERNANDO AVILA PESANTEZ

Teresa Milena Freire Aillón, Ing. Mg.
DIRECTORA CENTRO DE POSGRADOS

f. TERESA MILENA FREIRE AILLON Firmado digitalmente por TERESA MILENA FREIRE AILLON Fecha: 2024.10.01 12:40:58 -05'00'

Diego Gonzalo Coca Chanalata, Dr.
SECRETARIO GENERAL PUCESA

f. DIEGO GONZALO COCA CHANALATA Firmado digitalmente por DIEGO GONZALO COCA CHANALATA Fecha: 2024.10.02 08:53:12 -05'00'

Ambato – Ecuador

Octubre 2024

DEDICATORIA

EL presente trabajo de investigación está dedicado a mis padres Luis y Herminia quienes han creído en mi motivándome a seguir en mis estudios académicos los amo inmensamente. quiero agradecer especialmente a mi esposa Aracely quien me ha brindado su amor incondicionalmente y está conmigo en cada escalón de mi vida te amo inmensamente siempre agradecido por tu paciencia.

AGRADECIMIENTO

Quiero agradecer a Dios por haberme permitido continuar mis estudios académicos. Un agradecimiento especial a todas las personas que fueron parte fundamental en este proceso de investigación, compartiendo sus conocimientos y espero que la información del presente trabajo sea de utilidad para otras personas.

RESUMEN

Actualmente dentro la infraestructura técnica de los proveedores de Internet (ISP), se presentan inconvenientes dentro de los procesos de ruteo, específicamente el secuestro de rutas o BGP *Hijacks* y fuga de rutas o BGP *Route leaks* siguen presentes, consecuencia de ello los ISP continúan presentando pérdidas económicas y una debilitada reputación, por lo que resulta importante para cualquier proveedor garantizar el anuncio correcto de rutas y prefijos hacia el mundo en sus *routers* de borde.

Es así que este trabajo plantea como objetivo fortalecer el enrutamiento seguro a través de la implementación de *Mutually Agreed Norms for Routing Security* (MANRS). La metodología abarca la evaluación detallada de la infraestructura de red actual, seguida por el fortalecimiento de la seguridad del enrutamiento mediante la implementación de las mejores prácticas de MANRS.

Esto abarca el filtrado BGP, medidas *anti-spoofing*, coordinación de enrutamiento y validación de rutas a través de RPKI. Posterior a eso la implementación fue evaluada por un experto en el tema. Se espera que el ISP sea registrado como una empresa que implementa *Mutually Agreed Norms for Routing Security* (MANRS) en el sitio oficial del observatorio MANRS, lo que trae consigo una garantía de seguridad y un consecuente crecimiento de la reputación del proveedor.

Palabras clave: bgp, *hijacks, leaks*, manrs, isp, rpki.

ABSTRACT

Currently, within the technical infrastructure of Internet Service Providers (ISPs), there are problems within the routing processes, specifically BGP hijacks and BGP route leaks, which are still present. As a result, ISPs continue to present economic losses and a weakened reputation, so any provider needs to ensure the correct announcement of routes and prefixes to the world in their edge routers.

Thus, this search aims to strengthen secure routing through by implementing Mutually Agreed Norms for Routing Security (MANRS). The methodology encompasses a detailed assessment of the current network infrastructure while strengthening routing security and implementing MANRS best practices.

This process covers BGP filtering, anti-spoofing measures, routing coordination and route validation through RPKI. After that, a subject matter expert evaluated the implementation process. The ISP will register itself as a company implementing Mutually Agreed Norms for Routing Security (MANRS) on the official MANRS observatory site, which enhances security and a consequent growth of the provider's reputation.

Keywords: *bgp, hijacks, leaks, manrs, isp, rpki.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Internet es una herramienta esencial para las vidas, pero su creciente dependencia también ha aumentado la vulnerabilidad a los ataques cibernéticos. Uno de los componentes más críticos de Internet es el sistema de enrutamiento, que es responsable de dirigir los datos de un punto a otro. Los incidentes de enrutamiento pueden causar graves interrupciones en la trasmisión de datos causando daños económicos y comprometer sistemas, las medidas de seguridad existentes pueden ayudar a abordar algunos de estos incidentes, pero las soluciones que brindan suelen ser limitadas. Para proteger el ciberespacio, es importante que todos los actores involucrados trabajen juntos.

Las empresas deben trabajar con operadores de redes e infraestructura para garantizar que sus proveedores implementen las mejores prácticas de seguridad del enrutamiento. MANRS es una iniciativa impulsada por la comunidad que proporciona un conjunto de mejores prácticas para que los operadores de red mejoren la seguridad del sistema global de enrutamiento de Internet. (*MANRS-primer-enterprises-es.pdf,* 2021).

Para la organización *Join the MANRS Network Operator Program* (2023) las normas mutuamente acordadas para la seguridad del enrutamiento son un conjunto de recomendaciones para ayudar a proteger el Internet. MANRS se basan en cuatro acciones simples pero efectivas:

- Filtrado. - Evitar la propagación de información incorrecta de enrutado incorrecto.
- Anti-spoofing. - Evite el tráfico con direcciones IP de origen falsificadas.
- Coordinación. - Facilitar la comunicación y coordinación operativa global entre los operadores de redes.
- Información global. - Facilitar la validación de la información de enrutar a escala mundial.

Estas acciones han sido adoptadas por más de 700 organizaciones de todo el mundo, lo que las convierte en una de las iniciativas de seguridad de Internet más exitosas. las normas mutuamente acordadas para la seguridad del enrutamiento han contribuido a reducir significativamente la incidencia de incidentes, lo que ha ayudado a mantener la estabilidad y la seguridad de Internet. (Kruse, 2021)

La protección de datos es un derecho fundamental que debe ser respetado en todo momento. Las MANRS son una herramienta importante para ayudar a proteger los datos personales y la privacidad de los usuarios de Internet.

En particular, las MANRS son importantes para la protección de datos porque:

a.- Ayudan a prevenir la suplantación de identidad de enrutamiento, que puede usarse para robar datos personales o interrumpir los servicios en línea.

La suplantación de identidad de enrutamiento puede usarse para desviar el tráfico a un destino falso, lo que podría permitir que los atacantes intercepten datos personales.

Para la organización *Join the MANRS Network Operator Program* (2023) las normas mutuamente acordadas para la seguridad del enrutamiento ayudan a prevenir la suplantación de identidad de enrutamiento al implementar controles para verificar la identidad de los operadores de redes que envían anuncios de enrutamiento. Estos controles pueden ayudar a evitar que los atacantes tomen el control de los enrutadores y envíen anuncios de enrutamiento falsos.

b.- Promueven la coordinación entre los operadores de redes, lo que facilita la detección y la respuesta a los incidentes de seguridad.

Cuando un incidente de seguridad del enrutamiento ocurre, es importante que los operadores de redes puedan comunicarse entre sí para compartir información y coordinar su respuesta. Las MANRS promueven la coordinación entre los

operadores de redes al proporcionar directrices para la comunicación y la cooperación en caso de un incidente.

La coordinación entre los operadores de redes puede ayudar a acelerar la detección y la respuesta a los incidentes de seguridad del enrutamiento. Esto puede ayudar a reducir el impacto de los incidentes en la disponibilidad de Internet y en la seguridad de los datos personales.

c.- Fomentan la validación global de la información de enrutamiento, lo que ayuda a garantizar que los datos personales se transmitan de manera segura.

La validación global de la información de enrutamiento ayuda a garantizar que los datos personales se transmitan por la ruta más segura posible. Las MANRS fomentan la validación global al proporcionar directrices para la validación de la información de enrutamiento.

d. - La validación global de la información de enrutamiento puede ayudar a proteger los datos personales de ser interceptados por atacantes.
El sistema de enrutamiento de Internet es una infraestructura crítica que permite que los datos circulen por la red. Sin embargo, este sistema es vulnerable a una serie de amenazas, como el secuestro de prefijos BGP (*Borde Gatway Protocol*), las fugas de ruta y la suplantación de identidad.

Para abordar estas amenazas, la comunidad de operadores de red ha desarrollado las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS). MANRS es una iniciativa global que proporciona soluciones fundamentales para reducir las amenazas comunes al sistema de enrutamiento. (*MANRS-Network-Operators-Actions-v2.5.2.pdf,* 2021).

MANRS fue fundada en 2014 por un grupo de proveedores de servicios de Internet ISP (Proveedor de servicio de internet) preocupados por la seguridad del sistema de enrutamiento. La iniciativa se lanzó oficialmente en 2015 y ha crecido rápidamente desde entonces. (Freedman, y otros, 2014)

Los incidentes de seguridad de enrutamiento BGP son eventos en los que un actor malicioso o un error de configuración provoca que el tráfico de Internet se desvíe a una ruta incorrecta. Estos incidentes pueden tener un impacto significativo en la disponibilidad y el rendimiento de Internet.

Algunos ejemplos de incidentes de seguridad de enrutamiento BGP incluyen:

- En 2017, el tráfico de importantes servicios como Google, Apple, Facebook y Microsoft fue desviado hacia un misterioso AS (Sistema autónomo) ruso que nunca antes había operado.
- En 2020, un incidente de enrutamiento BGP provocó la interrupción del servicio de Google Cloud en Europa.

Ante la problemática de enrutamientos en los ISP la hipótesis es la adopción de las mejores prácticas de enrutamiento seguro definidas por MANRS reflejara el compromiso del ISP con la responsabilidad comunitaria de mantener la integridad de internet.

Por tal motivo, la presente investigación tiene como objetivo fortalecer la seguridad del enrutamiento con la implementación de Normas de Acuerdo Mutuo para la Seguridad del Enrutamiento (MANRS) en un ISP.

1. Desarrollar el estado del arte y la práctica de *Mutually Agreed Norms for Routing Security* (MANRS) en un ISP.

2. Evaluar la infraestructura de red respecto al anuncio de rutas actuales del ISP.

3. Determinar las prácticas de MANRS, que pueden ser incluidas en el ISP.

4. Proponer un modelo de implementación, de *Mutually Agreed Norms for Routing Security* (MANRS) en un ISP.

Para responder a la idea a defender se pretende fortalecer el enrutamiento con la implementación *Mutually Agreed Norms for Routing Security* (MANRS) en un ISP, dentro de la elaboración del estado del arte y la práctica de *Mutually Agreed Norms for Routing Security* (MANRS) en un ISP, se procede a evaluar la infraestructura de red respecto al anuncio de rutas actuales del ISP, para determinar las prácticas de MANRS, que pueden ser incluidas en el ISP, aplicar un modelo de implementación, de *Mutually Agreed Norms for Routing Security* (MANRS) en el ISP.

La metodología de investigación propuesta es adecuada para el estudio que se propone realizar. La revisión de la bibliográfica proporcionará una base sólida para comprender los beneficios y desafíos de la adopción de MANRS. Esta metodología permitirá no solo abordar la idea a defender de la adopción de las mejores prácticas de enrutamiento seguro definidas por MANRS reflejará el compromiso del ISP con la responsabilidad comunitaria, sino también fortalecer la seguridad del enrutamiento y contribuir al bienestar general de la comunidad de Internet. La evaluación de la infraestructura de red permitirá identificar los riesgos de seguridad existentes y las oportunidades de mejora. El desarrollo de un modelo de implementación ayudará a garantizar que las prácticas de MANRS se implementen correctamente. La implementación de las prácticas permitirá evaluar su efectividad. La evaluación permitirá garantizar que las prácticas se hayan implementado correctamente y que estén cumpliendo con los objetivos del estudio.

La puesta en marcha de las *Mutually Agreed Norms for Routing Security* (MANRS) en un Proveedor de Servicios de Internet (ISP) se justifica por la creciente vulnerabilidad de la infraestructura de enrutamiento frente a amenazas cibernéticas, especialmente la suplantación de identidad de enrutamiento. Esta vulnerabilidad no solo compromete la disponibilidad y el rendimiento de Internet, sino que también amenaza la seguridad y privacidad de los datos transmitidos a través de la red.

La adopción de MANRS se presenta como una medida proactiva y efectiva para abordar estos riesgos. La iniciativa, respaldada por más de 700 organizaciones a nivel mundial, ofrece un conjunto de prácticas fundamentales que incluyen filtrado, *anti-spoofing*, coordinación y validación global de la información de enrutamiento.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. *Mutually Agreed Norms for Routing Security* (MANRS)

Las normas mutuamente acordadas para la seguridad del enrutamiento (MANRS) es una iniciativa global, apoyada por la sociedad de internet *(Internet Society)*, que proporciona soluciones fundamentales para reducir amenazas comunes. MANRS ofrece acciones específicas a través de sus 4 programas para proveedor de servicio de internet (ISP), proveedor de intercambio de internet (IXP), proveedores de contenido (CDN) y proveedor de servicio de la nube (Cloud). (MANRS, 2023).

Historia *Mutually Agreed Norms for Routing Security* (MANRS)

Al inicio del 2014 un grupo pequeño de proveedores de internet (ISP) comenzó a trabajar en una forma de reunir a la comunidad de operadores de red para mejorar la seguridad del enrutamiento en el mundo. Esto se dio con el nombre de manifiesto de residencia de *routing*, y se produjo un conjunto de recomendaciones iniciales que se publicó en julio del 2014 para la revisión y comentarios de la comunidad de operadores de red.

Una vez que el periodo de revisión y retroalimentación culmino se consolido como normas mutuamente acordadas para la seguridad de enrutamiento y fue lanzado oficialmente en su sitio web MARNS. (Freedman, y otros, 2014).

Definiciones de términos

El presente trabajo detalla las acciones obligatorias y esperadas, es necesario dar definiciones de ciertos términos que tienen relación general en la comunidad de operadores de red.

Un sistema autónomo (AS) es un grupo de direcciones IP que son gestionadas por uno o más operadores de red que posee una clara y única política de ruteo. Cada sistema autónomo tiene un numero asociado lo cual es usado como identificador

para el sistema autónomo en el intercambio de información de ruteo externo. Los protocolos de enrutamiento externos como BGP son usados para el intercambio de información entre sistemas autónomos (AS). (Lacnic, 2023)

BGP. Es un protocolo de puerta de enlace exterior (EGP) que se utiliza para intercambiar información de enrutamiento entre enrutadores de diferentes sistemas autónomos (AS). La información de enrutamiento del BGP incluye la ruta completa a cada destino. El BGP utiliza la información de enrutamiento para mantener una base de datos de información de accesibilidad de red, que intercambia con otros sistemas BGP. El BGP usa la información de accesibilidad de la red para construir un gráfico de conectividad del AS, lo que permite que el BGP elimine los bucles de enrutamiento y aplique las decisiones de política a nivel del AS. (*Guía del usuario del BGP* | *Junos OS* | *Juniper Networks*, 2023.)

AS Path Prepending proporciona una herramienta para manipular el atributo BGP *AS_Path* anteponiendo múltiples entradas de un AS. AS *Path Prepending* se utiliza para despriorizar un ruta o camino alternativo. Al anteponer el AS local varias veces, los AS pueden hacer las rutas AS anunciadas parecen artificialmente más largas. La anteposición excesiva de ruta AS ha causado Problemas de enrutamiento en Internet. (Zeng et al., 2023).

Secuestros de prefijos BGP (Prefix hijacks). Un evento de secuestro de origen de prefijo es cuando el Sistema Autónomo de un adversario anuncia ilegítimamente un prefijo IP como perteneciente a otro AS. Si el secuestro se considera exitoso, el anuncio debe propagarse hacia tantos otros hablantes BGP como sea posible y ser aceptado en sus RIB. El resultado de este evento es que el adversario ha modificado la DFZ y, por lo tanto, se ha convertido en el AS de destino para el prefijo secuestrado, lo que resultará en la atracción (secuestro) de tráfico. (Kowalski & Mazurczyk, 2023)

Fugas de ruta (*Route leaks*). Una fuga de ruta accidental provocará una redirección a una ruta diferente a la prevista. Esta redirección puede o no sobrecargar algunos equipos y enlaces de red, lo que puede causar una degradación del rendimiento,

los dispositivos o las interconexiones no pueden procesar o transferir el aumento del tráfico. Los síntomas incluyen un mayor retraso de paquetes, pérdida parcial de paquetes o incluso descarte (*blackholing*) del tráfico. (Kowalski & Mazurczyk, 2023)

Operador de red. Es una organización que proporciona conectividad de internet a otra organización de red y a usuarios finales. (*MANRS-Network-Operators-Actions-v2.5.2.pdf*, 2021).

RIR. Registro regional de internet que gestiona la asignación y registro de recursos numéricos de internet dentro de una región del mundo. (*MANRS-Network-Operators-Actions-v2.5.2.pdf*, 2021).

Registro de Ruta de Internet (IRR). Un Registro de ruteo de Internet (IRR) es una base de datos donde los operadores pueden especificar sus políticas de ruteo y hacer pública esta información para que otros actores que forman parte del sistema de ruteo de Internet puedan utilizar esta información para configurar sus dispositivos. LACNIC IRR está disponible para los operadores de la región que tienen acceso a la plataforma MiLACNIC. Esta plataforma gestiona la información sobre el uso de los bloques de direcciones IPv4 e IPv6 y los números de sistema autónomos asignados en la región de servicios LACNIC. Todos los objetos de la RIR LACNIC son públicos y están disponibles a través de los servidores *File Transfer Protocol* (FTP) de LACNIC. También se pueden consultar a través de varias interfaces web y el servicio Whois. (*Internet Routing Registry (IRR),* 2023).

NIR. Registro nacional de internet que gestiona la asignación y registro de los recursos numéricos de internet para algunos países del mundo. (MARNS, 2023).

Autorizaciones de origen de ruta (ROA). Las ROA permiten a los titulares de prefijos dar fe de cómo se puede originar un prefijo, es decir, estableciendo los ASN de origen permitidos y el máximo Longitud del prefijo para un prefijo determinado. Especificar la longitud máxima del prefijo que sea más larga (más específica) que el prefijo real para el que se crea el ROA tendrá el efecto de cubrir también anuncios

más específicos. (Resource Public Key Infrastructure (RPKI) - Interconnect Help, 2023).

RPKI. Es una infraestructura de clave publica que proporciona criptográficamente medios verificables para asignar prefijos IP a los AS de origen, que previene tanto el secuestro de prefijos como el secuestro de subprefijos. Los propietarios de recursos de red deben registrar objetos RPKI para evitar que sus prefijos de IP sean secuestrados. (Li et al, 2023)

Ataques de sistema de nombre de dominio (DNS). Un ataque de amplificación en un DNS se ejecuta enviando muchas solicitudes a muchos *resolver* de DNS mientras se falsifica la dirección IP de la víctima; un atacante puede pedir muchas respuestas a los *resolver* de DNS para regresar a un destino, aunque solo utilice un sistema para realizar dicho ataque. (Seguridad de enrutamiento para legisladores, 2018).

El Protocolo de Internet IP (*Internet Protocol*). Es la tecnología, el conjunto de reglas de comunicación, que permite que todas estas diferentes redes funcionen unas con otras. El Protocolo de Internet especifica que cada dispositivo de la red global necesita un identificador numérico único, una dirección que permita encontrarlo sin posibilidad de error o confusión, lo que se conoce como una dirección IP. (Moreiras & Patara, 2019).

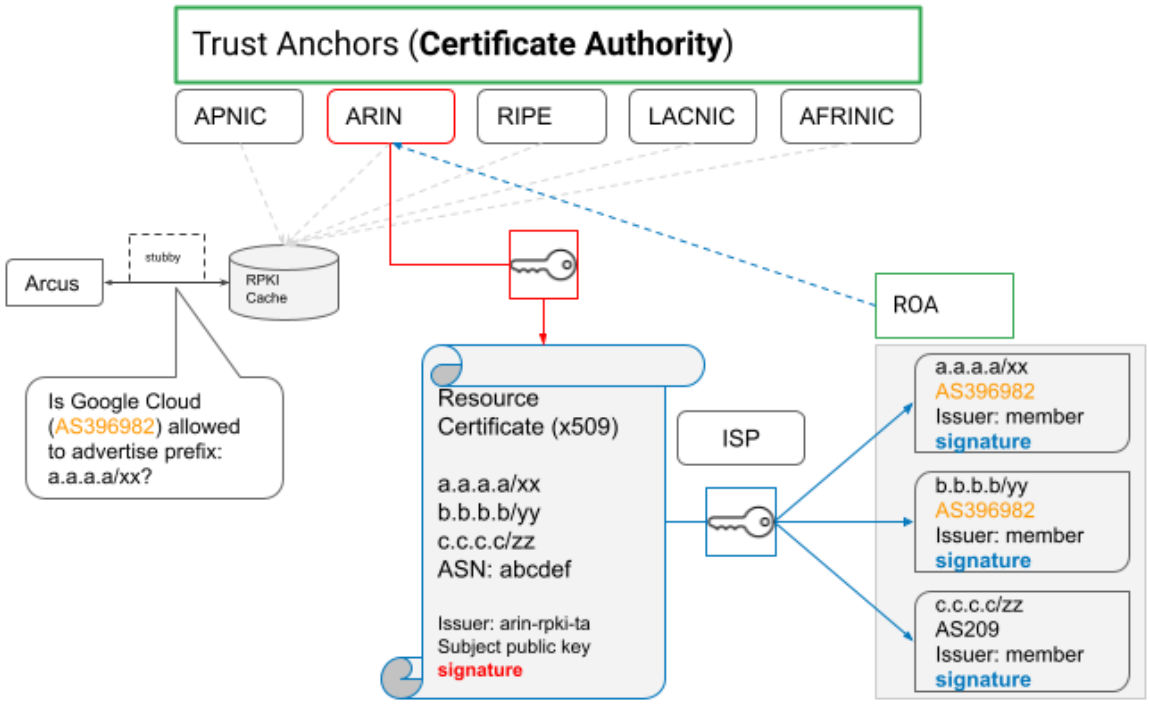
Para la organización Akamai (2023.) un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente. Desde un nivel detallado, un ataque DDoS o DoS es como un atasco de tráfico inesperado causado por cientos de solicitudes de transporte compartido falsas.

Para la organización *UDP-Based Amplification Attacks* | *CISA* (2019) los ataques de amplificación basados en UDP son ciertos protocolos de capa de aplicación que se basan en el protocolo de datagramas de usuario (UDP) se han identificado como

posibles vectores de ataque. Éstas incluyen sistema de nombres de dominio (DNS), protocolo de tiempo de red (NTP), protocolo ligero de acceso a directorios sin conexión (CLDAP), protocolo generador de caracteres (CharGEN), protocolo simple de descubrimiento de servicios (SSDP), *bittorrent*, protocolo simple de administración de red versión 2 (SNMPv2), mapa de puertos/Llamada a procedimiento remoto (RPC), cita del día (QOTD), sistema de nombres de dominio de multidifusión (mDNS), sistema básico de entrada/salida de red (NetBIOS), protocolo de red de terremotos, protocolo de vapor, protocolo de información de enrutamiento versión 1 (RIPv1), protocolo ligero de acceso a directorios (LDAP), protocolo trivial de transferencia de archivos (TFTP), memcached, y descubrimiento dinámico de servicios web (*WS-Discovery*).

RPKI permite declarar quién se le permite anunciar prefijos basados en un sistema de fideicomiso basado en certificados. Se utiliza una jerarquía de anclajes de confianza como autoridades de certificación que sigue la jerarquía para la asignación de números (diseñas IP y Números de Sistemas Autónomos) Figura 1 donde los Registros Regionales de Internet (RIR), Registros Nacionales de Internet (NIR) y los ISP emiten y firman certificados de IKI X.509 que contienen los recursos que han asignado. Los RIR asignan recursos a los NIR y los ISP, los NIR asignan recursos a los proveedores de servicios de Internet, y los proveedores de servicios de Internet asignan recursos a sus clientes.

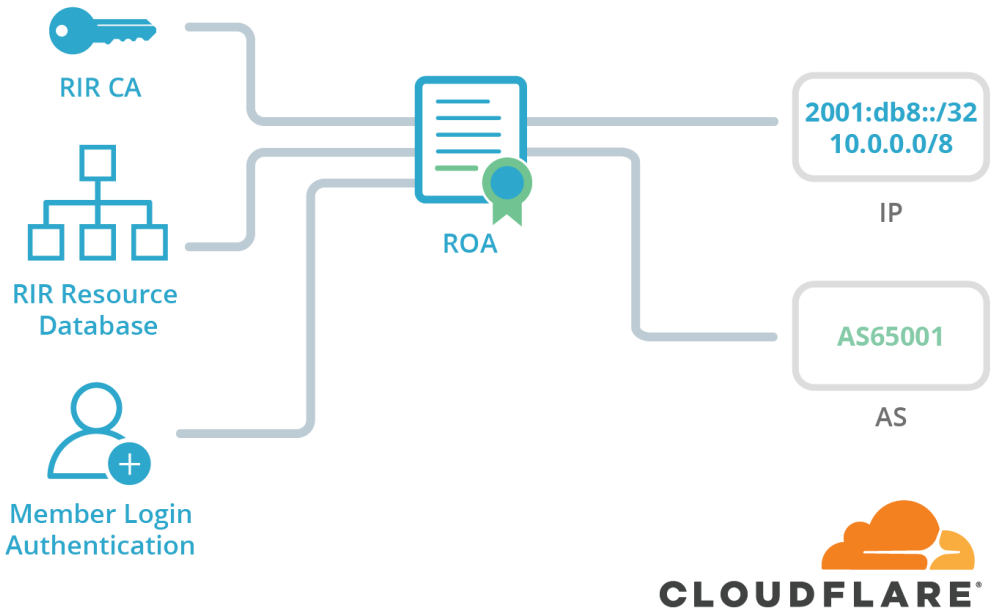
Figura 1. Infraestructura de clave pública de recursos (RPKI)



Fuente: tomada a partir de Resource Public Key Infrastructure (RPKI) - Interconnect Help (s.f.)

La infraestructura de clave pública de recursos (RPKI) es un método criptográfico para firmar registros que asocian una ruta con un número AS de origen que se muestra un diseño lógico en la Figura 2. Actualmente, los cinco RIR (AFRINIC, APNIC, ARIN, LACNIC y RIPE) proporcionan un método para que los miembros tomen un par IP/ASN y firmen un registro ROA (Autorización de origen de ruta). Levy (2018).

Figura 2. ROA (Autorización de origen de ruta)



Fuente: Tomada a partir de ROA (Autorización de origen de ruta) Levy (2018)

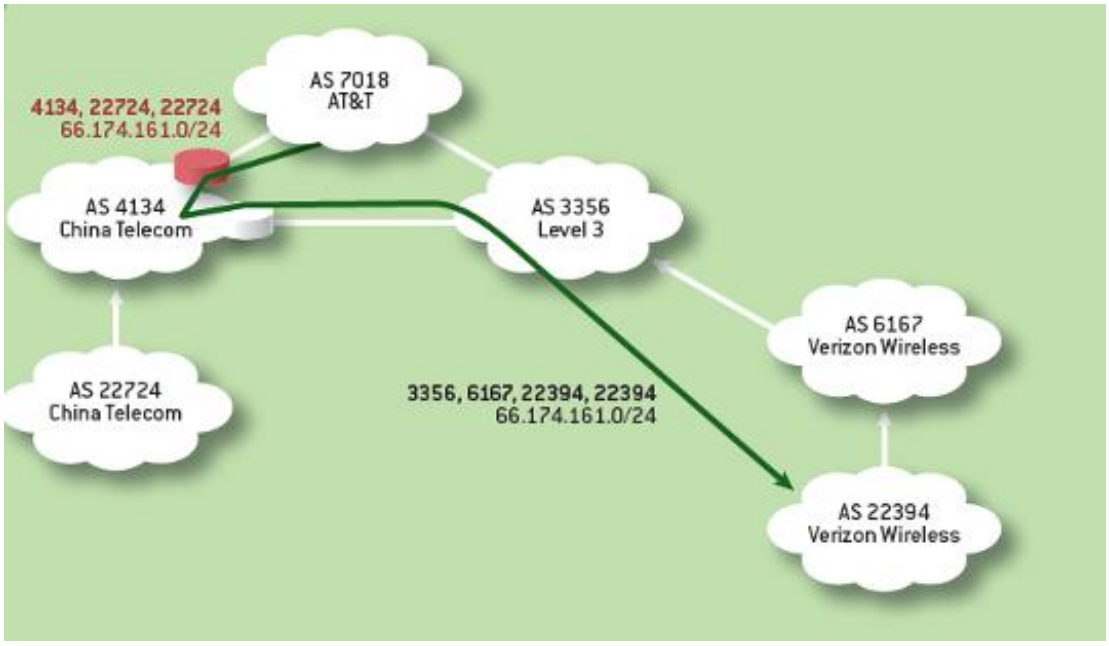
Incidentes de seguridad de enrutamiento GBP

Los incidentes de enrutamiento BGP pueden ser problemáticos por una variedad de razones. En algunos casos, simplemente interrumpen el flujo del tráfico legítimo de Internet, mientras que, en otros, pueden dar lugar a la desviación de las comunicaciones, lo que supone un riesgo para la seguridad por interceptación o manipulación. Los incidentes de enrutamiento ocurren con cierta regularidad y pueden variar mucho en el impacto operativo. (Mandory, 2023)

El 8 de abril de 2010, durante 18 minutos, China Telecom lanzó secuestros de prefijos para el 15 por ciento de los prefijos de Internet. Si bien no hay evidencia de que este incidente haya sido el resultado de algo más que una mala configuración, proporciona un ejemplo instructivo de un secuestro de prefijo clásico. La Figura 3 muestra uno de los secuestros AS 22724 de China Telecom secuestra el prefijo 66.174.161.0/24 de *Verizon Wireless*. La ruta falsa originada por AS 22724 se propaga a través del gráfico de nivel AS y eventualmente es seleccionada por *AT&T*

porque es más corta que la ruta legítima que se origina en AS 22394 de *Verizon Wireless*. Mientras tanto, *Level3* selecciona la ruta legítima porque es más corta que la ruta falsa. ruta. Por lo tanto, el tráfico de red se divide entre el AS secuestrador y el AS de origen legítimo, y la naturaleza de la división depende de las políticas de enrutamiento utilizadas por los AS individuales y la topología del gráfico de nivel de AS.

Figura 3. Secuestro de rutas de China



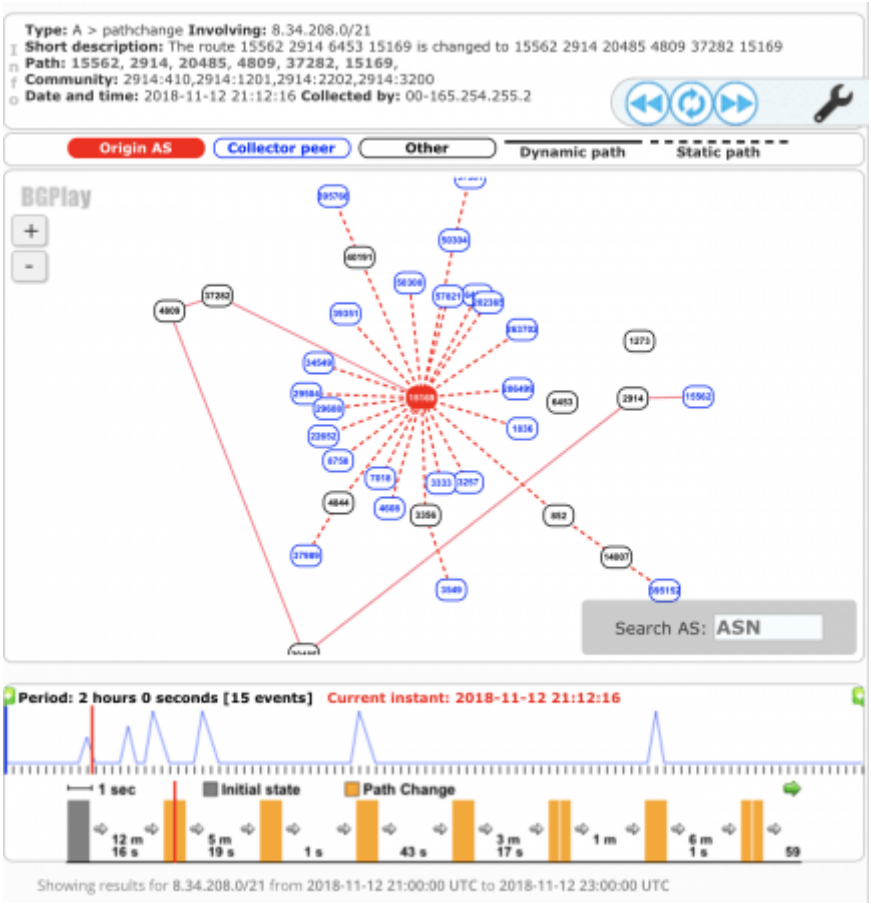
Fuente: tomada a partir de Goldberg (2023)

Para Siddiqui (2018) la fuga de ruta provoca una importante interrupción de Google, enfrentó una interrupción importante en muchas partes del mundo gracias a una fuga de BGP que muestra la Figura 4. Este incidente, causado por un ISP nigeriano, Mainone, ocurrió el 12 de noviembre de 2018 entre las 21.10 y las 22.35 UTC y fue identificado en tweets del servicio de monitoreo BGP *BGPMon*, así como del proveedor de monitoreo de *red Thousand Eyes*.

Para EHACKING (2018) *BGPmon* dice que el ISP de Nigeria anunció incorrectamente que alojaba 212 prefijos de la red de Google en cinco oleadas diferentes, por un total de 74 minutos. Este mal anuncio de enrutamiento se filtró hacia otros proveedores de servicios de Internet (ISP), lo que provocó que cada vez

más proveedores cercanos enviaran el tráfico destinado a Google a la red de *MainOne,* en lugar de las rutas BGP normales. Según los expertos de *ThousandEyes*, una compañía de seguridad en la nube, el camino que tomó este tráfico con mayor frecuencia fue uno a través de TransTelecom (AS 20485) en Rusia y China Telecom (AS 4809) en China.

Figura 4. Estadísticas de RIPE (Registro Regional de Internet para Europa)



Fuente: tomada a partir de Siddiqui (2018)

Para Madory (2019) en abril de 2010, China Telecom experimentó una fuga de enrutado que llamó mucho a la gente. China no secuestró el 15% del tráfico mundial durante 18 minutos, pero dejare una desacreditación más detallada de ese mito para otro momento. Mientras se analiza la filtración, nota algo peculiar. Cuando clasifica los aproximadamente 50.000 prefijos involucrados en la filtración basado en cuántas AS aceptaron las rutas filtradas, la mayor parte del impacto se limitó a las rutas chinas. Sin embargo, dos de las cinco principales rutas filtradas más propagadas (que se enumeran en la Tabla 1) eran rutas de los EE.UU. Había una

gran conspiración para interceptar el tráfico destinado a estas rutas, en realidad, se debió a algo mucho más preocupante: un *AS-PATH* gratuito antepuesto por la víctima.

Tabla 1. Rutas secuestradas de China Telecom

	Prefix	***Origin***	***Economy***	***Max Peer (%)***
1	202.100.192.0/19	4134	CN	97.05
2	202.100.224.0/19	4134	CN	96.46
3	12.4.196.0/22	12163	US	87.61
4	12.5.48.0/21	12163	US	87.61
5	59.42.0.0/16	4134	CN	87.02

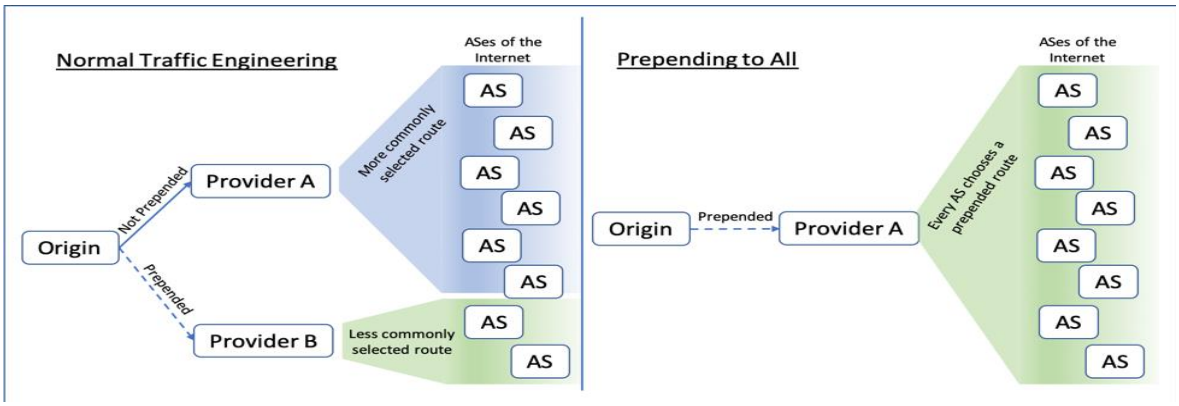
Fuente: tomada a partir de Madory (2019)

Durante la fuga de ruta, casi todos los AS de Internet prefirieron las rutas filtradas chinas para 12.5.48.0/21 y 12.4.196.0/22 porque, en ese momento, se anunciaban estos dos prefijos chinos a toda Internet a lo largo de la siguiente AS-PATH excesivamente *prepended AS-PATH*: 3257 7795 12163 12163 12163 12163 12163 12163 12163 12163 12163 12163 12163.

Con esta extraña configuración, prácticamente cualquier ruta ilegítima, ya sea un secuestro deliberado o una fuga inadvertida, sería preferida a través de la ruta legítima. Piensa en eso por un minuto. En este caso, la víctima está casi asegurando su victimización.

De acuerdo a Madory (2019) Uno pensaría que tales errores serían relativamente raros, especialmente ahora, casi 10 años después. Resulta que en este momento están sucediendo muchas cosas que se están *prepending* a todos Figura 5, y durante las filtraciones, no les va bien a quienes cometen este error.

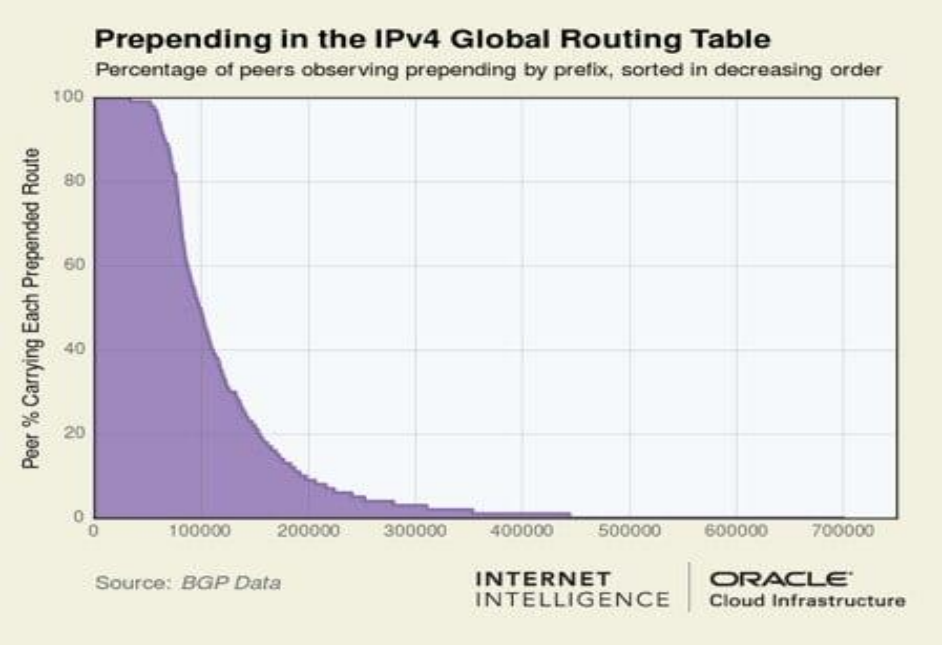
Figura 5. Ingeniería de tráfico normal *vs prepending* a todos.



Fuente: tomada a partir de Madory (2019)

Si bien se pueden debatir los méritos de *prepending o prepend* a un subconjunto de múltiples proveedores de transporte, es difícil ver la utilidad de *prepending* a cada proveedor. En esta configuración, el *prepending* ya no da forma a la propagación de la ruta. Simplemente está incentivando a los AS a elegir otro origen si uno apareciera repentinamente, ya sea por error o no. Entonces, cuántos prefijos en la tabla de enrutamiento global se anteponen a todos el número puede sorprenderle: de aproximadamente 750.000 rutas en la tabla de enrutamiento global IPv4, casi 60.000 rutas BGP se anteponen al 95 % o más de los cientos de fuentes BGP. Entonces, alrededor del 8% de la tabla de enrutamiento global o una de cada doce rutas BGP está configurada con anteposiciones para prácticamente todo Internet. Las 60.000 rutas incluyen entidades de todo tipo: gobiernos, instituciones financieras e incluso partes importantes de la infraestructura de Internet. La Figura 6 muestra el grado en que cada prefijo en las tablas de enrutamiento global IPv4 e IPv6 se antepone a otros AS de Internet. Se considera que al menos 100.000 prefijos IPv4 (13,3%) y más de 6.000 prefijos IPv6 (8,6%) preceden a más de la mitad de los pares. Sostiene que *prepending-to-all* es un riesgo autoinfligido e innecesario que sirve de poco. Aquellos que anteponen excesivamente sus rutas deben considerar este riesgo y ajustar su configuración de ruta.Madory (2019).

Figura 6. *Prepending* en las tablas de enrutamiento global IPv4 e IPv6.



Fuente: tomada a partir de Madory (2019)

Error de BGP Verizon provocó una falla catastrófica en cascada que destrozó a Cloudflare, Amazon, etc, como se aprecia en la Figura 7. Una pequeña empresa en el norte de Pensilvania se convirtió en un camino preferido de muchas rutas de Internet a través de Verizon (AS701), un importante proveedor de tránsito de Internet. Un proveedor de servicios de Internet en Pensilvania (AS33154 - DQE *Communications*) estaba utilizando un optimizador BGP en su red, lo que significaba que había muchas rutas más específicas en su red. Las rutas específicas prevalecen en rutas más generales (en la analogía de Waze, una ruta para, digamos, el Palacio de Buckingham es más específica que una ruta a Londres). DQE anunció estas rutas específicas a su cliente (AS396531 - *Allegheny Technologies* Inc).

Toda esta información fue enviada a su otro proveedor de tránsito (AS701 - Verizon), quien procedió a informar a toda Internet sobre estas rutas mejores. Estas rutas eran supuestamente mejor porque eran más granulares, más específicas. La fuga debería haberse detenido en Verizon. Sin embargo, contra las numerosas mejores prácticas descritas a continuación, la falta de filtrado de Verizon convirtió esto en un incidente importante que afectó a muchos servicios de Internet como

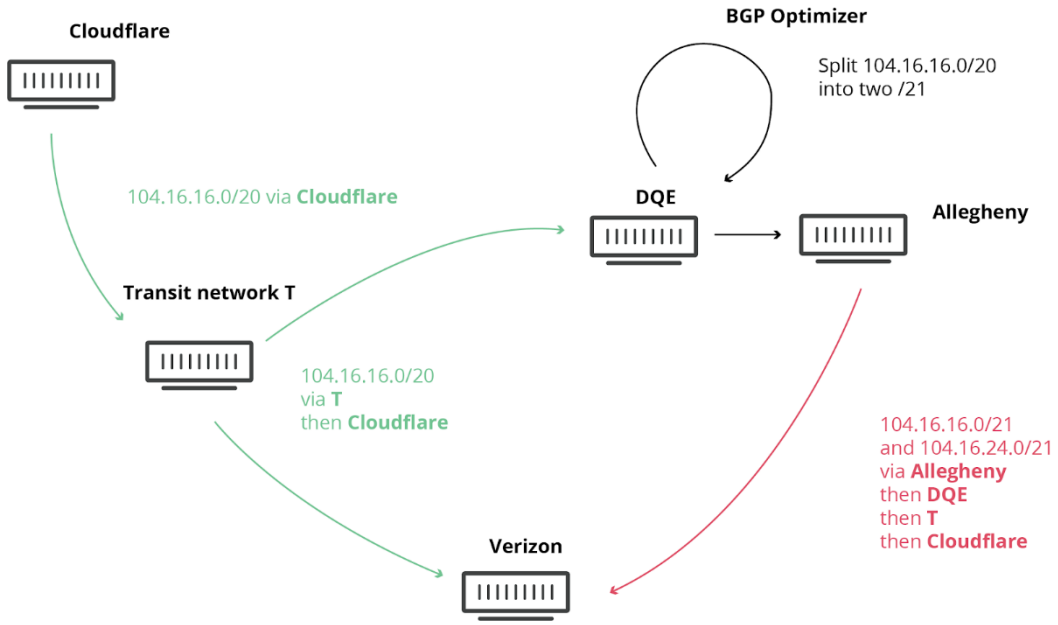
Amazon, Linode y Cloudflare. Lo que esto significa es que de repente Verizon, Allegheny y DQE tuvieron que lidiar con una estampida de usuarios de Internet tratando de acceder a esos servicios a través de su red. Ninguna de estas redes estaba adecuadamente equipada para hacer frente a este drástico aumento del tráfico, causando interrupciones en el servicio. Incluso si tenían suficiente capacidad DQE, Allegheny y Verizon no se les permitió decir que tenían la mejor ruta a Cloudflare, Amazon, Linode, etc. Strickx (2019)

Esos incidentes pueden ejercer mucha presión sobre la infraestructura y provocar caída de tráfico, proveer los medios para la inspección de tráfico o incluso usarse para realizar ataques de amplificación de servidores de nombres de dominio (DNS) o cualquier otro ataque de amplificación reflectiva.

Las prácticas recomendadas en la seguridad del enrutamiento ya están disponibles y se consideran muy efectivas en contra de estas formas de incidentes de enrutamiento. Tanto para las fugas de rutas como para las apropiaciones de ruta, los operadores de red pueden usar políticas de filtrado más sólidas y determinar cuándo es que las redes vecinas hacen anuncios perjudiciales. La validación de origen de una dirección IP puede usarse para encontrar tráfico falsificado a medida que entra o sale de una red. Después el tráfico falsificado puede filtrarse para evitar que llegue a su destino. Hay esfuerzos continuos por desarrollar herramientas aún más efectivas como la Validación del origen de la ruta (*Route Origin Validation, o ROV*) y fortalecer las existentes, como definir con más detalle una ruta viable en la tecnología *Unicast Reverse Path Forwarding* (uRPF).

Las Normas mutuamente acordadas para la seguridad del enrutamiento (*Mutually Agreed Norms for Routing Security,* o MANRS) son un conjunto de prácticas de referencia visibles para que los operadores de red mejoren la seguridad del sistema de enrutamiento global. (Seguridad de enrutamiento para legisladores, 2023).

Figura 7. Proceso de fuga de BGP.



Fuente: tomada a partir de Strickx (2019)

1.1. MANRS para proveedores de internet (ISP)

Los operadores de red tienen la responsabilidad colectiva de garantizar una infraestructura de enrutamiento robusta y segura a nivel mundial. La seguridad de su red depende de una infraestructura de enrutamiento que elimine a los malos actores y las configuraciones incorrectas accidentales que causan estragos en Internet. Cuantos más operadores de red trabajen juntos, menos incidentes habrá y menos daño podrán hacer.

Para *MANRS for Network Operators* (2023) el programa de Operadores de Red MANRS define los pasos mínimos que los operadores de red, como los proveedores de servicios de Internet, deben tomar para garantizar la seguridad y la resiliencia del sistema de enrutamiento global de Internet.

Acciones

Filtrado. Asegure la exactitud de sus propios anuncios y los de sus clientes a las redes adyacentes

***Anti-spoofing*.** Habilite la validación de direcciones de origen para al menos redes de clientes de código auxiliar de un solo hogar, sus propios usuarios finales e infraestructura

Coordinación. Mantenga la información de contacto actualizada y accesible a nivel mundial en bases de datos de enrutamiento comunes.

Información global. Publique sus datos para que otros puedan validarlos

Las dos primeras acciones (el filtrado y la *Anti-spoofing* de direcciones IP) abordan las causas raíz de los incidentes comunes de enrutamiento. Las siguientes dos (coordinación y validación global) ayudan a limitar el impacto de los incidentes y a disminuir la posibilidad de incidentes futuros.(*MANRS-primer-enterprises-es.pdf*, 2021).

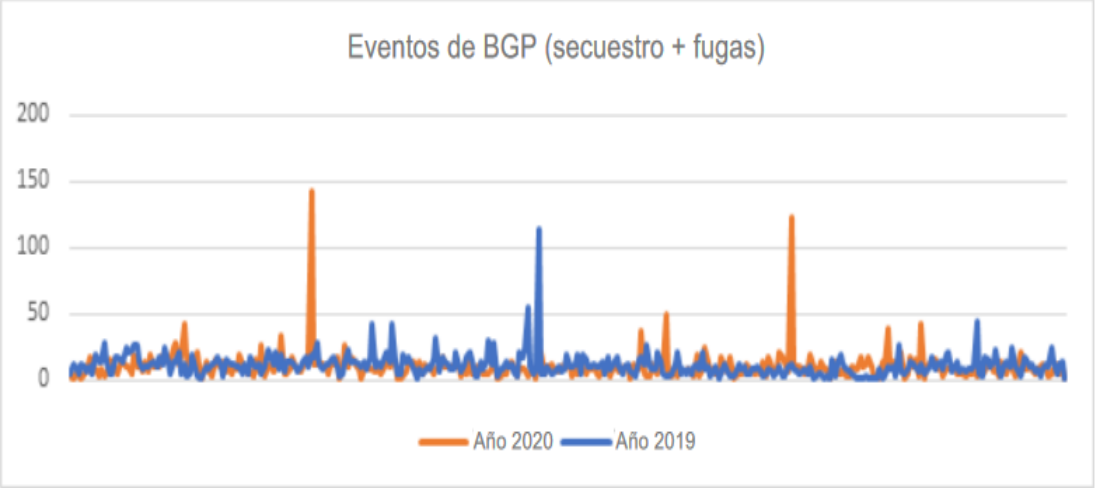
Para MANRS *MANRS-primer-enterprises-es.pdf (*s. f.) las empresas en 2020, hubo un total de 3,873 incidentes de red importantes que involucraron ataques relacionados con el protocolo *Border Gateway Protocol* (BGP) como muestra la Figura 8. De estos, el 64% fueron secuestros de ruta y el resto fueron fugas de ruta.

En 2019, hubo 4,232 incidentes importantes en la red que involucraron a BGP, de los cuales:

- El 3.8% de todas las redes fueron afectadas por un incidente de erutación
- El 2% de todas las redes fueron responsables de los 4,232 incidentes de seguridad de enrutamiento.

Estos incidentes pueden crear una tensión grave en la infraestructura, conllevar la caída del tráfico, permitir la inspección no autorizada del tráfico, ser utilizados para realizar ataques de denegación de servicio (DoS), que amenazan la continuidad comercial.

Figura 8. Eventos de BGP (secuestro + fugas).



Fuente: tomada a partir de *MANRS-primer-enterprises-es.pdf* (s. f.)

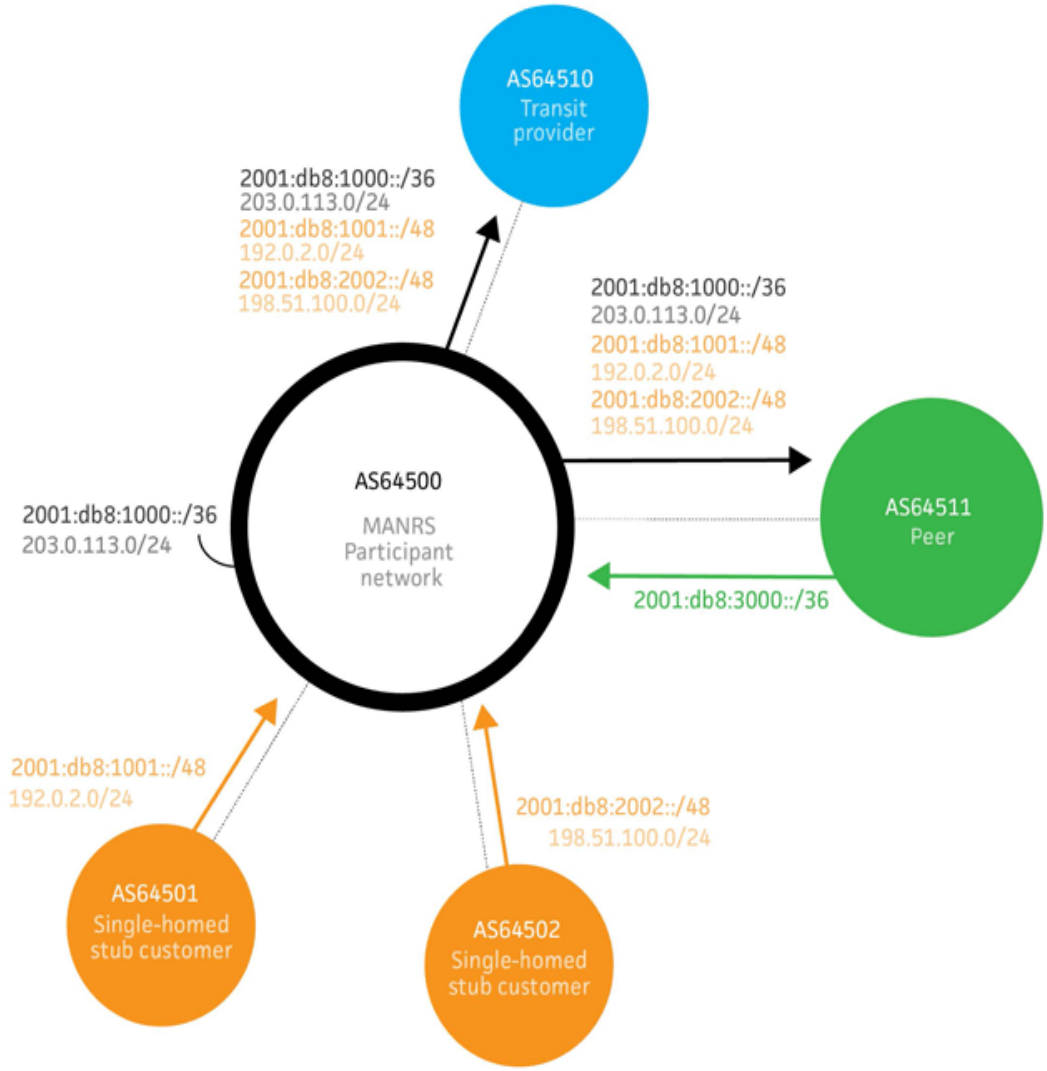
En julio de 2020, hubo dos incidentes de enrutamiento importantes en el sistema de enrutamiento global de BGP. Esto destacó la necesidad de que los operadores de redes implementen buenas prácticas de seguridad de enrutamiento. Estos incidentes afectaron a los principales proveedores de la red de América del Norte, incluidos TWC, *Rogers* y *Charter*, entre otros.

La única forma eficaz en que su empresa puede abordar las amenazas de seguridad de enrutamiento es eligiendo proveedores de servicios que sigan un conjunto establecido de pautas, como MANRS. Al elegir proveedores que adopten estas medidas, puede impulsar el mercado para construir redes más resistentes que, a su vez, hacen que la infraestructura de red global sea más segura. (*MANRS-primer-enterprises-es.pdf,* 2021).

Los operadores de red que estén de acuerdo con los principios e implementen las 4 acciones como mínimo pueden convertirse en participantes de MANRS. Esto le

da derecho a utilizar la insignia MANRS y aparecer en el sitio web de MANRS. La selección de las acciones es una evaluación del equilibrio entre los costes individuales pequeños e incrementales y el beneficio común potencial. Definen una línea base de seguridad mínima. Cualquier acción en particular no es una solución integral a los problemas esbozados. Para ejemplos de configuración, una topología simple, presentada en la Figura 9. (*MANRS-Network-Operators-Actions-v2.5.2.pdf,* 2021).

Figura 9. Topología de red simple.



Fuente: tomada a partir de MANRS-Network-Operators-Actions-v2.5.2.pdf (2021)

1.2. Observatorio de MANRS

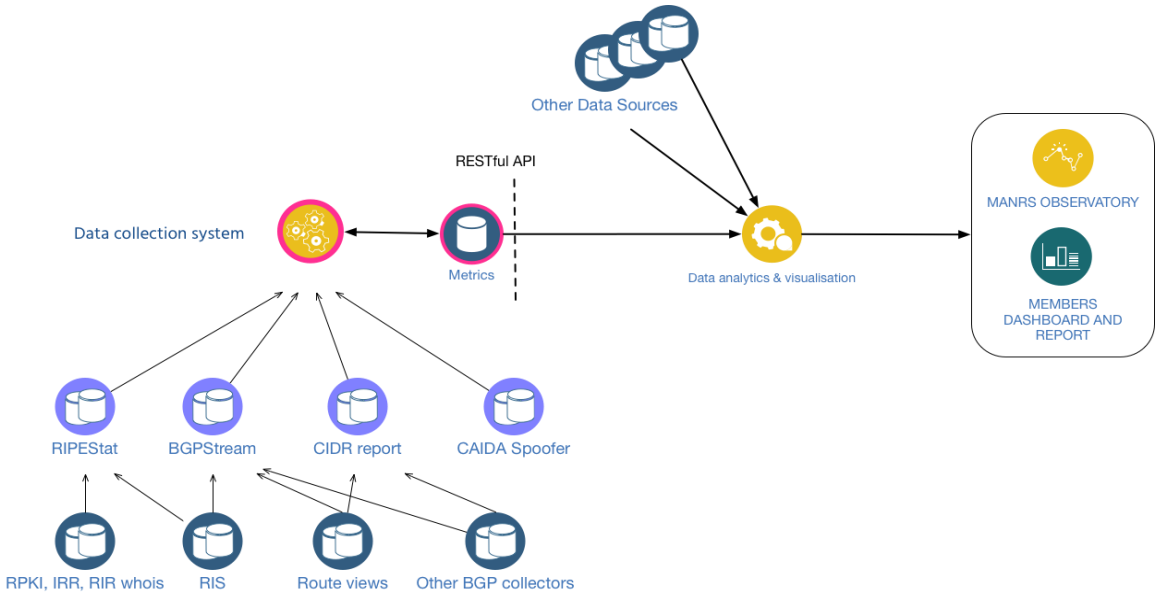
El Observatorio MANRS permite a sus miembros ver informes de incidencias detallados de las redes que operan. Por ejemplo, puedes ver qué prefijos no se han registrado todavía en el Registro de Enrutamiento de Internet (IRR, por sus siglas en inglés).A. (Robachevsky, 2020)

Para *MANRS Observatory* (2023) el Observatorio MANRS monitorea el estado de la seguridad del enrutamiento de Internet. Agrega datos para ayudar a los operadores de red a mejorar la seguridad de sus redes.

El Observatorio MANRS es una plataforma pública que:

- Mide el nivel de preparación MANRS de todas las redes que participan en el enrutamiento de Internet, lo que también sirve como indicación del estado de seguridad del enrutamiento.
- Presenta datos consolidados de seguridad de enrutamiento de varios socios (Figura 10) para regiones y economías específicas y realiza un seguimiento de su evolución a lo largo del tiempo.

Figura 10. Descripción general Observatorio MANRS



Fuente: tomada a partir de Observatorio MANRS. MANRS *Observatory* (2023)

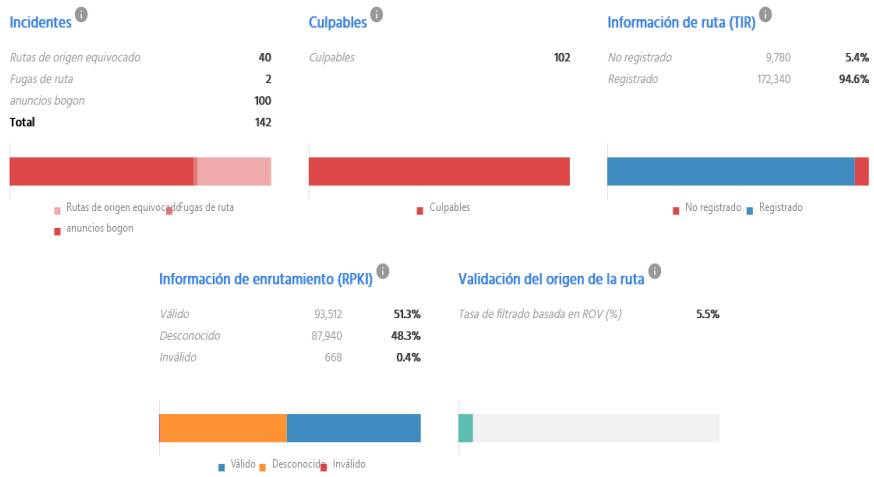
También se puede acceder a los datos recopilados a través de la API MANRS expone los datos recopilados por el proyecto MANRS (incluidos los datos proporcionados por el Observatorio MANRS), lo que ayuda a la integración y la automatización.

Los participantes de MANRS también pueden acceder a estadísticas e informes detallados para redes específicas a través del Panel de miembros. Los informes proporcionan una descripción histórica de una ASN miembro específica, según la acción MANRS, e información detallada relacionada con métricas específicas.

El estado de enrutamiento según observatorio de MANRS que muestra la figura 11 el número de incidentes y calidad de la informas de enrutamiento publicada en IRR y RPKI en la región y tiempos seleccionados.

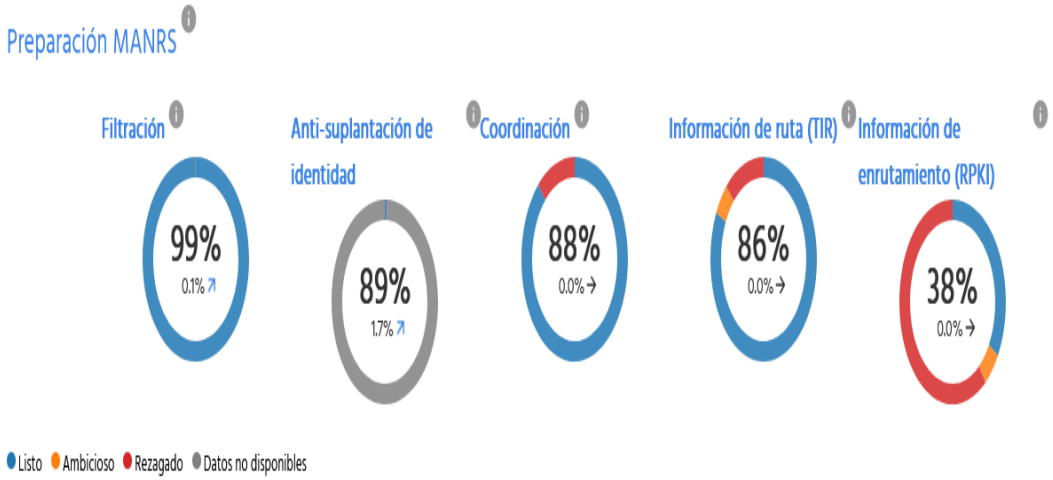
La preparación de MANRS indica un grado de qué tan bien se implementan las acciones de MANRS como muestra las Figuras 12 y 13. Se calcula utilizando un conjunto de métricas para cada Acción, calculadas a partir de diferentes fuentes de datos.

Figura 11. Estado de la seguridad del enrutamiento Lacnic diciembre 2023



Fuente: tomada a partir de Observatorio MANRS. MANRS *Observatory* (2023)

Figura 12. Preparación MANRS



Fuente: tomada a partir de MANRS *Observatory* (2023)

Figura 13. Vista global

Fuente: tomada a partir de MANRS *Observatory* (2023)

Para *MANRS-primer-enterprises-es.pdf* (s. f.) las acciones de MANRS definen los resultados en lugar de métodos específicos. Esto permite que la implementación cambie con la tecnología y ayuda a establecer las acciones de MANRS como mejores prácticas.

Junto con los incidentes de enrutamiento, MANRS busca abordar los desafíos del ecosistema en el sistema de enrutamiento global. MANRS mejora los incentivos económicos para la seguridad del enrutamiento al permitir que los operadores de redes demuestren su compromiso con:

- La seguridad: asegurando la infraestructura básica de Internet para una mayor seguridad global en Internet.
- Los clientes: asegurándose de que los servicios que brindan se adhieran a las mejores prácticas de seguridad de enrutamiento.
- La competencia: al garantizar que los incidentes de seguridad de enrutamiento no tengan un efecto en cascada sobre otros operadores de red.
- Personas formuladoras de políticas: asegurando una infraestructura nacional de Internet sólida y resiliente en apoyo de la agenda más amplia de la seguridad de Internet.

Un estudio independiente de 451 *Research*, encargado por *Internet Society*, descubrió que el enrutamiento, el secuestro y la interceptación del tráfico eran la principal preocupación de seguridad para las empresas. Los ataques de denegación de servicio distribuido (DDoS) y la suplantación de direcciones ocuparon el segundo lugar.

El 94% de las empresas dijeron que estaban dispuestas a pagar más por un proveedor que fuera participante de MANRS en una situación competitiva.

Esto destaca la importancia de la implementación de MANRS como indicador de las prácticas de seguridad sólidas de un operador de red.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de investigación

El presente proyecto de investigación adopta un enfoque metodológico deductivo, utilizando la técnica de C*hek List* evaluada por un especialista en el área de *networking*. La recolección de datos se centrará en la evidencia documental de los incidentes del enrutamiento BGP y como MANRS contribuye al aseguramiento del enrutamiento. Esto permitirá realizar un análisis exhaustivo que combina investigación de campo y revisión bibliográfica.

Enfoque metodológico de campo

De acuerdo a Arias, (2012) la investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información.

En el presente proyecto de investigación, se emplea un enfoque metodológico de campo centrado en la recolección directa de datos relacionados con el enrutamiento BGP implementado por el ISP, este enfoque proporcione recomendaciones específicas para mejorar las prácticas de seguridad de enrutamiento BGP, fortaleciendo así la seguridad y estabilidad de la red del ISP frente a amenazas de seguridad.

Método deductivo

Debido a que este trabajo se basa en la investigación de campo, se realizara un análisis exploratorio donde se abordara procesos, cambios y experiencias.

Técnica *Check List*

Se utilizará la técnica de *Check List* diseñada específicamente para evaluar el estado de seguridad del enrutamiento del ISP. Esta técnica será aplicada por un especialista en *networking,* con experiencia en normativas de seguridad y configuración de redes el formato de esta técnica se incorpora en el Anexo 1.

2.2. Metodología de desarrollo

De acuerdo a Oppenheimer (2011) esta metodología se basa en un diseño de *Top-Down*, haciendo referencia al modelo OSI; comienza desde las capas superiores, hasta las capas inferiores del modelo antes mencionado.

La metodología está enfocada para redes empresariales y empieza en las capas de aplicación, presentación, sesión y transporte antes que en las capas inferiores (red, enlace de datos, física) debido a que en estas capas se analizan: la situación actual de la red, los requerimientos, las limitaciones y su estructura lógica que se debe tomar en cuenta al momento del desarrollo de la metodología. (GUEVARA & QUIZHPI, 2017)

De acuerdo a Oppenheimer (2011) la metodología *Top-Down* para el diseño de redes incluye las siguientes fases:

- Fase I: Análisis de requerimientos
- Fase II: Diseño Lógico de red
- Fase III: Diseño Físico de red
- Fase IV: Probar, Optimizar y Documentar el diseño de la red

La iniciativa del presente trabajo nace de la comunidad de MANRS en la actualidad se ha visto muchos ataques y secuestros de rutas BGP por ende es primordial que los ISP brinden seguridad al navegar en internet.

Fase I. Análisis de requerimientos

En esta fase, los requerimientos para el desarrollo del trabajo son 4 acciones simples pero efectivas por parte de MANRS.

- Filtrado: Evitar la propagación de información incorrecta de enrutado incorrecto.
- *Anti-spoofing*: Evite el tráfico con direcciones IP de origen falsificadas.
- Coordinación: Facilitar la comunicación y coordinación operativa global entre los operadores de redes.
- Información global: Facilitar la validación de la información de enrutar a escala mundial.

En esta fase de análisis de requerimiento utilizare un *check list* por motivos de privacidad de los datos de la empresa se muestra en forma textual como muestra la Tabla 2 con la finalidad saber el estado actual del ISP basado en las 4 acciones de Normas Mutuamente Acordadas para la Seguridad del Enrutamiento **(**MANRS) en la seguridad de enrutamiento.

Tabla 2. CHECK LIST DE MANRS PARA ISP ESPECIALISTA

Fecha: 18/12/2023			
Nombre del especialista: Ing. Edison Euclides Segarra Guzmán, MSc.			
Acción 1: Prevenir la propagación de información incorrecta de enrutado			
Pregunta	**SI**	**NO**	**OBSERVACION**
¿El operador de red tiene un sistema para prevenir el anuncio de prefijos AS y/o IP que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red verifica los anuncios de sus clientes para asegurarse de que no estén anunciando prefijos que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red tiene un proceso para identificar y mitigar los anuncios incorrectos de enrutado?	**X**		Listas Bogons mediante BGP-Cymru- ACL

Acción 2: Evitar el tráfico con direcciones IP de origen falsificable			
¿El operador de red utiliza un sistema para validar las direcciones IP de origen?		**X**	
¿El operador de red prueba regularmente si su red es capaz de enviar paquetes con direcciones IP de fuente falsificada utilizando el software de CAIDA Spoofer para detectar posibles vulnerabilidades a ataques DDoS?		**X**	
Acción 3: Facilitar la comunicación y la coordinación operacionales mundiales			
¿La información de contacto del operador de red se encuentra actualizada en la base de datos RIR (o NIR) y/o en PeeringDB, y es accesible al menos a otros operadores de red registrados en PeeringDB?	**X**		
¿El operador de red documenta públicamente sus anuncios de enrutamiento previstos en el registro de enrutamiento RIR apropiado o en Routing Assets Database RADB?	**X**		
Acción 4: Facilitar la información de enrutamiento escala mundial			
¿El operador de red ha registrado todos los números AS y los prefijos IP que anuncia a otras redes en un IRR o RADB?	**X**		
¿El operador de red tiene ROA válidos para al menos el 90% de los prefijos IP o conjuntos de prefijos que están legítimamente autorizados a originar?	**X**		
¿El operador de red implementa RPKI como alternativa a la política de enrutamiento documentada públicamente para facilitar la información de enrutamiento a escala mundial?		**X**	

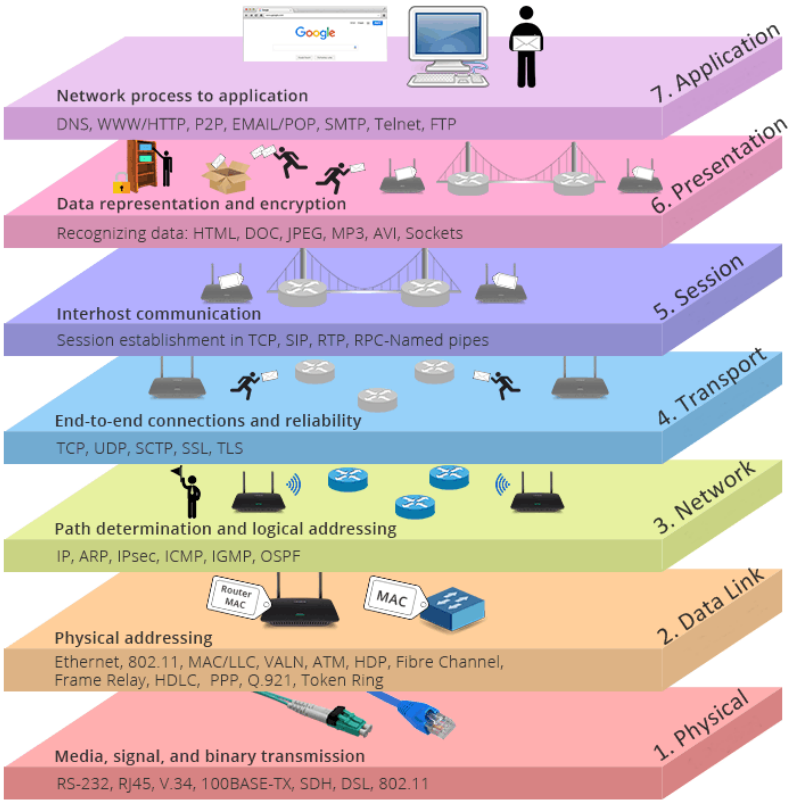
Fuente: elaboración propia

Fase II. Diseño lógico de red

Para Oppenheimer (2011) en esta fase trata de una topología lógica para el nuevo o red mejorada, direccionamiento de capa de red, denominación y programas de conmutación y enrutamiento, protocolos. El diseño lógico también incluye la utilización de MANRS.

El presente trabajo está enfocado en 4 acciones de MANRS por ende se enfoca a la capa de red basado en el modelo OSI, específicamente en la capa de red Figura 14.

Figura 14. Modelo OSI



Fuente: tomada partir de modelo OSI. *Protocolos de red básicos en la comprensión del modelo OSI* (2023).

Figura 15. Sesión BGP con Ufinet

```
FIBRA-RIO-B01-ZXR10#show bgp ipv4 unicast neighbor out 172.17.102.165
Routes Sent To This Neighbor:
Origin codes: i - IGP, e - EGP, ? - incomplete
Total number of routes: 10
Network          Next Hop        From           Metric LocPrf Path

45.188.232.0/24    172.17.102.166                          4.2600 i
45.188.233.0/24    172.17.102.166                          4.2600 i
45.188.234.0/24    172.17.102.166                          4.2600 i
45.188.235.0/24    172.17.102.166                          4.2600 i
168.194.148.0/24   172.17.102.166                          4.2600 i
168.194.149.0/24   172.17.102.166                          4.2600 i
168.194.150.0/24   172.17.102.166                          4.2600 i
170.238.0.0/22     172.17.102.166                          4.2600 4.2600 4.2600 i
190.52.192.0/20    172.17.102.166                          4.2600 i
200.107.248.0/21   172.17.102.166                          4.2600 i
```

Fuente: elaboración propia.

Figura 16. Sesión BGP con Telefónica

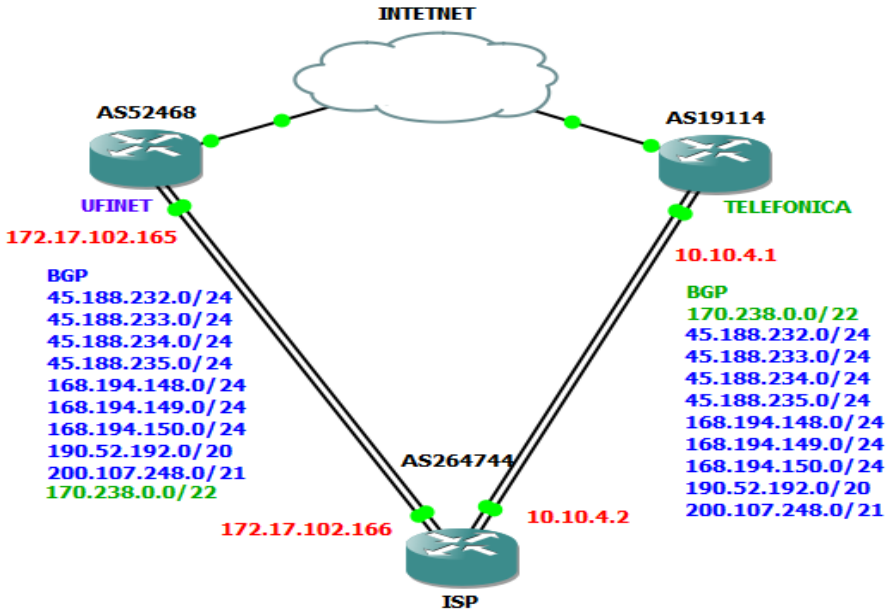
```
FIBRA-RIO-B01-ZXR10#show bgp ipv4 unicast neighbor out 10.10.4.1
Routes Sent To This Neighbor:
Origin codes: i - IGP, e - EGP, ? - incomplete
Total number of routes: 10
Network          Next Hop        From           Metric LocPrf Path

45.188.232.0/24    10.10.4.2                               4.2600 4.2600 4.2600 i
45.188.233.0/24    10.10.4.2                               4.2600 4.2600 4.2600 i
45.188.234.0/24    10.10.4.2                               4.2600 4.2600 4.2600 i
45.188.235.0/24    10.10.4.2                               4.2600 4.2600 4.2600 i
168.194.148.0/24   10.10.4.2                               4.2600 4.2600 4.2600 i
168.194.149.0/24   10.10.4.2                               4.2600 4.2600 4.2600 i
168.194.150.0/24   10.10.4.2                               4.2600 4.2600 4.2600 i
170.238.0.0/22     10.10.4.2                               4.2600 i
190.52.192.0/20    10.10.4.2                               4.2600 4.2600 4.2600 i
200.107.248.0/21   10.10.4.2                               4.2600 4.2600 4.2600 i
FIBRA-RIO-B01-ZXR10#
```

Fuente: elaboración propia

Se detalla una topología lógica basada en las sesiones BGP hacia los proveedores de internet Ufinet y Telefónica con los respectivos anuncios de prefijos como muestra la Figura 17.

Figura 17. Sesiones BGP con prefijos anunciados



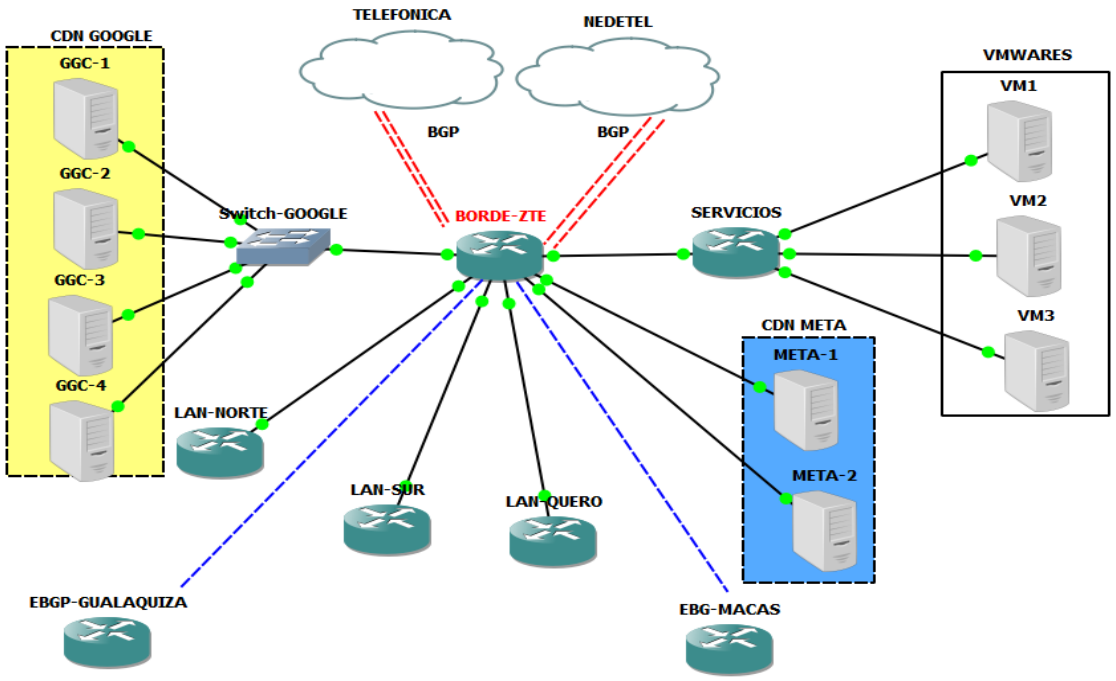
Fuente: elaboración propia

Fase III. Diseño físico de red

Para Oppenheimer (2011) durante la fase de diseño físico de red, tecnologías y productos específicos que realizan el log, se selecciona el diseño físico. El diseño de la red física comienza con la selección de tecnologías y dispositivos para redes de campus, incluidos cableado, *Ethernet switches*, acceso inalámbrico, y enrutadores.

El presente trabajo se enfoca en equipo enrutador de marca ZTE (Figura 19) mostrando la topología simple (Figura 18). El equito ZTE cumple el rol de enrutador que permite interconectar redes de área publica WAN con redes de área local LAN, todos los equipos de la red LAN y WAN están directamente conectados al equipo ZTE, localmente se tiene redes de entrega de contenido CDN de Google y Meta, 3 servidores locales.

Figura 18. Tipología simple del ISP



Fuente: elaboración propia

El equipo enrutador ZTE modelo ZXR10 M6000-5S, como se muestra en la Figura 19, está equipado con una configuración que soporta diversas conexiones. Cuenta con 30 puertos SFP que permiten conexiones tanto ópticas como eléctricas, junto con 10 puertos Ethernet, incluyendo 2 puertos de consola exclusivamente destinados para administración.

Figura 19. Enrutador ZTE ZXR10 M6000-5S.

Fuente: elaboración propia.

Entre los puertos especificados, los siguientes están conectados mediante cables de fibra óptica monomodo LC dúplex: xgei-0/1/0/1, xgei-0/1/0/12, xgei-0/1/0/7, xgei-0/2/0/7, xgei-0/2/0/8, xgei-0/2/0/9, xgei-0/2/0/10 y xgei-0/2/1/3. Por otro lado, los puertos xgei-0/1/0/5, xgei-0/1/0/6, xgei-0/1/0/8, xgei-0/1/0/9, xgei-0/1/0/10, xgei-0/2/0/1, xgei-0/2/0/3, xgei-0/2/0/5 y xgei-0/2/1/10 están conectados directamente a canales de fibra de 10Gb mediante módulos SFP+.

Esta disposición permite una versatilidad significativa en términos de conectividad y capacidad de transferencia de datos, adecuándose a las necesidades específicas de redes que requieren alta velocidad y fiabilidad en la transmisión de datos a través de conexiones ópticas y eléctricas.

Fase IV. Probar, Optimizar y Documentar el diseño de la red

Los pasos finales en el diseño de red de *Top-Down* es escribir e implementar un plan de prueba, construir un prototipo o piloto, optimizar el diseño de la red y documentar su trabajo con una propuesta de diseño de red. Si los resultados de su prueba indican algún problema de rendimiento, durante esta fase debe actualizar su diseño para incluir funciones de optimización como modelado del tráfico y mecanismos avanzados de conmutación y cola de enrutador. Oppenheimer (2011)

En esta fase se procede a ejecutar las 4 acciones dispuestas por MANRS.

Acción 1: Prevenir la propagación de información incorrecta de enrutado

El operador de red debe aplicar un sistema en el que solo anuncie a redes adyacentes los prefijos AS y los prefijos IP que ellos o sus clientes están legítimamente autorizados a originarse. El operador de red debe comprobar si los anuncios de sus clientes son correctos; específicamente, que cada cliente tiene legítimamente los números AS y el espacio de dirección IP que anuncian. *Network Operator Actions* (2023)

En el ISP, se implementa un sistema para evitar la difusión de información de enrutamiento incorrecta utilizando una lista de *bogons*, gestionada a través de sesiones BGP como se muestra en la Figura 20. *Team Cymru* es una organización especializada en la prevención del anuncio de rangos de direcciones AS (Sistema Autónomo) e IP que no están autorizados.

Figura 20. Sesiones BGP con CYMRU *Neighbor* 216.31.3.81 y 216.31.7.81

```
 neighbor 216.31.3.81 remote-as 65332
 neighbor 216.31.3.81 activate
 neighbor 216.31.3.81 description CYRUM 1
 neighbor 216.31.3.81 ebgp-multihop ttl 255
 neighbor 216.31.3.81 update-source loopback100
 neighbor 216.31.3.81 password encrypted HeWTQx0kKwlBpFMJsAgrusJjOH6IkKl2QK9G
HqmZZcl+bi+BPYaLqv/0XsjmdJ0s3bJK6vsjD1Lef17EDUK5R7O5s4UA=
 neighbor 216.31.3.81 route-map CYMRUBOGONS-V4 in
 neighbor 216.31.3.81 prefix-list cymru-out-v4 out
 neighbor 216.31.7.81 remote-as 65332
 neighbor 216.31.7.81 activate
 neighbor 216.31.7.81 description CYRUM 2
 neighbor 216.31.7.81 ebgp-multihop ttl 255
 neighbor 216.31.7.81 update-source loopback100
 neighbor 216.31.7.81 password encrypted HeWTQx0kKwlBpFMJsAgrusJjOH6IkKl2QK9G
HqmZZcl+bi+BPYaLqv/0XsjmdJ0s3bJK6vsjD1Lef17EDUK5R7O5s4UA=
 neighbor 216.31.7.81 route-map CYMRUBOGONS-V4 in
 neighbor 216.31.7.81 prefix-list cymru-out-v4 out
```

Fuente: elaboración propia.

El filtrado de *bogons* es parte esencial de las medidas de seguridad contra el spoofing, donde los operadores de red verifican los anuncios de sus clientes para asegurarse de que no estén difundiendo rangos de direcciones no autorizados. Además, el operador de red tiene procedimientos establecidos para identificar y mitigar cualquier anuncio erróneo de enrutamiento que pueda surgir.

Esta estrategia no solo protege la integridad de la red del ISP, sino que también garantiza que los recursos de direcciones IP se utilicen de manera legítima y segura, minimizando el riesgo de manipulaciones malintencionadas en el tráfico de Internet.

El equipo enrutador utilizado es el ZTE ZXR10 M6000-5S. Este dispositivo incorpora un sistema de no propagación de información incorrecta de enrutado mediante lista de *bogons*, gestionada a través de sesiones BGP como se muestra en la Figura 20 con *Neighbor* 216.31.3.81 y Figura 22 con *Neighbor* 216.31.7.81. Además, el ISP implementa filtrado de *bogons* como parte integral de su estrategia *anti-spoofing*. Este proceso implica la verificación de los anuncios de prefijos AS e IP por parte del operador de red para asegurarse de que no se estén anunciando prefijos no autorizados. El operador de red también tiene procedimientos

establecidos para identificar y mitigar cualquier anuncio incorrecto de enrutado que pueda surgir.

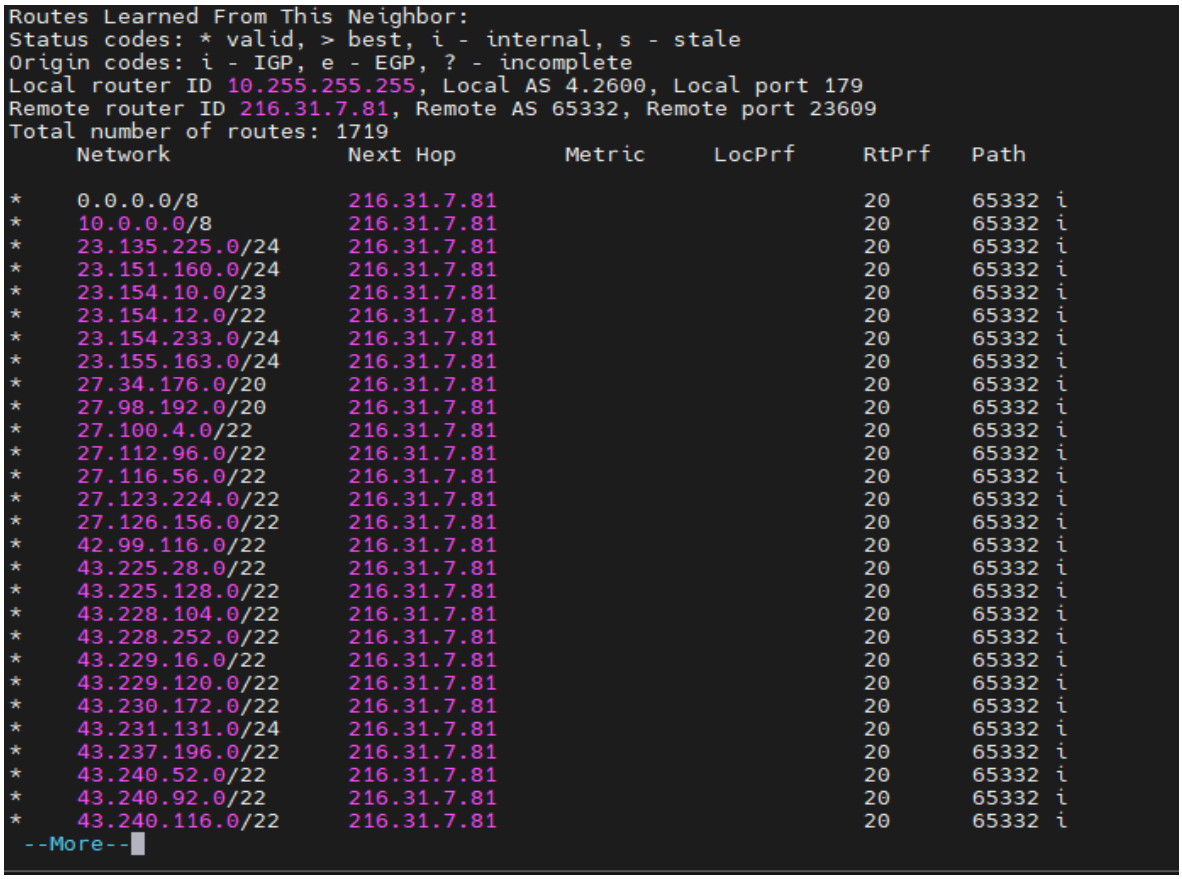
Figura 21. Lista de Bogons mediante BGP *neighbor* 216.31.3.81

```
Routes Learned From This Neighbor:
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Local router ID 10.255.255.255, Local AS 4.2600, Local port 179
Remote router ID 216.31.3.81, Remote AS 65332, Remote port 56891
Total number of routes: 1719
     Network             Next Hop        Metric     LocPrf     RtPrf   Path

*    0.0.0.0/8           216.31.3.81                           20      65332 i
*    10.0.0.0/8          216.31.3.81                           20      65332 i
*    23.135.225.0/24     216.31.3.81                           20      65332 i
*    23.151.160.0/24     216.31.3.81                           20      65332 i
*    23.154.10.0/23      216.31.3.81                           20      65332 i
*    23.154.12.0/22      216.31.3.81                           20      65332 i
*    23.154.233.0/24     216.31.3.81                           20      65332 i
*    23.155.163.0/24     216.31.3.81                           20      65332 i
*    27.34.176.0/20      216.31.3.81                           20      65332 i
*    27.98.192.0/20      216.31.3.81                           20      65332 i
*    27.100.4.0/22       216.31.3.81                           20      65332 i
*    27.112.96.0/22      216.31.3.81                           20      65332 i
*    27.116.56.0/22      216.31.3.81                           20      65332 i
*    27.123.224.0/22     216.31.3.81                           20      65332 i
*    27.126.156.0/22     216.31.3.81                           20      65332 i
*    42.99.116.0/22      216.31.3.81                           20      65332 i
*    43.225.28.0/22      216.31.3.81                           20      65332 i
*    43.225.128.0/22     216.31.3.81                           20      65332 i
*    43.228.104.0/22     216.31.3.81                           20      65332 i
*    43.228.252.0/22     216.31.3.81                           20      65332 i
*    43.229.16.0/22      216.31.3.81                           20      65332 i
*    43.229.120.0/22     216.31.3.81                           20      65332 i
*    43.230.172.0/22     216.31.3.81                           20      65332 i
*    43.231.131.0/24     216.31.3.81                           20      65332 i
*    43.237.196.0/22     216.31.3.81                           20      65332 i
*    43.240.52.0/22      216.31.3.81                           20      65332 i
*    43.240.92.0/22      216.31.3.81                           20      65332 i
*    43.240.116.0/22     216.31.3.81                           20      65332 i
 --More--
```

Fuente: elaboración propia.

Figura 22. Lista de Bogons mediante BGP *neighbor* 216.31.7.81



Fuente: elaboración propia.

Acción 2: Evitar el tráfico con direcciones IP de origen falsificadas. Filtración

Un operador de red debe implementar un sistema que permita la validación de la dirección de origen para su propia infraestructura y usuarios finales, y para cualquier red de clientes de *Stub* de un solo *Homed*. Esto debe incluir el filtrado anti-spoofing para evitar que los paquetes con una dirección IP de origen incorrecto entren o salgan de la red. Un operador de red debe probar si su red es capaz de enviar paquetes con direcciones IP de fuente falsificada utilizando el software de Centro de Análisis de Datos Aplicados de Internet CAIDA *Spoofer*. Esto es para alertar al operador de la red sobre si su red podría ser utilizada para originar ataques Distribuidos de Denegación de Servicios (DDos), al tiempo que se genera información de acceso público que permite que esa red sea verificada por otros. *Network Operator Actions* (2023)

De acuerdo a la organización CAIDA *CYMRU Bogon Reference Dataset* (2018) este conjunto de datos proporciona bogons diarios históricos, actuales y *fullbogons* compiladas por el *Team Cymru.* Los *bogons* son direcciones y bloques de red privados y reservados que la Autoridad de Números Asignados de Internet (IANA) no han asignado a un Registro Regional de Internet (RIR). Se encuentran comúnmente como direcciones de origen de ataques DDoS. Este conjunto de datos proporciona listas de bogon agregadas y no agregadas diarias que se actualizan a medida que se realizan asignaciones de IANA y reservas de prefijos especiales. Los *fullbogons* son un conjunto más grande que también incluye espacio IP que ha sido asignado a un RIR, pero que ese RIR no ha asignado a un ISP real u otro usuario final.

En el ISP, se ha implementado un sistema avanzado en el enrutador ZTE modelo ZXR10 M6000-5S para combatir el tráfico que utiliza direcciones IP de origen falsificado. Esto se logra mediante la integración del servicio de eliminación de tráfico no deseado (UTRS) de Team Cymru, utilizando una sesión BGP como se ilustra en la Figura 23 del sistema. Esta integración no solo refuerza la seguridad de la red, sino que también se convierte en una herramienta crucial para la mitigación proactiva de ataques de Denegación de Servicio Distribuido (DDoS). Al hacerlo, asegura la estabilidad y disponibilidad de los servicios para todos los clientes del ISP.

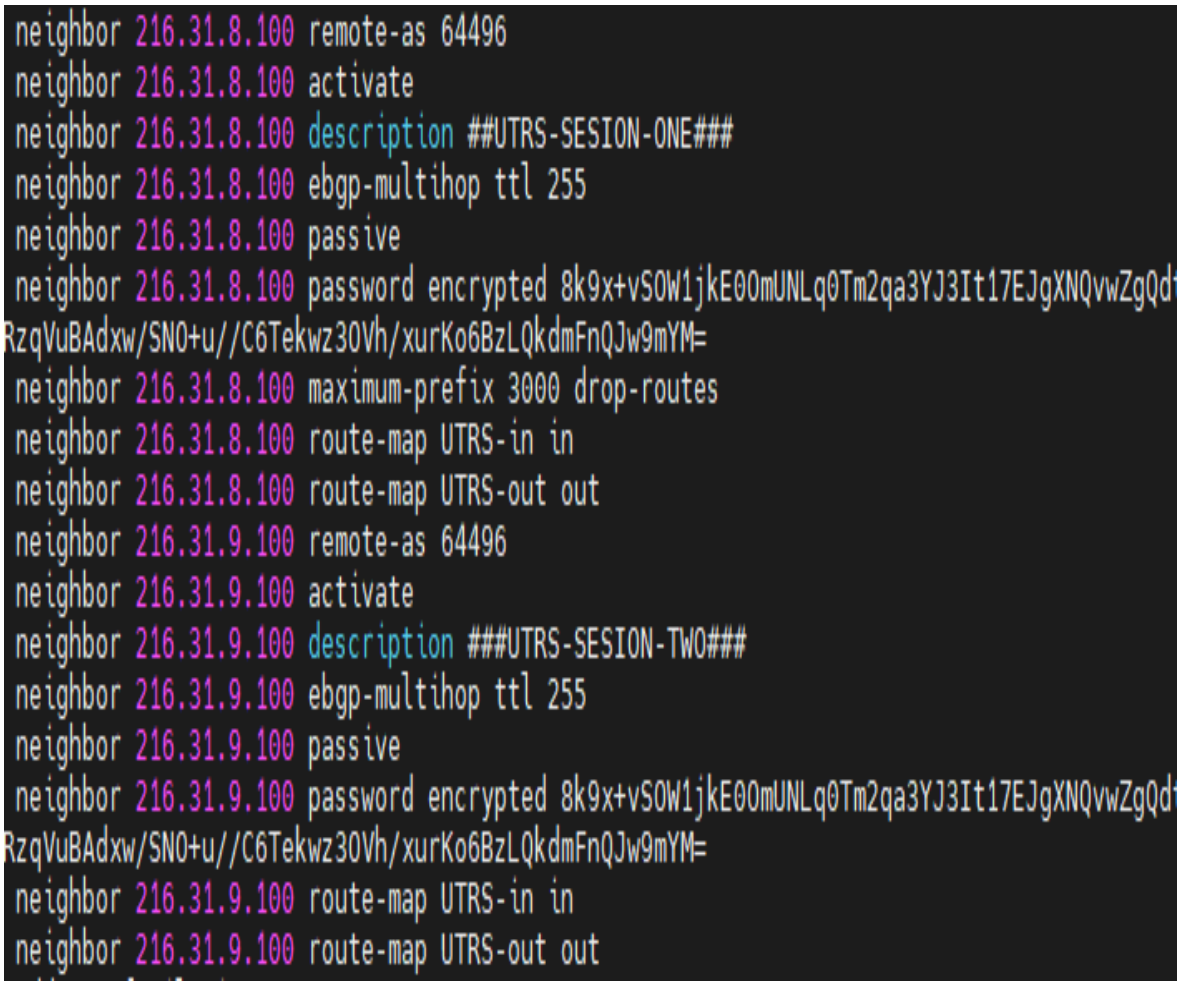
Además, se empleó técnicas como los agujeros negros activados a distancia (RTBH) a nivel mundial. Estas estrategias permiten bloquear selectivamente el tráfico malicioso antes de que afecte los sistemas, fortaleciendo así la postura de seguridad cibernética. Al participar en este enfoque colaborativo, no solo protege la infraestructura, sino que también contribuye a la protección general de Internet.

Para participar en el servicio basado en BGP alimentado por UTRS, es necesario completar el formulario disponible en la página oficial de *Team Cymru*, específicamente en la sección dedicada al UTRS, como se detalla en la Figura 24. Los datos requeridos incluyen información básica del solicitante, como nombre completo, correo electrónico corporativo, empresa, cargo, país, ASN (Número de

Sistema Autónomo) y las IPs para la sesión BGP. Además, el formulario incluye algunas preguntas adicionales para confirmar la elegibilidad y el propósito del uso del servicio.

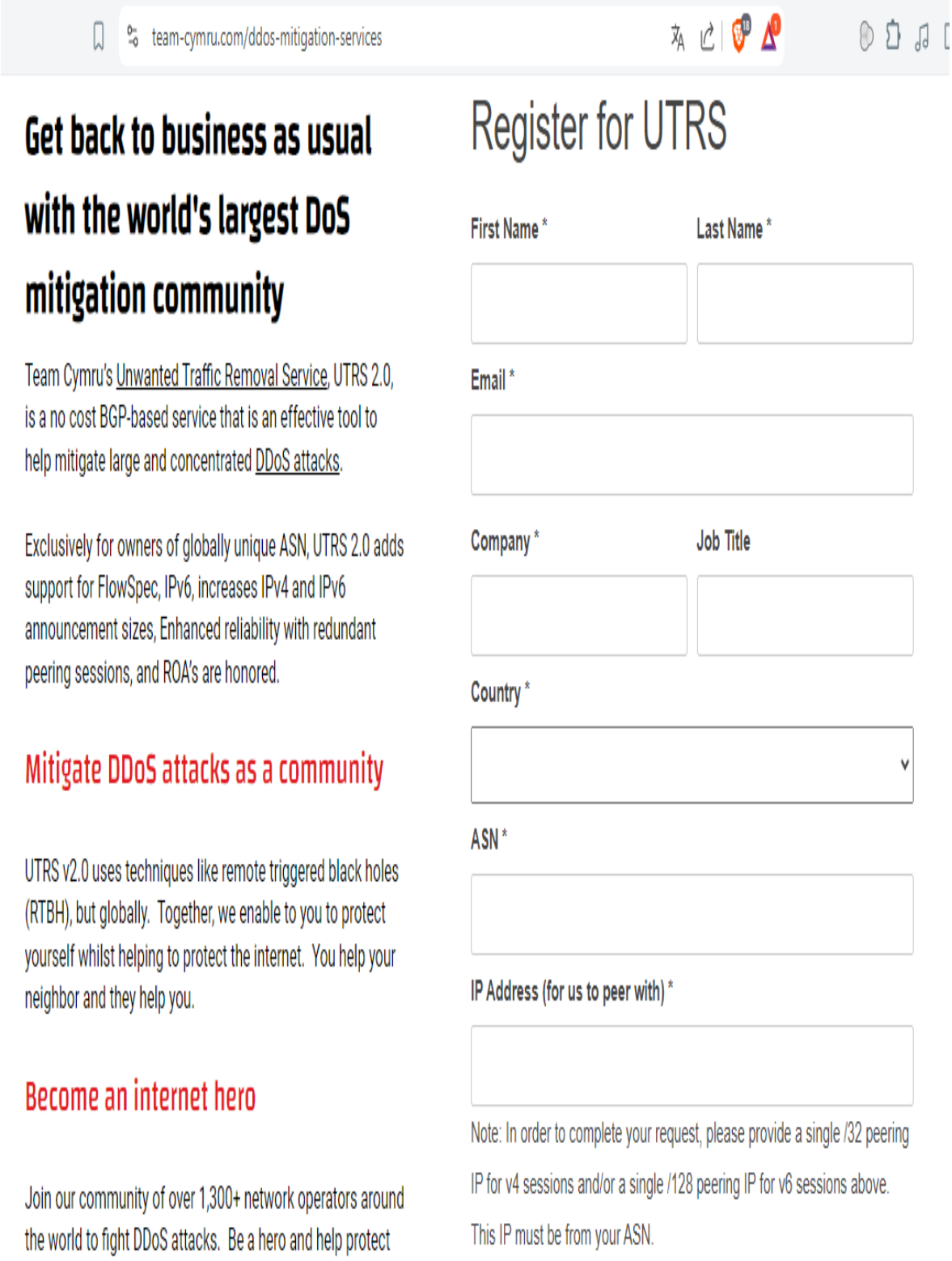
Este proceso asegura que todos los participantes proporcionen la información necesaria para configurar adecuadamente la sesión BGP y beneficiarse del servicio de eliminación de tráfico no deseado (UTRS), fortaleciendo así la seguridad y la integridad de la red del ISP.

Figura 23. Sesión BGP para mitigar ataques de DDoS



Fuente: elaboración propia

Figura 24. Registro de UTRS



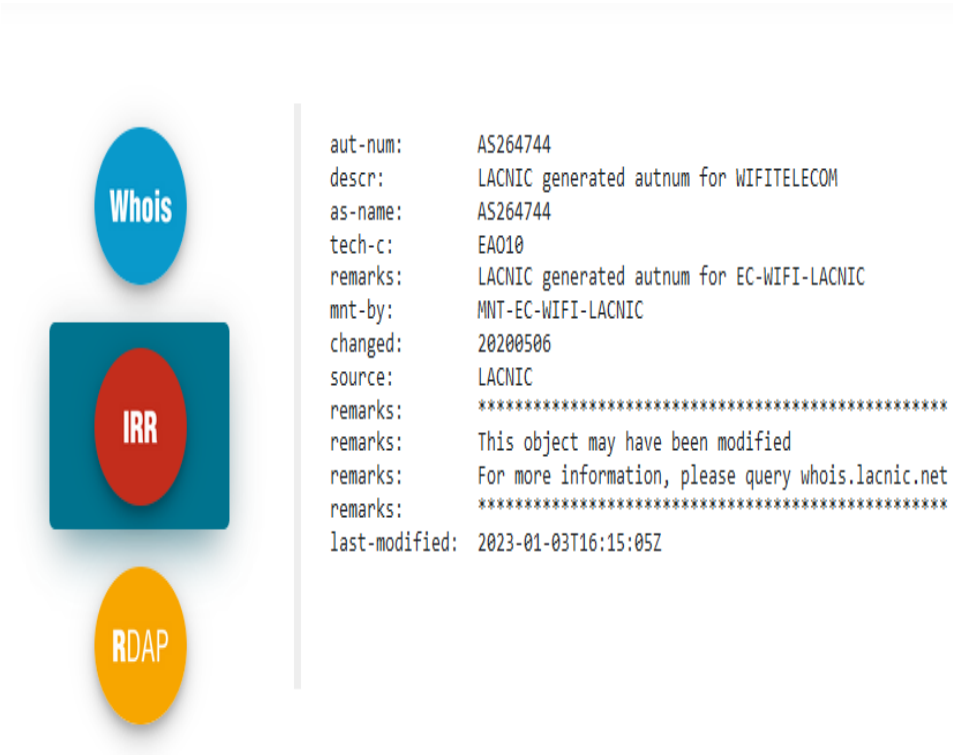
Fuente: tomada a partir de *Team Cymru* (2024)

Acción 3: Facilitar la comunicación y la coordinación operacionales mundiales

El operador de red debe asegurarse de que la información de contacto actualizada se introduce y mantiene en la base de datos RIR (o NIR) y/o en *PeeringDB*. Se recomienda encarecidamente que la información de contacto se haga pública, pero al mínimo estarán a disposición de otros operadores de la red registrados en PeeringDB. (*Network Operator Actions*, 2023)

El ISP cuenta con la comunicación y la coordinación operacionales mundiales a través del sistema de registro regional de internet RIR como es LACNIC para América Latina y partes de la región del caribe donde muestra la información del contacto del operador de red en la base de datos RIR y es accesible para otros operadores de red como se aprecia en la Figura 25.

Figura 25. Información IRR LACNIC



Fuente: tomada a partir de LACNIC (2023)

En la infraestructura del ISP, se ha implementado RPKI (*Resource Public Key Infrastructure*) mediante una máquina virtual basada en Debian 11. Esta máquina virtual está configurada con 1 CPU, 2 GB de RAM y 20 GB de almacenamiento. La implementación de RPKI permite al ISP validar y autenticar la información de enrutamiento mediante la asociación de recursos IP con sus propietarios legítimos.

Routinator 3000 es un software gratuito de código abierto desarrollado por *NLnet Labs* en el lenguaje de programación *Rust*. Es un validador de parte confiable de infraestructura de clave pública de recursos (RPKI) diseñado para ser seguro, portátil y liviano. El software se conecta a los anclajes de confianza de los cinco Registros Regionales de Internet (RIR): APNIC, AFRINIC, ARIN, LACNIC y RIPE NCC; descarga todos los certificados y ROA de varios repositorios, verifica las firmas y proporciona el resultado para su uso en BGP.

Esta implementación fortalece la seguridad y la integridad de la infraestructura de red del ISP al mitigar el riesgo de anuncios de enrutamiento maliciosos o incorrectos, proporcionando una capa adicional de protección contra posibles ataques de enrutamiento erróneo o manipulado.

Acción 4: Facilitar la información de encajar a escala mundial. IRR

Los operadores de redes deben documentar públicamente sus anuncios de enrutamiento previstos en el registro de enrutamientoRIR apropiado, *Routing Assets Database* RADB. Esto incluye los prefijos AS y los prefijos IP originarios de sus propias redes, así como las redes para las que prestan servicios de tránsito. Un operador de red puede aplicar alternativamente la acción 4: Facilitar la información de enrutamiento a escala mundial. RPKI Figura 26 en lugar de una política de enrutamiento documentada públicamente. (*Network Operator Actions*, 2023).

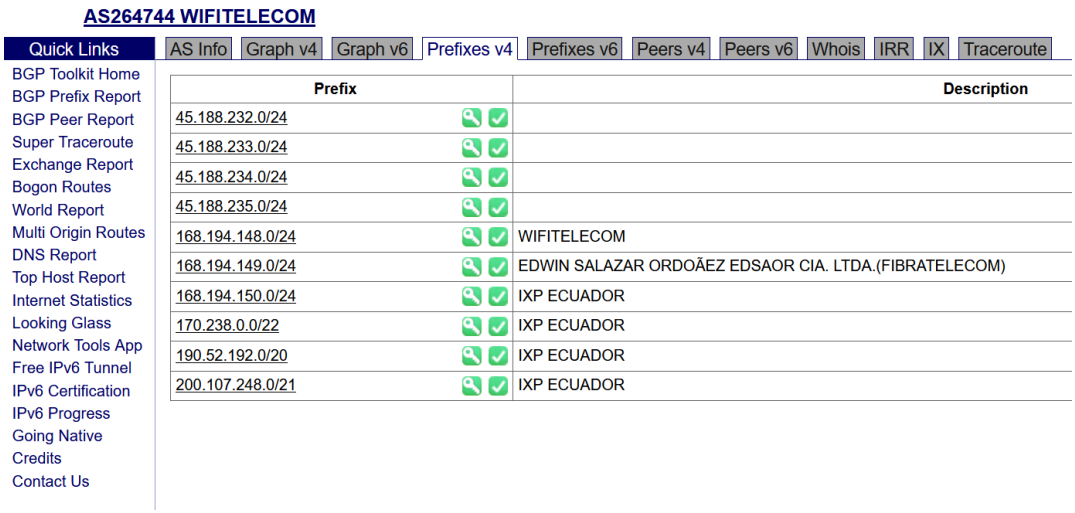
Figura 26. RPKI Validador

Prefijo	AS de Origen	Clasificación
168.194.148.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
168.194.149.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
168.194.150.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
170.238.0.0/22	ASN 264744 - WIFITELECOM	RPKI-valid
190.52.192.0/20	ASN 264744 - WIFITELECOM	RPKI-valid
200.107.248.0/21	ASN 264744 - WIFITELECOM	RPKI-valid
45.188.232.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
45.188.233.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
2803:3f60::/32	ASN 264744 - WIFITELECOM	RPKI-valid
2803:b4c0::/32	ASN 264744 - WIFITELECOM	RPKI-valid
45.188.234.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
2803:af40::/32	ASN 264744 - WIFITELECOM	RPKI-valid
168.194.148.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
168.194.149.0/24	ASN 264744 - WIFITELECOM	RPKI-valid
168.194.150.0/24	ASN 264744 - WIFITELECOM	RPKI-valid

Fuente: tomada a partir de Monitoreo FORT (2024)

El ISP facilita la documentación de la información de enrutamiento a escala mundial (Figura 27) donde el operador de red ha registrado todos los números de AS y los prefijos de IP que anuncia a otras redes en un IRR en este caso es LACNIC.

Figura 27. Información de prefijos



AS264744 WIFITELECOM

Quick Links | AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX | Traceroute

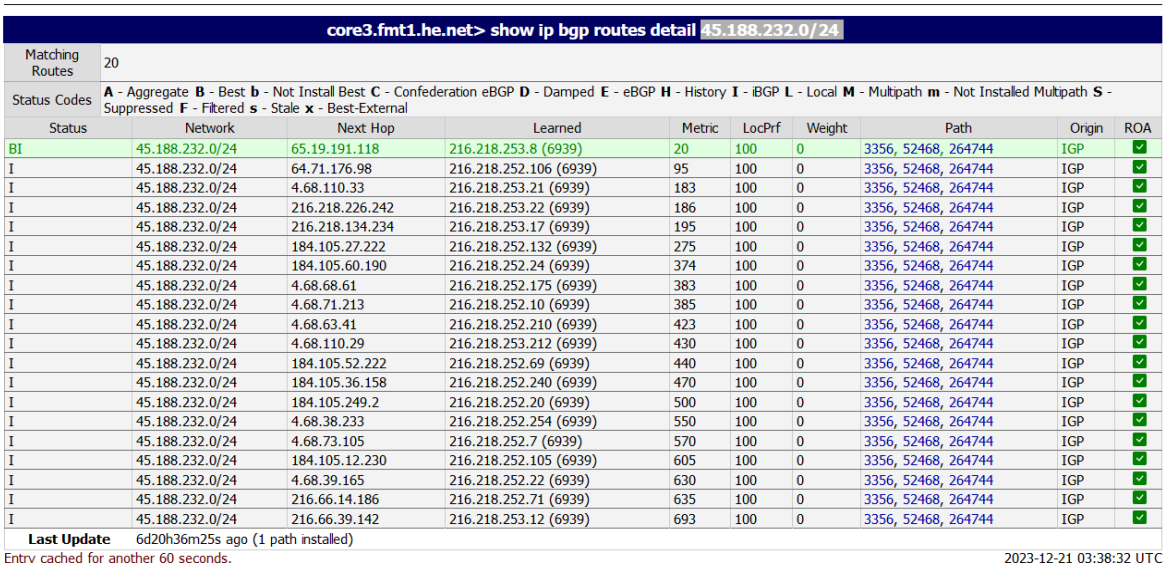
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Credits
Contact Us

Prefix	Description
45.188.232.0/24	
45.188.233.0/24	
45.188.234.0/24	
45.188.235.0/24	
168.194.148.0/24	WIFITELECOM
168.194.149.0/24	EDWIN SALAZAR ORDOÃEZ EDSAOR CIA. LTDA.(FIBRATELECOM)
168.194.150.0/24	IXP ECUADOR
170.238.0.0/22	IXP ECUADOR
190.52.192.0/20	IXP ECUADOR
200.107.248.0/21	IXP ECUADOR

Fuente: tomada a partir de Hurricane Electric (2023)

El ISP tiene ROA válidos para al menos el 90% de los prefijos IP o conjuntos de prefijos que están legítimamente autorizados a originarse se tomara cómo muestra el prefijo 45.188.232.0/24 que muestra la Figura 28.

Figura 28. Información de ROA *Looking Glass*



core3.fmt1.he.net> show ip bgp routes detail 45.188.232.0/24

Matching Routes: 20

Status Codes: **A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale **x** - Best-External

Status	Network	Next Hop	Learned	Metric	LocPrf	Weight	Path	Origin	ROA
BI	45.188.232.0/24	65.19.191.118	216.218.253.8 (6939)	20	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	64.71.176.98	216.218.252.106 (6939)	95	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.110.33	216.218.253.21 (6939)	183	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	216.218.226.242	216.218.253.22 (6939)	186	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	216.218.134.234	216.218.253.17 (6939)	195	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.27.222	216.218.252.132 (6939)	275	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.60.190	216.218.252.24 (6939)	374	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.68.61	216.218.252.175 (6939)	383	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.71.213	216.218.252.10 (6939)	385	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.63.41	216.218.252.210 (6939)	423	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.110.29	216.218.253.212 (6939)	430	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.52.222	216.218.252.69 (6939)	440	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.36.158	216.218.252.240 (6939)	470	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.249.2	216.218.252.20 (6939)	500	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.38.233	216.218.252.254 (6939)	550	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.73.105	216.218.252.7 (6939)	570	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	184.105.12.230	216.218.252.105 (6939)	605	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	4.68.39.165	216.218.252.22 (6939)	630	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	216.66.14.186	216.218.252.71 (6939)	635	100	0	3356, 52468, 264744	IGP	✓
I	45.188.232.0/24	216.66.39.142	216.218.253.12 (6939)	693	100	0	3356, 52468, 264744	IGP	✓

Last Update 6d20h36m25s ago (1 path installed)

Entry cached for another 60 seconds.

2023-12-21 03:38:32 UTC

Fuente: tomada a partir de Hurricane Electric (2023)

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

En este capítulo dedicado al análisis y validación de resultados, se llevó a cabo un análisis detallado de las acciones de MANRS implementadas en el enrutador. Esto incluye la configuración de políticas específicas y filtros diseñados para fortalecer la seguridad y la confiabilidad del enrutamiento en la red.

3.1. Acciones de MANRS implementadas en el enrutador

A continuación, se describe el análisis previo realizado antes de la implementación de estas medidas técnicas:

Filtro

Se analiza los ACLs existentes que permite únicamente los anuncios de rutas que sean legítimos y autorizados, provenientes de clientes y operadores de red verificados que se muestra en las Figuras 29 y 30. Esto asegura que solo la información de enrutamiento autorizada se propague dentro de la red.

En la figura 29, el ACL para la gestión del CPE (Equipo de Borde de Cliente) representa la configuración de reglas específicas en el enrutador. Estas reglas definen qué tipo de tráfico puede entrar o salir del equipo, según las políticas de seguridad y gestión de red establecidas por el ISP.

La figura 30 muestra un ACL CGNAT, el cual es una lista de control de acceso utilizada en el contexto de la traducción de direcciones de red. Esta lista establece las reglas que determinan cómo se traducen las direcciones IP y los puertos de los paquetes que pasan a través de un dispositivo CGNAT.

Figura 29. ACL de gestión CPE (Equipo de Borde de Cliente)

```
$
ipv4-access-list GESTION_CPE
  rule 10 permit ip 172.20.68.0 0.0.0.255 10.32.0.0 0.0.255.255
  rule 20 permit ip 10.32.0.0 0.0.255.255 172.20.68.0 0.0.0.255
  rule 30 permit ip 168.194.149.195 0.0.0.0 10.32.0.0 0.0.255.255
  rule 40 permit ip 10.32.0.0 0.0.255.255 168.194.149.195 0.0.0.0
  rule 50 permit ip 168.194.149.195 0.0.0.0 10.30.0.0 0.0.255.255
  rule 60 permit ip 10.30.0.0 0.0.255.255 168.194.149.195 0.0.0.0
  rule 70 permit ip 168.194.149.195 0.0.0.0 10.70.0.0 0.0.255.255
  rule 80 permit ip 10.70.0.0 0.0.255.255 168.194.149.195 0.0.0.0
  rule 90 permit ip 168.194.149.195 0.0.0.0 10.31.0.0 0.0.255.255
  rule 100 permit ip 10.31.0.0 0.0.255.255 168.194.149.195 0.0.0.0
  rule 110 permit ip 45.188.234.255 0.0.0.0 10.32.0.0 0.0.255.255
  rule 120 permit ip 10.32.0.0 0.0.255.255 45.188.234.255 0.0.0.0
```

Fuente: elaboración propia

Figura 29. ACL CGNAT (*Access Control List Carrier-Grade NAT*) Macas, Norte-1, Norte-2, Norte-3 y Quero.

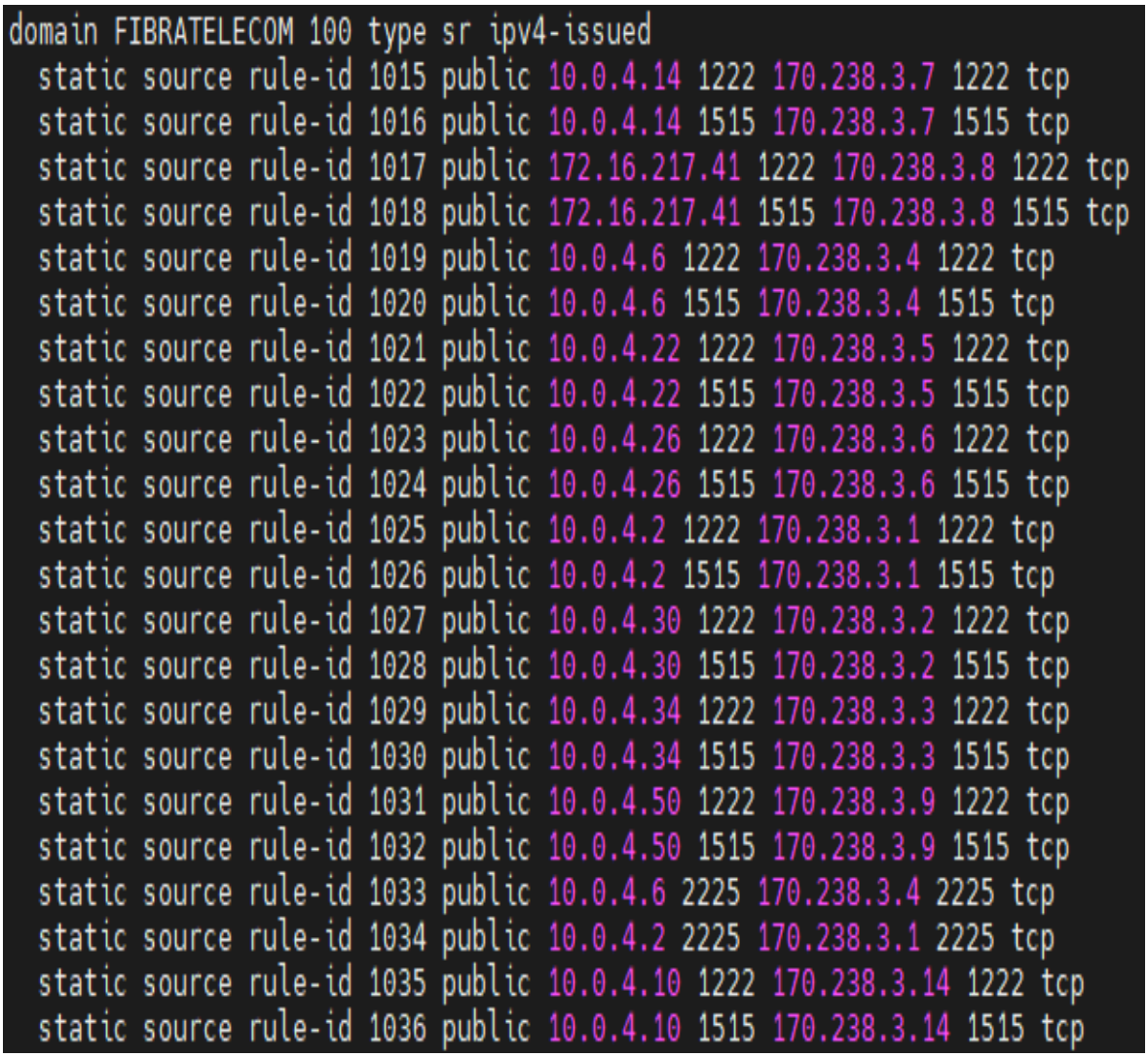
```
ipv4-access-list NAT-MACAS
  rule 10 permit 10.70.0.0 0.0.255.255
$
ipv4-access-list NAT-NORTE-1
  rule 10 permit 10.30.32.0 0.0.3.255
  rule 20 permit 10.30.36.0 0.0.3.255
  rule 30 permit 10.30.40.0 0.0.3.255
  rule 40 permit 10.30.44.0 0.0.3.255
  rule 50 permit 10.30.48.0 0.0.3.255
  rule 60 permit 10.30.52.0 0.0.3.255
  rule 70 permit 10.30.56.0 0.0.3.255
$
ipv4-access-list NAT-NORTE-2
  rule 10 permit 10.30.0.0 0.0.3.255
  rule 20 permit 10.30.4.0 0.0.3.255
  rule 30 permit 10.30.8.0 0.0.3.255
$
ipv4-access-list NAT-NORTE-3
  rule 10 permit 10.30.12.0 0.0.3.255
  rule 20 permit 10.30.16.0 0.0.3.255
  rule 30 permit 10.30.20.0 0.0.3.255
  rule 40 permit 10.30.24.0 0.0.3.255
  rule 50 permit 10.30.28.0 0.0.3.255
$
ipv4-access-list NAT-QUERO
  rule 10 permit 10.32.0.0 0.0.255.255
$
```

Fuente: elaboración propia

Se han implementado nuevos ACLs que bloquean todo el tráfico externo, permitiendo únicamente el acceso desde direcciones IP específicas a través de puertos específicos Figura 30.

Estos ACLs están configurados para proporcionar un control detallado sobre qué direcciones IP externas pueden establecer comunicación con direcciones IP internas mediante puertos específicos. Esta medida fortalece la seguridad de la infraestructura al restringir el acceso solo a conexiones que sean esenciales y autorizadas, reduciendo así posibles riesgos de seguridad.

Figura 30. Implementación de ACLs



Fuente: elaboración propia

Según el análisis realizado, se identificó que el ISP carecía de una herramienta como RPKI para validar la autenticidad de los prefijos de direcciones IP. Para abordar esta deficiencia, se implementó RPKI (*Infrastructure Public Key Infrastructure*) en la infraestructura del ISP mediante una máquina virtual basada en Debian 11. Esta máquina virtual está configurada con 1 CPU, 2 GB de RAM y 20 GB de almacenamiento. La implementación de RPKI permite al ISP verificar y autenticar la información de enrutamiento mediante la asociación de recursos IP con sus propietarios legítimos.

Routinator 3000 es un software gratuito y de código abierto desarrollado por *NLnet Labs* en el lenguaje de programación Rust. Se trata de un validador confiable de la infraestructura de clave pública de recursos (RPKI), diseñado para ser seguro, portátil y liviano. El software se conecta a los anclajes de confianza de los cinco Registros Regionales de Internet (RIR): APNIC, AFRINIC, ARIN, LACNIC y RIPE NCC. Descarga todos los certificados y ROA (*Route Origin Authorization*) de varios repositorios, verifica las firmas y proporciona el resultado para su uso en BGP.

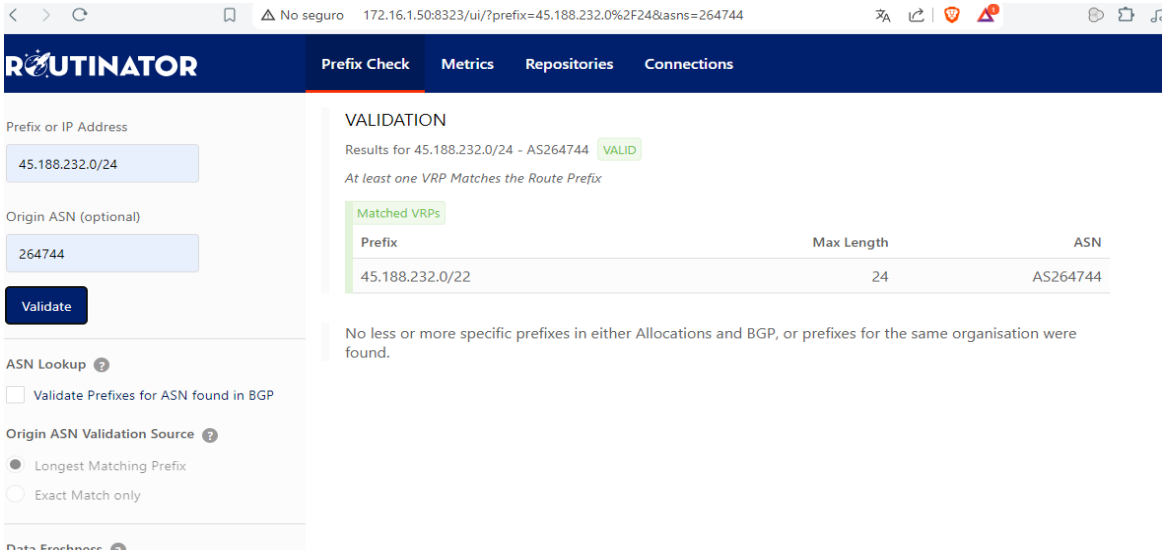
El proceso de implementación del sistema se llevó a cabo mediante la instalación y configuración de software especializado en una máquina virtual que opera con Debian 11. Este entorno fue cuidadosamente preparado para garantizar un funcionamiento óptimo y seguro. Durante esta fase, se realizaron configuraciones específicas para establecer relaciones de confianza entre los diferentes componentes del sistema. Esto fue fundamental para validar los anuncios de prefijos de IP, utilizando certificados y firmas digitales.

La utilización de estos mecanismos de seguridad es crucial, permite verificar que los anuncios de enrutamiento provengan exclusivamente de fuentes autorizadas y legítimas. Esta medida no solo fortalece la integridad de la red, sino que también previene posibles ataques o suplantaciones de identidad que podrían comprometer el funcionamiento del sistema.

A continuación, en la Figura 31, se ilustra el proceso de validación y las configuraciones implementadas, evidenciando cómo se logró establecer un entorno seguro y confiable.

La implementación garantiza que el sistema no solo cumpla con los requisitos operativos, sino que también se alinee con las mejores prácticas de seguridad en el ámbito del enrutamiento de IP. La combinación de software especializado, configuraciones precisas y mecanismos de validación robustos son esenciales para asegurar un desempeño eficaz y protegido de la red.

Figura 31. Información RPKI Routinator 3000.



Fuente: elaboración propia

Anti-spoofing

Según el análisis realizado, la prevención de *anti-spoofing* implica evitar que paquetes con direcciones de origen falsificadas, que no pertenecen a la red interna, puedan ingresar o salir de la red. Actualmente, no se ha implementado en el enrutador un sistema para verificar la autenticidad de las direcciones IP de origen que salen de la red, lo cual es crucial para proteger contra posibles ataques de *spoofing* perpetrados por agentes externos.

En respuesta a esta necesidad, en el ISP se implementó un sistema avanzado en el enrutador ZTE modelo ZXR10 M6000-5S para combatir el tráfico que utiliza direcciones IP de origen falsificado. Esto se logra mediante la integración del servicio de eliminación de tráfico no deseado (UTRS) de *Team Cymru*, utilizando una sesión BGP.

Esta integración no solo refuerza la seguridad de la red, sino que también se convierte en una herramienta crucial para la mitigación proactiva de ataques de Denegación de Servicio Distribuido (DDoS). Al hacerlo, asegura la estabilidad y disponibilidad de los servicios para todos los clientes del ISP.

Además, se empleó técnicas como los agujeros negros activados a distancia (RTBH) a nivel mundial. Estas estrategias permiten bloquear selectivamente el tráfico malicioso antes de que afecte los sistemas, fortaleciendo así la postura de seguridad cibernética. Al participar en este enfoque colaborativo, no solo protege la infraestructura, sino que también contribuye a la protección general de Internet.

Coordinación

Según el análisis realizado, se ha constatado que la coordinación operativa se lleva a cabo de manera efectiva mediante la actualización regular de la información de contacto y los registros de enrutamiento. Este proceso garantiza que la red esté preparada para gestionar cambios y contingencias de manera oportuna y eficiente.

Además, se observa una participación activa en comunidades de operadores, destacando la presencia y colaboración en eventos organizados por entidades clave como LACNIC. La asistencia a estos eventos presenciales no solo fortalece la colaboración con otros proveedores de servicios de Internet (ISPs), sino que también facilita el intercambio de mejores prácticas y el conocimiento sobre las últimas tendencias y desarrollos en el ámbito del enrutamiento y la seguridad de redes.

Esta interacción directa con la comunidad de operadores y la asistencia a eventos regionales específicos para ISPs demuestra un compromiso continuo con la mejora y la eficiencia en la gestión de redes, así como una adaptación proactiva a los desafíos y oportunidades emergentes en el sector de las telecomunicaciones y la infraestructura de Internet.

Validación global

Según el análisis, se ha confirmado que la validación global implica la publicación precisa y completa de los datos de enrutamiento, permitiendo que terceros puedan verificar la información proporcionada. El ISP ha establecido procedimientos robustos para garantizar que todos sus Anuncios de Sistemas Autónomos (ASN) y prefijos de direcciones IP sean registrados en bases de datos de Información de Registro de Rutas (IRR) y en el Registro de Bloques de Direcciones (RBD).

Además, el ISP ha implementado Certificados de Origen de Ruta (ROA) para todos los prefijos de IP que están legítimamente autorizados para originarse desde su red. Esta práctica no solo asegura la autenticidad de los anuncios de enrutamiento, sino que también fortalece la integridad y la confiabilidad de la información que se propaga a través de los sistemas de enrutamiento global.

Estas medidas reflejan un compromiso sólido del ISP con las mejores prácticas de gestión de enrutamiento, garantizando una red configurada de manera precisa y segura, capaz de cumplir con los estándares internacionales y proporcionar una experiencia estable y confiable a sus clientes y socios en la comunidad de Internet.

3.2. Validación de la propuesta

Según *MANRS-primer-enterprises-es.pdf* (2021) el 94% de las empresas dijeron que estaban dispuestas a pagar más por un proveedor que fuera participante de MANRS en una situación competitiva.

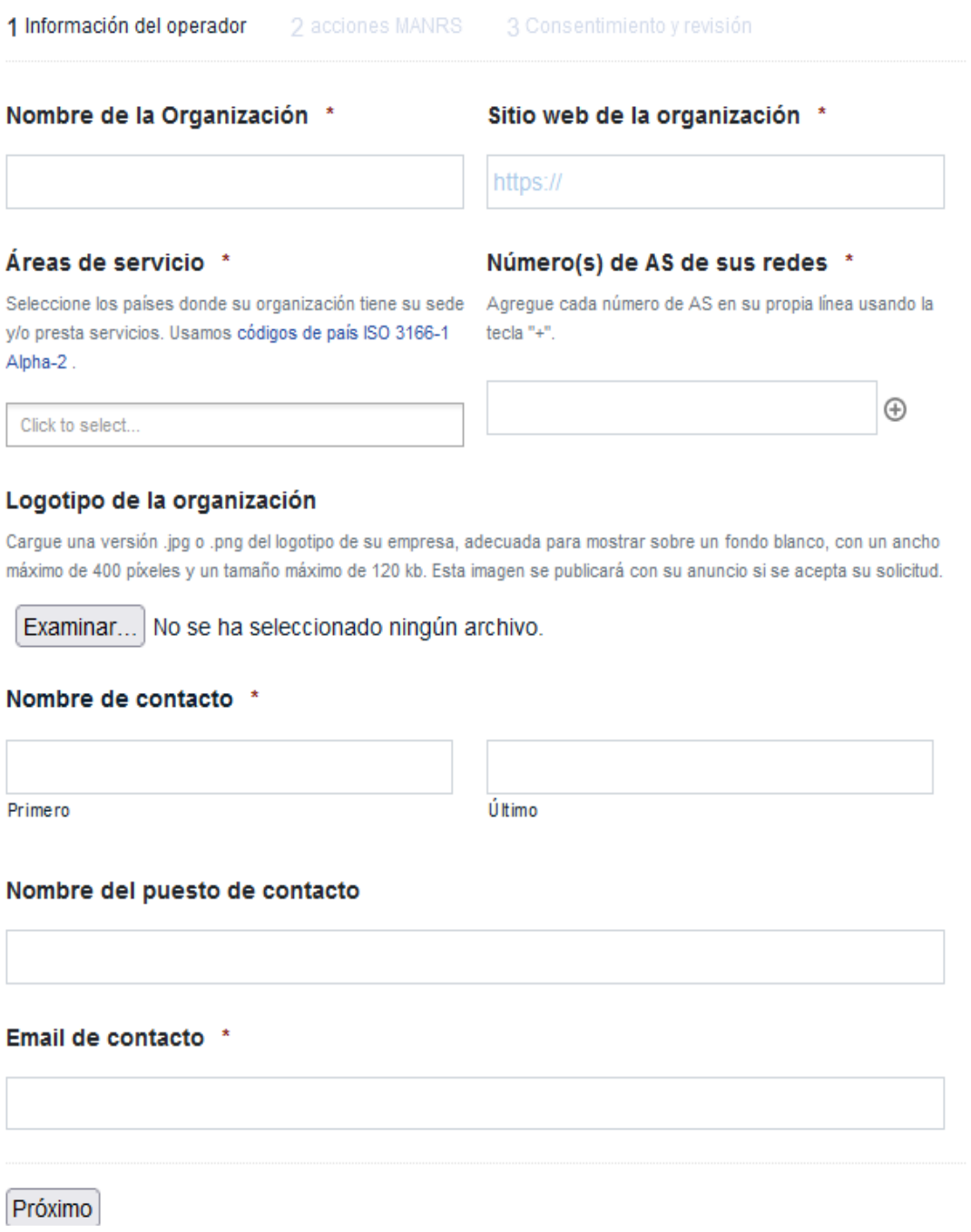
Esto destaca la importancia de la implementación de MANRS como indicador de las prácticas de seguridad sólidas de un operador de red.

La validación de la propuesta fue llevada a cabo por un experto certificado en *networking*, quien, tras la implementación, confirmó mediante un check list Anexo 3 que los resultados obtenidos demostraron que el ISP no solo adoptó, sino que también mejoró las cuatro acciones fundamentales de MANRS. Este logro se alcanzó mediante varias medidas clave, que incluyen la creación de nuevos Listados de Control de Acceso (ACLs), la implementación de un sistema anti-DDoS como UTRS en colaboración con *Team Cymru*, y la integración de un servidor de RPKI dentro de la infraestructura para la validación de Sistemas Autónomos (ASNs) y direcciones IP.

Para Robachevsky (2019) el Observatorio tiene dos vertientes: pública, abierta a todos, y privado, disponible para los participantes de MANRS. El usuario de la vista pública puede mirar el enrutar métricas y estadísticas de seguridad a nivel global, regional y económico. Mientras que los participantes de MANRS pueden ver el rendimiento de las redes individuales (de ¡más de 64.000!) e incluso profundizar en un informe mensual detallado de incidentes para las redes que operan.

De acuerdo a la organización *Join the MANRS Network Operator Program* (2023) los requisitos para la participación los principios MANRS dice al menos debe implementar una de las acciones esperadas para la mayor parte de su infraestructura de las cuatro acciones filtrado, *antispoofing*, coordinación e información global, una vez implementada las acciones debe llenar la solicitud con los campos con * es obligatorio como muestra la Figura 32.

Figura 32. Aplicación del operador de red. MANRS.



Fuente: tomada a partir de *Join the MANRS Network Operator Program* (2024)

Una vez enviada la solicitud puede consultar el estado de su participación marcadas con una casilla de verificación de acuerdo a las 4 acciones de acuerdo a los principios de MANRS como se muestra en la Figura 33. Network Operator Participants (2024)

Figura 33. Participantes del operador de red

Buscar participantes

pectáculo 10 entradas

Descargar CSV

Nombre de la Organización	Fecha de aprobación	Áreas servido	ASN	Acción 1 Filtración	Acción 2 Anti-suplantación de identidad	Acción 3 Coordinación	Acción 4 Información de ruta	
							TIR	RPKI
.pt	15 de octubre de 2018	PT	199993	✓	No data	100%	100%	100%
1-cuadrícula	24 de octubre de 2023	PARA	36943	✓		100%	100%	100%
10110770 Manitoba O/A Redes Vulpinas	19 de junio de 2022	California, EE. UU.	400442	✓		100%	100%	100%
2012 limitado	26 de abril de 2023	Hong Kong	4658	✓		100%	100%	94%
TELECOMUNICACIONES 3D LTDA	20 de noviembre de 2023	CAROLINA DEL SUR	52706	✓	100%	100%	100%	100%
3WACCES	31 de marzo de 2020	BR	269053	✓	49%	100%	100%	100%
76 Telecom Telecomunicações Ltda.	7 de julio de 2020	BR	262760, 262363	✓		50%	100%	100%

Fuente: tomada a partir de *Network Operator Participants* (2023)

3.3. Resultados

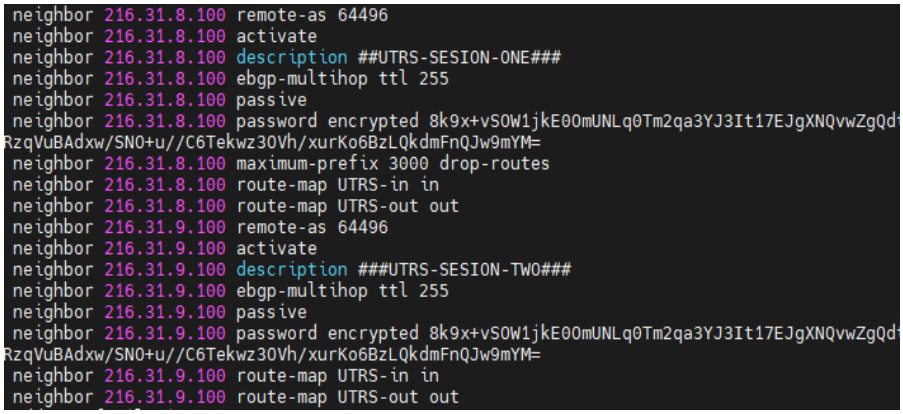
En base a los resultados del *check list* que muestra en el Anexo 1 dirigida al especialista de *networking* se halló que la acción 2 de evitar el tráfico con direcciones de IP de origen falsificable no estaba presente en la seguridad de

enrutamiento, por otra parte, también se obtuvo como resultado que el ISP no cuenta con la implantación de RPKI como alternativa de política de enrutamiento documentada públicamente para facilitar la información a escala mundial.

Con base a los resultados del *check list* del Anexo 2 se logró corregir la siguiente información del enrutador como muestra el Anexo 3. Donde puede apreciar el antes y después al aplicar las acciones de MANRS con los principios de reforzar la seguridad de enrutamiento del ISP, reflejando con el compromiso de la seguridad de Internet.

La acción 2 evitar el tráfico con direcciones IP de origen falsificable en el ISP se implementó una herramienta eficaz para mitigar ataques de DDoS por medio de la organización *Team Cymru* mediante *Unwanted Traffic Removal Service* UTRS con una sesión BGP podemos apreciar en Figura 34.

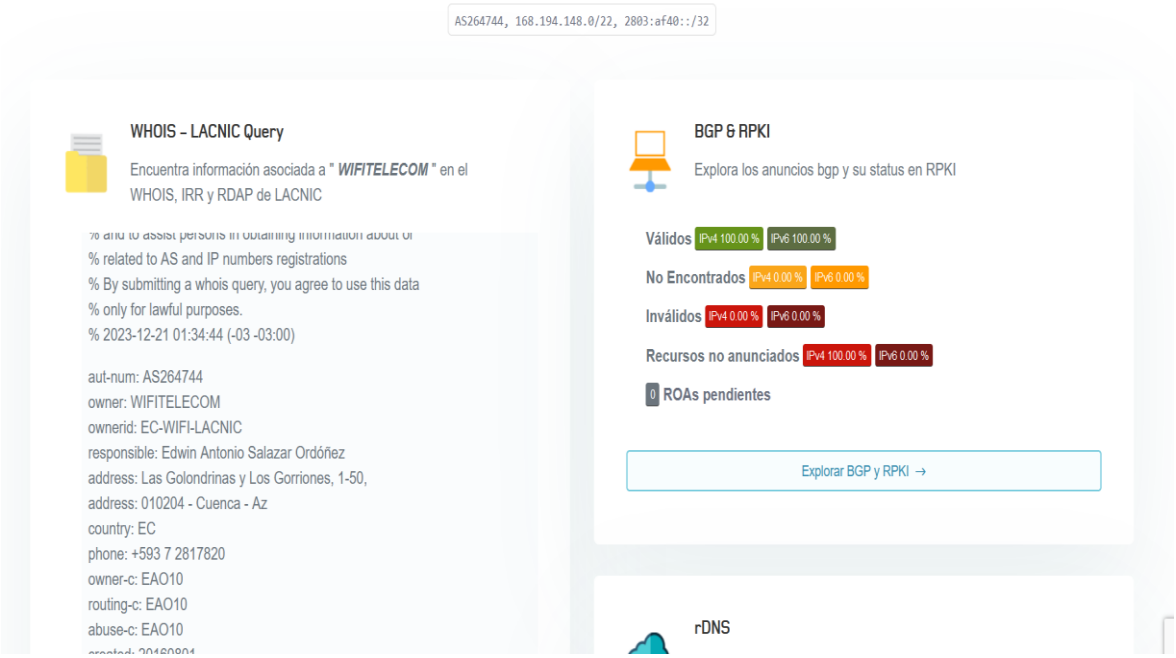
Figura 34. UTRS mediante BGP



Fuente: elaboración propia

La acción 4 facilitar la información de enrutamiento a escala mundial el ISP tiene implementado RPKI por IRR en este caso es LACNIC Figura 35. Donde se aprecia que la información global se encuentra actualizada mostrando el estado del RPKI para el ISP y el anuncio de sus prefijos marcados como válidos, esta información es publica accesible para todos los operadores de red.

Figura 35. Anuncios BGP y status en RPKI



Fuente: tomada a partir de LACNIC (2023)

En base a los resultados obtenidos de la investigación se fortalece la seguridad de enrutamiento seguro a través de *Mutually Agreed Norms for Routing Security* (MANRS), con la adopción de las mejores prácticas de enrutamiento seguro definidas por MANRS refleja el compromiso del ISP con la responsabilidad comunitaria de mantener la integridad de Internet.

CONCLUSIONES

- La revisión exhaustiva de la bibliografía ha proporcionado una comprensión profunda de las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS) y su relevancia en el contexto de los Proveedores de Servicios de Internet (ISP). Se ha identificado claramente la importancia de adoptar las mejores prácticas de enrutamiento seguro definidas por MANRS para garantizar la integridad y seguridad de la infraestructura de Internet.

- La evaluación de la infraestructura de red ha revelado información valiosa sobre las prácticas actuales de enrutamiento seguro en el ISP. Durante este análisis crítico, se identificaron áreas de mejora significativas y vulnerabilidades en la seguridad del enrutamiento, incluyendo los ACLs, las medidas anti-DDoS y la implementación de RPKI. Estos hallazgos sientan las bases fundamentales para la implementación efectiva de las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS).

- El ISP ha logrado elevar significativamente la seguridad y la confiabilidad de su infraestructura de red mediante la implementación de las prácticas recomendadas por MANRS. Esta adopción de las mejores prácticas de enrutamiento seguro, definidas por MANRS, subraya el compromiso del ISP con la responsabilidad comunitaria de preservar la integridad de Internet y prevenir posibles ataques cibernéticos en el futuro.

RECOMENDACIONES

- Después de la implementación de MANRS, es crucial llevar a cabo evaluaciones regulares de la infraestructura de seguridad para identificar posibles brechas o áreas de mejora.

- Implementar un sistema de monitoreo activo de incidentes para detectar y responder rápidamente a posibles violaciones de seguridad, garantizando una respuesta efectiva en caso de amenazas. Se recomienda herramientas como *Splunk, SolarWinds,* etc.

- Establecer una colaboración efectiva con autoridades gubernamentales y agencias de ciberseguridad para compartir información relevante y fortalecer la seguridad a nivel nacional.

- Incorporar principios de ciberseguridad desde las etapas iniciales del desarrollo de nuevos servicios y aplicaciones para garantizar una postura segura desde el principio.

BIBLIOGRAFÍA

Akamai. (s.f.). Obtenido de https://www.akamai.com/es/glossary/what-is-ddos

Arias, F. G. (2012). El ProyEcto dE InvEstIgacIón. Caracas: EITORIAL EPISTEME, C.A.

CYMRU Bogon Reference Dataset. (2018, diciembre 20). CAIDA. https://www.caida.org/catalog/datasets/bogons/

Cymru, T. (s.f.). Team Cymru. Obtenido de https://www.team-cymru.com/company

EHACKING. (2018, noviembre 13). Tráfico de Google secuestrado a través de pequeño ISP nigeriano. Blog EHCGroup. https://blog.ehcgroup.io/2018/11/13/19/47/38/4116/trafico-de-google-secuestrado-a-traves-de-pequeno-isp-nigeriano/delitos-informaticos/ehacking/

Electric, H. (20 de Diciembre de 2023). Hurricane Electric. Obtenido de https://bgp.he.net/AS264744#_prefixes

Freedman, D., George, W., Freedman, J., Freedman, A., Snijders, J., & Tony, T. (2014). manrs.org. Obtenido de https://www.manrs.org/about/history/

Goldberg, S. (s.f.). ACM . Obtenido de https://dl.acm.org/doi/fullHtml/10.1145/2668152.2668966

GUEVARA, J., & QUIZHPI, D. (9 de 2017). UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/14613/1/UPS%20-%20ST003251.pdf

Guía del usuario del BGP | Junos OS | Juniper Networks. (s. f.). Recuperado 9 de diciembre de 2023, de https://www.juniper.net/documentation/mx/es/software/junos/bgp/index.html

Internet Routing Registry (IRR). (s. f.). Recuperado 12 de diciembre de 2023, de https://www.lacnic.net/5921/2/lacnic/internet-routing-registry-irr

Join the MANRS Network Operator Program. (s. f.-a). MANRS. Recuperado 5 de diciembre de 2023, de https://www.manrs.org/netops/join/

Join the MANRS Network Operator Program. (s. f.-b). MANRS. Recuperado 20 de diciembre de 2023, de https://www.manrs.org/netops/join/

Kruse, M. (28 de 7 de 2021). internetsociety. Obtenido de https://www.internetsociety.org/es/blog/2021/07/nuevos-manuales-de-seguridad-de-enrutamiento-de-manrs-para-los-responsables-de-la-toma-de-decisiones/

Lacnic. (2 de Diciembre de 2023). Lacnic.net. Obtenido de https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomo-asn

LACNIC. (20 de Diciembre de 2023). LACNIC. Obtenido de https://query.milacnic.lacnic.net/search?id=AS264744

Lacnic-fasciculo-infraestructura-internet-es.pdf. (s. f.). Recuperado 10 de diciembre de 2023, de https://www.lacnic.net/innovaportal/file/978/4/lacnic-fasciculo-infraestructura-internet-es.pdf

Levy, M. (19 de 9 de 2018). cloudflare. Obtenido de https://blog.cloudflare.com/rpki/

Madory, D. (2019, julio 15). Excessive BGP AS-PATH prepending is a self-inflicted vulnerability. APNIC Blog. https://blog.apnic.net/2019/07/15/excessive-bgp-as-path-prepending-is-a-self-inflicted-vulnerability/

Mandory, D. (6 de Junio de 2023). Obtenido de https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/

MANRS for Network Operators. (s. f.). MANRS. Recuperado 2 de diciembre de 2023, de https://www.manrs.org/netops/

MANRS Observatory. (10 de 12 de 2023). Obtenido de https://observatory.manrs.org/#/overview

MANRS Observatory. (s. f.). MANRS. Recuperado 10 de diciembre de 2023, de https://www.manrs.org/manrs-observatory/

MANRS. (17 de Mayo de 2021). MANRS Actions for Network Operators. Obtenido de https://www.manrs.org/wp-content/uploads/2021/09/MANRS-Network-Operators-Actions-v2.5.2.pdf

MANRS-Network-Operators-Actions-v2.5.2.pdf. (s. f.). Recuperado 2 de diciembre de 2023, de https://www.manrs.org/wp-content/uploads/2021/09/MANRS-Network-Operators-Actions-v2.5.2.pdf

MANRS-primer-enterprises-es.pdf. (s. f.). Recuperado 10 de diciembre de 2023, de https://www.manrs.org/wp-content/uploads/2021/07/MANRS-primer-enterprises-es.pdf

MARNS. (2024). MANRS. Obtenido de manrs.org: https://www.manrs.org/about/

Moreiras, A., & Patara, R. (2019, agosto 19). Https://www.lacnic.net/innovaportal/file/978/4/lacnic-fasciculo-infraestructura-internet-es.pdf. https://www.lacnic.net/innovaportal/file/978/4/lacnic-fasciculo-infraestructura-internet-es.pdf

Network Operator Actions. (s. f.). MANRS. Recuperado 13 de diciembre de 2023, de https://www.manrs.org/netops/network-operator-actions/

Network Operator Participants. (s. f.). MANRS. Recuperado 20 de diciembre de 2023, de https://www.manrs.org/netops/participants/

Oppenheimer, P. (2011). Top-down network design: A systems analysis approach to enterprise network design (3. ed., 1. print). Cisco Press.

Resource Public Key Infrastructure (RPKI) - Interconnect Help. (s.f.). Obtenido de https://support.google.com/interconnect/answer/12342476?hl=en

Robachevsky, A. (13 de 8 de 2019). Internet Society. Obtenido de https://www.internetsociety.org/blog/2019/08/manrs-observatory-monitoring-the-state-of-internet-routing-security/

Robachevsky, A. (2020, noviembre 12). Nuevas funciones en el Observatorio MANRS: Más informativo, más intuitivo y más fácil de usar. Internet Society. https://www.internetsociety.org/es/blog/2020/11/nuevas-funciones-en-el-observatorio-manrs-mas-informativo-mas-intuitivo-y-mas-facil-de-usar/

Seguridad de enrutamiento para legisladores. (s. f.). Internet Society. Recuperado 10 de diciembre de 2023, de https://www.internetsociety.org/es/resources/doc/2018/seguridad-de-enrutamiento-para-legisladores/

Siddiqui, A. (16 de 11 de 2018). MANRS. Obtenido de https://www.manrs.org/2018/11/route-leak-causes-major-google-outage/

Strickx, T. (24 de 6 de 2019). MANRS. Obtenido de https://www.manrs.org/2019/06/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/

UDP-Based Amplification Attacks | CISA. (2019, diciembre 18). https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks

Zeng, M., Li, D., Zhang, P., Xie, K., & Huang, X. (2023). Federated Route Leak Detection in Inter-domain Routing with Privacy Guarantee. ACM Transactions on Internet Technology, 23(1), 12:1-12:22. https://doi.org/10.1145/3561051

ANEXOS

Anexo 1: Formato *C*heck list

Fecha: 18/12/2023			
Nombre del especialista:			
Acción 1: Prevenir la propagación de información incorrecta de enrutado			
Pregunta	**SI**	**NO**	**OBSERVACION**
¿El operador de red tiene un sistema para prevenir el anuncio de prefijos AS y/o IP que no estén autorizados?			
¿El operador de red verifica los anuncios de sus clientes para asegurarse de que no estén anunciando prefijos que no estén autorizados?			
¿El operador de red tiene un proceso para identificar y mitigar los anuncios incorrectos de enrutado?			
Acción 2: Evitar el tráfico con direcciones IP de origen falsificable			
¿El operador de red utiliza un sistema para validar las direcciones IP de origen?			
¿El operador de red prueba regularmente si su red es capaz de enviar paquetes con direcciones IP de fuente falsificada utilizando el software de CAIDA Spoofer para detectar posibles vulnerabilidades a ataques DDoS?			
Acción 3: Facilitar la comunicación y la coordinación operacionales mundiales			
¿La información de contacto del operador de red se encuentra actualizada en la base de datos RIR (o NIR) y/o en PeeringDB, y es accesible al menos a otros operadores de red registrados en PeeringDB?			
¿El operador de red documenta públicamente sus anuncios de enrutamiento previstos en el registro de enrutamiento RIR apropiado o en Routing Assets Database RADB?			
Acción 4: Facilitar la información de enrutamiento a escala mundial			
¿El operador de red ha registrado todos los números AS y los prefijos IP que anuncia a otras redes en un IRR o RADB?			
¿El operador de red tiene ROA válidos para al menos el 90% de los prefijos IP o conjuntos de prefijos que están legítimamente autorizados a originar?			
¿El operador de red implementa RPKI como alternativa a la política de enrutamiento documentada públicamente para facilitar la información de enrutamiento a escala mundial?			

Anexo 2: *Check list* realizado por un especialista

CHECK LIST **DE MANRS PARA ESPECIALISTA**

Fecha: 18/12/2023			
Nombre del especialista: Mg. Edison Euclides Segarra Guzmán			
Acción 1: Prevenir la propagación de información incorrecta de enrutado			
Pregunta	**SI**	**NO**	**OBSERVACION**
¿El operador de red tiene un sistema para prevenir el anuncio de prefijos AS y/o IP que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red verifica los anuncios de sus clientes para asegurarse de que no estén anunciando prefijos que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red tiene un proceso para identificar y mitigar los anuncios incorrectos de enrutado?	**X**		Listas Bogons mediante BGP-Cymru- ACL
Acción 2: Evitar el tráfico con direcciones IP de origen falsificable			
¿El operador de red utiliza un sistema para validar las direcciones IP de origen?		**X**	
¿El operador de red prueba regularmente si su red es capaz de enviar paquetes con direcciones IP de fuente falsificada utilizando el software de CAIDA Spoofer para detectar posibles vulnerabilidades a ataques DDoS?		**X**	
Acción 3: Facilitar la comunicación y la coordinación operacionales mundiales			
¿La información de contacto del operador de red se encuentra actualizada en la base de datos RIR (o NIR) y/o en PeeringDB, y es accesible al menos a otros operadores de red registrados en PeeringDB?	**X**		
¿El operador de red documenta públicamente sus anuncios de enrutamiento previstos en el registro de enrutamiento RIR apropiado o en Routing Assets Database RADB?	**X**		
Acción 4: Facilitar la información de enrutamiento a escala mundial			
¿El operador de red ha registrado todos los números AS y los prefijos IP que anuncia a otras redes en un IRR o RADB?	**X**		
¿El operador de red tiene ROA válidos para al menos el 90% de los prefijos IP o conjuntos de prefijos que están legítimamente autorizados a originar?	**X**		
¿El operador de red implementa RPKI como alternativa a la política de enrutamiento documentada públicamente para facilitar la información de enrutamiento a escala mundial?		**X**	

Realizado por: Edison Ríos

EDISON EUCLIDES SEGARRA GUZMAN

Ing. Edison Euclides Segarra Guzmán, MSc.

Anexo 3: *Check list* de MANRS corregido

***CHECK LIST* DE MANRS CORREGIDO EN BASE A LOS RESULTADOS**

Fecha: 18/12/2023			
Nombre: Mg. Edison Euclides Segarra Guzmán			
Acción 1: Prevenir la propagación de información incorrecta de enrutado			
Pregunta	**SI**	**NO**	**OBSERVACION**
¿El operador de red tiene un sistema para prevenir el anuncio de prefijos AS y/o IP que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red verifica los anuncios de sus clientes para asegurarse de que no estén anunciando prefijos que no estén autorizados?	**X**		Listas Bogons mediante BGP-Cymru- ACL
¿El operador de red tiene un proceso para identificar y mitigar los anuncios incorrectos de enrutado?	**X**		Listas Bogons mediante BGP-Cymru- ACL
Acción 2: Evitar el tráfico con direcciones IP de origen falsificable			
¿El operador de red utiliza un sistema para validar las direcciones IP de origen?	**X**		UTRS mediante BGP-Cymru
¿El operador de red prueba regularmente si su red es capaz de enviar paquetes con direcciones IP de fuente falsificada utilizando el software de CAIDA Spoofer para detectar posibles vulnerabilidades a ataques DDoS?	**X**		UTRS mediante BGP-Cymru
Acción 3: Facilitar la comunicación y la coordinación operacionales mundiales			
¿La información de contacto del operador de red se encuentra actualizada en la base de datos RIR (o NIR) y/o en PeeringDB, y es accesible al menos a otros operadores de red registrados en PeeringDB?	**X**		
¿El operador de red documenta públicamente sus anuncios de enrutamiento previstos en el registro de enrutamiento RIR apropiado o en Routing Assets Database RADB?	**X**		
Acción 4: Facilitar la información de enrutación a escala mundial			
¿El operador de red ha registrado todos los números AS y los prefijos IP que anuncia a otras redes en un IRR o RADB?	**X**		
¿El operador de red tiene ROA válidos para al menos el 90% de los prefijos IP o conjuntos de prefijos que están legítimamente autorizados a originar?	**X**		
¿El operador de red implementa RPKI como alternativa a la política de enrutamiento documentada públicamente para facilitar la información de enrutamiento a escala mundial?	**X**		IRR – LACNIC RPKI- FORT

Firmado electrónicamente por:
EDISON EUCLIDES
SEGARRA GUZMAN

Ing. Edison Euclides Segarra Guzmán, MSc