UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRÍA EN COMPUTACIÓN

MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"OPTIMIZACIÓN DE LA SEGURIDAD EN EL TRÁFICO DE ENTRADA DE LA RED CENTRAL DE AIRMAXTELECOM MEDIANTE LA IMPLEMENTACIÓN DE RPKI PARA LA MITIGACIÓN DE ATAQUES DE SECUESTRO DE RUTAS"

Trabajo de titulación previo a la obtención del título de Magister en Computación con mención en Seguridad Informática

Línea de investigación: Seguridad de la información.

AUTOR:

Carlos Andrés Benavides Sánchez

DIRECTOR:

Farinango Endara Henry Patricio

Ibarra – Ecuador 2026

DEDICATORIA

Dedico este trabajo a mi esposa y a mi hijo por su comprensión, apoyo incondicional y guía constante durante mi formación académica y personal.

A mis padres Delia y Nilo, quienes han sido una fuente fundamental de motivación, paciencia y fortaleza para culminar esta etapa importante de mi vida.

A mi hermano, Willian, por su cariño, respaldo y compañía a lo largo de mi camino.

AGRADECIMIENTO

A la Virgen del Carmen y a Dios, por acompañarme, iluminar mi camino y brindarme la fortaleza necesaria para mantenerme firme durante mi formación académica.

A mi familia, por su paciencia, consejos, apoyo y buenos deseos, los cuales han sido fundamentales para alcanzar la culminación de mi meta.

Al MSc. Henry Farinango y al MSc. Fabián Cuzme, por compartir sus conocimientos, experiencia y valioso tiempo, orientándome durante el proceso de investigación y construcción del conocimiento necesario para el desarrollo de mi trabajo de titulación.

A la Universidad Técnica del Norte, por brindarme nuevamente la oportunidad de formarme en su entorno académico y científico, esta vez como maestrante, posterior a mi formación como ingeniero.

A Airmaxtelecom Soluciones Tecnológicas S.A., por la apertura, confianza y facilidades otorgadas para la ejecución de mi tesis.

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
APELLIDOS Y NOMBRES:	Benavides Sánchez Carlos Andrés

DATOS DE LA OBRA	
TÍTULO:	OPTIMIZACIÓN DE LA SEGURIDAD EN EL TRÁFICO DE ENTRADA DE LA RED CENTRAL DE AIRMAXTELECOM MEDIANTE LA IMPLEMENTACIÓN DE RPKI PARA LA MITIGACIÓN DE ATAQUES DE SECUESTRO DE RUTAS
AUTOR (ES):	Benavides Sánchez Carlos Andrés
FECHA: DD/MM/AAAA	02/05/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática
DIRECTOR /ASESOR:	MSc. Farinango Henry, MSc. Fabian Cuzme

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 2 días del mes de junio de 2026

EL AUTOR:

(Firma)…. Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CARLOS ANDRES BENAVIDES SANCHEZ
…….
Nombre: Benavides Sánchez Carlos Andrés

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

Ibarra, 12 de mayo de 2026

Dr. Jorge Gordón
Decano (e)
Facultad de Posgrado

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado **Optimización de la seguridad en el tráfico de entrada de la red central de Airmaxtelecom mediante la implementación de rpki para la mitigación de ataques de secuestro de rutas** del maestrante **Benavides Sánchez Carlos Andrés** de la Maestría de Computación Mención Seguridad Informática certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	*FARINANGO ENDARA HENRY*	Validar únicamente en FirmaEC. Firmado electrónicamente por: HENRY PATRICIO FARINANGO ENDARA
Asesor/a	*CUZME RODRIGUEZ FABIÁN*	Validar únicamente en FirmaEC. Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ

ÍNDICE DE CONTENIDO

DEDICATORIA II

AGRADECIMIENTO III

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE IV

ÍNDICE DE TABLAS IX

ÍNDICE DE FIGURAS X

RESUMEN XII

ABSTRACT XIII

CAPÍTULO I 1

PROBLEMA DE INVESTIGACIÓN 1

1.1 PLANTEAMIENTO DEL PROBLEMA 1

1.2 INTERROGANTES DE LA INVESTIGACIÓN 2

1.3 OBJETIVOS DE LA INVESTIGACIÓN 3

1.3.1 Objetivo General 3

1.3.2 Objetivos específicos 3

1.4 HIPÓTESIS 3

1.4.1 Hipótesis de Trabajo 3

1.4.2 Hipótesis Alternativa 4

1.5 CATEGORIZACIÓN DE VARIABLES 4

1.6 JUSTIFICACIÓN 4

CAPÍTULO II 6

MARCO REFERENCIAL 6

2.1 ANTECEDENTES 6

2.2 MARCO TEÓRICO 16

2.2.1 Introducción a la seguridad de enrutamiento BGP 16

2.2.2 Origen y fundamento del RPKI 17

2.2.3 Identificación de amenazas en BGP 19
2.2.4 Validación del origen de rutas: Route Origin Validation (ROV) 20
2.2.5 Herramientas y plataformas de mitigación 21
2.2.6 Evaluación de riesgos en infraestructura de ISP 23
2.2.7 Participación de LACNIC en la implementación de RPKI 24
2.2.8 Incidentes de enrutamiento, integridad y rendimiento del servicio de Internet 25
2.3 Marco Legal 26
2.3.1 Obligaciones de los Proveedores de Servicio de Internet en Ecuador 26
CAPÍTULO III 29
MARCO METODOLÓGICO 29
3.1 Descripción del área del estudio 29
3.2 Enfoque y tipo de investigación 30
3.3 Procedimiento de investigación 30
3.3.1 Revisión bibliográfica y documental 30
3.3.2 Diagnóstico inicial de la red 34
3.3.3 Identificación y valoración de activos 35
3.3.4 Valoración CIA y cálculo del valor del activo 36
3.3.5 Identificación de amenazas de secuestro de rutas 36
3.3.6 Identificación de vulnerabilidades 38
3.3.7 Escalas de valoración de amenaza y vulnerabilidad 39
3.3.8 Cálculo del riesgo actual 40
3.3.8 Tratamiento del riesgo 42
3.3.9 Diseño de la solución técnica 42
3.3.10 Implementación y configuración 46
3.3.11 Creación de ROA en cuenta miLacnic 49
3.3.12 Instalación y configuración del validador RPKI Routinator 52
3.3.13 Evaluación mediante monitoreo y recolección de datos 58
3.4 Consideraciones Bioéticas 60
CAPÍTULO IV 62
RESULTADOS Y DISCUSIÓN 62

4.1 RESULTADOS DE LA REVISIÓN DEL ESTADO DEL ARTE 62
4.2 RESULTADOS DEL ANÁLISIS DE VULNERABILIDADES VALIDACIÓN DE RUTAS 64
4.3 RESULTADO DE APLICACIÓN DEL SISTEMA DE VALIDACIÓN RPKI 69
CONCLUSIONES Y RECOMENDACIONES 83
GLOSARIO DE TÉRMINOS 86
REFERENCIAS 92
ANEXOS 98

ÍNDICE DE TABLAS

Tabla 1 Sistema RPKI y BGP Hijacking 12
Tabla 2 Criterios de selección de fuentes para la revisión documentable 31
Tabla 3 Estado de prefijos IPv4 validados con ROA a nivel Global 32
Tabla 4 Estado de prefijos IPv4 validados con ROA a nivel Sur Americano 33
Tabla 5 Fases metodológicas 34
Tabla 6 Identificación de activos 35
Tabla 7 Valoración de activos con modelo CIA 36
Tabla 8 Análisis de amenazas 37
Tabla 9 Clasificación de vulnerabilidades 38
Tabla 10 Rango de amenaza 39
Tabla 11 Rango de vulnerabilidad 39
Tabla 12 Rango y nivel de riesgo 40
Tabla 13 Cálculo del valor del activo y riesgo 40
Tabla 14 Relación de activos con amenazas y vulnerabilidades 41
Tabla 15 Tratamiento de riesgo 42
Tabla 16 Herramientas de validación RPKI 44
Tabla 17 Definición de política de filtrado BGP basada en validación RPKI 45
Tabla 18 Recursos IPv4, ASN y protocolos 46
Tabla 19 Parámetros de configuración de cliente RPKI 57
Tabla 20 Parámetros de evaluación antes de la implementación de RPKI 59
Tabla 21 Parámetros de evaluación después de la implementación de RPKI 60
Tabla 22 Elementos técnicos identificados en el estado del arte 62
Tabla 23 Controles implementados 64
Tabla 24 Eventos de hijacks de base de datos RadarQrator 70
Tabla 25 Clasificación de eventos de hijacks 73
Tabla 26 Comparación de parámetros de rendimiento antes y después 74
Tabla 27 Comparación de métricas ICMP hacia 8.8.8.8 antes y después 78
Tabla 28 Comparación de métricas ICMP hacia 1.1.1.1 antes y después de la implementación de RPKI 81

ÍNDICE DE FIGURAS

Figura 1 Verificación de cadena de búsqueda en la IEEE Explore 7
Figura 2 Adopción RPKI - IPv4 Global 32
Figura 3 Adopción de RPKI – IPv4 en América del Sur 33
Figura 4 Ubicación de RPKI en el modelo OSI 43
Figura 5 Ejemplo de validación de prefijo IPv4 45.70.*.*/24 con AS271933 44
Figura 6 Número de sistema autónomo asignado a Airmaxtelecom S.A. 47
Figura 7 Prefijo público IPv4 asignado al ASN 271933 perteneciente a Airmaxtelecom Soluciones Tecnológicas S.A. 47
Figura 8 Software Routinator alojado en un subdominio del ISP 48
Figura 9 Lista de anuncios vía BGP válidos en herramienta tools de LACNIC 49
Figura 10 Menú principal con el módulo de RPKI 49
Figura 11 Formulario para creación de ROA 50
Figura 12 Ingreso de prefijo IPv4 público con máscara /22 y máscara /24 3 50
Figura 13 Estado de acciones previas a grabar el ROA 51
Figura 14 Mensaje de confirmación de creación de ROA 51
Figura 15 Lista de ROAs creados para la organización 51
Figura 16 Agregación de repositorio Nlnet Labs 52
Figura 17 Instalación de Routinator en sistema operativo Ubuntu 52
Figura 18 Validación de versión de software routinator 53
Figura 19 Estado de routinator activo 53
Figura 20 Cambio de puertos de archivo de configuración de Routinator 54
Figura 21 Estado de la herramienta de RPKI 54
Figura 22 Sistema web de validación de ROA con RPKI 55
Figura 23 Respuesta en formato JSON 55
Figura 24 Configuración de RTR en router de borde 56
Figura 25 Sesión RTR establecida desde router Huawei 58
Figura 26 ROA creado para el prefijo 45.70.*.*/* con ASN 271933 66
Figura 27 Propagación global y estado de validación RPKI del prefijo 45.70.*.*/22 66
Figura 28 Protocolo RTR (RPKI-to-Router) entre el router de borde y el validador local 67

Figura 29 Políticas de enrutamiento 67
Figura 30 Estadísticas de coincidencia de RPKI activo 68
Figura 31 Detalle de prefijos BGP con estado "invalid" 68
Figura 32 Sesión establecida entre el validador RPKI y el router NE8000 69
Figura 33 Prueba de ping y paquetes perdidos antes de implementar RPKI 75
Figura 34 Prueba de ping durante el rango 8:00h – 10:00h después 76
Figura 35 Prueba de ping en rango de horario de 13:00h – 15:00h 77
Figura 36 Prueba de ping en rango de horario de 18:00h – 20:00h 77
Figura 37 Prueba de ping y paquetes perdidos antes de implementar RPKI 78
Figura 38 Prueba de ping durante el rango 8:00h – 10:00h después 80
Figura 39 Prueba de ping durante el rango 13:00h – 15:00h después 80
Figura 40 Prueba de ping durante el rango 18:00h – 20:00h después 81

RESUMEN

La presente investigación aborda la problemática asociada a la vulnerabilidad del protocolo Border Gateway Protocol frente a ataques de secuestro de rutas o BGP Hijacking, una amenaza que compromete la disponibilidad, integridad y estabilidad del tráfico de Internet. En el caso de Airmaxtelecom Soluciones Tecnológicas S.A., se identificó la ausencia de mecanismos de validación de rutas basados en Resource Public Key Infrastructure, situación que incrementaba el riesgo de aceptación y propagación de rutas inválidas dentro de la red central del proveedor de servicios de Internet. El objetivo del estudio fue fortalecer la seguridad del enrutamiento BGP mediante la implementación de RPKI para mitigar ataques de secuestro de rutas y mejorar la integridad del tráfico de entrada. La investigación se desarrolló bajo un enfoque cuantitativo, de tipo aplicada, descriptiva y analítica. Se emplearon técnicas de revisión bibliográfica, análisis de riesgos y monitoreo técnico de red. Como instrumentos se utilizaron registros de configuración, consultas BGP, pruebas ICMP, reportes históricos del ASN 271933 y herramientas de validación como Routinator, Radar Qrator y Cloudflare Radar. La unidad de análisis estuvo conformada por los prefijos IPv4, routers de borde, sesiones eBGP y políticas de enrutamiento de Airmaxtelecom. Los resultados evidenciaron la creación y propagación correcta de objetos ROA, la clasificación de rutas válidas, inválidas y no encontradas, así como la reducción progresiva de eventos de hijacking entre 2023 y 2026. Se concluye que la implementación de RPKI fortaleció la seguridad del enrutamiento, mejoró el control sobre los anuncios BGP y redujo la exposición ante incidentes de secuestro de rutas. Además, las pruebas de latencia y pérdida de paquetes realizadas antes y después de la implementación mostraron estabilidad operativa, sin degradación significativa del servicio, confirmando que la integración de RPKI puede aplicarse en proveedores sin afectar la conectividad ni el rendimiento de la red.

Palabras clave: BGP hijacking, seguridad informática, enrutamiento, validación de rutas, proveedores ISP.

ABSTRACT

This research addresses the vulnerability of the Border Gateway Protocol (BGP) to route hijacking attacks, a threat that compromises the availability, integrity, and stability of internet traffic. In the case of Airmaxtelecom Soluciones Tecnológicas S.A., the absence of route validation mechanisms based on Resource Public Key Infrastructure (RPKI) was identified, increasing the risk of invalid routes being accepted and propagated within the internet service provider's core network. The objective of this study was to strengthen BGP routing security by implementing RPKI to mitigate route hijacking attacks and improve the integrity of incoming traffic. The research employed a quantitative, applied, descriptive, and analytical approach. Techniques included literature review, risk analysis, and technical network monitoring. Instruments used included configuration logs, BGP queries, ICMP tests, historical reports from ASN 271933, and validation tools such as Routinator, Radar Qrator, and Cloudflare Radar. The unit of analysis consisted of IPv4 prefixes, edge routers, eBGP sessions, and Airmaxtelecom routing policies. The results demonstrated the correct creation and propagation of Route Admin Objects (ROAs), the classification of valid, invalid, and unfound routes, and the progressive reduction of route hijacking events between 2023 and 2026. It is concluded that the implementation of RPKI strengthened routing security, improved control over BGP advertisements, and reduced exposure to route hijacking incidents. Furthermore, latency and packet loss tests performed before and after implementation showed operational stability, without significant service degradation, confirming that RPKI integration can be applied by providers without affecting network connectivity or performance.

Keywords: hijacking, information security, routing, route validation, ISP providers.

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

En el entorno actual de las telecomunicaciones, los proveedores de servicios de Internet (ISP) enfrentan desafíos cada vez más complejos en materia de seguridad y estabilidad del enrutamiento. Una de las amenazas más críticas es el hijacking del protocolo BGP (Border Gateway Protocol), el cual se refiere a la alteración intencionada de los anuncios de prefijos IP con el objetivo de desviar el tráfico hacia redes no autorizadas (Huston & Bush, 2018). El tipo de ataque compromete gravemente la disponibilidad, integridad y confidencialidad de los datos en tránsito, lo que puede traducirse en afectaciones operativas y reputacionales para los operadores involucrados (RIPE NCC, 2023).

De acuerdo con Gilad (2017) a pesar de los avances en mecanismos de protección como RPKI (Resource Public Key Infrastructure), su adopción aún presenta limitaciones que impiden una defensa integral contra este tipo de incidentes. En consecuencia, la implementación efectiva de RPKI y otras medidas de validación de rutas se ha convertido en una prioridad para garantizar la confianza y la resiliencia del sistema de enrutamiento global (Cooper & Harman, 2020).

Pese a que RPKI ha demostrado ser una solución técnicamente viable y efectiva para fortalecer la seguridad del enrutamiento, su adopción a nivel global aún es limitada. Muchos operadores no han implementado validadores, no generan ROAs (Route Origin Authorization), o simplemente desconocen las implicaciones de esta tecnología. Cooper y Harman (2020) advierten que la baja adopción de RPKI se debe tanto a la falta de conocimiento como a la percepción de complejidad operativa en su despliegue y mantenimiento. En consecuencia, persiste una brecha significativa entre las capacidades técnicas existentes y su aplicación práctica en entornos reales.

En el caso particular de Airmaxtelecom Soluciones Tecnológicas S.A., un proveedor de servicio de internet ecuatoriano, la red central que gestiona el tráfico de entrada de sus clientes aún no ha incorporado un sistema de validación de rutas mediante un sistema RPKI.

Esta situación representa una debilidad crítica en la arquitectura de red, dado que la empresa está expuesta a anuncios no verificados que pueden afectar tanto su operación como la calidad del servicio entregado. En un entorno competitivo, donde los usuarios exigen estabilidad, velocidad y disponibilidad constante, cualquier interrupción o degradación del servicio puede traducirse en pérdidas económicas y deterioro de la imagen institucional.

Sin embargo, antes de implementar esta tecnología, es fundamental comprender su impacto en el contexto específico de la red de Airmaxtelecom Soluciones Tecnológicas S.A. No se trata simplemente de habilitar una función en los routers de borde, sino de evaluar su efecto real sobre indicadores como latencia, pérdida de paquetes, propagación de rutas, y en última instancia, la experiencia del usuario final. Adicionalmente, se deben identificar los retos técnicos, operativos y humanos que podrían influir en su adopción y mantenimiento a largo plazo.

Por lo tanto, surge la necesidad de desarrollar una investigación aplicada que permita evaluar el efecto de la implementación del protocolo RPKI en la red de Airmaxtelecom, esta investigación centra en determinar si su uso contribuye efectivamente a minimizar los incidentes de enrutamiento, mejorar la eficiencia del tráfico entrante, y garantizar la integridad y el rendimiento del servicio prestado. Al mismo tiempo, debe considerar los factores internos que pueden facilitar o dificultar su implementación, con el fin de generar recomendaciones concretas para su despliegue sostenible.

1.2 Interrogantes de la investigación

En función del problema expuesto previamente, se formulan a continuación las preguntas de investigación que orientarán el desarrollo de este estudio:

- ¿De qué manera la implementación del protocolo RPKI en los enrutadores de borde de Airmaxtelecom contribuye a prevenir el secuestro de rutas IPv4 mediante la validación del origen de los anuncios BGP?
- ¿Qué variación se evidencia en la frecuencia y severidad de los ataques de BGP hijacking en la red de Airmaxtelecom antes y después de la implementación de validación RPKI?

- ¿Qué cambios en la latencia y la pérdida de paquetes se observan tras la implementación de RPKI en la red de Airmaxtelecom, y cómo estos afectan la calidad del servicio percibido por el usuario final?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Fortalecer la seguridad del enrutamiento BGP en la red central de Airmaxtelecom mediante la implementación de la infraestructura RPKI, para mitigar ataques de secuestro de rutas y asegurar la integridad del tráfico de entrada.

1.3.2 Objetivos específicos

- Realizar una revisión sistemática del estado del arte, para establecer las bases técnicas y normativas de la implementación en la red central.
- Analizar el estado actual de la seguridad en el enrutamiento BGP de la red central y caracterizar las amenazas de secuestro de rutas identificadas.
- Implementar un sistema de validación de rutas (ROA) basado en RPKI para la detección y prevención de ataques de secuestro de rutas IPv4.
- Evaluar la incidencia de ataques de BGP hijacking mediante la monitorización y análisis de las rutas validadas por RPKI antes y después de la implementación.

1.4 Hipótesis

1.4.1 Hipótesis de Trabajo

La presente investigación adopta un enfoque metodológico cuantitativo, debido a que la implementación de RPKI (Resource Public Key Infrastructure) será evaluada mediante indicadores medibles antes y después de su aplicación, tales como incidentes asociados a BGP hijacking, rutas inválidas detectadas, rutas válidas, rutas no encontradas, latencia y pérdida de paquetes en la red central de Airmaxtelecom Soluciones Tecnológicas S.A.

Al elevar el nivel de seguridad y la eficiencia del tráfico de entrada en la red central de Airmaxtelecom, mediante la implementación de RPKI, se podrá minimizar los incidentes de enrutamiento y garantizar la integridad y el rendimiento del servicio.

1.4.2 Hipótesis Alternativa

Al elevar el nivel de seguridad y la eficiencia del tráfico de entrada en la red central de Airmaxtelecom, mediante la implementación de RPKI, se NO se podrá MINIMIZAR los incidentes de enrutamiento y garantizar la integridad y el rendimiento del servicio

1.5 Categorización de variables

Las variables que se derivan de la hipótesis planteada son:

- **Variable independiente:** Nivel de seguridad y eficiencia del tráfico de entrada en la red central de Airmaxtelecom Soluciones Tecnológicas S.A., mediante la implementación de RPKI.
- **Variable dependiente**: Incidentes de enrutamiento, integridad y el rendimiento del servicio.

1.6 Justificación

En el ecosistema actual de las telecomunicaciones, la seguridad del enrutamiento global se ha convertido en una prioridad estratégica para los proveedores de servicios de Internet (ISP), dada la creciente sofisticación de las amenazas cibernéticas y la criticidad del tráfico que circula la red de redes Internet. Uno de los vectores de ataque más relevantes en este contexto es el BGP hijacking, que consiste en la manipulación maliciosa de anuncios de prefijos IP con el objetivo de redirigir tráfico hacia redes no autorizadas, afectando gravemente la disponibilidad, integridad y rendimiento de los servicios (Huston & Bush, 2018).

La necesidad de adoptar mecanismos de validación como RPKI se fundamenta en la creciente sofisticación de ataques al protocolo BGP. Airmaxtelecom, al no disponer de tales mecanismos, está expuesta a alteraciones maliciosas que pueden degradar el servicio ofrecido a sus clientes. Esta investigación se alinea con las buenas prácticas promovidas por LACNIC y MANRS, y contribuirá a mejorar la postura de seguridad de la empresa, generar conocimiento replicable y fortalecer la confianza en los servicios de conectividad regionales.

La implementación del protocolo RPKI (Resource Public Key Infrastructure) se presenta como una solución viable y altamente recomendada para validar el origen de los anuncios BGP, permitiendo que los enrutadores identifiquen y descarten rutas inválidas o maliciosas antes de ser propagadas. Diversos estudios han demostrado que la adopción de un sistema RPKI permite disminuir la superficie de ataque en las redes de los ISP y mitigar eficazmente eventos de secuestro de rutas (Gilad ,2017; Cooper & Harman, 2020).

El presente proyecto tiene como objetivo general elevar el nivel de seguridad y la eficiencia del tráfico de entrada en la red central de Airmaxtelecom mediante la implementación de RPKI, el proyecto se enmarca en las buenas prácticas internacionales promovidas por organismos como MANRS (Mutually Agreed Norms for Routing Security) y los registros regionales de Internet como LACNIC, que recomiendan la adopción de RPKI como un componente esencial de las políticas de enrutamiento seguras. Pues, la iniciativa no solo permite alinear a Airmaxtelecom Soluciones Tecnológicas S.A. con estándares internacionales, sino que también fortalece su posicionamiento competitivo en el mercado al garantizar un servicio más seguro y confiable.

La necesidad de esta investigación radica en proporcionar una solución técnica y operativa que permita minimizar los riesgos asociados a incidentes de enrutamiento, aumentar la resiliencia de la red y mejorar la experiencia del usuario. En un entorno donde la seguridad del enrutamiento no puede darse por sentada, la validación de rutas se convierte en un requisito esencial para la integridad del tráfico IP y la sostenibilidad del negocio. En definitiva, este proyecto no solo busca implementar una solución técnica, sino también generar conocimiento práctico aplicable a otros ISP de tamaño medio en la región, aportando valor al ecosistema de Internet a nivel nacional.

CAPÍTULO II
MARCO REFERENCIAL

2.1 Antecedentes

Para determinar los trabajos relacionados con la presente propuesta de investigación, se ha realizado una revisión de literatura preliminar, siguiendo un protocolo de búsqueda estandarizado para estudios de esta naturaleza. En primera instancia, se definió una cadena de búsqueda orientada a contestar la interrogante de investigación: ¿De qué manera la implementación del protocolo RPKI en los enrutadores de borde de Airmaxtelecom contribuye a prevenir el secuestro de rutas IPv4 mediante la validación del origen de los anuncios BGP?

Cadena de búsqueda utilizada, para encontrar los artículos relevantes que permitan abordar estas interrogantes, se construyó la siguiente cadena de búsqueda: ("All Metadata":RPKI) OR ("All Metadata":Resource Public Key Infrastructure) AND ("All Metadata":BGP hijacking) OR ("All Metadata":prefix hijacking) AND ("All Metadata":route hijacking). La cadena planteada busca combinar términos relacionados con los mecanismos de validación de rutas (RPKI) y las principales amenazas de seguridad, secuestro de prefijos y rutas en BGP hijacking.

La cadena de búsqueda fue ejecutada principalmente en la base de datos IEEE Xplore, reconocida por su alta calidad, rigor científico y pertinencia en las áreas de ingeniería y tecnologías de la información. Así mismo se establecieron criterios de inclusión orientados a garantizar la selección de estudios relevantes, actualizados y alineados con los objetivos de la investigación. Se aplicaron los siguientes criterios de inclusión:

- Artículos publicados en los últimos cinco (5) años, como conferencias y artículos de alto nivel.
- Artículos que hagan referencia explícita a eventos de BGP hijacking, prefix hijacking o route hijacking en el contexto de validaciones basadas en RPKI.

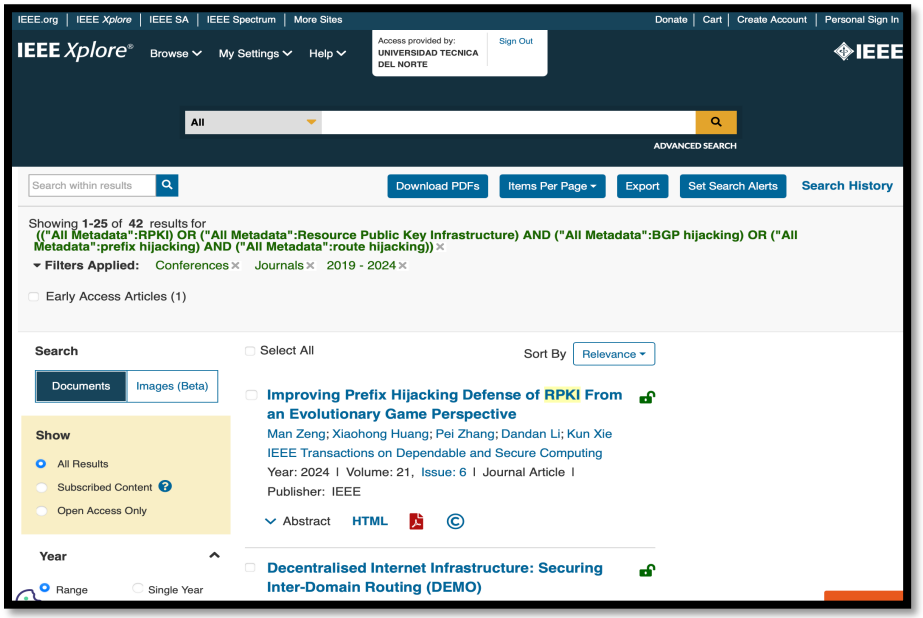
Con respecto a los resultados de la búsqueda, se obtuvo un total de 42 publicaciones distribuidas entre artículos científicos indexados, conferencias especializadas y trabajos de

investigación aplicada relacionados con seguridad de enrutamiento, BGP hijacking y Resource Public Key Infrastructure (RPKI). Posteriormente, se realizó un proceso de depuración y evaluación metodológica basado en los criterios de inclusión previamente establecidos, considerando aspectos como actualidad de la publicación, pertinencia temática, enfoque técnico, aplicabilidad en entornos ISP y relación directa con mecanismos de validación de rutas mediante RPKI y ROV. Como resultado de esta revisión preliminar, los 42 documentos fueron considerados relevantes para el contexto general de la investigación.

Sin embargo, únicamente 15 artículos fueron seleccionados para el análisis crítico y detallado del estado del arte, debido a que presentaban un mayor nivel de aporte científico, profundidad técnica y evidencia empírica relacionada con la mitigación de ataques BGP hijacking y la implementación práctica de RPKI en infraestructuras de red. Los artículos restantes fueron excluidos del análisis exhaustivo por presentar información redundante, enfoques teóricos similares, limita relación con el objetivo específico del estudio o menor profundidad metodológica. En la figura 1 se resume el proceso de identificación, filtrado y selección de publicaciones utilizadas en la investigación.

Figura 1

Verificación de cadena de búsqueda en la IEEE Explore



Nota. Captura de pantalla de IEEE Xplore donde se evidencia la cadena de búsqueda utilizada para recuperar estudios relacionados con RPKI y ataques BGP hijacking. El prompt empleado fue: *("All Metadata":RPKI)*

OR ("All Metadata":"Resource Public Key Infrastructure") AND ("All Metadata":"BGP hijacking") OR ("All Metadata":"prefix hijacking") AND ("All Metadata":"route hijacking"). Elaboración propia.

Posteriormente, se realizó el análisis de los resúmenes de los 15 artículos seleccionados preliminarmente, con el propósito de identificar aquellos estudios con mayor pertinencia:

Según Friedemann (2022) la implementación del Resource Public Key Infrastructure (RPKI) ha cobrado relevancia mundial como respuesta a los riesgos persistentes del secuestro de rutas BGP y otras amenazas en el plano de enrutamiento de Internet. El estudio destaca que la validación del origen de rutas (ROV) basada en RPKI permite a los sistemas autónomos (AS) verificar la legitimidad de los anuncios de prefijos IP, mejorando así tanto la integridad como la resiliencia del servicio, pues esta tecnología es considerada esencial para los operadores de red que buscan minimizar interrupciones y garantizar servicios estables frente a ataques deliberados o errores de configuración (Li & Lin, 2023).

En la propuesta de He (2021) se plantea una alternativa descentralizada llamada cadena de confianza RPKI (ROAchain), basada en blockchain, que busca mitigar las limitaciones del modelo jerárquico tradicional del RPKI. El estudio sugiere que, al distribuir el control de los certificados de autorización de rutas (ROA), se mejora la transparencia, la trazabilidad de eventos y la resistencia ante manipulaciones externas, lo cual es especialmente útil para entornos ISP que operan en regiones donde la confianza en las autoridades centrales es limitada.

Por otra parte, Wang (2024) presentan a Resource Public Key Infrastructure RPKI Sentinel (RPKI), una plataforma de control de emergencia en el enrutamiento que permite revocar rutas maliciosas o redirigir tráfico de alto volumen durante incidentes de seguridad, utilizando la política local *Simplified Local Internet Number Resource Management with the NIR System* (SLURM), esta solución ha demostrado una capacidad de respuesta inferior a 70 ms y una precisión superior al 98 %, lo que respalda su aplicabilidad en la protección proactiva de los proveedores de servicio de internet de tamaño mediano.

Por otro lado, Li (2022) propone una mejora en la codificación de los ROA mediante el concepto de Hanging ROA, un esquema que, además de mantener la seguridad, logra

mejorar la eficiencia de procesamiento y sincronización de validaciones en los routers. De esta manera se contribuye a reducir la latencia y el uso de recursos en el plano de control, promoviendo una experiencia de usuario más fluida y un servicio más confiable en contextos de alta demanda de los usuarios finales.

Según Milolidakis (2023) menciona que el secuestro de rutas BGP (BGP hijacking) sigue siendo una de las amenazas más persistentes contra la infraestructura de enrutamiento de Internet, afectando a organizaciones como Amazon, Google y entidades gubernamentales. A través de simulaciones y experimentos reales con la plataforma PEERING, los autores demostraron que atacantes sofisticados pueden evitar ser detectados por colectores de rutas públicos mediante técnicas como el AS-path poisoning y anuncios selectivos, lo que les permite desviar tráfico sin ser identificados. De esta manera la vulnerabilidad pone en entredicho la eficacia de los sistemas de monitoreo actuales y resalta la urgencia de mecanismos de validación más robustos como el RPKI.

En el análisis realizado por Jaw (2024) se identificó que el 22.9 % de los anuncios de prefijos por parte de sistemas autónomos con comportamiento sospechoso eran inválidos bajo RPKI, lo que indica la existencia de una proporción considerable de posibles ataques de BGP hijacking que no están siendo mitigados adecuadamente. Además, se observó que muchos de estos anuncios eran aceptados por otras redes, evidenciando la falta de adopción de validación de origen de rutas (ROV) en una parte significativa del ecosistema global, esta carencia permite que anuncios maliciosos sigan teniendo efecto operativo en la red global de Internet.

Por otro lado, Rodday (2024) destaca que la implementación de políticas de seguridad de enrutamiento basadas en RPKI puede servir como medida preventiva eficaz frente a ataques de hijacking, pero también advierten que errores en la configuración de los ROA pueden producir falsos positivos y afectar la disponibilidad del servicio. Por lo cual, la situación puede generar resistencia en algunos operadores para aplicar políticas de rechazo automático de rutas inválidas, lo que perpetúa la vulnerabilidad de las rutas legítimas frente a ataques de secuestro.

Desde una perspectiva más técnica, Xu (2019) explican que el atributo AS_PATH del protocolo BGP registra la secuencia de sistemas autónomos (AS) por los que atraviesa una ruta antes de llegar a su destino, permitiendo identificar el origen y recorrido de los anuncios de enrutamiento. Sin embargo, debido a la ausencia de mecanismos nativos de validación criptográfica, este atributo puede ser manipulado por actores maliciosos para falsificar rutas aparentemente legítimas. En este sentido, los ataques de BGP hijacking pueden clasificarse según el prefijo afectado y el tipo de alteración aplicada sobre el AS_PATH, utilizando técnicas que desvían tráfico hacia redes no autorizadas y dificultan su detección mediante mecanismos tradicionales de monitoreo.

Hlavacek et al., (2018) subrayan que la resiliencia ante ataques de BGP hijacking no depende únicamente de la adopción de RPKI, sino también de la robustez del ecosistema de validadores, la disponibilidad de los repositorios RPKI y la correcta sincronización de datos entre los participantes. En este sentido, medir y mejorar la resiliencia del sistema completo se convierte en una prioridad, ya que fallos en cualquiera de estos componentes pueden abrir la puerta a ataques exitosos aun cuando existan ROAs correctamente configurados.

Por otro lado, Ebrima et al. (2026)analizan la evolución de eventos seriales de BGP hijacking y evidencian que una proporción significativa de anuncios inválidos continúa propagándose en Internet a pesar de la existencia de mecanismos de validación basados en RPKI. Los autores identifican que aproximadamente el 22.9 % de los eventos estudiados infringían validaciones de origen de rutas, lo que demuestra que la adopción parcial de políticas ROV entre sistemas autónomos limita la efectividad de las estrategias actuales de mitigación. En este contexto, el estudio destaca la necesidad de incrementar la implementación coordinada de validación de rutas para fortalecer la seguridad y resiliencia del ecosistema global de enrutamiento BGP.

Por otro lado, Mitseva et al. (2020) señalan que el protocolo BGP mantiene vulnerabilidades críticas debido a la ausencia de mecanismos nativos de autenticación y validación de rutas, lo que facilita ataques como prefix hijacking y route leaks. A través de la revisión de amenazas y mecanismos de defensa, los autores destacan que las tecnologías basadas en Resource Public Key Infrastructure (RKPI) constituyen una de las alternativas más efectivas para fortalecer la seguridad del enrutamiento interdominio. Sin embargo,

advierten que la limitada adopción global y las dificultades operativas de implementación continúan reduciendo la efectividad de estas soluciones frente a incidentes de secuestro de rutas en internet.

Por otro lado, Tsai et al. (2021) proponen un mecanismo denominado SD-BROV, basado en la integración de tecnologías Software Defined Networking (SDN) y Resource Public Key Infrastructure (RPKI) para fortalecer la validación de origen de rutas BGP en puntos de intercambio de internet. Por lo cual destacan que la combinación de detección y mitigación frente a ataques de BGP hijacking. Sin embargo, señalan que la efectividad del modelo depende de la interoperabilidad entre las plataformas de validación y de la capacidad de adaptación de la infraestructura de red frente a cambios dinámicos en el enrutamiento.

De acuerdo con Mirdita et al. (2023) analizan las vulnerabilidades presentes en implementaciones de validadores Resource Public Key Infrastructure (RPKI), evidenciando que fallos en los procesos de validación pueden comprometer la seguridad del enrutamiento BGP y facilitar ataques de secuestro de rutas. Los autores identifican inconsistencias críticas en distintos validadores Route Origin Validation (ROV), capaces de degradar los mecanismos de verificación y permitir la aceptación errónea de anuncios maliciosos. En este sentido, el estudio destaca la necesidad de fortalecer los procesos de auditoría y validación en infraestructuras RPKI para garantizar la confiabilidad y resiliencia del ecosistema global de enrutamiento.

Según Fontugne et al. (2021) presentan RPKI MIRO como una herramienta orientada al monitoreo e inspección de objetos Resource Public Key Infrastructure (RPKI) diseñada para detectar inconsistencias y anomalías en certificados y objetos ROA utilizados en la validación de rutas BGP. Por lo tanto, destacan que el monitoreo continuo de repositorios RPKI permitiendo identificar errores de configuración, objetos expirados y eventos que pueden comprometer la efectividad de Route Origin Validation (ROV). En este sentido, el estudio evidencia que la supervisión activa de la infraestructura RPKI constituye un componente fundamental para fortalecer la seguridad y confiabilidad del ecosistema de enrutamiento global.

Por otro lado, Kowalski et al. (2023) realizan una revisión integral sobre seguridad del enrutamiento en redes de área amplia, abordando amenazas asociadas al protocolo BGP, mecanismos de prevención y estrategias de mitigación basadas en validación de rutas. Los autores destacan que la adopción de tecnologías como Resource Public Key Infrastructure (RPKI) y Route Origin Validation (ROV) representa un avance significativo para fortalecer la seguridad del ecosistema de Internet. Sin embargo, señalan que la implementación heterogénea entre sistemas autónomos y la falta de coordinación global continúan siendo factores que limitan la efectividad de las medidas de protección frente a ataques de secuestro y filtrado de rutas.

Conclusión de la revisión de literatura:

En base al análisis de los estudios citados se determina que existen múltiples enfoques, tecnologías emergentes y mecanismos de mejora orientados a fortalecer la seguridad del enrutamiento interdominio mediante la implementación del Resource Public Key Infrastructure (RPKI). Las investigaciones revisadas abordan desde soluciones descentralizadas como ROAchain, hasta plataformas reactivas como RPKI Sentinel y optimizaciones en los esquemas de codificación de ROAs. Asimismo, se evidencia que el secuestro de rutas BGP (BGP hijacking) continúa siendo una amenaza latente debido a la baja adopción de validación de rutas (ROV) y a la falta de sincronización efectiva entre sistemas autónomos. A continuación, se resume lo más relevante en la Tabla 1:

Tabla 1

Sistema RPKI y BGP Hijacking

Art. N°	Autor	Año de publicación	Entorno tecnológico	Factores de éxito	Factores de riesgo / hallazgos clave
1	Friedemann, P. H., Rodda, N., & Rodosek, G. D.	2022	Infraestructura global RPKI	Uso de validadores robustos, sincronización eficiente y adopción de ROV	Falta de adopción plena y sincronización entre AS limita efectividad
2	He, G., Su, W., Gao, S., Yue, J., & Das, S. K.	2021	ISP y redes distribuidas	Arquitectura descentralizada para mayor trazabilidad y	Centralización de RPKI tradicional expone a

				resistencia a manipulaciones	vulnerabilidades estructurales
3	Wang, Y., Xu, M., Hua, C., Zhang, J., Li, K., Li, Z., & Yang, B.	2024	Proveedores de servicios de internet	Reacción rápida ante incidentes mediante revocación/redirección de rutas (SLURM)	Falsos positivos pueden afectar disponibilidad si no se configuran adecuadamente
4	Li, Y., Zou, H., Chen, Y., Xu, Y., Ma, Z., Ma, D., Hu, Y., & Xie, G.	2022	Redes con alta demanda de tráfico	Compresión eficiente de ROAs para reducir latencia y uso de recursos	Mayor complejidad de implementación inicial en routers
5	Milolidakis, A., Bühler, T., Wang, K., Chiesa, M., Vanbever, L., & Vissicchio, S.	2023	Entornos académicos y simulados	Evasión de detección por parte de atacantes mediante AS-path poisoning	Limitada cobertura de colectores públicos para detectar ataques sofisticados
6	Jaw, E., Müller, M., Hesselman, C., & Nieuwenhuis, L.	2024	Redes de datos (Route Collectors)	Alta proporción de prefijos inválidos aceptados por la red, bajo uso de ROV	Anuncios inválidos siguen siendo aceptados por muchas redes
7	Rodday, N., Cunha, Í., Bush, R., Katz-Bassett, E., Rodosek, G. D., Schmidt, T. C., &	2024	Normativa y políticas de seguridad	Mejora en políticas de seguridad con base en implementación de RPKI	Errores de configuración pueden generar rechazo de rutas legítimas

	Wählisch, M.				
8	Xu, W., Chang, D., & Li, X. (s/f).	2019	Entorno técnico de validación BGP	Clasificación de ataques y validación de AS_PATH para detección precisa	Ataques sigilosos con prefijos exactos son difíciles de detectar sin validación
9	Hlavacek, T., Herzberg, A., Shulman, H., & Waidner, M.	2018	Infraestructura operativa de validadores	Evaluación combinada control/data-plane para caracterizar debilidades del sistema	La efectividad depende del ecosistema completo, repositorio, validador, sincronización)
10	Ebrina J, Müller, M.; Hesselman, C.; Nieuwenhuis , L. J. M.	2026	Enrutamiento BGP y eventos de secuestro de rutas	Reproducción y evaluación de eventos seriales de BGP hijacking	Evolución y persistencia de eventos de secuestro de rutas en Internet
11	Mitseva, A., Kotronis, V., et al.	2020	Seguridad del enrutamiento BGP e Internet global	Implementación de mecanismos de validación y defensa basados en RPKI	La ausencia de autenticación nativa en BGP facilita ataques como prefix hijacking y route leaks, limitando la seguridad
12	Tsai, P. W., et al.	2021	Puntos de intercambio de Internet (IXP), SDN y validación RPKI	Integración de SDN y RPKI para mejorar la detección y mitigación de ataques BGP hijacking	La interoperabilidad entre plataformas y la adaptación dinámica de la infraestructura influyen en la efectividad del

					sistema de validación
13	Mirdita, D., Schulmann, H., Vogel, N., & Waidner, M.	2023	Infraestructura RPKI y validadores Route Origin Validation (ROV)	Fortalecimiento de procesos de validación y auditoría en sistemas RPKI	Vulnerabilidades e inconsistencias en validadores pueden degradar la validación y permitir la aceptación de anuncios BGP maliciosos
14	Fontugne, R., Shah, A., & Aben, E.	2021	Infraestructura RPKI y monitoreo de objetos ROA	Monitoreo continuo e inspección de objetos RPKI para fortalecer la validación de rutas	Errores de configuración y anomalías en objetos ROA pueden comprometer la efectividad de Route Origin Validation (ROV)
15	**Kowalski, M., et al.**	**2023**	**Seguridad del enrutamiento en redes WAN y protocolo BGP**	**Implementación de RPKI y ROV para fortalecer la validación de rutas**	**La implementación heterogénea y la falta de coordinación global limitan la efectividad frente a ataques de secuestro y filtrado de rutas**

Nota. La tabla presenta una síntesis de estudios relacionados con la implementación de Resource Public Key Infrastructure y los ataques de BGP Hijacking, destacando aplicaciones, beneficios, riesgos y hallazgos relevantes en entornos de seguridad del enrutamiento en Internet. Elaboración propia.

Las organizaciones del sector de telecomunicaciones y tecnología han comenzado a adoptar mecanismos establecidos como el Resource Public Key Infrastructure (RPKI) para fortalecer la validación de rutas BGP y prevenir incidentes de secuestro de rutas (BGP

hijacking). La implementación de RPKI ha sido aplicada en redes de distintos tamaños: desde proveedores de servicios locales hasta operadores de infraestructura global, así como también en entornos académicos, gubernamentales y de investigación.

Entre los beneficios identificados se encuentra la mejora sustancial de la integridad del enrutamiento global, la reducción de propagación de rutas inválidas y la mitigación proactiva de ataques que comprometen la disponibilidad del servicio. Sin embargo, uno de los principales retos radica en los costos de adopción y en la necesidad de contar con personal técnico especializado que conozca el ecosistema RPKI (validadores, ROAs, sincronización con repositorios de Registro Regionales de Internet), así como en las dificultades de coordinación entre múltiples Sistemas Autónomos (AS) para alcanzar una validación efectiva (Rodday & Cunha, 2024).

Es necesario interpretar con precaución ciertos resultados reportados en estudios previos. Por ejemplo, Milolidakis et al., (2023) señalan que los atacantes aún pueden evadir los mecanismos de detección tradicionales si los colectores de rutas no están adecuadamente distribuidos. En este mismo sentido, algunos modelos de despliegue presentan limitaciones si no se acompañan de políticas de rechazo automatizado en los routers BGP.

De acuerdo con el análisis de la literatura, la presente propuesta de implementación de RPKI aplicada a un Proveedor de Servicio de Internet (ISP) regional como Airmaxtelecom Soluciones Tecnológicas S.A. puede contribuir al fortalecimiento del ecosistema de enrutamiento seguro en Ecuador y Regional. Además, puede servir como modelo replicable para otros ISP o entidades que gestionan infraestructura crítica o servicios digitales expuestos a ataques de red.

2.2 Marco Teórico

2.2.1 Introducción a la seguridad de enrutamiento BGP

El Border Gateway Protocol (BGP) es el protocolo de enrutamiento que permite el intercambio de información de accesibilidad entre sistemas autónomos (AS) en Internet. Establecido en su versión actual como BGP-4 (RFC 4271), constituye la base sobre la cual se sustenta la conectividad global de la red, facilitando la propagación eficiente de rutas IP entre entidades administrativas independientes (Scott & Johnstone, 2024). Sin embargo, uno

de los principales problemas que enfrenta este protocolo es su diseño orientado a la funcionalidad más que a la seguridad.

BGP opera sobre una arquitectura distribuida y basada en la confianza implícita entre pares, lo cual lo hace inherentemente vulnerable a ataques como el secuestro de prefijos (prefix hijacking), la falsificación de rutas mediante manipulación del atributo AS_PATH, y los route leaks. Las vulnerabilidades permiten que un actor malicioso o mal configurado propague anuncios de rutas incorrectos, los cuales son aceptados y reenviados por otros sistemas autónomos sin verificación, afectando la integridad y disponibilidad del tráfico global (Bush & Austein, 2020).

A lo largo del tiempo, diversos incidentes han evidenciado las limitaciones de seguridad de BGP. Uno de los casos más conocidos ocurrió en 2008, cuando Pakistan Telecom, al intentar bloquear el acceso local a YouTube, anunció incorrectamente un prefijo que abarcaba toda la red del servicio de video, provocando una interrupción global durante varias horas (Ciaffaglione & Scagnetto, 2025). De manera similar, en 2018, un incidente de BGP hijacking permitió que una parte del tráfico hacia Amazon Web Services fuera redirigido a través de una red de minería de criptomonedas, lo que ocasionó pérdidas económicas y exposición de datos sensibles (Apostolaki & Zohar, 2017)

Los eventos demuestran que las debilidades estructurales de BGP pueden ser explotadas para comprometer la confiabilidad del ecosistema de Internet. En consecuencia, la comunidad técnica y los organismos de gobernanza de Internet han promovido la adopción de mecanismos de seguridad como el Resource Public Key Infrastructure (RPKI), orientados a validar la legitimidad de los anuncios de rutas y mitigar los riesgos asociados al enrutamiento inseguro. De este modo, se podría fortalecer la seguridad del plano de control del enrutamiento, por tanto, es un objetivo estratégico para proteger la infraestructura crítica digital a nivel mundial (Rodday & Cunha, 2024).

2.2.2 Origen y fundamento del RPKI

El Resource Public Key Infrastructure (RPKI) surge como una solución técnica a los problemas estructurales de seguridad del Border Gateway Protocol (BGP), en particular

frente a la suplantación de prefijos y otras formas de manipulación del enrutamiento global de Internet. La necesidad de un mecanismo confiable para validar la legitimidad de los anuncios de rutas fue reconocida por la comunidad técnica a través del grupo de trabajo Secure Inter-Domain Routing (SIDR) del Internet Engineering Task Force (IETF), lo que condujo a la estandarización del RPKI en el año 2012 mediante el RFC 6480 (Carle & Ott, 2021).

De acuerdo con Akiwate et al., (2020) el fundamento de RPKI se basa en la criptografía de clave pública y sigue una arquitectura jerárquica que permite a los Registros Regionales de Internet (RIRs) como LACNIC en América Latina y el Caribe emite certificados X.509 vinculados a recursos de numeración IP y números de sistemas autónomos (ASN). A través de estos certificados, los titulares de recursos pueden publicar objetos conocidos como Route Origin Authorizations (ROA), los cuales especifican qué sistemas autónomos están autorizados a anunciar determinados prefijos IP, pues los objetos se almacenan en repositorios públicos y son consultados por validadores RPKI para determinar la validez de los anuncios recibidos vía BGP (Li et al.,2022).

El RPKI forma así una infraestructura de confianza que permite a los routers BGP aplicar políticas de validación denominadas Route Origin Validation (ROV), lo que permite rechazar anuncios considerados inválidos. A diferencia de otros enfoques más complejos como BGPsec, RPKI y ROV han demostrado ser viables en implementaciones reales sin introducir una sobrecarga significativa en el plano de control (Kristoff & Bush, 2020).

La implementación del RPKI ha avanzado progresivamente en varias regiones del mundo. En América Latina, LACNIC ha desempeñado un papel central en la difusión de esta tecnología, facilitando herramientas de implementación y capacitando a operadores de red para emitir y gestionar sus ROA (Nawrocki & Koch, 2021). Gracias a esta infraestructura, se ha logrado una mayor visibilidad, trazabilidad y control sobre los anuncios de rutas, lo que representa un avance significativo en la mitigación de incidentes de enrutamiento malicioso o accidental.

2.2.3 Identificación de amenazas en BGP

Según Scott (2024) una de las principales vulnerabilidades radica en que los anuncios de rutas recibidos por los routers BGP no son validados criptográficamente, lo que permite que se propaguen rutas falsas o manipuladas con facilidad. Una de las amenazas más conocidas es el secuestro de prefijos en el cual un sistema autónomo malicioso o mal configurado anuncia un prefijo IP que no le pertenece. Por lo tanto, este tipo de ataque puede resultar en la redirección del tráfico legítimo hacia rutas no autorizadas, permitiendo desde la interrupción del servicio hasta la interceptación de información.

Un caso paradigmático que evidencia las limitaciones estructurales del Border Gateway Protocol ocurrió en el año 2008, cuando Pakistan Telecom, en un intento por restringir el acceso a la plataforma YouTube a nivel local, anunció de manera errónea un prefijo IP más específico que el legítimo correspondiente al servicio. Debido al modelo de enrutamiento basado en confianza implícita que caracteriza a BGP, dicho anuncio fue aceptado y propagado por múltiples sistemas autónomos a nivel global, redirigiendo el tráfico destinado a YouTube hacia una red no autorizada. El evento generó una interrupción masiva del servicio durante varias horas, afectando a millones de usuarios en distintas regiones del mundo (Mahajan & Rodrig, 2020).

Más allá de tratarse de un error de configuración, este incidente puso en evidencia la fragilidad del enrutamiento interdominio, demostrando cómo una acción local puede escalar rápidamente a un problema global en ausencia de mecanismos de validación de origen de rutas, lo que ha motivado el desarrollo e implementación de soluciones como el RPKI para mitigar este tipo de vulnerabilidades.

Otra amenaza relevante es el envenenamiento de rutas que consiste en manipular la información del AS_PATH para alterar la selección de rutas por parte de otros sistemas autónomos. Aunque algunas técnicas de envenenamiento han sido utilizadas con fines defensivos, también pueden ser explotadas para desviar el tráfico o provocar inestabilidad en la red ((Schomp & Bhardwaj, 2020). El falsificado del atributo AS_PATH también representa una amenaza significativa, ya que los atacantes pueden insertar o eliminar identificadores de sistemas autónomos para modificar la aparente legitimidad de una ruta,

esto puede causar que el tráfico pase por rutas inesperadas o maliciosas, comprometiendo su integridad y privacidad (Scott & Johnstone, 2024)

Del mismo modo, los llamados route leaks, donde un sistema autónomo redistribuye rutas de una fuente a destinos no previstos, por ejemplo, entre dos proveedores que introducen trayectorias subóptimas y pueden sobrecargar enlaces críticos. Por lo tanto, estos incidentes no siempre son maliciosos, pero su impacto en la eficiencia del enrutamiento es significativo (Shen & Wang, 2024).

La falta de mecanismos para verificar la autenticidad de los anuncios BGP sigue siendo el principal facilitador de estas amenazas, esta situación evidencia la necesidad urgente de mecanismos de validación como el RPKI, que permite verificar si un anuncio es legítimo a través de certificados criptográficos. La implementación de RPKI y la validación del origen de rutas (ROV) se presentan como medidas efectivas para contrarrestar muchas de estas vulnerabilidades (Wirtgen & Bonaventure, 2022).

2.2.4 Validación del origen de rutas: Route Origin Validation (ROV)

Según Li y Lin (2023) la Route Origin Validation (ROV) es un mecanismo derivado de la implementación del Resource Public Key Infrastructure (RPKI) que permite a los routers BGP verificar la legitimidad de los anuncios de rutas, específicamente si el sistema autónomo (AS) que anuncia un prefijo IP está autorizado para hacerlo. La validación se realiza mediante la comparación de los anuncios BGP con los objetos ROA (Route Origin Authorizations) publicados en los repositorios RPKI. Si el anuncio coincide con un ROA válido, se clasifica como “válido”; si contradice un ROA, como “inválido”; y si no existe información suficiente, como “desconocido”.

La funcionalidad de ROV se implementa en el plano de control de los routers BGP, y su principal objetivo es prevenir el secuestro de prefijos, que ocurre cuando un AS anuncia bloques IP que no le han sido asignados. Mediante políticas de enrutamiento definidas por cada operador, es posible rechazar rutas inválidas o darles una prioridad menor. De esta forma, ROV fortalece la integridad del sistema de enrutamiento y reduce la propagación de rutas maliciosas o erróneas (Schmidt & Irazabal, 2021).

A diferencia de soluciones más complejas como BGPsec, que implican la firma criptográfica de todo el camino AS_PATH, ROV es relativamente fácil de implementar y no requiere cambios significativos en la infraestructura de los operadores, pues su adopción se ha acelerado gracias al soporte de diversos fabricantes de hardware de red y validadores como Routinator, rpki-client y FORT Validator, que permiten sincronizar localmente los datos de los repositorios RPKI y generar listas de prefijos válidos para ser utilizadas por los routers (Schmidt & Irazabal, 2021).

La efectividad de ROV depende del nivel de implementación de RPKI y de la cooperación entre redes. Según estudios realizados por el IETF, si bien ROV no puede eliminar todos los vectores de ataque en BGP, sí reduce de manera significativa la superficie de exposición al filtrar rutas que no están respaldadas por certificados válidos (Jawad & Matic, 2022). Además, la evidencia empírica sugiere que su adopción masiva contribuiría a la reducción de incidentes como el secuestro de tráfico, route leaks y envenenamiento de rutas.

En regiones como América Latina y el Caribe, la implementación de ROV está en crecimiento gracias a los esfuerzos de LACNIC y las campañas de concienciación impulsadas por MANRS (Piet & Nwoji, 2023). La experiencia demuestra que la combinación de capacitación técnica, herramientas accesibles y regulación adecuada puede acelerar la adopción de esta medida de seguridad esencial para un ecosistema de Internet más confiable.

2.2.5 Herramientas y plataformas de mitigación

La mitigación de vulnerabilidades en el sistema de enrutamiento BGP requiere de un conjunto de herramientas y plataformas que permitan detectar, prevenir y responder eficazmente ante incidentes como el secuestro de rutas, route leaks y envenenamiento de caminos. Las soluciones se dividen en dos grandes categorías: las que implementan directamente mecanismos de validación de rutas, como RPKI y ROV, y las que ofrecen capacidades de monitoreo, visualización y alerta ante comportamientos anómalos (Meng & Guo, 2022).

Entre las herramientas orientadas a la validación de rutas RPKI destacan Routinator desarrollado por Nlnet Labs, rpki-client proyecto del equipo de OpenBSD y FORT Validator

creado por NIC México, permiten a los operadores mantener una copia local sincronizada de los certificados y objetos ROA publicados por los repositorios RPKI. De este modo, los routers pueden aplicar políticas de validación de rutas en tiempo real sin depender de una conexión constante a los servidores remotos (Anderson & Salamatian, 2022)Su instalación es compatible con sistemas operativos tipo UNIX, y suelen integrarse fácilmente en infraestructuras existentes de ISPs o centros de datos.

Por otro lado, existen herramientas de monitoreo como RIPEstat, BGPMon, BGPStream de caída, Radar Qrator, BGP HE y Cloudflare Radar, que permiten observar la visibilidad de prefijos en la tabla global de rutas, identificar anomalías en el comportamiento de propagación y recibir alertas en tiempo real sobre posibles incidentes de seguridad. Por consiguiente, las plataformas recopilan datos de colectores de rutas globales y redes participantes, ofreciendo visualizaciones sobre rutas válidas, inválidas y fugas de rutas (leaks), además de información histórica para análisis forense (Kunze & Wehrle, 2021).

Una iniciativa relevante a nivel global es MANRS (Mutually Agreed Norms for Routing Security), liderada por Internet Society, que define un conjunto de buenas prácticas para operadores de red, proveedores de tránsito, IXPs y CDN. Estas recomendaciones incluyen la implementación de RPKI, filtrado de prefijos, coordinación y reporte de incidentes. MANRS también proporciona herramientas de validación y evaluación del estado de las redes respecto a las normas recomendadas (Mutually Agreed Norms for Routing Security, 2026)

Asimismo, algunos fabricantes de equipos de red como Cisco, Juniper y MikroTik han incorporado en sus sistemas operativos soporte nativo para RPKI, lo cual ha facilitado su despliegue a gran escala. Los dispositivos permiten a los operadores aplicar filtros basados en los resultados de validación (valid, invalid, not found), y definir rutas de respaldo o alternativas para mantener la continuidad del servicio (Mutually Agreed Norms for Routing Security, 2026).

El uso combinado de estas herramientas permite crear una infraestructura de defensa en profundidad, donde la validación de origen, el monitoreo en tiempo real y la colaboración comunitaria actúan de forma complementaria para proteger el sistema de enrutamiento. La

adopción de estas plataformas en América Latina ha sido impulsada por LACNIC mediante capacitaciones técnicas, laboratorios virtuales y recursos educativos, con el objetivo de fortalecer la resiliencia de la región ante incidentes de enrutamiento.

2.2.6 Evaluación de riesgos en infraestructura de ISP

La evaluación de riesgos en la infraestructura de los Proveedores de Servicios de Internet (ISP) es un componente esencial para garantizar la continuidad operativa, la seguridad de los servicios de conectividad y la protección del ecosistema digital en su conjunto. Dado que los ISP gestionan redes troncales y sistemas autónomos que participan activamente en el enrutamiento. Por ello, una adecuada gestión del riesgo debe contemplar tanto las vulnerabilidades técnicas como los impactos operacionales, legales y reputacionales asociados.

De acuerdo con Ortiz y Vizñay (2020) el proceso de evaluación de riesgos en los ISP debe comenzar con la identificación de activos críticos, tales como routers de borde, servidores de validación, enlaces de tránsito, configuraciones de políticas BGP y certificados RPKI. Posteriormente, se realiza un análisis de amenazas, que incluye tanto eventos externos (ataques de secuestro de rutas, campañas de desinformación, errores en terceros) como internos (fallas de configuración, negligencia operativa, exposición de credenciales). Estos riesgos deben evaluarse bajo criterios de probabilidad e impacto, para así priorizar acciones correctivas y preventivas (ISO/IEC 27005: 2018, 2018)

Una de las debilidades más críticas identificadas en entornos de proveedores de servicios de Internet (ISP) radica en la falta de mecanismos robustos para la validación del origen de rutas, como el Resource Public Key Infrastructure (RPKI). Esta carencia facilita que anuncios de rutas no autorizadas sean aceptados y difundidos dentro del sistema de enrutamiento, comprometiendo no solo la estabilidad del ISP afectado, sino también la de sus clientes y redes de tránsito asociadas, generando efectos encadenados de alcance amplio (Zapata & Páez, 2026). En este contexto, coinciden en que aquellos ISP que no incorporan controles de validación son significativamente más vulnerables, tanto a convertirse en víctimas de ataques de enrutamiento como a actuar, de manera involuntaria, como intermediarios en la propagación de rutas maliciosas.

Además, la gestión de riesgos debe incorporar la evaluación de la resiliencia operativa, lo cual implica verificar la redundancia de rutas, la capacidad de detección temprana de incidentes y la existencia de protocolos de respuesta y recuperación, esto es especialmente importante en el caso de países con limitada infraestructura física, donde la conectividad depende en gran parte de unos pocos enlaces internacionales o acuerdos de peering.

Los marcos metodológicos, como ISO/IEC 27005, NIST SP 800-30 y MAGERIT, ofrecen directrices sobre cómo evaluar, tratar y monitorear riesgos relacionados con la seguridad de la información y el enrutamiento. En el contexto ecuatoriano, estas metodologías pueden ser adaptadas al Esquema Gubernamental de Seguridad de la Información (EGSI) impulsado por el MINTEL, que establece criterios para proteger la infraestructura digital del país (Proaño, 2024).

En definitiva, la evaluación de riesgos en ISPs no debe limitarse a una auditoría puntual, sino que debe integrarse como una práctica continua, multidisciplinaria y proactiva. El monitoreo constante, la colaboración con organizaciones regionales como LACNIC y la inversión en tecnologías como RPKI representan pilares clave para reducir la exposición al riesgo y aumentar la confiabilidad de los servicios de Internet.

2.2.7 Participación de LACNIC en la implementación de RPKI

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC, 2023) desempeña un papel estratégico en la promoción, adopción y operación del Resource Public Key Infrastructure (RPKI) en la región, como uno de los cinco Registros Regionales de Internet (RIRs), LACNIC tiene la responsabilidad de administrar los recursos de numeración IP (IPv4, IPv6) y los números de sistema autónomo (ASN), además de facilitar mecanismos que garanticen la seguridad y estabilidad del enrutamiento.

Con el objetivo de fortalecer la resiliencia del ecosistema regional, LACNIC ofrece una plataforma integral de gestión de RPKI que permite a los titulares de recursos generar, administrar y revocar objetos Route Origin Authorization (ROA). Por lo cual, esta herramienta ha sido diseñada con una interfaz amigable y un alto grado de automatización, de modo que incluso operadores sin conocimientos criptográficos avanzados puedan

participar activamente en la validación de rutas. A través de esta plataforma, los operadores pueden establecer qué sistemas autónomos están autorizados para anunciar determinados prefijos IP, lo que permite proteger la integridad de la información propagada mediante BGP (AEPROVI, 2020).

Además de proveer la infraestructura técnica, LACNIC ha desplegado una serie de acciones educativas y de acompañamiento técnico en toda la región, incluyendo capacitaciones presenciales y virtuales, publicaciones, laboratorios prácticos, webinars y campañas de sensibilización sobre la importancia de RPKI. En este sentido, el rol pedagógico de LACNIC ha sido crucial para reducir las barreras de entrada y acelerar la adopción de esta tecnología entre pequeños y medianos ISP, universidades y entidades gubernamentales (LACNIC, 2023).

LACNIC también colabora activamente con iniciativas globales como MANRS (Mutually Agreed Norms for Routing Security), promovida por Internet Society, y participa en foros como IETF, ICANN y la Red de CSIRTs de América Latina, en donde promueve la interoperabilidad y el cumplimiento de estándares internacionales en la validación de rutas. Asimismo, publica regularmente estadísticas sobre la cobertura de RPKI en la región, permitiendo monitorear el crecimiento y detectar brechas o zonas con baja adopción (LANIC, 2026).

En el caso de Ecuador, la participación de LACNIC ha permitido que diversos actores incluyendo ISP, universidades, IXPs y organismos públicos inicien procesos de implementación de RPKI, contribuyendo así a reducir la superficie de ataque asociada a incidentes de BGP hijacking. Es decir, la colaboración técnica y comunitaria no solo ha fortalecido la infraestructura digital del país, sino que ha sentado las bases para la creación de políticas públicas orientadas a la seguridad del enrutamiento.

2.2.8 Incidentes de enrutamiento, integridad y rendimiento del servicio de Internet

Los incidentes de enrutamiento constituyen una de las amenazas más graves para la integridad, disponibilidad y rendimiento de los servicios de Internet. Pues los eventos que incluyen el secuestro de rutas (prefix hijacking), route leaks, falsificación de AS_PATH, o

propagación de rutas inválidas, pueden generar disrupciones significativas en la conectividad global. En un entorno altamente interconectado como el de hoy, un error o ataque local puede tener consecuencias globales, afectando a miles de sistemas autónomos, proveedores de servicios, aplicaciones y usuarios finales (Guerra, 2019).

Para contrarrestar estos riesgos, se han propuesto soluciones como la implementación del Resource Public Key Infrastructure (RPKI) y la Validación de Origen de Rutas (ROV). Al verificar que el AS anunciante está autorizado mediante objetos ROA firmados criptográficamente, los routers pueden rechazar rutas inválidas y prevenir muchos de estos incidentes antes de que se propaguen. Según estudios de Buenaño (2024) la adopción de RPKI puede reducir significativamente los casos de secuestro de rutas, siempre que los operadores configuren políticas estrictas de validación y rechazo.

No obstante, el impacto de los incidentes de enrutamiento va más allá del plano técnico. También afecta la confianza de los usuarios, la reputación de los operadores y puede tener consecuencias legales en casos de violación de datos o interrupción de servicios críticos. Por esta razón, la gestión proactiva del enrutamiento, el monitoreo en tiempo real y la cooperación entre operadores, reguladores y organismos técnicos como LACNIC e ISOC son claves para fortalecer la resiliencia del sistema global de Internet.

En conclusión, garantizar la integridad del enrutamiento y proteger el rendimiento del servicio requiere una combinación de medidas técnicas, marcos normativos y colaboración transnacional. El fortalecimiento del ecosistema mediante la adopción de RPKI, la implementación de estándares y el monitoreo continuo permitirá reducir la exposición a incidentes y sostener la estabilidad de los servicios digitales ante un entorno cada vez más dependiente de la conectividad segura.

2.3 Marco Legal

2.3.1 Obligaciones de los Proveedores de Servicio de Internet en Ecuador

En el contexto ecuatoriano, los Proveedores de Servicios de Internet (ISP) tienen responsabilidades fundamentales en el mantenimiento de la seguridad, integridad y continuidad operativa de las redes de telecomunicaciones. Estas obligaciones están reguladas

por un conjunto de normativas nacionales que buscan proteger tanto a los usuarios finales como a la infraestructura crítica del país.

Uno de los pilares normativos es la Ley Orgánica de Telecomunicaciones (2024) la cual establece que los proveedores deben garantizar la prestación eficiente, segura y continua del servicio, así como colaborar con las autoridades para la gestión de riesgos tecnológicos. De forma complementaria, la Ley Orgánica de Protección de Datos Personales (2021) exige la adopción de medidas técnicas que aseguren la confidencialidad, integridad y disponibilidad de los datos que circulan a través de sus redes, lo cual se relaciona directamente con la integridad del enrutamiento y la protección frente a incidentes como secuestros de rutas o interceptación no autorizada de tráfico.

De la misma forma, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ha emitido resoluciones que exhortan a los ISPs a implementar controles que mitiguen las vulnerabilidades del protocolo BGP. Aunque actualmente no existe una norma obligatoria para la implementación de RPKI, ARCOTEL promueve la adopción de estándares internacionales y buenas prácticas como las propuestas por el Esquema Gubernamental de Seguridad de la Información y la comunidad MANRS (Mutually Agreed Norms for Routing Security).

El EGSI, establecido mediante el Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003, plantea que las instituciones del sector público y por extensión, las entidades que operan infraestructura crítica de telecomunicaciones deben implementar sistemas de gestión de seguridad de la información (SGSI) alineados con la norma ISO/IEC 27001. Esto incluye la identificación de activos críticos, evaluación de amenazas, y aplicación de controles técnicos adecuados. En este contexto, la validación de rutas mediante RPKI puede ser considerada una medida concreta para mitigar riesgos en el plano de control del enrutamiento, fortaleciendo la postura de seguridad de los operadores.

Adicionalmente, los ISPs tienen la obligación de asegurar mecanismos de trazabilidad, reportar incidentes de seguridad a las autoridades competentes y garantizar la interoperabilidad de sus sistemas con las plataformas nacionales de ciberseguridad, como los centros de respuesta ante incidentes (CSIRT). La falta de implementación de estas medidas

puede no solo conllevar sanciones regulatorias, sino también generar impactos reputacionales y técnicos significativos, especialmente en un entorno donde la resiliencia digital es un factor clave para el desarrollo económico y social.

En resumen, los proveedores de servicios de Internet en Ecuador deben asumir un rol activo en la protección de la infraestructura de enrutamiento, promoviendo la adopción de tecnologías como RPKI, colaborando con organismos como LACNIC y ARCOTEL, y alineándose con marcos normativos nacionales e internacionales que refuerzan la seguridad del ecosistema de Internet.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 Descripción del área del estudio

El área de estudio de la presente investigación se desarrolla en la red troncal y de distribución del centro de datos de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A., ubicada en la ciudad de Ibarra, Ecuador. En primer lugar, a partir del diagnóstico realizado, se identificó que esta infraestructura constituye un componente crítico para la prestación del servicio de Internet, ya que soporta la conectividad de clientes residenciales, empresariales y entidades gubernamentales. En este contexto, el centro de datos dispone de equipos de enrutamiento de nivel proveedor que operan bajo el Border Gateway Protocol, así como de servidores DNS, sistemas de autenticación PPPoE, plataformas de monitoreo y enlaces de interconexión con proveedores de tránsito IP tanto a nivel nacional como internacional.

Por consiguiente, considerando que la estabilidad del enrutamiento exterior es un factor determinante para garantizar la disponibilidad y continuidad del servicio, el estudio se enfoca específicamente en el análisis e implementación de mecanismos de seguridad orientados a la validación de rutas. En este sentido, se incorpora el uso del Resource Public Key Infrastructure (RPKI), una tecnología desarrollada por la Internet Engineering Task Force y promovida en la región por LACNIC, la cual permite verificar la legitimidad de los anuncios de rutas BGP.

De manera operativa, el entorno de estudio comprende la configuración de routers principales, la implementación de servidores validadores y la gestión de bases de datos de autorizaciones de origen (ROA), todo ello se ejecuta dentro de un entorno controlado, lo que permite simular distintos escenarios de enrutamiento, tales como rutas legítimas, inválidas y no validadas. De esta forma, se busca analizar de manera precisa el comportamiento del sistema frente a posibles amenazas, así como evaluar el impacto de la implementación de RPKI en la seguridad y estabilidad de la red.

3.2 Enfoque y tipo de investigación

El enfoque adoptado en la presente investigación es de carácter cuantitativo en la medida en que se fundamenta debido a la recolección, medición y análisis de datos objetivos y verificables, orientados a explicar el comportamiento de las variables especificas dentro del sistema de enrutamiento (Rodríguez, 2020). En este sentido, su aplicación en el presente estudio se evidencia en el uso de indicadores técnicos medibles, tales como el número de rutas inválidas detectadas, la reducción de prefijos maliciosos aceptados, los niveles de latencia, el tiempo de convergencia del Border Gateway Protocol y las métricas de pérdida de paquetes. De acuerdo con Schomp y Bhardwaj (2020) las variables permiten evaluar de manera precisa el impacto de la implementación de mecanismos de seguridad como el RPKI y la Route Origin Validation (ROV) en la infraestructura del proveedor de servicios de Internet (ISP).

Asimismo, el estudio se enmarca en un tipo de investigación aplicada, ya que busca resolver un problema concreto en un contexto real, mediante la implementación de una solución tecnológica orientada a mejorar la seguridad del enrutamiento. Según Alarcón (2018) la investigación aplicada tiene como finalidad generar conocimiento útil para la solución de problemas prácticos, lo que se alinea con el propósito de este trabajo al evaluar el impacto del RPKI en una red operativa.

De igual manera, presenta un alcance descriptivo y explicativo, puesto que no solo describe el comportamiento de las variables analizadas, sino que también interpreta las relaciones causales entre la implementación de RPKI/ROV y la reducción de vulnerabilidades en el sistema de enrutamiento (Guevara, 2020).

3.3 Procedimiento de investigación

La metodología seguida en esta investigación se estructura las siguientes etapas:

3.3.1 Revisión bibliográfica y documental

La revisión metodológica permitió construir un marco teórico y un marco referencial robusto considerando el contexto global y regional en la adopción la adopción de RPKI, para ello se consultaron en bases especializadas documentos técnicos, estándares internacionales

y reportes de organismos en internet. Las fuentes técnicas vinculadas con RPKI, BGP, BGP hijacking y la seguridad del enrutamiento en redes para ISPs se basaron en la búsqueda de documentos de alto nivel como IEEE Xplore, Scopus, además de documentación técnica proporcionada por organismos como LACNIC y ICANN.

Tabla 2

Criterios de selección de fuentes para la revisión documentable

Criterio	Descripción
Temática	Relación con BGP, RPKI, ROA, ROV, BGP hijacking.
Validez técnica	Documentos de alto nivel, instituciones académicas y organizaciones como LACNIC, IETF, ICANN
Aplicabilidad	Documentación de los últimos 5 años para justificar la implementación de RPKI sobre la red central del ISP Airmaxtelecom Soluciones Tecnológicas S.A. con versiones actualizadas
Alcance geográfico	Inclusión de fuentes de contexto regional, global para contextualizar el estado del arte.

Nota. La presenta los criterios utilizados para la selección de fuentes bibliográficas relacionadas con Resource Public Key Infrastructure y seguridad del enrutamiento. Elaboración propia.

El estado del arte se examinó desde dos perspectivas: la global y la regional, esta distinción facilitó la organización del marco teórico y referencial con mayor solidez. En el plano global, se revisaron investigaciones y documentos técnicos que explican la consolidación de RPKI como un mecanismo orientado a reforzar la seguridad del enrutamiento interdominio. De acuerdo con Rodday et al. (2024) señala que RPKI posibilita vincular de forma criptográfica los recursos de numeración de Internet como prefijos IPv4, IPv6 y números de sistema autónomo (ASN) con sus dueños legítimos, incrementando la confiabilidad de los anuncios de rutas BGP.

En la Tabla 3 se presentan los valores específicos de la cantidad de rutas válidas, inválidas y no encontradas, junto con los porcentajes que estas representan respecto a los prefijos visualizados en las tablas globales de IPv4, con base en las cifras publicadas por APNIC Labs entre 2019 y 2025: https://stats.labs.apnic.net/roa. Es importante tener en cuenta que estas estadísticas no se refieren a la cantidad de prefijos asignados a un país, sino a los prefijos efectivamente enrutados.

Tabla 3

Estado de prefijos IPv4 validados con ROA a nivel Global

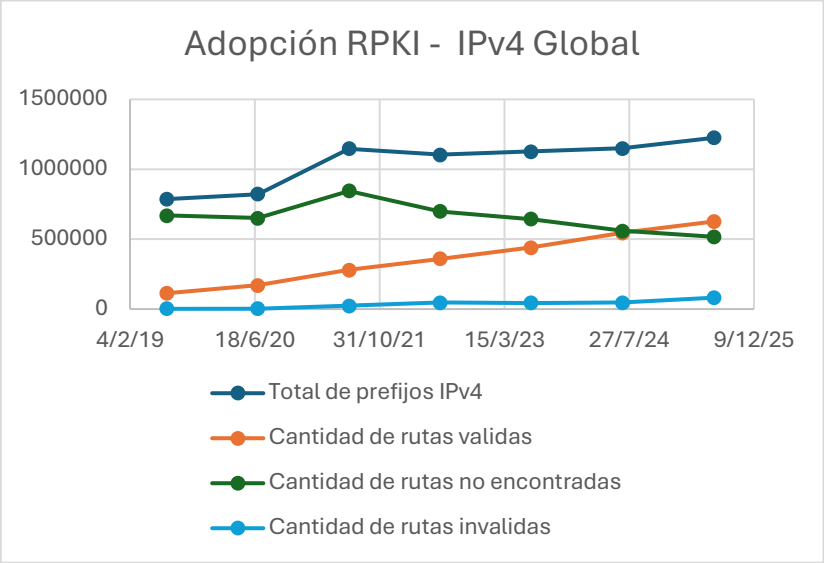
Fecha	Total, de prefijos IPv4	Cantidad de rutas validas	Cantidad de rutas no encontradas	Cantidad de rutas invalidas	% validas	% no encontradas	% invalidas
1/7/2019	786521	113175	669538	3808	14,39%	85,13%	0,48%
1/7/2020	822907	169188	651278	2441	20,56%	79,14%	0,30%
1/7/2021	1147860	279119	844373	24368	24,32%	73,56%	2,12%
1/7/2022	1104660	359074	698516	47070	32,51%	63,23%	4,26%
1/7/2023	1126092	440334	642709	43049	39,10%	57,07%	3,82%
1/7/2024	1149928	546361	557993	45574	47,51%	48,52%	3,96%
1/7/2025	1225027	626454	517062	81511	51,14%	42,21%	6,65%

Nota. La tabla presenta la evolución del estado de validación de prefijos IPv4 mediante objetos ROA a nivel global entre 2019 y 2025, considerando rutas válidas, no encontradas e inválidas dentro del ecosistema de Resource Public Key Infrastructure. Datos adaptados de LACNIC (2025).

A nivel global, la adopción de RPKI muestra una tendencia favorable visualizar la Figura 2, ya que las rutas válidas superan a las no encontradas a partir de 2025. No obstante, el crecimiento de rutas inválidas evidencia la necesidad de mantener procesos de monitoreo, revisión y depuración de ROA.

Figura 2

Adopción RPKI - IPv4 Global



Nota: Datos adaptados de LACNIC (Vega, 2025).

Tabla 4

Estado de prefijos IPv4 validados con ROA a nivel Sur Americano

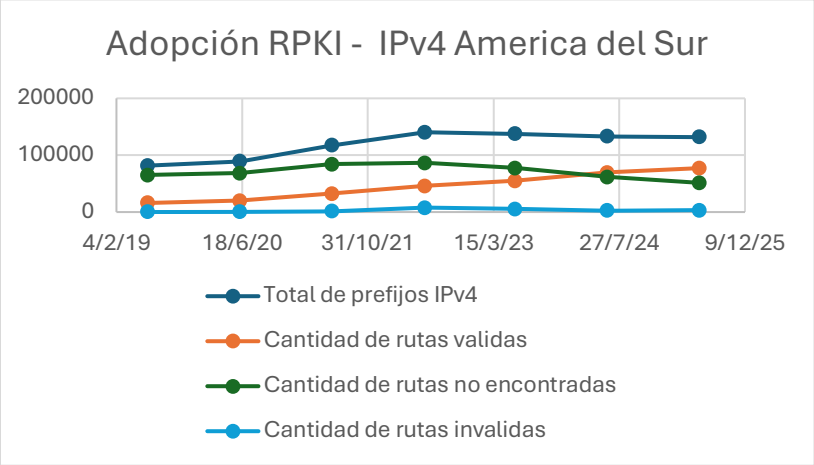
Fecha	Total, de prefijos IPv4	Cantidad de rutas validas	Cantidad de rutas no encontradas	Cantidad de rutas invalidas	% validas	% no encontradas	% invalidas
10/6/2019	81684	15964	65318	402	19,54%	79,96%	0,49%
10/6/2020	89071	20212	68585	274	22,69%	77,00%	0,31%
10/6/2021	117608	32177	84083	1348	27,36%	71,49%	1,15%
16/6/2022	140364	45852	86655	7857	32,67%	61,74%	5,60%
10/6/2023	137492	54679	77555	5258	39,77%	56,41%	3,82%
10/6/2024	133371	69309	61584	2478	51,97%	46,17%	1,86%
10/6/2025	131787	77243	51400	3144	58,61%	39,00%	2,39%

Nota: (LANIC, 2026).

El crecimiento de rutas válidas en América del Sur está directamente relacionado con la reducción de rutas sin ROA. Esto evidencia una mejora en la cobertura de RPKI y una mayor madurez operativa gracias a las políticas, capacitaciones y talleres impulsados por LACNIC, los resultados se visualizan en la Figura 3.

Figura 3

Adopción de RPKI – IPv4 en América del Sur



Nota: Datos adaptados de LACNIC (Vega, 2025).

Como resultado de esta fase, se obtuvo una base conceptual y normativa para definir los criterios de diseño, implementación y evaluación del sistema de validación de rutas en la red central de Airmaxtelecom Soluciones Tecnológicas S.A alineando la investigación con buenas prácticas internacionales y con la evolución regional de la seguridad del enrutamiento.

3.3.2 Diagnóstico inicial de la red

Para demostrar el diagnóstico inicial de la red central de AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., se emplearon instrumentos de recolección de información técnica orientados a establecer una línea base previa a la implementación de RPKI. Estos instrumentos permiten evidenciar el estado operativo de los routers de borde, las sesiones BGP, los prefijos IPv4 anunciados, el ASN, las políticas de enrutamiento, el estado inicial de ROA/ROV. El análisis de vulnerabilidades se desarrollará bajo un enfoque descriptivo, técnico y aplicado a las fases de la Tabla 5.

Tabla 5

Fases metodológicas

Fase	Actividad	Resultado
1	Identificación y valoración de activos	Inventario de activos vinculados a BGP y RPKI.
2	Levantamiento de evidencias técnicas	Registros, configuraciones, consultas y salidas de comandos.
3	Identificación de amenazas	Catálogo de amenazas reales o potenciales de BGP hijacking.
4	Identificación de vulnerabilidades	Debilidades técnicas, operativas o documentales que incrementan la exposición.
5	Cálculo del riesgo actual	Valor del riesgo mediante la relación entre activo, amenaza y vulnerabilidad.
6	Definición del tratamiento del riesgo	Controles técnicos y operativos basados en RPKI, ROA, ROV y monitoreo.
7	Resultado del análisis	Línea base de seguridad previa a la implementación de RPKI.

Nota. La tabla presenta las fases metodológicas aplicadas para el análisis de riesgos y la implementación de Resource Public Key Infrastructure en la red central de Airmaxtelecom Soluciones Tecnológicas S.A. Elaboración propia.

3.3.3 Identificación y valoración de activos

La primera fase consiste en seleccionar los activos previamente identificados y clasificados en el apartado de la Tabla 6, especialmente aquellos que obtuvieron criticidad alta mediante el modelo CIA (Confidentiality, Integrity, Availability).

Tabla 6

Identificación de activos

Código	Activo	Relación con BGP/RPKI	Riesgo
A-01	ASN	Identifica el origen legítimo de los anuncios BGP.	Anuncios no autorizados o erróneos.
A-02	Prefijos IPv4 públicos	Recursos IP anunciados hacia Internet mediante protocolo BGP.	Secuestro de rutas, redirección de tráfico.
A-03	Router de borde BGP	Establece sesiones con proveedores y recibe rutas externas.	Aceptación de rutas inválidas e interrupción o degradación del servicio de Internet
A-04	Sesiones eBGP	Intercambio de rutas con sistemas autónomos externos.	Ingreso de rutas no validadas, propagación de rutas inválidas.
A-05	Políticas de enrutamiento	Controlan aceptación, preferencia y rechazo de rutas.	Errores de filtrado
A-06	Validador RPKI Routinator	Proporciona información de validación a los routers.	Pérdida de capacidad para clasificar rutas válidas, inválidas y no encontradas.
A-07	Servicio RTR	Comunica el validador RPKI con los routers.	Routers con información desactualizada.
A-08	Cuenta LACNIC	Permite administrar recursos de numeración y publicar ROA.	Errores en creación de objetos ROA.

Nota. La tabla presenta los activos críticos identificados en la infraestructura de enrutamiento asociados con Border Gateway Protocol y Resource Public Key Infrastructure, así como los principales riesgos vinculados a su operación y seguridad. Elaboración propia.

3.3.4 Valoración CIA y cálculo del valor del activo

La valoración de los activos se realizará mediante el modelo CIA, considerando confidencialidad, integridad y disponibilidad.

Tabla 7

Valoración de activos con modelo CIA

Nivel	Valor	Confidencialidad	Integridad	Disponibilidad
Bajo	1	La divulgación no genera afectación significativa al enrutamiento BGP.	La modificación genera impacto leve o fácilmente corregible.	La interrupción no afecta de forma relevante la operación.
Medio	2	La divulgación expone información interna de red.	La modificación afecta parcialmente rutas, políticas.	La interrupción afecta parcialmente la operación.
Alto	3	La divulgación compromete, configuraciones críticas, topologías de red lógicas	La modificación permite rutas inválidas, anuncios no autorizados.	La interrupción afecta continuidad del servicio.

Nota. La tabla presenta los activos críticos identificados en la infraestructura de enrutamiento asociados con Border Gateway Protocol y Resource Public Key Infrastructure, así como los principales riesgos vinculados a su operación y seguridad. Elaboración propia.

Fórmula para el valor del activo

$$VA = \frac{C + I + D}{3}$$

Donde: VA es el valor del activo; **C** es confidencialidad; **I** es integridad; y **D** es disponibilidad.

3.3.5 Identificación de amenazas de secuestro de rutas

Las amenazas se caracterizan considerando escenarios reales o potenciales de BGP hijacking, fugas de rutas, errores de origen y fallas en los mecanismos de validación RPKI.

Tabla 8

Análisis de amenazas

Código	Amenaza	Descripción	Tipo
AM-01	Anuncio no autorizado de prefijo IPv4	Un ISP anuncia un prefijo con un ASN externo que no pertenece a Airmaxtelecom.	Intencionado / Accidental
AM-02	Anuncio de prefijo más específico	Una organización anuncia un prefijo más específico para desviar el tráfico a una red ilegitima.	Intencionado
AM-03	Fuga de rutas BGP	Un proveedor propaga rutas que no se debería anunciar que contienen errores de validaciones.	Accidental / operativo
AM-04	Error de origen BGP	Un prefijo legítimo se anuncia con un ASN de origen incorrecto.	Accidental
AM-05	Manipulación de políticas de enrutamiento	Modificaciones indebidas en las políticas de enrutamiento BGP.	Intencionado / accidental
AM-06	Falta de disponibilidad del servicio de RPKI	El cliente RPKI no puede consultar información actualizada de validación.	Operativo
AM-07	Error en la publicación de ROA	Una configuración incorrecta puede clasificar rutas válidas como inválidas	Operativo
AM-08	Ausencia de monitoreo de rutas inválidas	No se identifican a tiempo los eventos asociados a BGP hijacking.	Organizacional

Nota. La tabla presenta las amenazas identificadas en la infraestructura de Border Gateway Protocol y Resource Public Key Infrastructure que pueden afectar la seguridad del enrutamiento. Elaboración propia.

3.3.6 Identificación de vulnerabilidades

Las vulnerabilidades corresponden a condiciones técnicas, operativas, documentales que incrementan la exposición de la red central frente a amenazas de secuestro de rutas.

Tabla 9

Clasificación de vulnerabilidades

Código	Vulnerabilidad	Activo afectado	Descripción
VUL-01	Ausencia de ROA para prefijos IPv4	Prefijos IPv4 públicos	No existe registro de autorización criptográfica para validar el origen legítimo del prefijo.
VUL-02	Falta de validación RPKI/ROV en routers de borde	Router de borde BGP	El router puede aceptar rutas inválidas y no autorizadas.
VUL-03	Políticas BGP sin clasificación por estado RPKI	Políticas de enrutamiento	No se diferencian rutas válidas, inválidas o no encontradas.
VUL-04	Dependencia exclusiva de filtros manuales	Sesiones eBGP	Los controles básicos no pueden detectar errores de origen de rutas.
VUL-05	Manipulación de atributo AS_PATH	ASN	Suplantación de identidad mediate el AS_PATH.
VUL-06	Punto único de falla en el validador RPKI	Validador RPKI Routinator	La indisponibilidad del servidor compromete la integridad de la tabla de enrutamiento global válida.
VUL-07	Configuración incorrecta de ROA	Cuenta LACNIC	Un ROA mal definido puede invalidar rutas legítimas y provocar

			interrupción de tráfico.
VUL-08	Documentación incompleta de políticas de enrutamiento	Servicio RTR	Dificulta la conectividad entre el sistema Routinator y el cliente-rpki.

Nota. La tabla presenta las vulnerabilidades identificadas en Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

3.3.7 Escalas de valoración de amenaza y vulnerabilidad

Tabla 10

Rango de amenaza

Nivel de amenaza	Valor	Criterio adaptado a BGP/RPKI
Bajo	1	La ocurrencia es poco probable o requiere condiciones especiales.
Medio	2	La ocurrencia es probable por errores de configuración, fallas operativas o dependencia de terceros.
Alto	3	La ocurrencia es muy probable o el activo está expuesto a Internet, proveedores externos o múltiples sesiones BGP.

Nota. La tabla presenta los niveles de amenaza aplicados al entorno de Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

Tabla 11

Rango de vulnerabilidad

Nivel de vulnerabilidad	Valor	Criterio adaptado a BGP/RPKI
Bajo	1	Existe un control adecuado y aplicado correctamente.
Medio	2	Existen controles parciales, pero no reducen totalmente la exposición.
Alto	3	No existe un control implementado o el control actual es insuficiente.

Nota. La tabla presenta los niveles de vulnerabilidad aplicados al entorno de Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

3.3.8 Cálculo del riesgo actual

El riesgo actual se calculará relacionando el valor del activo con el nivel de amenaza y el nivel de vulnerabilidad.

Fórmula de riesgo:

$$Riesgo\ BGP/RPKI = VA * Amenaza * Vulnerabiliad$$

Tabla 12

Rango y nivel de riesgo

Rango de Resultado	Nivel de riesgo	Interpretación
1 a 3	Bajo	El riesgo puede ser aceptado.
4 a 8	Medio	El riesgo requiere seguimiento y aplicación de controles focalizados.
9 a 27	Alto	La naturaleza del Riesgo requiere una acción inmediata de mitigación.

Nota. La tabla presenta la clasificación de niveles de riesgo aplicada al entorno de Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

Tabla 13

Cálculo del valor del activo y riesgo

Activo	Amenaza	Vulnerabilidad	VA	Amenaza	Vulnerabilidad	Riesgo	Nivel
Prefijos IPv4 públicos	Anuncio no autorizado	Ausencia de ROA	2,67	3	3	24,03	Alto
Router de borde BGP	Aceptación de ruta inválida	Falta de ROV	3,00	3	3	27,00	Alto
Políticas de enrutamiento	Aceptación de anuncios inseguros	Sin clasificación RPKI	3,00	3	3	27,00	Alto
Validador RPKI	Indisponibilidad del servicio	Punto único de falla	2,67	2	2	10,68	Alto

Nota. La tabla presenta el cálculo del valor del activo y el nivel de riesgo asociado a amenazas y vulnerabilidades identificadas en el entorno de Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

La siguiente matriz relaciona los activos críticos con amenazas, vulnerabilidades, impacto y controles propuestos.

Tabla 14

Relación de activos con amenazas y vulnerabilidades

Activo	Vulnerabilidad	Amenaza	Impacto esperado	Control propuesto
Prefijos IPv4 públicos	Ausencia de ROA para prefijos IPv4	Anuncio no autorizado del prefijo	Redirección o pérdida de tráfico	Crear ROA en LACNIC
ASN	Falta de validación de origen	Suplantación del origen de ruta	Afectación de reputación y alcance	Validar origen mediante RPKI
Router de borde BGP	Falta de validación RPKI/ROV en routers de borde	Aceptación de ruta inválida	Secuestro parcial de tráfico	Activar validación RPKI en peers BGP
Sesiones eBGP	Dependencia exclusiva de filtros manuales	Fuga de rutas o ruta mal originada	Inestabilidad de enrutamiento	Filtrado por estado RPKI (Válido, Inválido, No encontrado)
Políticas de enrutamiento	Políticas BGP sin clasificación por estado RPKI	Aceptación de anuncios inseguros	Propagación de rutas no deseadas	Crear política para valid/invalid/NotFound en el tráfico inbound
Validador RPKI	Punto único de falla en el validador RPKI	Pérdida de validación	Operación sin información RPKI actualizada	Redundancia de servidor RPKI
Servicio RTR	Falla de comunicación	Router sin datos VRP	Validación incompleta	Supervisar puerto RTR
Cuenta LACNIC	Configuración incorrecta de ROA	Ruta legítima marcada inválida	Pérdida de alcance del prefijo	Registro de cambios y monitoreo

Nota. La tabla presenta la relación entre activos, vulnerabilidades y amenazas identificadas en el entorno de Border Gateway Protocol y Resource Public Key Infrastructure, así como los controles propuestos para su mitigación. Elaboración propia.

3.3.8 Tratamiento del riesgo

Para los riesgos clasificados como altos se propone como tratamiento principal la mitigación o reducción del riesgo.

Tabla 15

Tratamiento de riesgo

Vulnerabilidad	Control propuesto	Relación con RPKI
Ausencia de ROA	Crear ROA para prefijos IPv4 en LACNIC	Autoriza el origen legítimo del prefijo.
Falta de ROV	Configurar validación RPKI en routers de borde	Permite aceptar o rechazar rutas según estado de validación.
Políticas BGP incompletas	Crear route-policy para valid/invalid/notfound	Aplica decisiones de seguridad sobre rutas recibidas.
Falta de monitoreo	Integrar logs RPKI/BGP a herramientas de monitoreo	Detecta eventos de rutas inválidas o sospechosas.
Falla del validador	Monitorear Routinator y servicio RTR	Asegura disponibilidad de la información de validación.
Error en ROA	Aplicar revisión técnica antes de publicar ROA	Evita invalidar rutas legítimas.

Nota. La tabla presenta los controles propuestos para el tratamiento de riesgos identificados en el entorno de Resource Public Key Infrastructure y Border Gateway Protocol. Elaboración propia.

El análisis de vulnerabilidades evidenció una exposición crítica de la red central ante el secuestro de rutas, riesgo elevado por la ausencia de controles criptográficos en el origen y políticas de BGP permisivas. Estos hallazgos fundamentan la implementación de una infraestructura RPKI, estableciendo un fuerte control que minimiza la probabilidad de aceptar rutas no autorizadas o invalidas fortaleciendo la postura de seguridad institucional.

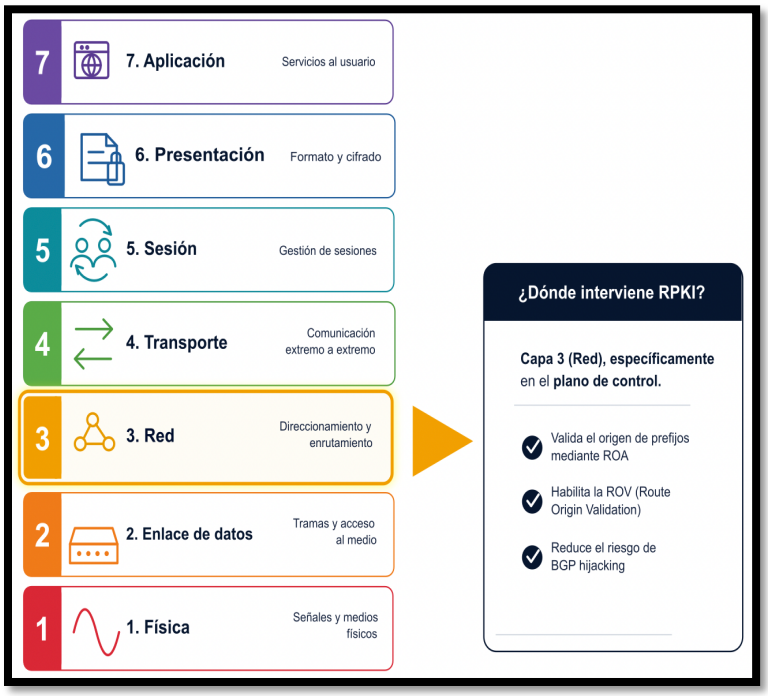
3.3.9 Diseño de la solución técnica

Se planificó la implementación de RPKI utilizando validadores como Routinator y rpki-client, configurando filtros en routers que acepten rutas validadas con origen confiable, se descarten las rutas invalidad y se permita aceptan las rutas que no se encuentran los registros ROA. RPKI se relaciona principalmente con la Capa 3: Red, debido a que protege la información de enrutamiento utilizada por BGP mediante la validación del origen de

prefijos IP. Su función se desarrolla en el plano de control como se muestra en la figura 4 y no en el transporte de datos de usuario.

Figura 4

Ubicación de RPKI en el modelo OSI



Elaboración Propia

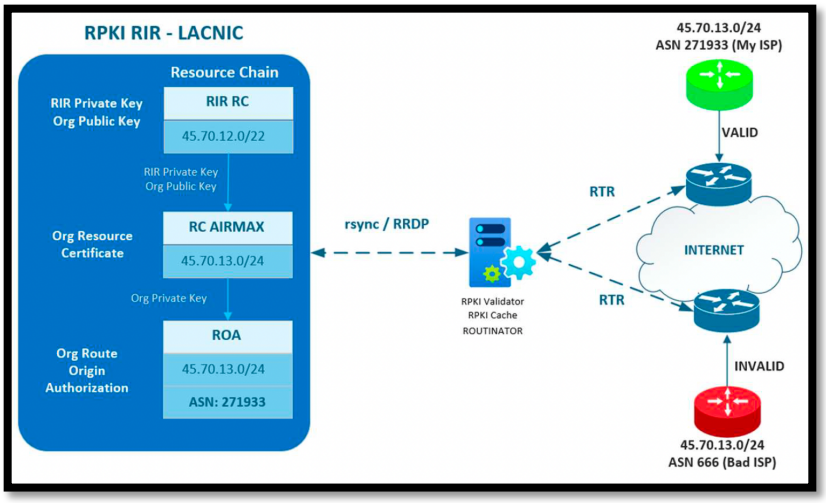
La Figura 5 presenta un ejemplo del proceso de validación RPKI aplicado al prefijo IPv4 45.70.*.*/24 asociado al ASN 271933. En la parte izquierda se representa la cadena de recursos administrada por LACNIC, donde se certifica la asignación del bloque IP y se publica el objeto ROA correspondiente. Este ROA autoriza que el prefijo 45.70.*.*/24 sea originado únicamente por el ASN 271933 perteneciente a la organización.

El funcionamiento de RPKI inicia con la publicación del ROA en la infraestructura del RIR. Posteriormente, el validador RPKI, implementado mediante Routinator, consulta la información publicada por LACNIC a través de rsync o RRDP y construye una caché local con los prefijos autorizados. Esta información es entregada al router de borde mediante el protocolo RTR, permitiendo que las rutas BGP recibidas sean comparadas con los registros ROA existentes.

En el escenario mostrado, cuando el prefijo 45.70.*.*/24 es anunciado por el ASN 271933, la ruta se clasifica como válida, debido a que coincide con la autorización registrada en el ROA. Por el contrario, si el mismo prefijo es anunciado por un ASN 666 no autorizado representado en la figura, esta ruta se identifica como inválida.

Figura 5

Ejemplo de validación de prefijo IPv4 45.70..*/24 con AS271933*



Elaboración Propia

Como se observa en la Tabla 16, LACNIC cumple el rol de plataforma de gestión para la creación de los objetos ROA asociados a los prefijos asignados a la organización. Routinator actúa como validador RPKI, encargado de recolectar y verificar la información publicada en los repositorios RPKI y almacenarla localmente. Finalmente, el router Huawei NE8000 utiliza esta información para aplicar políticas de enrutamiento que permitan aceptar rutas válidas, identificar rutas no encontradas y rechazar rutas inválidas mediante el protocolo RTR.

Tabla 16

Herramientas de validación RPKI

Herramienta	Función	Detalle
Routinator	Recolector y validador RPKI	Software que permite realizar la validación de origen de confianza.

Huawei NE8000	Router de Borde	Permite la integración de validaciones con RPKI mediante políticas de enrutamiento.
LACNIC	Plataforma de gestión de ROA	Permite crear las autorizaciones de origen de los prefijos asignados a la organización.

Nota. La tabla presenta las herramientas utilizadas para la validación de Resource Public Key Infrastructure y la gestión de seguridad en el enrutamiento de Border Gateway Protocol. Elaboración propia.

La Tabla 17 presenta el diseño de la política de filtrado BGP basada en el estado de validación RPKI de las rutas recibidas. En esta política, las rutas se clasifican en tres estados: válidas, inválidas y no encontradas. Para las rutas válidas se permite su aceptación, debido a que el prefijo IP y el ASN de origen coinciden con un ROA autorizado. En el caso de las rutas inválidas, se plantea su rechazo, ya que el ASN que anuncia el prefijo no corresponde con la autorización registrada.

Para las rutas con estado *NotFound* o no encontradas, se propone una política conservadora que permite su aceptación inicial, pero con menor preferencia. Esto se debe a que no todos los sistemas autónomos de Internet cuentan actualmente con ROA publicados para sus prefijos. Además, en escenarios de peering con IXP para el consumo de CDNs, es común recibir anuncios de rutas cuyo estado RPKI aparece como no encontrado, por lo que su rechazo inmediato podría afectar la disponibilidad o el alcance hacia ciertos destinos.

Tabla 17

Definición de política de filtrado BGP basada en validación RPKI

Estado RPKI	Significado	Política de filtrado
Valid	Prefijo IP y ASN valido con ROA autorizado	Aceptar ruta
Invalid	El prefijo no corresponde al ASN autorizado	Rechazar ruta
NotFound	No existe un registro ROA para el prefijo	Aceptar ruta temporalmente o cambiar preferencia

Nota. La tabla presenta la política de filtrado aplicada en Border Gateway Protocol según el estado de validación de Resource Public Key Infrastructure. Elaboración propia.

Con el objetivo de garantizar la integridad en el intercambio de prefijos con los diversos carriers mediante sesiones BGP, es imperativo implementar una arquitectura de validación basada en el protocolo RPKI (Resource Public Key Infrastructure). Esta infraestructura permite verificar la legitimidad de los anuncios de ruta; a continuación, se detalla un modelo de configuración para el filtrado de tráfico entrante (inbound), diseñado para mitigar riesgos de seguridad como el secuestro de rutas (hijacking).

3.3.10 Implementación y configuración

Se instalaron y configuraron los servidores validadores, se registraron los ROA ante LACNIC, y se integró el sistema de validación con los routers BGP. Las pruebas se realizaron en horarios de bajo tráfico para minimizar el impacto en la red de producción, los recursos que se utilizaron se muestran en la Tabla 18.

Tabla 18

Recursos IPv4, ASN y protocolos

Recurso	Valor	Detalle
ASN	271933	Sistema autónomo asignado al ISP Airmaxtelecom Soluciones Tecnológicas S.A.
Prefijo IPv4	45.70.*.*/*	Bloque asignado por LACNIC
RIR	LACNIC	Registro Regional de Recursos de Internet
Protocolo de enrutamiento	BGP	Protocolo de enrutamiento de borde
Validador RPKI	Routinator	Software validador de RPKI

*Nota***.** La tabla presenta los recursos IPv4, ASN, protocolos y herramientas utilizados en la implementación de Resource Public Key Infrastructure en la red de Airmaxtelecom Soluciones Tecnológicas S.A. Elaboración propia.

La Figura 6 muestra una evidencia de un aplicativo de WHOIS propio de Lacnic el cual permite validar prefijos IPv4 públicos relacionados con el número de sistema autónomo 271933 perteneciente a la organización Airmaxtelecom Soluciones Tecnológicas S.A.

Figura 6

Número de sistema autónomo asignado a Airmaxtelecom Soluciones Tecnológicas S.A.

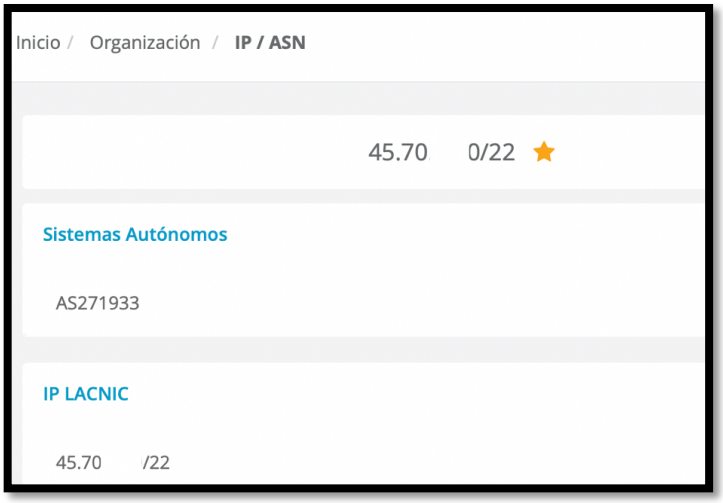


Fuente: (LACNIC, 2026).

Se puede apreciar en la Figura 7 el prefijo IPv4 45.70.*.*/* y el ASN 271933 asignado al ISP Airmaxtelecom Soluciones Tecnológicas S.A. dentro de la cuenta MILACNIC

Figura 7

Prefijo público IPv4 asignado al ASN 271933 perteneciente a Airmaxtelecom Soluciones Tecnológicas S.A.



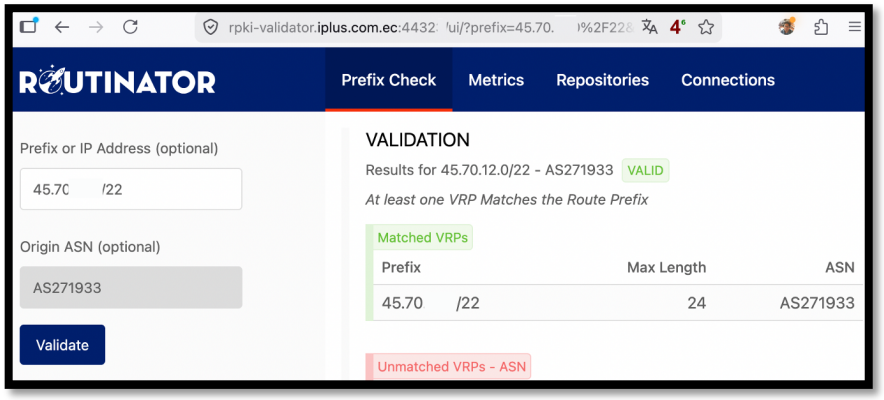
Fuente: (LACNIC, 2026).

En la Figura 8 se ilustra la interfaz gráfica de Routinator, un software de validación RPKI. En este escenario, la herramienta se encuentra desplegada de manera local bajo la infraestructura del proveedor de servicios, lo que permite realizar consultas de integridad sobre las tablas de rutas globales sin depender exclusivamente de validadores externos y con la información recuperada del RIR regional.

La imagen muestra el proceso de verificación para el prefijo 45.70.*.*/22 asociado al AS271933. El resultado arroja un estado "VALID", lo cual indica que el anuncio BGP obtenido en la red coincide plenamente con un registro de autorización de origen (ROA) firmado criptográficamente.

Figura 8

Software Routinator alojado en un subdominio del ISP



Fuente: (Routinator, 2026).

En la Figura 9 se presenta la visualización de los anuncios BGP desde la perspectiva de LACNIC, el Registro de Direccionamiento de Internet para América Latina y el Caribe. Esta herramienta de consulta externa permite verificar en tiempo real cómo los prefijos de un Sistema Autónomo (en este caso, el AS271933) son percibidos por la comunidad global.

A diferencia del validador local Routinator analizado previamente, esta vista confirma que la configuración de los Objetos de Autorización de Origen (ROA) ha sido propagada correctamente hacia los repositorios de los Trust Anchors.

Figura 9

Lista de anuncios vía BGP válidos en herramienta tools de LACNIC



Fuente: (LACNIC, 2026).

3.3.11 Creación de ROA en cuenta miLacnic

Como parte del proceso de implementación de Resource Public Key Infrastructure, se realizó la creación de objetos ROA en la plataforma miLacnic, con el propósito de validar el origen legítimo de los prefijos IPv4 asociados al sistema autónomo de la organización. A continuación, se describen los procesos:

- Ingresar al sitio https://milacnic.lacnic.net con las credenciales asignadas a la organización al momento de inscribirse en LACNIC
- Ir al menú contextual de la organización en la opción **[Servicios] / [RPKI]** y accede al apartado de RPKI, ver Figura 10:

Figura 10

Menú principal con el módulo de RPKI

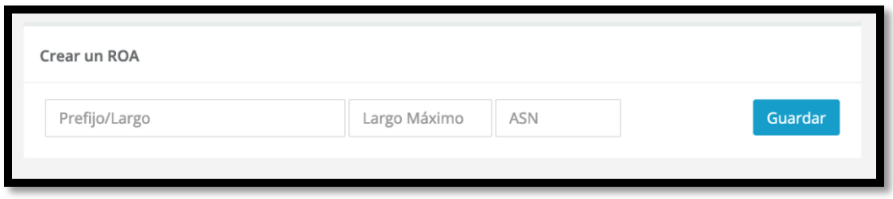


Fuente: (LACNIC, 2026).

En la sección RPKI, encontrará la interfaz de creación de ROAs. Seleccione la opción [Crear un ROA], podrá crear un único ROA ver Figura 11:

Figura 11

Formulario para creación de ROA



Fuente: (LACNIC, 2026).

1) Como primer paso para crear el ROA deberá ingresar la siguiente información, ver Figura 12:

- En [Prefijo/Largo] Indique el bloque y prefijo correspondientes para crear el ROA
- En [Largo Máximo] Especifique el prefijo más detallado que desea autorizar para anuncios BGP.
- En [ASN] Ingrese el número de sistema autónomo que realizará el anuncio del bloque.

Figura 12

Ingreso de prefijo IPv4 público con máscara /22 y máscara /24 para prefijo detallado con el AS271933



Fuente: (LACNIC, 2026)

En este escenario, el ROA autoriza la publicación del bloque 45.70.12.0/22 mediante el AS271933. La configuración permite además subsegmentos más específicos hasta un máximo de /24 (por ejemplo, el 45.70.12.0/24). Por el contrario, un anuncio del bloque 45.70.11.0/21 resultaría en un estado de "no encontrado" al exceder el tamaño del bloque

definido. Por otra parte, cualquier intento de anuncio desde un ASN distinto será marcado como inválido. Al dar clic en la opción [Guardar] podrá [Confirmar], previsualizar los cambios con [Preview] o [Cancelar] ver Figura 13.

Figura 13

Estado de acciones previas a grabar el ROA

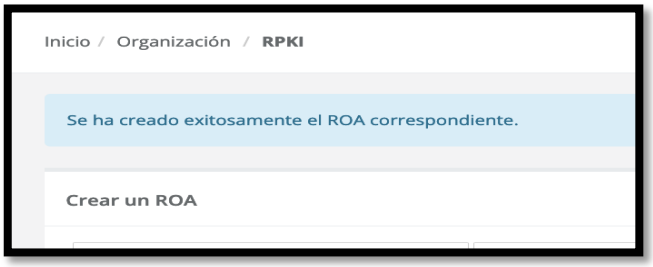


Fuente: (LACNIC, 2026).

2) Al hacer clic en [Confirmar], se creará el ROA especificado y se mostrará el siguiente mensaje de confirmación, ver Figura 14:

Figura 14

Mensaje de confirmación de creación de ROA

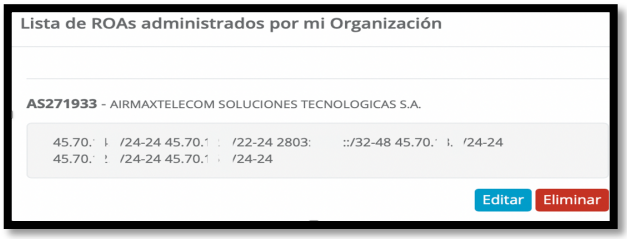


Fuente: (LACNIC, 2026).

Para validar los ROA creados dar clic en el menú RPKI, ver Figura 15:

Figura 15

Lista de ROAs creados para la organización



Fuente: (LACNIC, 2026).

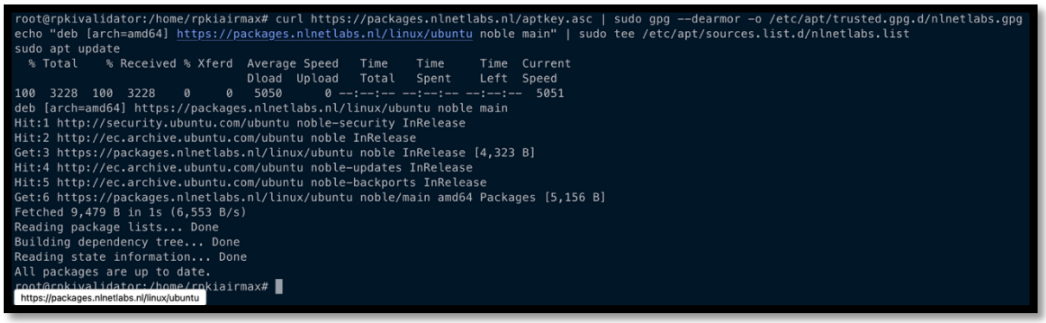
3.3.12 Instalación y configuración del validador RPKI Routinator

Para implementar el sistema de validación de rutas basado en RPKI, se instaló el validador Routinator sobre un servidor Ubuntu. Este validador permite descargar, validar y procesar los objetos RPKI publicados por los RIR, en el caso de estudio se obtienen los datos del RIR LACNIC, y posteriormente entregar la información validada a los enrutadores de borde mediante el protocolo RTR.

Como primer paso se debe actualizar el sistema operativo base, en este caso debemos de actualizar en nuestro servidor de ubuntu e instalar la herramienta de curl para posterior uso. En la Figura 16 se evidencia la incorporación del repositorio oficial de la herramienta Routinator e instalación en el servidor ubuntu.

Figura 16

Agregación de repositorio Nlnet Labs



En la Figura 17 se muestra el uso e instalación del paquete Routinator previamente configurado en el repositorio.

Figura 17

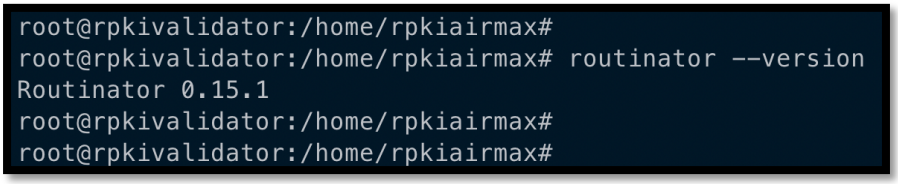
Instalación de Routinator en sistema operativo Ubuntu



Para validar la versión instalada de Routinator se utiliza el comando routinator --versión si el software fue instalado correctamente nos deberá mostrar la versión que se está ejecutando en consola como muestra la Figura 18:

Figura 18

Validación de versión de software routinator

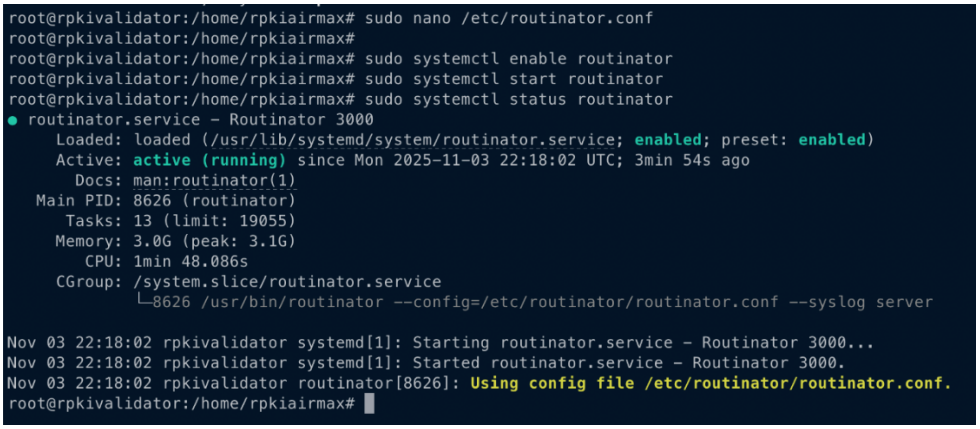


En la Figura 19 podemos apreciar el estado de Routinator, para crear la de inicio automático se adjuntas los siguientes comandos a ejecutar en el CLI:

- sudo systemctl enable routinator
- sudo systemctl start routinator
- sudo systemctl status routinator

Figura 19

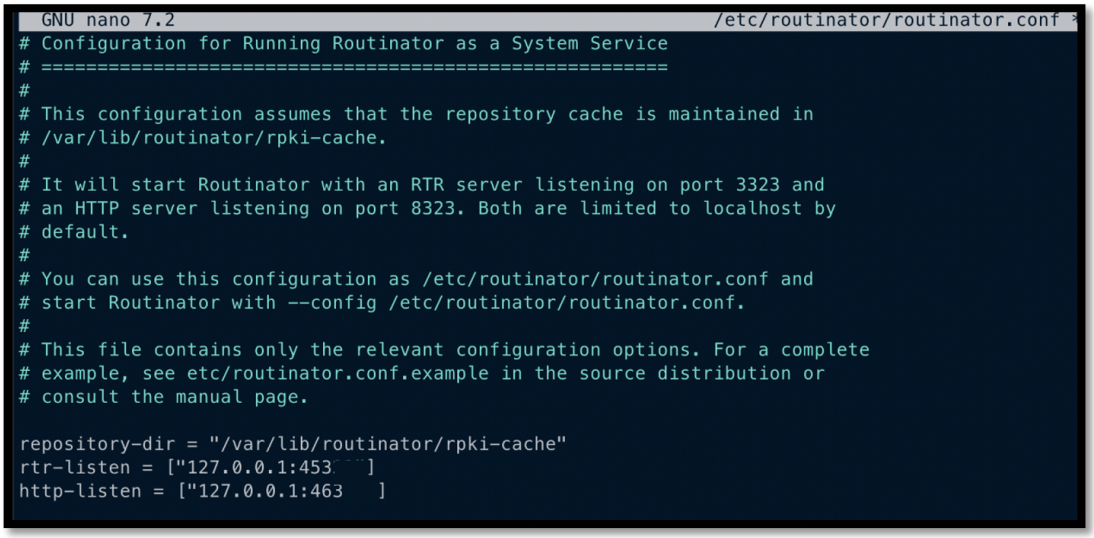
Estado de routinator activo



Para cumplir con parámetros de seguridad se debe editar el archivo de configuración, este archivo está ubicado en /etc/routinator/routinator.conf los principales cambios a realizar son el cambio de los puertos por defecto como se muestra en la Figura 20:

Figura 20

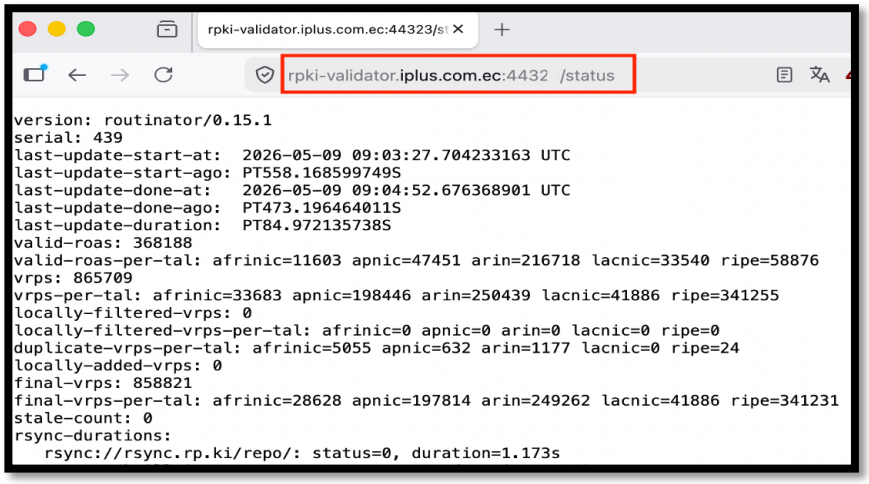
Cambio de puertos de archivo de configuración de Routinator



Después de realizar la configuración del cambio de los puertos se requiere reiniciar el servicio con el siguiente comando sudo systemctl restart routinator. Para la validación del servicio web vamos a abrir la IP o dominio de nuestro servidor seguido del puerto configurado con el endpoint /status como se muestra en la Figura 21.

Figura 21

Estado de la herramienta de RPKI

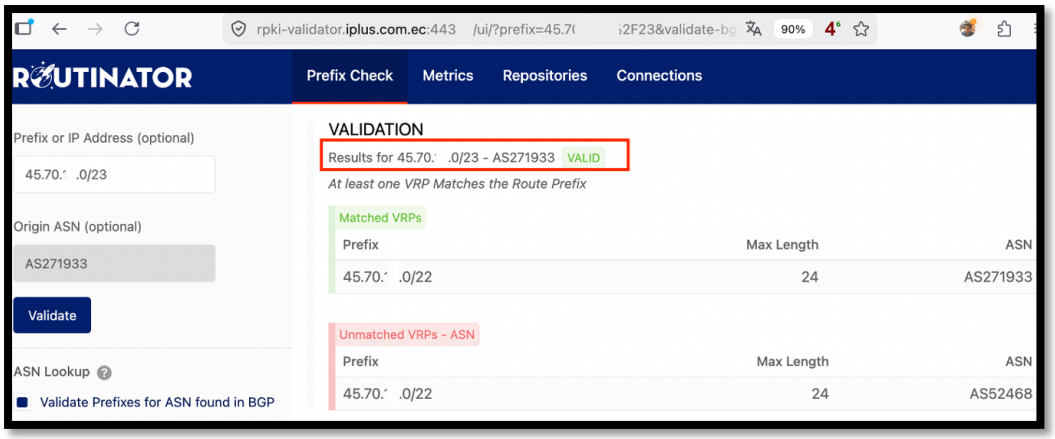


Fuente: (Routinator, 2026).

En la Figura 22 se muestra el acceso a la interfaz web de routinator, en esta interfaz web podemos realizar las consultas de los prefijos y la validación del ROA.

Figura 22

Sistema web de validación de ROA con RPKI



Fuente: (Routinator, 2026).

En la Figura 23 se presenta una consulta mediante línea de comandos, cuya respuesta en formato JSON coincide con la información visualizada en la interfaz gráfica.

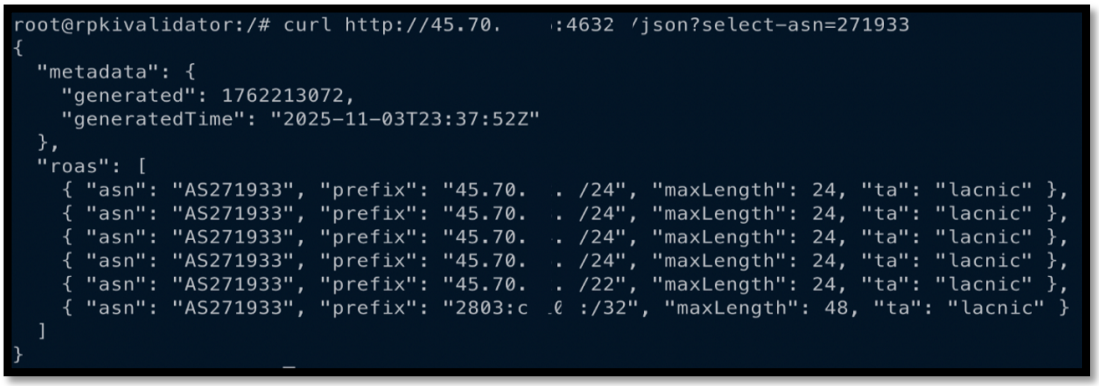
Ejemplo de consulta por CLI:

curl http://45.70.*.*:4632*/json?select-asn=271933

curl http://45.70.*.*:4632*/json?select-prefix=45.70.*.*/24

Figura 23

Respuesta en formato JSON



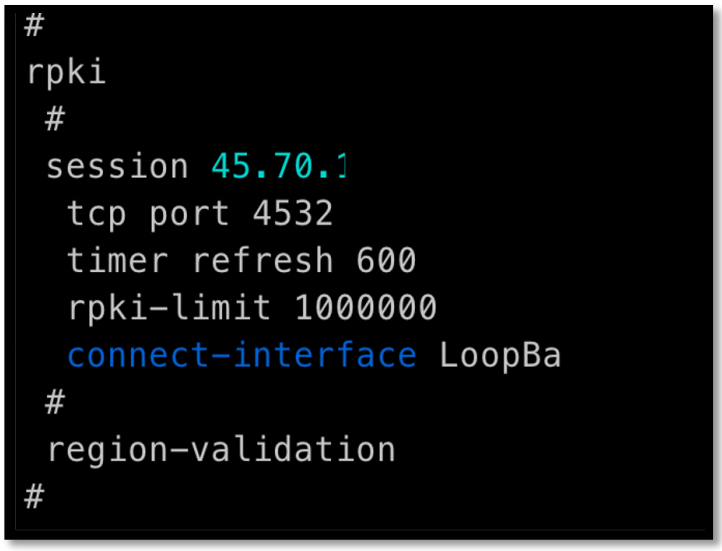
Fuente: (Routinator, 2026).

Para la integración de RPKI en el router de borde Huawei NE8000, se configuró el protocolo RTR hacia el servidor Routinator ubicado en la red central de Airmaxtelecom. Esta sesión permite que el router consuma la información validada de los ROA publicados en la infraestructura RPKI descargada desde los repositorios de LACNIC. Una vez establecida la sesión, se habilitó la validación de origen dentro del proceso BGP, permitiendo que las rutas recibidas sean clasificadas como válidas, inválidas y no encontradas.

Con base en esta clasificación, se implementó una política de importación BGP denominada RPKI-IN-FILTER-ROUTINATOR, cuya función es rechazar los anuncios con estado invalid, aceptar los anuncios valid y permitir temporalmente los anuncios not-found. Esta estrategia permite fortalecer la seguridad del plano de control BGP sin interrumpir rutas legítimas que aún no cuentan con registros ROA publicados, a continuación, se muestra las líneas de configuración en el router de borde. La Figura 24 muestra la configuración RTR en el router Huawei NE8000 y en la Tabla 19 se describe los parámetros para establecer una sesión con el servidor RPKI.

Figura 24

Configuración de RTR en router de borde



Elaboración propia.

Tabla 19

Parámetros de configuración de cliente RPKI

Parámetro	Valor	Descripción
session	45.70.x.x	Dirección IP del servidor Routinator.
tcp port	4532*	Puerto RTR utilizado por Routinator.
timer refresh	600	Intervalo de actualización de la información RPKI, en segundos.
rpki-limit	1000000	Límite máximo de registros RPKI aceptados por el router.
connect-interface	Loopback	Interfaz origen usada por el router para establecer la sesión RTR.

Nota. La tabla presenta los parámetros utilizados para la configuración del cliente de Resource Public Key Infrastructure y la comunicación RTR entre el router y el servidor validador. Elaboración propia.

A continuación, se presenta un modelo de filtros utilizados en las políticas de enrutamiento para controlar las rutas aprendidas desde los peers con los cuales se establecen sesiones BGP. Es importante mencionar que, para aplicar de forma efectiva la validación de rutas mediante RPKI, el router debe recibir una tabla parcial o completa de rutas de Internet. Esto se debe a que la validación RPKI requiere evaluar cada prefijo recibido frente a los registros ROA disponibles.

Por el contrario, cuando el router recibe únicamente una ruta por defecto, como 0.0.0.0/0, no es posible aplicar de manera efectiva la clasificación de rutas en los estados válida, inválida o no encontrada, ya que no se dispone de los prefijos específicos necesarios para realizar dicha validación. Por esta razón, la funcionalidad de RPKI resulta más útil y precisa cuando se trabaja con rutas específicas provenientes de una tabla parcial o completa de Internet:

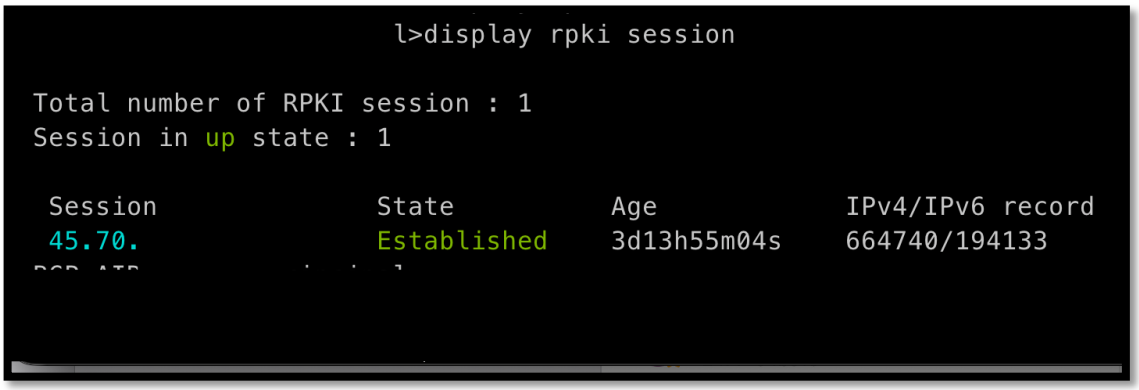
- route-policy RPKI-IN-FILTER-ROUTINATOR deny node 10
- Rechaza todas las rutas inválidas
- if-match rpki-resource-validation invalid#
- route-policy RPKI-IN-FILTER-ROUTINATOR permit node 20

- Acepta todas las rutas válidas
- if-match rpki-resource-validation valid#
- route-policy RPKI-IN-FILTER-ROUTINATOR permit node 30
- Acepta las rutas con estado ROA no encontrado
- if-match rpki-resource-validation not-found#

En la Figura 25 se detalla la adyacencia RTR (RPKI-to-Router) configurada en el nodo central. Se observa cómo el router Huawei NE8000 mantiene una sesión activa con el caché local (Routinator), permitiendo el aprendizaje y la gestión de la base de datos de prefijos autorizados provenientes del Trust Anchor de LACNIC para la posterior validación de rutas BGP.

Figura 25

Sesión RTR establecida desde router Huawei



Fuente: (LACNIC, 2026).

3.3.13 Evaluación mediante monitoreo y recolección de datos

La evaluación se plantea con un enfoque comparativo antes/después, debido a que permite observar el comportamiento de la red central en dos momentos: el escenario previo a la implementación de RPKI y el escenario posterior a la integración del validador RPKI con el router de borde. Este enfoque se utiliza para contrastar parámetros de rendimiento y seguridad asociados al enrutamiento BGP.

El análisis metodológico no se limita al rendimiento de la red. Su componente principal es la capacidad de identificar rutas inválidas mediante RPKI, ya que este estado representa anuncios cuyo origen no coincide con la autorización registrada en los ROA y, por tanto, constituye una señal técnica relevante para la detección y mitigación de posibles eventos de BGP hijacking.

La medición de latencia y pérdida de paquetes se emplea como línea base de estabilidad del servicio. La medición de rutas válidas, inválidas y no encontradas se utiliza como criterio de seguridad para determinar la efectividad del mecanismo de validación de origen.

En esta fase se levanta una línea base que permite documentar el comportamiento inicial del enrutamiento y los antecedentes asociados a posibles eventos de BGP hijacking sobre el ASN 271933, ver Tabla 20 con los parámetros a evaluar.

***Tabla* 20**

Parámetros de evaluación antes de la implementación de RPKI

Parámetro	Forma de levantamiento	Evidencia
Latencia	Medición ICMP hacia destinos de referencia.	Gráficas de monitoreo, ping
Pérdida de paquetes	Medición de paquetes enviados y recibidos.	Ping, monitoreo o registros de disponibilidad.
Rutas BGP recibidas	Consulta de tablas BGP por peer.	Información del router antes de aplicar políticas RPKI.
Eventos de hijacking	Revisión de reportes históricos del ASN 271933.	Archivos recopilados de herramienta Radar Qrator

Nota. La tabla presenta los parámetros utilizados para la evaluación inicial del comportamiento de Border Gateway Protocol antes de la implementación de Resource Public Key Infrastructure. Elaboración propia.

En la Tabla 21 se evidencia los parámetros a validar después de la implementación del validador RPKI Routinator con el router Huawei NE8000 M4 mediante el protocolo RTR. En esta fase, el router clasifica las rutas BGP según su estado de validación de origen: valid, invalid o not-found, y el contador de rutas según la clasificación de RPKI.

Tabla 21

Parámetros de evaluación después de la implementación de RPKI

Parámetro	Evidencia
Sesión RPKI establecida	Captura del comando display rpki
Conectividad RTR	Evidencia de conectividad entre router y servidor RPKI.
Clasificación de rutas	Tabla BGP con códigos V válida, I inválida y N no encontrada.
Rutas inválidas detectadas	Contadores de rutas inválidas.
Rutas válidas y not-found permitidas	Contadores de rutas no encontradas.
Latencia y estabilidad posterior	Gráficas ICMP y registros de monitoreo.

Nota. La tabla presenta los parámetros utilizados para la evaluación posterior a la implementación de Resource Public Key Infrastructure en el entorno de Border Gateway Protocol. Elaboración propia.

En consecuencia, la evaluación permitirá establecer una comparación técnica entre el estado inicial de la red y el escenario posterior a la implementación de RPKI. Para ello, se considerarán evidencias obtenidas desde el router de borde, el validador RPKI y las herramientas de monitoreo, con el fin de verificar la variación de parámetros como latencia, pérdida de paquetes y, principalmente, la detección y mitigación de rutas inválidas. De esta manera, se aportará una base metodológica objetiva para determinar la contribución de RPKI en la reducción de la exposición de la red central ante posibles eventos de BGP hijacking.

3.4 Consideraciones Bioéticas

Aunque esta investigación no involucra seres humanos ni datos sensibles de carácter personal, se ha tenido en cuenta un conjunto de principios bioéticos y de responsabilidad profesional durante todo el desarrollo del proyecto:

- Confidencialidad de la información: Todos los datos técnicos recolectados están relacionados exclusivamente con configuraciones de red, y no se accedió a información de carácter privado, de usuarios o de clientes.
- Autorización institucional: La intervención en la red fue realizada con autorización expresa de la gerencia de AIRMAXTELECOM SOLUCIONES TECNOLOGICAS S.A., bajo protocolos controlados y sin interrumpir el servicio a usuarios finales.

- Responsabilidad profesional y técnica: Se tomaron todas las precauciones necesarias para evitar impactos adversos en la calidad del servicio. Además, se documentaron todos los cambios en un entorno de control de versiones y auditoría.
- Respeto a normativas locales e internacionales: La investigación se enmarca en el cumplimiento de la normativa técnica de la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones del Ecuador), así como de los lineamientos establecidos por LACNIC para la gestión de recursos numéricos.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

En este capítulo se presentan los resultados obtenidos durante el desarrollo de la investigación orientada a fortalecer la seguridad del enrutamiento BGP en la red central de Airmaxtelecom Soluciones Tecnológicas S.A. mediante la implementación de infraestructura RPKI con la herramienta Routinator. Los resultados se ordenaron en función de los objetivos específicos, con el propósito de demostrar la evaluación de la solución implementada.

La investigación considera evidencias técnicas obtenidas mediante revisión, levantamiento de activos críticos, análisis de amenazas asociadas a BGP hijacking, creación de ROA en LACNIC, despliegue del validador Routinator, integración con el enrutador de borde Huawei NE8000 con el protocolo RTR y filtrado de rutas válidas, rutas inválidas y rutas no encontradas.

El capítulo se enfoca en demostrar que la implementación de RPKI no debe evaluarse únicamente desde parámetros de rendimiento, sino principalmente desde su perspectiva para mejorar la visibilidad del estado de validación de rutas de ingreso y permitir la mitigación de anuncios inválidos asociados a posibles eventos de secuestro de rutas.

4.1 Resultados de la revisión del estado del arte

Como resultado de la revisión bibliográfica, documental y normativa, se identificaron los fundamentos técnicos necesarios para comprender la problemática de seguridad asociada al protocolo BGP y la importancia de RPKI como mecanismo de validación criptográfica del origen de rutas en la Tabla 22 se muestra los elementos técnicos considerados en el estudio.

Tabla 22

Elementos técnicos identificados en el estado del arte

Elemento	Resultado
BGP	Protocolo esencial para el intercambio de rutas entre sistemas autónomos.
BGP hijacking	Amenaza que puede provocar redirección, interrupción o interceptación de tráfico mediante anuncios indebidos de prefijos.

RPKI	Herramienta que permite validar criptográficamente el origen de los prefijos IP.
ROA	Objeto que autoriza a un ASN específico a originar un prefijo con una longitud máxima determinada.
ROV	Proceso mediante el cual el router valida si una ruta BGP es válida, inválida o no encontrada.
LACNIC	RIR regional utilizada para la gestión de recursos y creación de ROA.
Routinator	Sistema validador de RPKI utilizado para consumir información global de ROA y entregarla a los routers mediante RTR.

Nota. La tabla presenta los principales elementos técnicos identificados en el estado del arte relacionados con Border Gateway Protocol y Resource Public Key Infrastructure. Elaboración propia.

La revisión permitió establecer que BGP, al ser el protocolo encargado del intercambio de rutas entre sistemas autónomos, no incorpora de forma nativa mecanismos suficientes para verificar si un ASN está autorizado a anunciar un prefijo IP determinado. Esta circunstancia representa una vulnerabilidad estructural que puede ser explotada mediante ataques de secuestro de rutas.

De igual forma, se comprobó que RPKI fortalece la seguridad del enrutamiento mediante la creación de objetos ROA, los cuales autorizan directamente a un ASN a originar determinados prefijos IPv4 y pueden clasificar los anuncios BGP como válidos, inválidos o no encontrados.

A nivel global, la adopción de RPKI se ha incrementado como respuesta técnica ante incidentes de seguridad relacionados con anuncios BGP erróneos, accidentales o maliciosos. Operadores de tránsito, puntos de intercambio de tráfico, proveedores de servicio de internet han incorporado la validación de origen como parte de sus políticas de seguridad de enrutamiento.

A nivel regional, particularmente en América Latina y el Caribe, los registros regionales de Internet han promovido el uso de RPKI como mecanismo para mejorar la confiabilidad del enrutamiento. Para organizaciones que administran recursos asignados por LACNIC, la creación de ROA constituye una medida fundamental para proteger los prefijos propios frente a anuncios no autorizados.

4.2 Resultados del análisis de vulnerabilidades validación de rutas

El diagnóstico inicial permitió identificar los componentes físicos, lógicos y documentales que intervienen en el proceso de enrutamiento BGP de la red central de Airmaxtelecom. Para ello, se consideraron los routers de borde, sesiones BGP, ASN, prefijos anunciados, proveedores de tránsito, políticas de enrutamiento, herramientas de monitoreo y configuraciones asociadas a la propagación de rutas.

La red central utiliza BGP para el intercambio de rutas con proveedores de IP Transit, CDNs y para la publicación de prefijos propios asociados al ASN de la empresa. Antes de la implementación de RPKI, se carecía de buenas prácticas operativas, sin contar con una validación criptográfica basada en ROA.

Por lo cual, la situación permitió identificar como principal debilidad la ausencia de un mecanismo local en el router de borde para clasificar las rutas recibidas como válidas, inválidas o no encontradas. Por tanto, la detección de posibles rutas asociadas a hijacking no se podía aplicar porque se recibía una ruta por defecto, adicionalmente se estableció controles como se muestran en la Tabla 23.

Tabla 23

Controles implementados

Control	Resultado	Evidencia
Crear ROA para prefijos IPv4 en LACNIC	Se registraron autorizaciones ROA para los prefijos 45.70.*.*/*, asociando cada bloque IP con el ASN 271933. Esto permitió que los prefijos de Airmaxtelecom puedan ser validados por terceros mediante RPKI.	Ver Figura 26 con la creación del objeto ROA desde el portal de, posteriormente visualizar Figura 27 para comprobar el estado de la propagación del prefijo con estado válido en un sistema de validación de rutas público como Radar CloudFlare.
Configurar validación RPKI en router de borde	Se habilitó la consulta RPKI desde los routers de borde hacia el validador Routinator	La Figura 28 muestra la conectividad del router de borde hacia el validador RPKI local

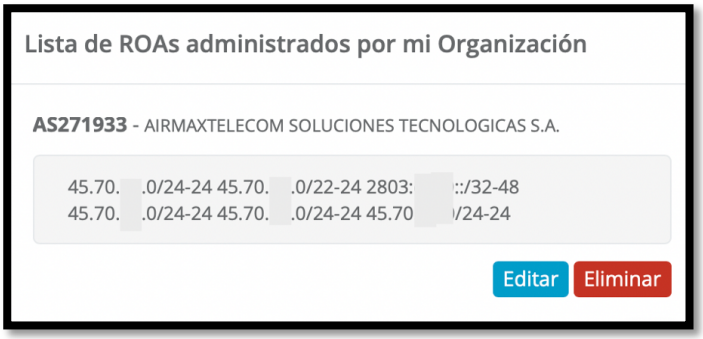
	mediante el protocolo RTR y clasifica 3 tipos de estados de RPKI	
Crear route-policy	Se implementaron políticas de enrutamiento para diferenciar rutas válidas, inválidas y no encontradas.	Configuración de route-policy, para prefijos con estado invalid y rutas aceptadas como valid o not-found, ver Figura 29 con las políticas de enrutamiento aplicadas en el router NE8000. La Figura 30 muestra el total de rutas válidas, inválidas y no encontradas en el peer aplicado el route policy. En la Figura 31 se visualizan los prefijos IPv4 categorizados con estado 'invalid' debido a una discrepancia en el Número de Sistema Autónomo (ASN).
Routinator y servicio RTR	Se supervisó la disponibilidad del validador RPKI y del servicio RTR, garantizando que los routers de borde puedan consultar de forma continua la información de validación.	Estado del servicio Routinator, con protocolo RTR activo, ver Figura 32 con la sesión establecida por el puerto 45323.

Nota. La tabla presenta los controles implementados para fortalecer la validación de rutas mediante Resource Public Key Infrastructure en el entorno de Border Gateway Protocol, junto con sus resultados y evidencias técnicas. Elaboración propia.

La Figura 26 muestra la creación de los ROA asociados a los prefijos administrados por Airmaxtelecom Soluciones Tecnológicas S.A. con el ASN 271933. De esta manera, el proceso contribuye a la adopción y validación RPKI, ya que permite declarar qué sistema autónomo puede anunciar los prefijos IP de la organización asignados.

Figura 26

ROA creado para el prefijo 45.70..*/* con ASN 271933*

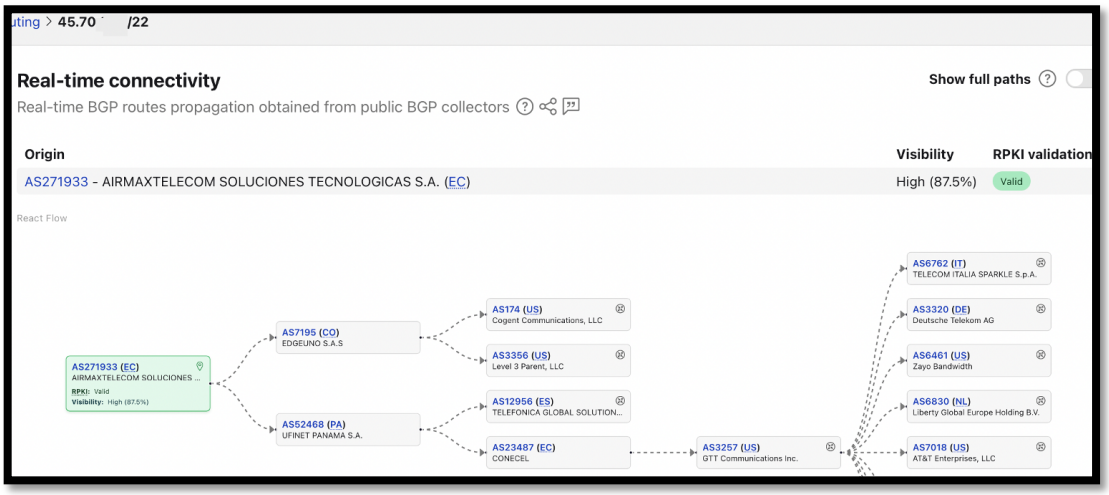


Fuente: (LACNIC, 2026)

Un validador global de RPKI como CloudFlare Radar reconoce como válido el anuncio de prefijo 45.70.*.*/22 anunciado vía BGP, y su coincidencia con el ROA registrado en la plataforma de LACNIC, ver Figura 27.

Figura 27

Propagación global y estado de validación RPKI del prefijo 45.70..*/22*

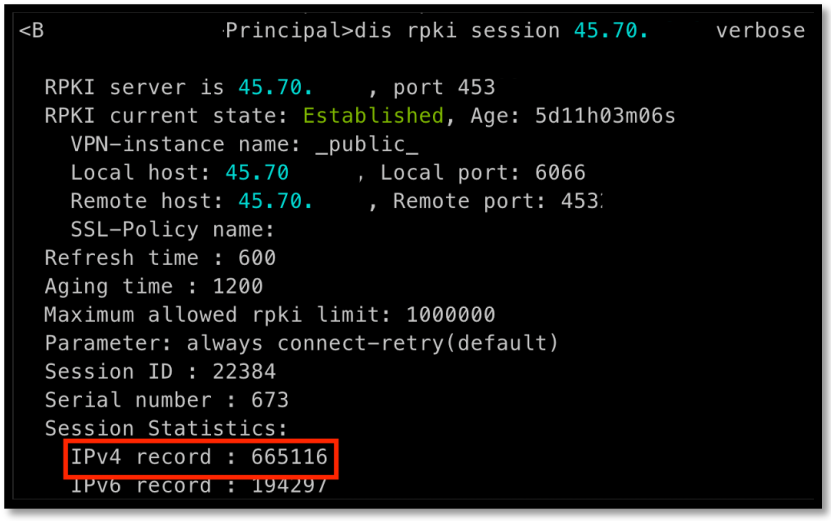


Fuente: (CloudFlare, 2026).

La Figura 28 muestra una sesión establecida con el protocolo RPKI-to-router entre un router de marca Huawei con el sistema validador de RPKI local instalado en un servidor de Airmaxtelecom Soluciones Tecnológicas S.A.

Figura 28

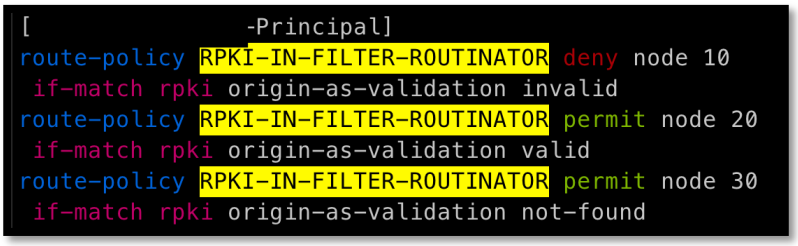
Protocolo RTR (RPKI-to-Router) entre el router de borde y el validador local



RPKI dispone de 3 estados de clasificación de rutas invalid, valid y not-found que se pueden utilizar en políticas de enrutamiento y determinar una acción cuando se cumpla la condición como se visualiza en la Figura 29 donde en el index 10 de niegan las rutas que contengan el marcador invalid, se permitan aprender las rutas cuando contengan el marcador valid y not-found.

Figura 29

Políticas de enrutamiento

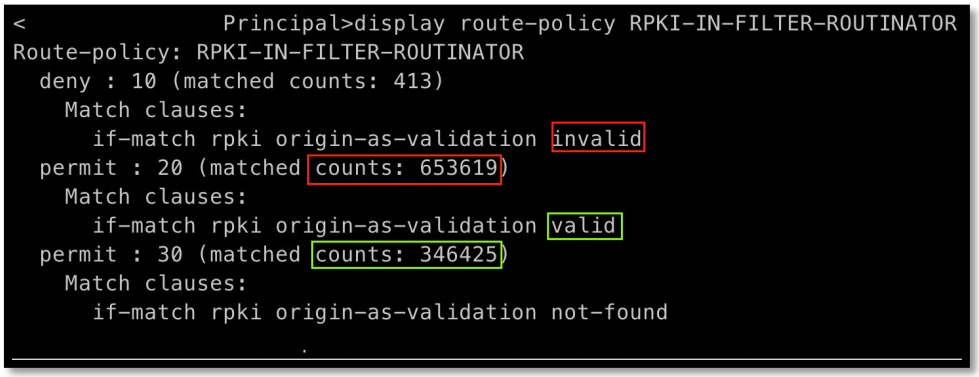


La Figura 30 muestra las estadísticas de coincidencia de la política RPKI activa en el router. Los contadores permiten comprobar cuántas rutas han coincidido con cada condición definida en la política, destacando los registros clasificados como invalid**,** valid **y** not-found**.** Por lo tanto, estos valores constituyen una evidencia técnica del funcionamiento de la

validación RPKI dentro del plano de control BGP y con ello mitigar eventos de BGP hijacking.

Figura 30

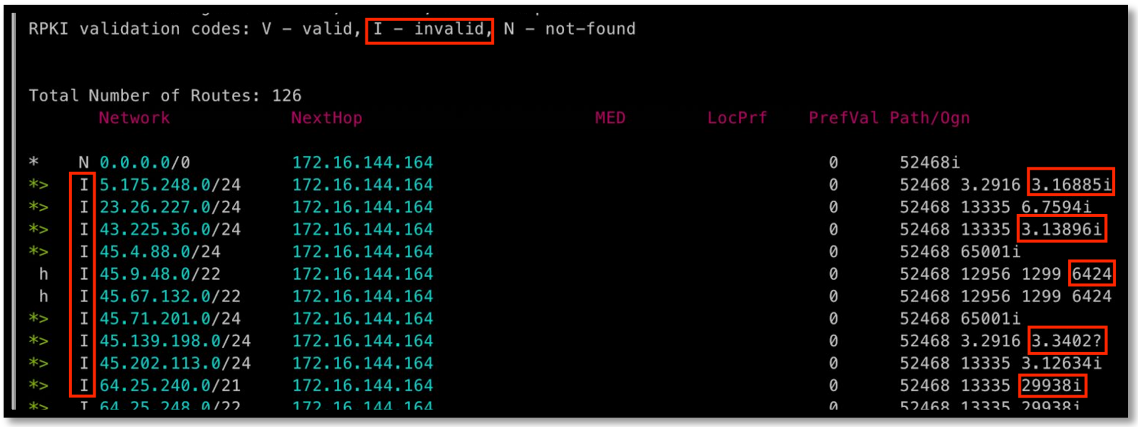
Estadísticas de coincidencia de RPKI activo



La Figura 31 presenta el detalle de los prefijos BGP clasificados con estado invalid dentro de la tabla de enrutamiento global recibida por el router de borde del peer 172.16.*.*, adicional se evidencia que en el número de sistema dentro del AS_PATH en algunos prefijos es privado y solo se utilizan en sesiones iBGP.

Figura 31

Detalle de prefijos BGP con estado "invalid" en la tabla de enrutamiento global



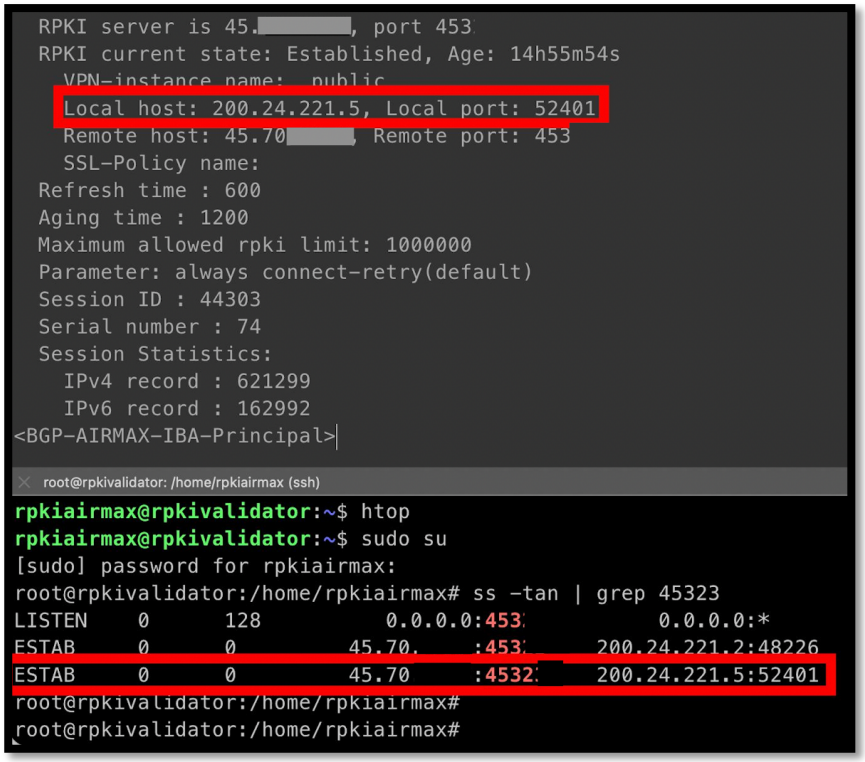
La Figura 32 muestra el estado de la sesión de tipo Established**,** lo que confirma que existe conectividad operativa entre el router de borde y el servidor Routinator. También se evidencia el uso del puerto 453**, junto con parámetros como el tiempo de actualización,

tiempo de envejecimiento, límite máximo de registros RPKI y la cantidad de registros IPv4 e IPv6 disponibles para consulta.

De forma complementaria, la parte inferior de la Figura 32 muestra la verificación del servicio desde el servidor Linux donde opera el validador RPKI. El uso del comando relacionado con el puerto 453** permite comprobar que el servicio RTR se encuentra activo y escuchando conexiones, lo cual respalda la disponibilidad del validador local.

Figura 32

Sesión establecida entre el validador RPKI y el router NE8000



4.3 Resultado de aplicación del sistema de validación RPKI

En el ecosistema de interconexión global, el protocolo BGP carece de mecanismos nativos de validación de origen de rutas, lo cual lo hace vulnerable a ataques de secuestro de prefijos. En respuesta a esta problemática, AIRMAXTELECOM ha iniciado la implementación de RPKI (Resource Public Key Infrastructure), una solución criptográfica

diseñada para autenticar que los sistemas autónomos (AS) que anuncian prefijos tienen autorización para hacerlo.

La validación de origen mediante RPKI permite a Airmaxtelecom Soluciones Tecnológicas S.A. proteger su espacio de direccionamiento, detectar anuncios ilegítimos y mitigar ataques como el BGP hijacking. Esta acción no solo incrementa la seguridad de la red interna y la de sus clientes, sino que también contribuye al ecosistema global del enrutamiento confiable.

Airmaxtelecom Soluciones Tecnológicas S.A. es una empresa ecuatoriana que opera como proveedor de servicios de Internet. Su infraestructura incluye sistemas autónomos y prefijos IPv4 e IPv6 asignados por LACNIC. Dado el crecimiento sostenido del tráfico y de los clientes corporativos y residenciales, la organización enfrenta riesgos significativos relacionados con la integridad del enrutamiento inter-AS.

Como parte de su compromiso con la seguridad, la empresa está implementando controles técnicos como la validación RPKI y la monitorización de rutas mediante plataformas como, RADAR Qrator ver Tabla 24 con los datos de eventos de secuestro de rutas.

Tabla 24

Eventos de hijacks de base de datos RadarQrator

ASN	Hijacker	Hijacker Prefix	ASN Afectado	ISP Afectado	Prefijo afectado	Año	Severidad
271933	AIRMAXTELECOM	45.70.*2.0/24	52468	UFINET	45.70.*2.0/22	2023	high
271933	AIRMAXTELECOM	45.70.*2.0/24	264668	NEGOCIOS	45.70.*2.0/22	2023	high
271933	AIRMAXTELECOM	45.70.*2.0/24	52468	UFINET	45.70.*2.0/24	2023	high
271933	AIRMAXTELECOM	45.70.*2.0/24	264668	NEGOCIOS	45.70.*2.0/24	2023	high
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low

52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	medium
60566		45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*2.0/24	2023	low
60566		45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
60566		45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*2.0/24	2023	low
60566		45.70.*2.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low

52468	UFINET	45.70.**2.0/32	271933	AIRMAXTELECOM	45.70.*3.0/22	2023	low
52468	UFINET	45.70.**2.0/32	271933	AIRMAXTELECOM	45.70.*3.0/22	2024	medium
52468	UFINET	45.70.**2.0/32	271933	AIRMAXTELECOM	45.70.*3.0/22	2024	medium
262378	Compuservice	45.70.*3.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2024	low
262378	Compuservice	45.70.*5.0/22	271933	AIRMAXTELECOM	45.70.*5.0/22	2024	low
262378	Compuservice	45.70.*2.0/24	271933	AIRMAXTELECOM	45.70.*2.0/24	2024	low
262378	Compuservice	45.70.*4.0/22	271933	AIRMAXTELECOM	45.70.*4.0/22	2024	low
268976	Weclix	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*2.0/24	2024	low
268976	Weclix	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*5.0/22	2024	low
268976	Weclix	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*4.0/22	2024	low
268976	Weclix	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*3.0/22	2024	low
52925	Ascenty	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*4.0/22	2024	low
52925	Ascenty	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*5.0/22	2024	low
52925	Ascenty	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*3.0/22	2024	low
52925	Ascenty	45.0.0.0/8	271933	AIRMAXTELECOM	45.70.*2.0/24	2024	low
53427	TGLOBAL-NETWORKS	45.70.*2.0/24	271933	AIRMAXTELECOM	45.70.*2.0/24	2025	low
53427	TGLOBAL-NETWORKS	45.70.*5.0/22	271933	AIRMAXTELECOM	45.70.*5.0/22	2025	low
53427	TGLOBAL-NETWORKS	45.70.*4.0/22	271933	AIRMAXTELECOM	45.70.*4.0/22	2025	low

53427	TGLOBAL-NETWORKS	45.70.*3.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2025	low
52741	MC	45.70.*3.0/22	271933	AIRMAXTELECOM	45.70.*3.0/22	2025	low
52741	MC	45.70.*4.0/22	271933	AIRMAXTELECOM	45.70.*4.0/22	2025	low
52741	MC	45.70.*5.0/22	271933	AIRMAXTELECOM	45.70.*5.0/22	2025	low
52741	MC	45.70.*2.0/24	271933	AIRMAXTELECOM	45.70.*2.0/24	2025	low

***Nota*.** La tabla presenta los eventos de BGP Hijacking identificados sobre los prefijos IPv4 asociados al ASN 271933 de Airmaxtelecom, considerando ASN involucrados, prefijos afectados, año y nivel de severidad. Elaboración propia.

Tabla 25

Clasificación de eventos de hijacks

Año	Estado	Registros	Severidad alta	Severidad media	Severidad baja
2023	Sin RPKI	25	4	1	20
2024	Sin RPKI	14	0	2	12
2025	Con RPKI	8	0	0	8
2026	Con RPKI	0	0	0	0

Nota. La tabla presenta la clasificación de eventos de BGP Hijacking registrados antes y después de la implementación de Resource Public Key Infrastructure, considerando cantidad de registros y nivel de severidad. Elaboración propia.

Los datos muestran que la implementación de RPKI contribuye a reducir la incidencia de eventos asociados a posibles secuestros de rutas BGP. En el período previo a la implementación, correspondiente a 2023 y 2024, se registraron 39 eventos, incluyendo 4 de severidad alta y 3 de severidad media. En contraste, durante el período con RPKI, correspondiente a 2025 y 2026, se registraron únicamente 8 eventos, todos de severidad baja, la creación de la autorización de origen de ruta desde la cuenta MiLacnic en la fecha 26 de

abril del año 2025 es el paso inicial para evitar los eventos de secuestro de rutas que respaldan los datos obtenidos.

La reducción representa una disminución del 79,49 % en los registros observados. Además, la ausencia de eventos de severidad alta y media en el período posterior permite evidenciar una mejora en el comportamiento de seguridad del enrutamiento.

La Tabla 26 evidencia el comportamiento de la red antes y después de la implementación de RPKI, se consideraron parámetros básicos de rendimiento como la latencia, la pérdida de paquetes y desviación estándar. Estos indicadores fueron levantados mediante pruebas ICMP extraídas por medio del protocolo SNMP desde el router de borde Huawei NE8000 hacia un destino de referencia en Internet y con pruebas mediante la herramienta MTR, utilizando como punto de prueba el DNS público de Google 8.8.8.8 y cloudflare 1.1.1.1 debido a que son uno de los servicios más utilizados y comunes en procesos de diagnóstico, verificación de conectividad y solución de problemas en redes.

Tabla 26

Comparación de parámetros de rendimiento antes y después de la implementación de RPKI

Parámetro	**Ruta de prueba**	**Forma de evidencia**	**Antes de implementar RPKI**	**Después de implementar RPKI**	**Evidencia**
Latencia	8.8.8.8	Medición ICMP hacia destino de referencia mediante pruebas de ping	Min 17ms Prom 17,2ms Max 18ms	Min 16,1ms Prom 17,1ms Max 20,5ms	Ver Figura 33 donde se hace la prueba al dns 8.8.8 antes de implementar RPKI y Figura 34, Figura 35 y Figura 36 después de implementar la herramienta de validación de rutas en diferentes rangos de horarios
Pérdida de paquetes	8.8.8.8	Medición de paquetes enviados, recibidos y perdidos mediante pruebas ICMP.	0%	0,0003%	

Desviación estándar		Toma de múltiples muestras de latencia en distintos horarios.	0,2	0,3	Visualizar Tabla 27 con el resumen general del análisis de la información recopilada
Latencia	1.1.1.1	Medición ICMP hacia destino de referencia mediante pruebas de ping	Min 9,1ms Prom 9,1ms Max 9,9ms	8ms	Ver Figura 37 donde se hace la prueba al dns 1.1.1.1 antes de implementar RPKI y Figura 38,Figura 39 y Figura 40 después de implementar la herramienta de validación de rutas
Pérdida de paquetes	1.1.1.1	Medición de paquetes enviados, recibidos y perdidos mediante pruebas ICMP.	0%	0,0007%	
Desviación estándar		Toma de múltiples muestras de latencia en distintos horarios.	0,2	0,8	Visualizar Tabla 28 con el resumen general del análisis de la información recopilada

Nota. La tabla presenta la comparación de latencia y pérdida de paquetes antes y después de la implementación de Resource Public Key Infrastructure. Elaboración propia.

La Figura 33 muestra la prueba de conectividad realizada antes de la implementación de RPKI, utilizando la herramienta MTR hacia la dirección IP 8.8.8.8**,** correspondiente al DNS público de Google, la herramienta MTR combina funciones de ping y trazo de ruta para recopilar datos desde un equipo hasta un destino.

Figura 33

*Prueba de ping y paquetes perdidos antes de implementar **RPKI***

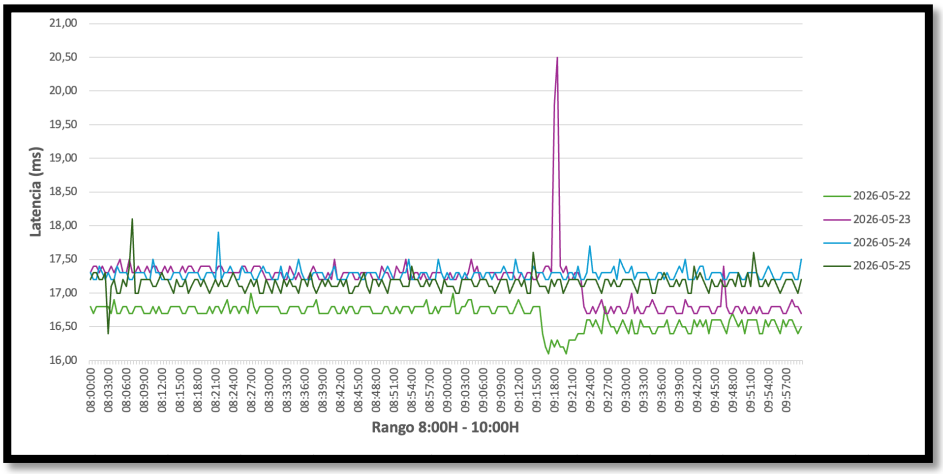
```
                                My traceroute  [v0.95]
             (45.70     ) -> 8.8.8.8 (8.8.8.8)
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets               Pings
 Host                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. edge-     -70-45.iplus.com.ec       0.0%  3221    0.1   0.1   0.1   0.7   0.2
 2. 10.12.19.1                          0.0%  3221    0.9   0.7   0.5  27.3   1.2
 3. 218.81.78.181                       0.1%  3221   17.3  18.6  17.1  46.2   3.9
 4. 142.250.167.108                     0.0%  3220   17.8  17.6  17.5  19.7   0.3
 5. 192.178.97.105                      0.0%  3220   17.6  17.5  17.4  19.6   0.3
 6. 142.250.215.109                     0.0%  3220   17.1  17.0  16.9  18.4   0.2
 7. dns.google                          0.0%  3220   17.2  17.1  17.0  18.0   0.2
```

Nota. La herramienta MTR muestra una latencia promedio de 17,1ms, con un valor mínimo de 17ms, valor máximo de 18ms y sin pérdida de paquetes de un total de 3220 paquetes enviados. La desviación estándar de 0,2 indica la variabilidad en la respuesta ICMP es estable.

La Figura 34, Figura 35 y Figura 36 presentan las pruebas de conectividad realizadas después de la implementación de RPKI hacia la dirección IP 8.8.8.8 en varios rangos de horarios. Esta verificación permite comparar el comportamiento de la red luego de activar la validación de origen de rutas, las políticas de filtrado de rutas BGP no causan degradación en el servicio**.**

Figura 34

Prueba de ping durante el rango 8:00h – 10:00h después de implementar RPKI

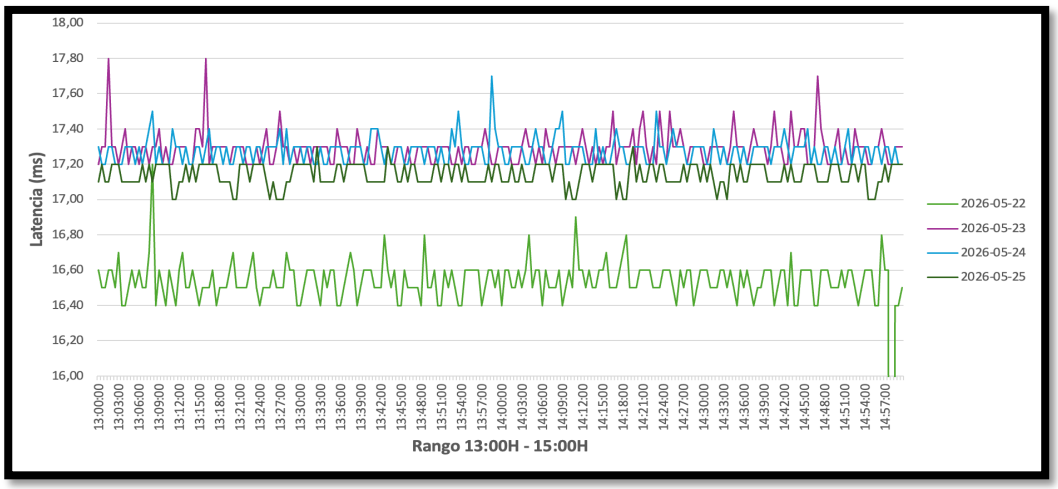


Nota. La figura muestra la variación de la latencia en el intervalo de 8h00 a 10h00 correspondientes a los días 22, 23,24 y 25 de mayo de 2026 con un comportamiento estable promedio de 17ms, el día 22 de mayo de 2026 se evidencia una ligera reducción de latencia cercana a los 16ms, y el día 23 de mayo

de 2026 un pico aislado de 20,5ms, el cual no representa una degradación del servicio. Elaboración propia.

Figura 35

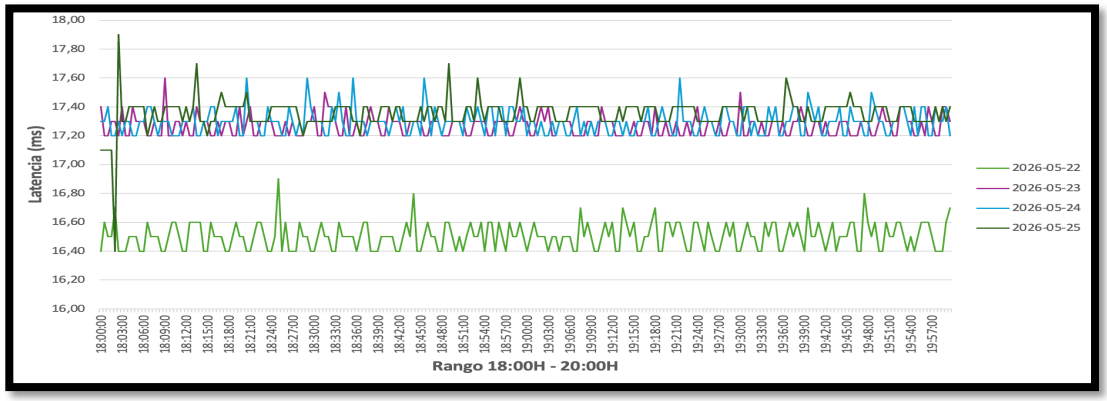
Prueba de ping en rango de horario de 13:00h – 15:00h después de implementar RPKI



Nota. La figura presenta la variación de latencia durante el periodo evaluado, evidenciando un comportamiento estable en la mayoría de las muestras, con valores promedio próximos a 17ms, adicional se observa que el día 22 de mayo de 2026 tiene un promedio de 16ms. Elaboración propia.

Figura 36

Prueba de ping en rango de horario de 18:00h – 20:00h después de implementar RPKI



Nota. La figura muestra la latencia registrada entre las 18h00 y 20h00 durante los días evaluados. En general, los valores se mantienen estables y próximos a 17 ms, mientras que el 22 de mayo de 2026 se observa una latencia ligeramente menor, sin evidenciar afectación continua del servicio. Elaboración propia.

De acuerdo con los datos registrados en la Tabla 27, antes de la implementación de RPKI se obtuvieron 3220 muestras válidas, sin pérdida de paquetes, con una latencia

promedio de 17,2 ms y una desviación estándar de 0,2 ms. Después de la implementación, se registraron 2880 muestras totales, de las cuales 2879 fueron válidas, evidenciando una pérdida mínima equivalente a 0,03 % aproximadamente. La latencia promedio se mantuvo en 17,1 ms, con una desviación estándar de 0,3 ms.

Tabla 27

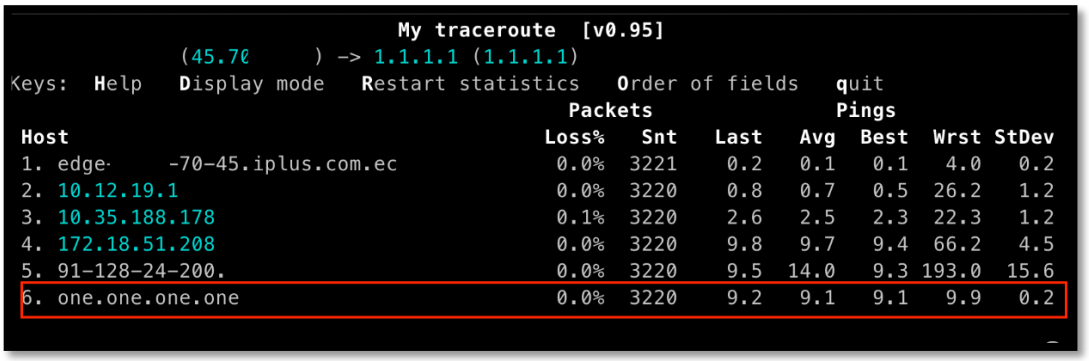
Comparación de métricas ICMP hacia 8.8.8.8 antes y después de la implementación de RPKI

Estado	Muestras totales	Muestras válidas	Perdida %	Min. ms	Prom. ms	Max. ms	Desv. Estándar
Antes de implementar RPKI	3220	3220	0	17	17,2	18	0,2
Después de implementar RPKI	2880	2879	0,0003	16,1	17,1	20,5	0,3

La Figura 37 presenta la prueba de conectividad efectuada antes de la implementación de RPKI, mediante el uso de mensajes ICMP dirigidos a la dirección IP 1.1.1.1

Figura 37

*Prueba de ping y paquetes perdidos antes de implementar **RPKI***



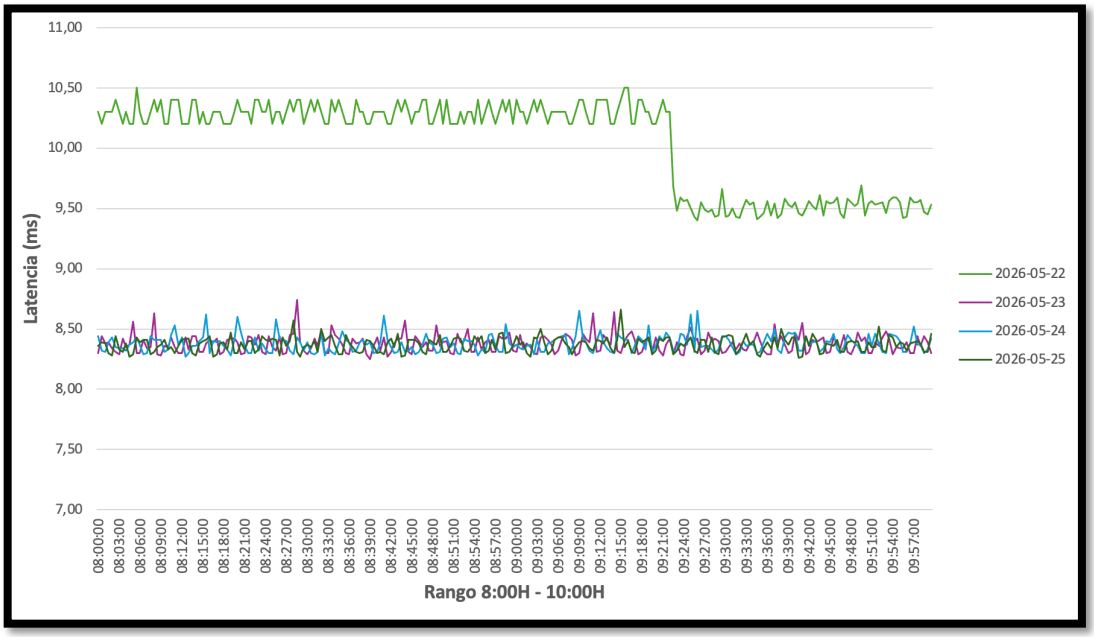
Nota. La herramienta MTR muestra una latencia promedio de 9,1ms, con un valor mínimo de 9,1ms, valor máximo de 9,9ms y con una pérdida de paquetes de cero por ciento de 3220 paquetes enviados. La desviación estándar de 0,2 evidencia una baja variabilidad en las respuestas ICMP, lo que refleja un comportamiento estable durante el periodo analizado.

Al comparar las pruebas de Figura 38, Figura 39 y Figura 40 se observa que la comunicación hacia el destino se mantiene estable en los diferentes horarios de recopilación

de datos ICMP. Los resultados permiten determinar que la implementación de RPKI no afectó de forma negativa la latencia ni la pérdida de paquetes, debido a que RPKI opera sobre el plano de control BGP y no directamente sobre el reenvío de paquetes.

Figura 38

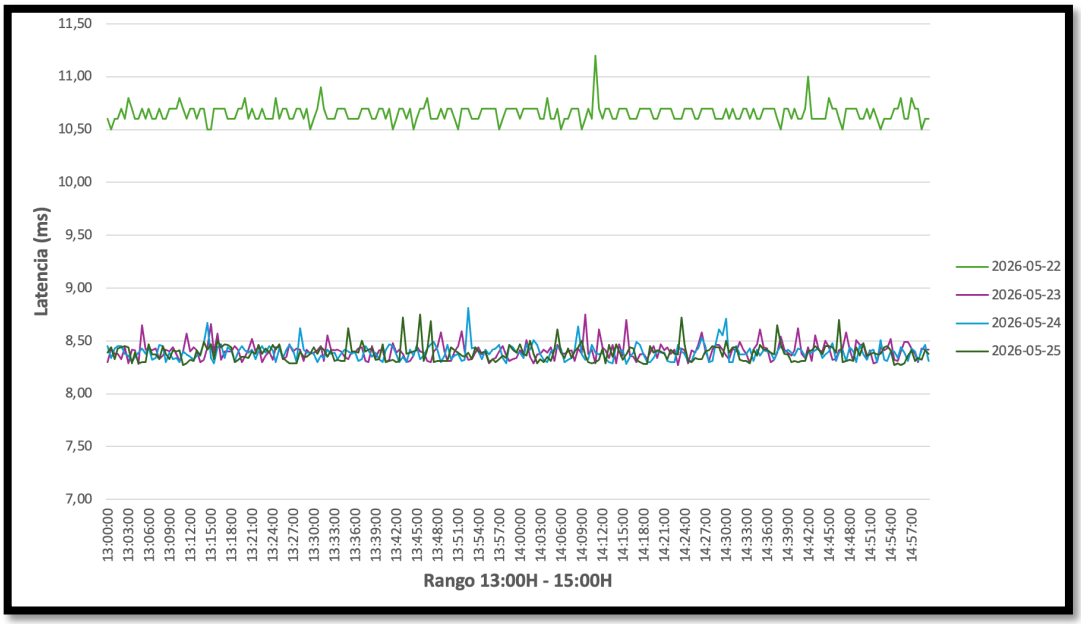
Prueba de ping durante el rango 8:00h – 10:00h después de implementar RPKI



Nota. La figura presenta la latencia registrada entre las 8h00 y 10h00 durante los días evaluados. En general, los valores se mantienen estables y cercanos a 8,5ms, mientras que el 22 de mayo de 2026 se observa una latencia superior hasta las 9h21, sin evidenciar impacto del servicio. Elaboración propia.

Figura 39

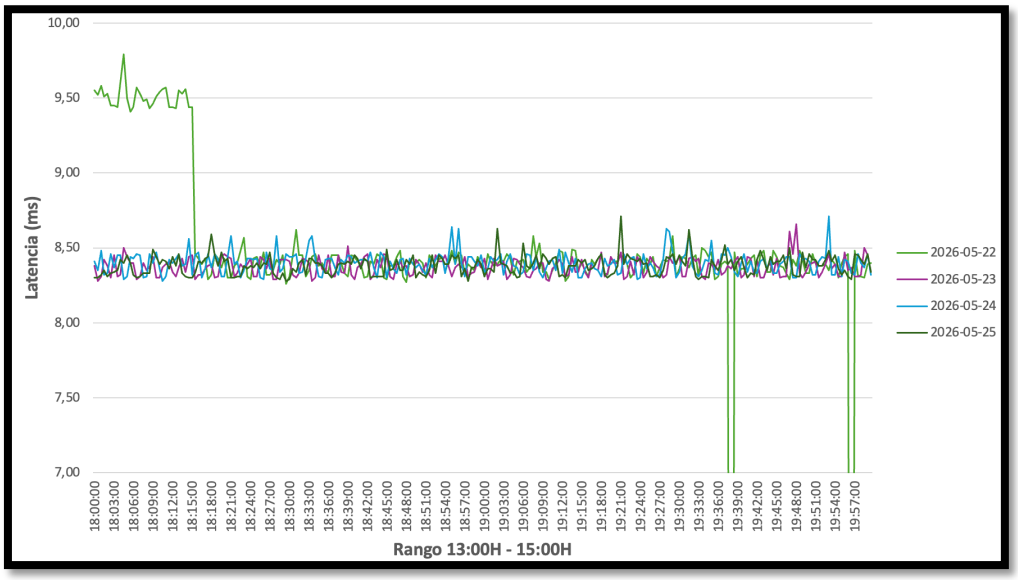
Prueba de ping durante el rango 13:00h – 15:00h después de implementar RPKI



Nota. La figura presenta la latencia registrada entre las 13h00 a 15h00 durante los días evaluados. De general, los valores se mantienen un comportamiento a 8,5ms, mientras que el 22 de mayo de 2026 se observa una latencia promedio de 10,6ms estables. Elaboración propia.

Figura 40

Prueba de ping durante el rango 18:00h – 20:00h después de implementar RPKI



Nota. La figura muestra que en la mayoría de las muestras de latencia el promedio es de 8,5ms durante el rango de 18h00 a 20h00. El 22 de mayo de 2026 se observa una pérdida de información a las 19h38 y 19h56, sin registrar impacto sobre el servicio. Elaboración propia.

Tabla 28

Comparación de métricas ICMP hacia 1.1.1.1 antes y después de la implementación de RPKI

Estado	Muestras totales	Muestras válidas	Perdida %	Min. ms	Prom. ms	Max. ms	Desv. Estándar
Antes de implementar RPKI	3220	3220	0	17	17,2	18	0,2
Después de implementar RPKI	2880	2878	0,0007	8,25	8,7	11,2	0,8

Al comparar las pruebas antes y después, se evidencia que la latencia conserva un comportamiento estable, demostrando que la validación RPKI no introduce retardos significativos en el tráfico de datos, se debe considerar que, para aprovechar los recursos de CPU, la validación de rutas inválidas se debe ejecutar al inicio de las políticas de enrutamiento para descartarlas y no consumir recursos valiosos del router de borde, a partir del 31 de marzo de 2026 se integra la herramienta de Routinator a la par de las Route Policy en el router Huawei NE8000 complementando la fortaleza de la solución propuesta.

Se concluye que la aplicación del sistema de validación de rutas basado en RPKI está empezando a cumplir su función como mecanismo de prevención y detección temprana de ataques de hijacking, alineándose con el objetivo de fortalecer la seguridad y eficiencia del tráfico en la red de Airmaxtelecom Soluciones Tecnológicas S.A.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Dentro de la revisión del estado del arte, se realizó una búsqueda y análisis de los principales elementos técnicos orientados al fortalecimiento de la seguridad del enrutamiento BGP. La recopilación de información relevante sobre RPKI, secuestro de rutas BGP, ROA y ROV permitió comprender los fundamentos teóricos necesarios y relacionarlos con su aplicación práctica en un sistema de validación de rutas, orientado a mejorar la seguridad frente a posibles eventos de secuestro de rutas.

El análisis del estado actual de la red central de Airmaxtelecom Soluciones Tecnológicas S.A permitió reconocer los activos críticos y asociarlos a vulnerabilidades, riesgos asociados al proceso de networking mediante el enrutamiento eBGP con peers de IP Transit o CDNs. Se evidencio que al recibir una ruta por defecto no se puede aplicar la validación RPKI debido a que las rutas no se pueden clasificar como válidas, inválidas y no encontradas, adicional la ausencia de objetos ROA abre las posibilidades de eventos de BGP hijacking.

La creación de ROAs en la cuenta de LACNIC permitió autorizar los prefijos IPv4 45.70.*.*/22 con el ASN 271933 perteneciente a la organización Airmaxtelecom Soluciones Tecnológicas S.A., esta acción mejoró la protección de los recursos asignados al proveedor de servicio de internet a nivel regional y contribuyo al fortalecimiento de rutas válidas en ecosistema global de internet cuando se verifique la legitimidad de los anuncios por BGP.

Con respecto a la implementación de un sistema RPKI local, el uso de Routinator junto con el router Huawei NE8000 M4 permitió integrar la validación del origen de rutas mediante la sincronización de la base de datos alojada en el Registro Regional de Internet. A través del protocolo RTR, el router de borde pudo recibir la información de validación y aplicar políticas de enrutamiento para clasificar las rutas en la tabla local como válidas, inválidas o no encontradas.

Además, la evaluación realizada antes y después de la implementación permitió evidenciar que RPKI no introdujo una degradación observable en las pruebas de conectividad. Los valores de latencia se mantuvieron con rangos similares gracias a la robustez del equipo Huawei NE8000 el cual está diseñado para trabajar con grandes volúmenes de tráfico y políticas avanzadas en anuncios BGP, por otra parte, la pérdida de paquetes tras implementar RPKI fue mínima, lo que garantiza que la calidad del servicio no sufrió ninguna degradación perceptible.

Recomendaciones

A la Universidad Técnica del Norte, que continúe brindando acceso a plataformas virtuales, bases de datos científicas, bibliotecas digitales y recursos académicos especializados. Esto permitirá que futuras investigaciones relacionadas con seguridad en redes, enrutamiento BGP, RPKI y protección de infraestructuras críticas cuenten con sustento científico y técnico actualizado.

A la empresa Airmaxtelecom Soluciones Tecnológicas S.A., que continúe invirtiendo en infraestructura tecnológica robusta para fortalecer la seguridad, disponibilidad y escalabilidad de su red central. Adicional se recomienda que se implemente un segundo servidor RPKI local en alta disponibilidad o respaldo, con el objetivo de mantener resiliencia ante fallas del servidor principal Routinator.

A los administradores y operadores de red, que mantengan una revisión periódica de los ROA publicados en los Registros Regionales de Internet, especialmente cuando existan cambios en prefijos IPv4, longitudes máximas que se anunciar a los IP Transit. Esta práctica es necesaria para evitar configuraciones incorrectas que puedan provocar que rutas legítimas sean clasificadas como inválidas por otros sistemas autónomos que aplican validación RPKI.

Al personal técnico del área de redes, que realice auditorías periódicas de las políticas de enrutamiento aplicadas en los routers de borde, principalmente aquellas asociadas a la validación RPKI. Por lo tanto, esto permitirá verificar que las rutas inválidas sean rechazadas correctamente, que las rutas válidas sean aceptadas y que las rutas no encontradas sean tratadas de acuerdo con la política operativa definida por la empresa.

A futuros investigadores, que amplíen el alcance de este estudio hacia la validación de rutas IPv6 mediante RPKI, considerando que el crecimiento del tráfico IPv6 requiere mecanismos de seguridad similar a los aplicados en IPv4. Esto permitiría mantener una política homogénea de protección para todos los recursos asignados a la organización.

GLOSARIO DE TÉRMINOS

ARCOTEL. Agencia de Regulación y Control de las Telecomunicaciones del Ecuador. Es la entidad pública responsable de regular y controlar el uso del espectro radioeléctrico y la prestación de servicios de telecomunicaciones. En el contexto de un ISP, constituye una referencia institucional para aspectos regulatorios, continuidad, calidad del servicio, seguridad de comunicaciones y protección de usuarios (Agencia de Regulación y Control de las Telecomunicaciones, 2024)

ASN. Autonomous System Number o Número de Sistema Autónomo. Es un identificador único asignado a una red o conjunto de redes bajo una misma administración técnica y política de enrutamiento. En BGP, el ASN identifica el dominio administrativo que origina, recibe o propaga rutas hacia otros Sistemas Autónomos (LANIC, 2023).

AS-PATH. Atributo de BGP que contiene la secuencia de Sistemas Autónomos atravesados por una ruta. Este atributo ayuda a prevenir bucles y puede influir en la selección de rutas. Aunque un AS-PATH más corto suele ser preferido, la decisión final depende de las políticas de enrutamiento del operador y de otros atributos BGP (Xu, 2019).

BGP. Border Gateway Protocol o Protocolo de Pasarela de Borde. Es el protocolo de enrutamiento interdominio utilizado para intercambiar información de conectividad entre Sistemas Autónomos en Internet. BGP permite aplicar políticas de enrutamiento y seleccionar rutas mediante atributos como AS-PATH, LOCAL_PREF, MED y NEXT_HOP (Scott & Johnstone, 2024).

BGP hijacking. Secuestro de rutas BGP. Es un incidente en el cual un Sistema Autónomo anuncia, de manera maliciosa o accidental, prefijos IP que no le pertenecen o que no está autorizado a originar. Este evento puede provocar redirección de tráfico, interrupción del servicio, pérdida de disponibilidad, interceptación de tráfico o degradación de la reputación del operador afectado (Milolidakis et al., 2023).

BGPsec. Extensión de BGP orientada a proporcionar protección criptográfica sobre el camino de Sistemas Autónomos incluido en los anuncios BGP, este busca proteger la integridad del AS-PATH mediante firmas digitales asociadas a los Sistemas Autónomos que propagan el anuncio (Rodday & Cunha, 2024).

Blockchain. Tecnología de registro distribuido en la que la información se agrupa en bloques enlazados criptográficamente. Aunque comparte el uso de criptografía con otros mecanismos de seguridad, no debe confundirse con RPKI. RPKI se basa en certificados digitales, jerarquía de recursos y objetos firmados para validar autorizaciones de enrutamiento, mientras que blockchain se orienta a registros distribuidos y consenso entre participantes (Rodday & Cunha, 2024).

CDN. Content Delivery Network o Red de Distribución de Contenido. Es una infraestructura distribuida que almacena o entrega contenido desde ubicaciones cercanas al usuario final. Para un ISP, la interconexión con CDNs puede reducir latencia, optimizar consumo de tránsito internacional y mejorar la experiencia de acceso a servicios de video, aplicaciones web y contenido estático (Anderson & Salamatian, 2022).

CSIRT. Computer Security Incident Response Team o Equipo de Respuesta ante Incidentes de Seguridad Informática. Es un equipo especializado en prevenir, coordinar, gestionar y responder a incidentes de ciberseguridad. En Ecuador, EcuCERT actúa como centro de respuesta a incidentes informáticos de ARCOTEL y contribuye a la seguridad de las redes de telecomunicaciones e Internet (Buenaño, 2024).

EGSI. Esquema Gubernamental de Seguridad de la Información. En Ecuador, es un marco orientado a preservar la confidencialidad, integridad y disponibilidad de la información mediante gestión de riesgos y selección de controles de seguridad (Proaño, 2024).

Hanging ROA. Término asociado a propuestas de codificación o gestión de ROA en RPKI. En el enfoque operativo de esta tesis, puede entenderse como una autorización ROA que permanece publicada pese a cambios en la relación técnica o administrativa del prefijo, del

ASN autorizado o del proveedor. Esta condición puede generar autorizaciones residuales o resultados inesperados durante la validación de origen. Para evitar ambigüedad, se recomienda explicar el término dentro del alcance de la investigación y relacionarlo con la correcta gestión del ciclo de vida de los ROA (Li et al., 2022).

IETF. Internet Engineering Task Force. Es la comunidad internacional responsable del desarrollo de estándares técnicos de Internet mediante documentos RFC. En esta tesis, la IETF es relevante porque protocolos y mecanismos como BGP, RPKI, ROV y BGPsec se encuentran especificados en RFC publicados dentro de este ecosistema técnico (Carle & Ott, 2021).

ISP. Internet Service Provider o Proveedor de Servicios de Internet. Es una organización que ofrece conectividad a Internet a usuarios residenciales, empresas, entidades públicas u otros operadores. En el contexto de esta investigación, el ISP administra infraestructura de red, enlaces de tránsito, sesiones BGP, políticas de enrutamiento, prefijos IPv4/IPv6 y recursos asociados a su Sistema Autónomo (Ortiz & Vizñay, 2020).

IXP. Internet Exchange Point o Punto de Intercambio de Internet. Es una infraestructura donde múltiples Sistemas Autónomos se interconectan para intercambiar tráfico directamente. Su uso permite reducir dependencia de tránsito, mejorar latencia y optimizar el intercambio de tráfico local o regional entre operadores, redes académicas, empresas y CDNs (AEPROVI, 2020).

LACNIC. Latin American and Caribbean Internet Addresses Registry. Es el Registro Regional de Internet para América Latina y el Caribe. Administra recursos de numeración de Internet, como direcciones IP versión 4, versión 6 y ASN. Para un ISP ecuatoriano, LACNIC es la entidad regional ante la cual se gestionan recursos propios, certificados RPKI y objetos asociados al enrutamiento (LANIC, 2026).

MANRS. Mutually Agreed Norms for Routing Security. Es una iniciativa global que promueve buenas prácticas para mejorar la seguridad del enrutamiento en Internet. Sus

acciones incluyen filtrado de rutas, prevención de suplantación de direcciones, coordinación operativa y publicación de información para validación por terceros (Mutually Agreed Norms for Routing Security, 2026).

MINTEL. Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador. Es el órgano rector del desarrollo de las tecnologías de la información y comunicación, telecomunicaciones, espectro radioeléctrico y sociedad de la información. En esta tesis puede citarse como referencia institucional para políticas públicas, transformación digital y lineamientos TIC en Ecuador (Proaño, 2024).

OpenBSD. Sistema operativo libre, tipo UNIX, basado en 4.4BSD. Es reconocido por su énfasis en portabilidad, estandarización, corrección de código, seguridad proactiva y criptografía integrada. En entornos de red, OpenBSD es relevante por herramientas como OpenSSH y PF, utilizadas ampliamente en administración y seguridad de sistemas (Friedemann, 2022).

Peering. Relación de interconexión entre dos Sistemas Autónomos para intercambiar tráfico directamente. Puede ser público, a través de un IXP, o privado, mediante enlaces dedicados. Para un ISP, el peering permite reducir costos de tránsito, mejorar latencia y optimizar el acceso a redes de contenido u otros operadores (AEPROVI, 2020).

Prefijo IP. Bloque de direcciones IPv4 o IPv6 expresado mediante notación CIDR, por ejemplo, 45.70.*2.0/22 o 2803:c42::/32. En BGP, los prefijos representan redes alcanzables que pueden ser anunciadas por un ASN hacia otros Sistemas Autónomos. En RPKI, los prefijos se asocian a ROA para validar qué ASN está autorizado a originarlos (Jaw et al., 2024).

Proveedor de tránsito. Operador que brinda conectividad hacia Internet global a otro Sistema Autónomo. A diferencia del peering, donde se intercambia tráfico hacia redes específicas, el tránsito permite alcanzar redes de terceros y recibir rutas globales o parciales.

Para un ISP, los proveedores de tránsito son esenciales para conectividad internacional, redundancia y disponibilidad (Guerra, 2019).

RIR. Regional Internet Registry o Registro Regional de Internet. Es una organización responsable de administrar, asignar y registrar recursos numéricos de Internet en una región geográfica específica. Estos recursos incluyen direcciones IPv4, IPv6 y ASN, utilizados por proveedores de Internet, operadores, centros de datos, instituciones y organizaciones con infraestructura propia (LANIC, 2023).

ROA. Route Origin Authorization o Autorización de Origen de Ruta. Es un objeto firmado digitalmente dentro de RPKI que permite verificar que el titular de un bloque de direcciones IP ha autorizado a un Sistema Autónomo específico a originar rutas para uno o varios prefijos. Un ROA normalmente incluye el prefijo, el ASN autorizado y la longitud máxima permitida del anuncio (Bush & Austein, 2020).

ROAchain. Cadena de validación RPKI o cadena de confianza RPKI. Hace referencia al proceso mediante el cual un ROA se valida criptográficamente desde una autoridad de confianza, pasando por certificados de recursos, autoridades certificadoras y objetos firmados, hasta llegar a los datos utilizados para la validación del origen de rutas. En redacción académica se recomienda utilizar el término cadena de confianza RPKI para mayor claridad (He et al., 2021).

Route leaks. Fugas de rutas. Son incidentes en los que un Sistema Autónomo propaga anuncios BGP más allá del alcance previsto por las políticas de enrutamiento. A diferencia del secuestro de rutas, una fuga puede involucrar rutas legítimamente aprendidas, pero anunciadas incorrectamente a otros proveedores o pares, causando rutas subóptimas, congestión, pérdida de conectividad o redirección no deseada del tráfico (Shen & Wang, 2024).

ROV. Route Origin Validation o Validación del Origen de Rutas. Es el proceso mediante el cual una ruta BGP recibida se compara con la información RPKI disponible para determinar

si el ASN de origen está autorizado a anunciar el prefijo. El resultado puede clasificarse como Valid, Invalid o NotFound, según la coincidencia con los Validated ROA Payloads (Li & Lin, 2023)

RPKI. Resource Public Key Infrastructure o Infraestructura de Clave Pública de Recursos. Es una infraestructura criptográfica diseñada para mejorar la seguridad del enrutamiento en Internet mediante la asociación verificable de recursos numéricos, como prefijos IPv4/IPv6 y ASN, con sus titulares legítimos. RPKI permite publicar objetos firmados, como los ROA, utilizados en la validación del origen de rutas (Rodday el at.,2024).

SGSI. Sistema de Gestión de Seguridad de la Información. Es un conjunto organizado de políticas, procesos, controles, responsabilidades y procedimientos orientados a gestionar riesgos de seguridad de la información. Bajo el enfoque de ISO/IEC 27001, un SGSI permite establecer, implementar, mantener y mejorar la protección de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27005:2018, 2018).

SIDR. Secure Inter-Domain Routing. Fue un grupo de trabajo de la IETF orientado al desarrollo de mecanismos para mejorar la seguridad del enrutamiento inter-dominio, incluyendo la arquitectura RPKI y objetos asociados a la validación de rutas (Carle & Ott, 2021).

SLURM. Simplified Local Internet Number Resource Management with the RPKI. Es un mecanismo que permite a un operador crear una vista local personalizada de la información RPKI mediante afirmaciones locales o filtros controlados. Puede utilizarse en validadores RPKI para gestionar excepciones operativas sin modificar los repositorios globales (Wang et al.,2024).

UNIX. Familia y estándar de sistemas operativos multiusuario y multitarea. El término UNIX corresponde a una marca y especificación administrada por The Open Group. Muchos sistemas modernos son considerados tipo UNIX o inspirados en UNIX, aunque no todos cuentan con certificación oficial UNIX (Ciaffaglione & Scagnetto, 2025).

REFERENCIAS

Li, W., & Lin, Z. (2023). RoVista: Medición y análisis de la validación del origen de la ruta (ROV) en RPKI. *2*(1), 73-88. doi:https://doi.org/10.1145/3618257.3624806

Rodday, N. C.-B. (2024). The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects. *IEEE Transactions on Network and Service Management*. doi:https://doi.org/10.1109/TNSM.2023.3327455

Jaw, E. M. (2024). Poster: Quantifying the Proportion of Hijacked Prefixes Among the Identified Prefix Hijackers. *IEEE 32nd International Conference on Network Protocols (ICNP)*. doi:https://doi.org/10.1109/ICNP61940.2024.10858587

Milolidakis, A. B. (2023). On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. *IEEE Access*. doi:https://doi.org/10.1145/3618257.3624824

Li, Y. Z. (2022). The Hanging ROA: A Secure and Scalable Encoding Scheme for Route Origin Authorization. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*. doi:https://doi.org/10.1016/j.comnet.2022.109036

Wang, Y. X. (2024). RPKI Sentinel: An Efficient RPKI-based Routing Emergency Control Platform. *International Conference on Networking and Network Applications (NaNA)*. doi:https://doi.org/10.1109/TNSM.2024.3361987

He, G. S. (2021). ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing. *IEEE Transactions on Network and Service Management*. doi:https://doi.org/10.1016/j.comnet.2021.108543

Friedemann, P. H. (2022). Assessing the RPKI Validator Ecosystem. *Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*. doi:https://doi.org/10.1145/3274694.3274743

Xu, W. C. (2019). On the classification and false alarm of invalid prefixes in RPKI based BGP route origin validation. *FIP/IEEE Symposium on Integrated Network and Service Management (IM)*. doi:https://doi.org/10.1109/ACCESS.2021.3067428

Hlavacek, T. H. (2018). Practical Experience: Methodologies for Measuring Route Origin Validation. *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. doi:https://doi.org/10.1145/3131365.3131369

Rodday, N., & Cunha, Í. (2024). La infraestructura de clave pública de recursos (RPKI): Una encuesta sobre mediciones y perspectivas futuras. *IEEE Transactions on*

Network and Service Management, 21, 21(2), 2353–2373. doi:https://doi.org/10.1109/TNSM.2023.3327455

Scott, B., & Johnstone, M. (2024). Un estudio de técnicas avanzadas de detección de ataques al Protocolo de Puerta de Enlace Fronteriza. *Sensores, 24*(19). doi:https://doi.org/10.3390/s24196414

Bush, R., & Austein, R. (2020). The Resource Public Key Infrastructure (RPKI) to Router Protocol. *3*(1). doi:https://doi.org/10.17487/RFC8210

Ciaffaglione, A., & Scagnetto, I. (2025). Mecanización de entornos tipo en HOAS débiles. *Informática Teórica, 606*(1), 57-78. doi:https://doi.org/10.1016/j.tcs.2015.07.019

Apostolaki, M., & Zohar, A. (2017). Secuestrando Bitcoin: Enrutando ataques a criptomonedas. *Simposio IEEE sobre Seguridad y Privacidad*, 375-392. doi:https://doi.org/10.1109/SP.2017.29

Carle, G., & Ott, P. (2021). RPKI-based Routing Security: Deployment and Design Considerations. *Asociación de Maquinaria de Computación*. doi:https://doi.org/10.1145/3485983

Akiwate, G., Jonker, M., Sommese, R., & Foster, I. (2020). Cuestiones sin resolver: prevalencia, persistencia y peligros de delegaciones. *IMC '20: Actas de la Conferencia de Medición de Internet de ACM*, 281 - 294. doi:https://doi.org/10.1145/3419394.34236

Kristoff, J., & Bush, R. (2020). Sobre la medición de las partes que dependen de RPKI. *IMC '20: Actas de la Conferencia de Medición de Internet de ACM*, 484 - 491. doi:https://doi.org/10.1145/3419394.3423622

Nawrocki, M., & Koch, M. (2021). Reexpedidores transparentes: un componente desapercibido de la infraestructura abierta de DNS. *CoNEXT '21: Actas de la 17ª Conferencia Internacional sobre Tecnologías y Tecnologías de Redes Emergentes*, 454 - 462. doi:https://doi.org/10.1145/3485983.3494872

Scott, B., Johnstone, M., & Szewczyk, P. (2024). Un estudio de técnicas avanzadas de detección de ataques al Protocolo de Puerta de Enlace Fronteriza. *Sensores, 24*(19). doi:https://doi.org/10.3390/s24196414

Mahajan, R., & Rodrig, M. (2020). Análisis del comportamiento a nivel MAC de las redes inalámbricas en la naturaleza. 75 - 86. doi:https://doi.org/10.1145/1159913.1159923

Schomp, K., & Bhardwaj, O. (2020). Akamai DNS: Proporcionando respuestas autorizadas a las preguntas del mundo. 465 - 478. doi:https://doi.org/10.1145/3387514.340588

Shen, C., & Wang, R. (2024). Técnica de detección de fugas de rutas del protocolo de Border Gateway basada en características de grafos y aprendizaje automático. *Electrónica, 13*(20). doi:https://doi.org/10.3390/electronics13204072

Wirtgen, T., & Bonaventure, O. (2022). A first step towards checking BGP routes in the dataplane. *Digital Library, 1*(1), 50 - 57. doi:https://doi.org/10.1145/3527974.3545723

Schmidt, R., & Irazabal, M. (2021). FlexRIC: an SDK for next-generation SD-RANs. *Digital Library*, 411 - 425. doi:https://doi.org/10.1145/3485983.3494870

Jawad, S., & Matic, S. (2022). Profundiza en el ecosistema backend de IoT. *IMC '22: Actas de la 22ª Conferencia de Medición de Internet de la ACM*, 488 - 503. doi:https://doi.org/10.1145/3517745.3561431

Piet, J., & Nwoji, D. (2023). GGFAST: Automating Generation of Flexible Network Traffic Classifiers. *ACM SIGCOMM '23: Actas de la Conferencia ACM SIGCOMM 2023*, 850 - 866. doi:https://doi.org/10.1145/3603269.3604840

Meng, Z., & Guo, Y. (2022). Lograr una latencia baja y constante para comunicaciones inalámbricas en tiempo real con el bucle de control más corto. *Digital Library*, 193 - 206. doi:https://doi.org/10.1145/3544216.354422

Anderson, S., & Salamatian, L. (2022). iGDB: conectando las capas física y lógica de internet. 433 - 448. doi:https://doi.org/10.1145/3517745.3561443

Kunze, I., & Wehrle, K. (2021). L, Q, R y T: ¿qué primo de spin bit ha llegado para quedarse? *1*(1), 22 - 28. doi:https://doi.org/10.1145/3472305.3472319

Mutually Agreed Norms for Routing Security. (2026). doi:https://doi.org/10.1109/ICDCS51616.2021.00085

Ortiz, J., & Vizñay, J. (2020). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo del conocimiento*, 174-195. doi: 10.23857/pc.v4i7.1029

ISO/IEC 27005: 2018. (2018). International Organization for Standardization. *Information technology*. Obtenido de . https://www.iso.org/standard/75281.html

Zapata, J., & Páez, S. (2026). Estudio comparativo de herramientas open Source para la validación automatizada de servicios de un ISP después de trabajos programados. *Polo del conocimiento, 11*(3), 1239-1260. doi:10.23857/pc.v11i3.11279

Proaño, M. (2024). *Propuesta metodológica de gestion de riesgos de seguridad de la información para la coordinación de tecnologías de la informacion y comunicaciones de la asociacion de municipalidades ecuatorianas, tomando como referencia la normativa NTE INEN ISO/EC 27005.* Universidad Técnica del Norte. Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/16685/2/PG%201947%20TRABAJO%20DE%20GRADO.pdf

AEPROVI. (2020). *Historial: Implementación de RPKI y validación de origen BGP en NAP.EC.* Obtenido de https://aeprovi.org.ec/ixp/historial-rpki-en-napec/

LANIC. (2026). *Fortaleciendo a Internet: LACNIC y NIC.br.* Obtenido de https://intrarede.nic.br/files/apresentacao/arquivo/2457/2026-Fortaleciendo-a-Internet-LACNIC-NICBR.pdf

Guerra, V. (2019). *Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil.* Universidad Católica de Santiago de Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/13883/1/T-UCSG-PRE-ING-CIS-247.pdf

Buenaño, J. (2024). *Plan de respuesta a incidentes de seguridad cibernetica para hospital publico.* Universidad Politecnica Salesiana. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/29344/1/UPS-CT011844.pdf

Agencia de Regulación y Control de las Telecomunicaciones. (abril de 2024). *Estadísticas de Seguridad de Redes de Telecomunicaciones.* Obtenido de https://www.ecucert.gob.ec/wp-content/uploads/2024/07/Estadistica-abril-24.pdf

Asamblea Nacional. (21 de mayo de 2021). *Ley orgánica de protección de datos personales.* Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Rodríguez. (2020). Generalidades acerca de las técnicas de investigación cuantitativa. *Sistema Institucional de investigación de Unitex, 2*(1), 9-39. Obtenido de https://dialnet.unirioja.es/descarga/articulo/4942053.pdf

Alarcón, P. (2018). Una metodología comparativa crítica aplicada al sistema constitucional ecuatoriano. *Derecho y Sociedad*. Obtenido de https://repositorio.uasb.edu.ec/bitstream/10644/7089/1/SDS-003-Alarcon-Una%20metodologia.pdf

Guevara, G. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas y de investigación-acción). *Recimundo*, 163-173. Obtenido de https://dialnet.unirioja.es/descarga/articulo/7591592.pdf

Vega, E. (31 de 08 de 2025). *https://webdev.lacnic.net.* Recuperado el 2026, de Informes LACNIC: https://webdev.lacnic.net/wp-content/uploads/2025/09/lacnic-evolucion-global-regional-adopcion-rpki-es.pdf

LACNIC. (2026). *Dashboard de herramientas de monitoreo y análisis de Internet*. Obtenido de https://tools.labs.lacnic.net/tools/dashboard?id=271933

Routinator. (05 de 2026). *Routinator*. Obtenido de Routinator : https://rpki-validator.iplus.com.ec:44323/ui/

CloudFlare. (05 de 2026). *Radar CloudFlare*. Obtenido de Radar CloudFlare: https://radar.cloudflare.com/routing/prefix/45.70.12.0/22

LACNIC. (2023). *Infraestructura de Internet en América Latina y el Caribe.* Obtenido de https://www.lacnic.net/innovaportal/file/978/4/lacnic-fasciculo-infraestructura-internet-es.pdf

Li, B., Cui, T., Wang, Z., Bai, W., & Zhang, L. (2020). Socksdirect: los sockets de centro de datos pueden ser rápidos y compatibles. *Digital Library*. doi:https://doi.org/10.1145/3341302.3342071

Ebrima, M., Müller, M., & Hesselman, C. (2026). Estudio de reproducibilidad y evaluación de la evolución de eventos de secuestro de BGP en serie. *IEEE Transactions on Network and Service Management, 23*, 3602-3621. doi:doi: 10.1109/TNSM.2026.3671613

Mitseva, A., Panchenko, A., & Engel, T. (2020). El estado de las cosas en la seguridad de BGP: Un repaso de ataques y defensas. *Science Direct, 124*, 45-60. Obtenido de

https://www.sciencedirect.com/science/article/abs/pii/S014036641731068X?via%3Dihub

Tsai, P., Risdi, A., Hui, M., Permal, S., & Chaw, T. (2021). SD-BROV: Una protección mejorada contra secuestros BGP con validación de rutas en eXchange definido por software. *13*(7). Obtenido de https://doi.org/10.3390/fi13070171

Mirdita, D., Schulmann, H., Vogel, N., & Waidner, M. (2023). El CURE de vulnerabilidades en la validación RPKI. *Cornell University*. doi:https://dx.doi.org/10.14722/ndss.2024.241093

Fontugne, R. S. (2021). RPKI MIRO: Monitoreo e Inspección de Objetos RPKI. *RIPE NCC / ACM Internet Measurement Conference, 2*(1). Obtenido de https://www.bing.com/ck/a?!&&p=1e2751be202e8eb55494414a7e7b524a3c7f5c6c888dcc85fb5842d267dc46c6JmltdHM9MTc3OTc1MzYwMA&ptn=3&ver=2&hsh=4&fclid=1db86982-a513-65a6-1226-7f80a40f64c0&psq=RPKI+MIRO%3a+Monitoreo+e+Inspecci%c3%b3n+de+Objetos+RPKI&u=a1aHR0cHM6Ly9

Kowalski, M., & Mazurczyk, W. (2023). Hacia la seguridad del enrutamiento mutuo en redes de área amplia: una revisión de alcance de amenazas y contramedidas. *Redes informáticas*. Obtenido de https://www.sciencedirect.com/science/article/pii/S1389128623002232

ANEXOS

Ibarra, 4 de mayo de 2026

CERTIFICADO DE IMPLEMENTACIÓN DE PROYECTO TÉCNICO

De mi consideración:

Por medio de la presente, se hace constar formalmente la implementación y puesta en marcha del proyecto de titulación titulado: "**OPTIMIZACIÓN DE LA SEGURIDAD EN EL TRÁFICO DE ENTRADA DE LA RED CENTRAL DE AIRMAXTELECOM MEDIANTE LA IMPLEMENTACIÓN DE RPKI PARA LA MITIGACIÓN DE ATAQUES DE SECUESTRO DE RUTAS**", bajo la autoría y ejecución técnica del Ing. **Carlos Andrés Benavides** con cédula **1004134977**.

La implementación ejecutada en la infraestructura de red de Airmaxtelecom ha cubierto satisfactoriamente los siguientes hitos técnicos:

- Despliegue de validadores de caché para la sincronización de la base de datos global de ROAs (Route Origin Authorizations).
- Configuración de sesiones RPKI-Router en los equipos de borde de la red central para la validación de prefijos en tiempo real.
- Establecimiento de filtros de enrutamiento basados en estados de validación (Valid, Invalid, Unknown), garantizando el descarte automático de anuncios maliciosos o erróneos (BGP Hijacking).

Tras la finalización del despliegue, se ha verificado una mejora sustancial en la resiliencia de la red central, mitigando proactivamente los riesgos de interceptación de tráfico y asegurando que el flujo de datos hacia nuestros usuarios finales se mantenga por rutas legítimas y autorizadas.

Se extiende la presente para los fines legales y académicos que el interesado considere convenientes.

Atentamente,

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MIGUEL ANGEL
VALLEJOS BENAVIDES

Ing. Miguel Vallejos Msc.
Gerente General