EXPLORANDO EL UNIVERSO IPV6

para la innovación de un mundo interconectado

Raúl Bareño Gutiérrez



compensar | fundación universitaria

EXPLORANDO EL UNIVERSO IPv6

PARA LA INNOVACIÓN DE UN MUNDO INTERCONECTADO

Raúl Bareño Gutiérrez

compensar
fundación universitaria

compensar | fundación universitaria

Rectora (e)
Margarita Añez Sampedro

Vicerrectora académica (e)
Carolina Guzmán Ruiz

Decano Facultad de Ingeniería y Tecnología
Nelson Felipe Rosas Jiménez

Director de Programa
Paul Alexander Díaz Montaña

Directora de Investigación y Transferencia
Gareth Barrera Sanabria

Fundación Universitaria Compensar
Facultad de Ingeniería y Tecnología

Bareño Gutiérrez, Raúl.

Explorando el universo IPv6: para la innovación de un mundo interconectado / Raúl Bareño Gutiérrez -- Bogotá: Fundación Universitaria Compensar, 1a.ed. 2024

138 ; 24 cm.
ISBN 978-958-792-657-6 e-ISBN 978-958-792-658-3
1. Ingeniería 2. Redes 3. Conectividad I. Tít.
600 cd.

Primera edición: Bogotá, Colombia, febrero de 2024
ISBN 978-958-792-657-6

© Raúl Bareño Gutiérrez
© Fundación Universitaria Compensar
Avda. Calle 32 No. 17-30 - Tel. (+57 601) 3380666
www.ucompensar.edu.co - E-mail: gbarreras@ucompensar.edu.co
Bogotá, Colombia

Este libro es resultado de investigación de acuerdo con los criterios de Minciencias, todos los capítulos incluidos en él son productos de investigaciones desarrolladas por sus autores. Fueron arbitrados bajo el sistema doble ciego por pares reconocidos avalados por Minciencias.

Los planteamientos y argumentos presentados en los capítulos del libro son responsabilidad única y exclusiva de sus autores, por lo tanto, los compiladores y la Universidad que respalda esta obra actúan como un tercero de buena fe.

Coordinador: Raúl Bareño Gutiérrez
Diagramación de interiores: Oscar Javier Avendaño Yossa
Los costos editoriales fueron asumidos por la Fundación Universitaria Compensar.

Impreso y hecho en Colombia
Printed and made in Colombia

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro y otros medios, sin el permiso previo y por escrito de los titulares del Copyright.

Contenido

Introducción 11

Direcciones IPV6: fundamentales hacia el infinito de las redes conectando el mundo del mañana y hoy 15

Protocolo IPV6: navegando hacia el futuro de la conectividad bajo estándares RFC 33

Protegiendo el futuro de las telecomunicaciones, en la era de las direcciones IPV6: desafíos y soluciones para un mundo más conectado y global 61

Políticas y estrategias para una conectividad sostenible y exitosa hacia la transición a IPV6 sin fronteras en américa del sur: desafíos y recomendaciones 79

La revolución de las direcciones IPV6: impactando el futuro traspasando fronteras de las telecomunicaciones en américa del sur 107

Conclusiones generales por capitulo 133

Índice de tablas

Tabla 1.1. Comparativo según autores de la necesidad de la implementación de las direcciones IPv6 24
Tabla 2.1. Los RFC más relevantes de las distintas áreas o partes de la tecnología 38
Tabla 2.2. Descripción de estándares referentes 41
Tabla 2.3. Otros RFC referentes 42
Tabla 2.4. Comparativo entre autores referentes 50
Tabla 3.1. Estándares que respaldan la seguridad en la transición a las direcciones IPv6 para la implementación de servicios y protocolos 67
Tabla 3.2. IPSec triada de la seguridad 69
Tabla 3.3. Autores referentes al campo de estudio de la seguridad sobre IPV6 70
Tabla 3.4. Autores según framework ISO, COBIT, ITIL y NIST 73
Tabla 4.1. Aspectos relevantes acordes a las políticas públicas en Argentina 85
Tabla 4.2. Aspectos relevantes acordes a las políticas públicas de Perú 87
Tabla 4.3. Aspectos relevantes acordes a las políticas públicas de Brasil 89
Tabla 4.4. Aspectos relevantes acordes a las políticas públicas de Chile 90
Tabla 4.5. Aspectos relevantes acordes a las políticas públicas de Colombia 91
Tabla 4.6. Aspectos relevantes acordes a las políticas públicas de Ecuador 93
Tabla 4.7. Aspectos relevantes acordes a las políticas públicas de Uruguay 94
Tabla 4.8. Aspectos relevantes acordes a las políticas públicas de Venezuela 95
Tabla 4.9. Aspectos relevantes acordes a las políticas públicas para el mundo 96
Tabla 5.1. Aspectos de transición hacia IPv6 por país 113
Tabla 5.2. Porcentajes y estimados en años para la transición 116
Tabla 5.3. Argentina 117

Tabla 5.4. Brasil 118
Tabla 5.5. Chile 119
Tabla 5.6. Colombia 120
Tabla 5.7. Perú 122
Tabla 5.8. Ecuador 123
Tabla 5.9. Uruguay 124
Tabla 5.10. Paraguay 125
Tabla 5.11. Venezuela 126

Introducción

En la actualidad y a nivel mundial, se encuentra en un periodo de transición de las direcciones o del protocolo IPv4 al protocolo IPv6, siendo fundamental para Suramérica el fortalecimiento de su infraestructura de telecomunicaciones y de actualización de sus servicios tecnológicos por parte de los diferentes proveedores de internet y de todos los sectores de la economía, para la adaptación rápida a este nuevo protocolo que permita la integración a las nuevas tecnologías disruptivas y convergentes.

Es así que la Facultad de Ingeniería de la Fundación Universitaria Compensar, dentro del proyecto educativo institucional articulado con el sector empresarial, apoya la dinámica de las organizaciones público-privadas en la transición hacia el protocolo IPv6, además de la generación de proyectos de investigación e innovación sobre el desarrollo e investigación de la industria; por ello, sus investigadores apoyan fuertemente el currículo académico de los 6 programas de pregrado (Ingeniería de Sistemas, Ingeniería de Telecomunicaciones, Ingeniería de Software, Ingeniería Industrial, Ingeniería Multimedia y Ciencias de Datos) y sus 2 programas de posgrado (especialización en Seguridad Informática y especialización en Big Data). Además de ello, van a la vanguardia de las nuevas necesidades de la industria 4.0 y 5.0, proponiendo a los lectores de este libro 5 capítulos de alto impacto y articulados con sus aliados estratégicos hacia el sector productivo.

El primer capítulo destaca la importancia y necesidad de las direcciones IPv6, debido al agotamiento de las direcciones IPv4, siendo una necesidad en todos los contextos económicos, educativos y gubernamentales debido a su impacto en una amplia gama de áreas, como la automatización, el IoT, la seguridad informática, las soluciones en la nube y la inteligencia artificial, entre otras. Se debe garantizar la continuidad y crecimiento de Internet, ya que ofrece un espacio de direcciones mucho más amplio y permite una mayor escalabilidad. A medida que IPv6 se vuelva más común, es crucial abordar los desafíos de seguridad asociados con su implementación. Lo que destaca es la importancia de implementar prácticas de seguridad sólidas y actualizadas para proteger la integridad de los servicios y datos en sus redes.

En el segundo capítulo, se destaca la transición a IPv6, un proceso necesario debido al agotamiento de direcciones IPv4, y los beneficios potenciales que

ofrece IPv6, como un mayor espacio de direcciones y una mejor seguridad. Los estándares RFC desempeñan un papel fundamental en la transición a IPv6, proporcionando directrices y especificaciones técnicas para la implementación y el funcionamiento de IPv6 en redes. Los mecanismos de transición más comunes mencionados en los estándares RFC incluyen Dual Stack, Tunneling y Translation, que permiten una coexistencia gradual de IPv4 e IPv6 en las redes.

En el marco del tercer capítulo, se destaca la implementación de IPv6 y se presentan importantes desafíos en términos de seguridad. La adopción de este nuevo protocolo de Internet amplía el espacio de direcciones y brinda diversas ventajas, pero también introduce vulnerabilidades que deben abordarse adecuadamente. El framework IPSec se destaca como una solución efectiva para garantizar la seguridad en las comunicaciones basadas en IPv6. Proporciona mecanismos de autenticación, confidencialidad, integridad y disponibilidad a través de la implementación de diferentes protocolos y servicios de seguridad. La autenticación es esencial para garantizar que las comunicaciones en IPv6 sean realizadas por entidades legítimas. IPSec ofrece mecanismos sólidos de autenticación, como el uso de claves criptográficas y certificados digitales, para verificar la identidad de los participantes en las comunicaciones.

En el marco del cuarto capítulo, se pone en evidencia cómo los países de América del Sur han reconocido la importancia de la transición a IPv6 y han implementado políticas públicas para fomentar su uso. Las políticas públicas desempeñan un papel fundamental en la promoción y adopción de IPv6. Es esencial que los gobiernos de la región establezcan marcos regulatorios adecuados, fomenten la capacitación y concientización y promuevan la colaboración entre los sectores público y privado para impulsar la transición. Entre las ventajas de las políticas para IPv6 se encuentran la ampliación del espacio de direcciones IP, la mejora en la escalabilidad y enrutamiento de la red, así como el impulso a la innovación y nuevos servicios digitales en diversos sectores, como la salud, educación, gobierno, industria y comercio.

Dentro del capítulo 5, se destaca que es inminente que América del Sur debe forzar la transición al protocolo IPv6 que le permita mejorar los servicios y las infraestructuras de telecomunicaciones presentes y futuras para poder fortalecer la cantidad masiva de dispositivos y las nuevas soluciones tecnológicas que se interconectarán y apoyen la transformación digital, la automatización, la ciberseguridad, el internet de las cosas, el block-chain, las tecnologías disruptivas, las industrias 4.0 y 5.0, la inteligencia artificial, las soluciones cloud computing, las redes definidas por software, entre otros, que les permitan la

penetración masiva a IPv6 y que fortalezcan la región y la economía de manera global en todos los sectores público-privados.

Basado en lo anterior, la Fundación Universitaria Compensar y los investigadores del Grupo de Investigación en Ingeniería de Sistemas GIIS presentan parte de sus investigaciones para toda la comunidad empresarial y académica desde una mirada holística y de alto impacto en la comunidad científica hacia proyectos de I+D+i que apoyen la transformación digital hacia las industrias 4.0 y 5.0, acordes con las nuevas tendencias y tecnologías disruptivas.

Direcciones IPV6: fundamentales hacia el infinito de las redes conectando el mundo del mañana y hoy

IPv6 addresses: fundamentals towards the infinity of networks connecting the world of tomorrow and today

Autores:

Raúl Bareño Gutiérrez.
rbarenog@ucompensar.edu.co

Luz Dary Arias Villamizar.
ludaarvi@gmail.com.co

Fran Edwar Pérez Ortiz.
frperezo@sena.edu.co

Resumen

Con un número creciente de dispositivos conectados actualmente en Internet y su constante crecimiento se llegó al agotamiento de direcciones IPv4; por ello, se impulsa la necesidad de adoptar IPv6 como una solución para enfrentar el problema en el campo de las telecomunicaciones en cuanto a sus ventajas y su potencial para abordar los desafíos planteados y los beneficios de adaptación al permitir una expansión de red sin problemas y mejorar la seguridad.

La investigación se enfocó en la implementación y ventajas de IPv6, bajo la metodología de Barbara Kitchenham, en una revisión sistemática de la literatura existente, análisis comparativos y la recopilación de datos de estudios de casos de entidades públicas y privadas que la han implementado. Los resultados encontrados permiten resaltar los nuevos servicios y soluciones tecnológicas hacia una expansión de redes fluida para asegurar el crecimiento continuo de dispositivos conectados. Se destacan las mejoras en seguridad y privacidad inherentes. Revela el potencial transformador al revolucionar el panorama de las telecomunicaciones ofreciendo una cantidad virtualmente infinita de direcciones, lo que garantiza el crecimiento sostenible de la red de manera eficiente y la capacidad de respuesta de sus redes en un mundo cada vez más interconectado para brindar soporte a la próxima generación de dispositivos, avances tecnológicos, aplicaciones sostenibles y escalables de las redes en el futuro bajo un entorno netamente digital.

Palabras claves

Protocolo IPv6, direcciones IPv6, telecomunicaciones, transición, seguridad, nuevas soluciones de interconexión.

Abstract

With an increasing number of devices currently connected to the Internet and its constant growth, IPv4 addresses were exhausted; therefore, the need to adopt IPv6 is promoted as a solution to the problem in the field of telecommunications in terms of its advantages. And it's potential to address the challenges posed and the benefits of adaptation by enabling seamless network expansion and improving security. The research focused on the implementation and advantages of IPv6, under the Barbara Kitchenham methodology, in a systematic review of the existing literature, comparative analysis, and the collection of data from case studies of public-private entities that have implemented it. The results found They allow us to highlight the new

services and technological solutions towards a smooth network expansion to ensure the continuous growth of connected devices. Inherent security and privacy enhancements are highlighted. Revealing the transformative potential of revolutionizing the telecommunications landscape by offering a virtually infinite number of addresses, ensuring sustainable network growth efficiently, and improving the responsiveness of your networks in an increasingly interconnected world towards providing support to the next generation of devices, technological advances, and sustainable and scalable applications of networks in the future in a purely digital environment.

Keywords

IPv6 protocol, IPv6 addresses, telecommunications, transition, security, and new interconnection solutions.

Este capítulo es resultado del proyecto de investigación titulado "**MODELO DE TRANSICIÓN AL PROTOCOLO IPV6 PARA PYMES Y MIPYMES COLOMBIANAS APLICANDO MODELOS DE MACHINE LEARNING**" con código de aprobación del Comité de Investigaciones #PI0220231, proyecto financiado con una asignación de 21.000.000 millones Mcte, en la actualidad en fase de ejecución.

Institución financiadora: **Fundación Universitaria Compensar**

Introducción

El IP versión 6 (IPv6) está diseñado para superar las limitaciones del estándar actual (IPv4). IPv4 permite a los sistemas finales comunicarse y formar la base de la Internet como la conocemos hoy. Sin embargo, una de las principales limitaciones de IPv4 es el espacio limitado de la cantidad de direcciones (Ali, A. N. A., 2012). El crecimiento de los nuevos dispositivos con IP activo y el crecimiento de regiones subdesarrolladas han alimentado la necesidad de más direcciones.

Por ello, la Dirección de Protocolo de Internet versión 6 (IPv6) es un estándar de protocolo de comunicación de red; se hace necesario un sistema de direccionamiento de Internet más escalable y adaptable (Bao, C., Huitema, C., Bagnulo, M., Boucadair, M. & Li, X., 2010). El estándar IPv6 permite una cantidad mayor de direcciones IP únicas y ofrece mejoras en la seguridad, la movilidad y la calidad del servicio (Makaya, C. & Pierre, S., 2008). Según varios estudios, incluyendo una investigación de CISCO en 2020, la adopción de IPv6 ha aumentado çsignificativamente en los últimos años (Ashraf, S., Muhammad, D. & Aslam, Z., 2020).

Las direcciones IPv6 son un conjunto de 128 bits que se dividen en ocho grupos de 16 bits cada uno. Cada grupo se representa en formato hexadecimal y se separa de los demás por el carácter ":". Sigue esta estructura: 2010:db8:85a3:0:0:8a2e:370:7334 (Deering, S., Haberman, B., Jinmei, T., Nordmark, E. & Zill, B., 2005). Existen algunas convenciones para simplificar la representación de las direcciones IPv6: los ceros iniciales se pueden omitir en cada grupo, pero solo en una instancia. Si hay dos o más grupos consecutivos con valor cero, se pueden representar con ":" (Barrientos-Avendaño, E., Rico-Bautista, D., Coronel-Rojas, L. A. & Cuesta-Quintero, F. R., 2019; Kawamura, S. & Kawashima, M., 2010).

Además, existen varios tipos de direcciones IPv6: Unicast: identifican una única interfaz de red y se pueden asignar a una sola máquina. Multicast: identifican un grupo de interfaces de red y se usan para enviar paquetes a ese grupo de forma simultánea. Anycast: identifican a varias interfaces de red, pero solo se envían paquetes a uno de ellos (normalmente, al que está más cerca del emisor) (Chandra, D. G., Kathing, M. & Kumar, D. P., 2013; Hinden, R., O'Dell, M. & Deering, S., 1998).

Este nuevo protocolo, IPv6, crea un conjunto de 340 sextillones de direcciones IP disponibles (más de 7,9 × 1.028 veces las direcciones ofrecidas por IPv4). Los diferentes sectores no tendrán que inquietarse por quedarse sin direcciones IP únicas en el futuro previsible (Chen, J. L., Chang, Y. C. & Lin, C. H., 2004).

Algunas diferencias en cuanto a la seguridad entre IPv6 e IPv4 son:

Tamaño de direcciones: las direcciones IPv6 son más largas que las IPv4, lo que significa que hay más direcciones posibles, lo que hace más difícil la tarea de los hackers de encontrar una dirección específica (Hagen, S., 2006; Yang, T., Hou, B., Cai, Z., Wu, K., Zhou, T. & Wang, C., 2022).

Integridad de paquetes: IPv6 tiene una validación de integridad incorporada en los paquetes que lo hace menos vulnerable a ataques de manipulación de paquetes (Rye, E. C. & Beverly, R., 2020).

Autenticación: IPv6 tiene un marco integrado para autenticar el tráfico de red, lo que puede proporcionar una fuerte protección contra la suplantación del paquete (Law, Y. N., Lai, M. C., Tan, W. L. & Lau, W. C., 2008).

Encriptación: el protocolo de seguridad de IPv6, IPSec, ofrece una encriptación más sólida que el protocolo de seguridad de IPv4, lo que garantiza una mayor protección contra el espionaje (Cui, T., Liu, C., Gou, G., Shi, J. & Xiong, G., 2019; Wen, X., Xu, C., Guan, J., Su, W. & Zhang, H., 2010).

En general, se considera que la seguridad de IPv6 es más robusta y mejor diseñada que la de IPv4. Sin embargo, tanto IPv4 como IPv6 no son inmunes a los ataques, por lo que es importante tomar medidas para proteger su red en todo momento (Thomson, S., Narten, T. & Jinmei, T., 2007).

Debido a ello, en la presente investigación se efectuó la pregunta de investigación: ¿cuál es la importancia de conocer e implementar el protocolo IPv6 en redes empresariales, considerando sus ventajas y desventajas?

Metodología

En cuanto a los métodos basados en la Revisión Sistemática de la Literatura (RSL) de Barbara Kitchenham (Irshad, M., 2016) enfocados a las direcciones IPv6, se validaron aspectos como: determinar los criterios que serán utilizados para seleccionar los estudios relevantes que serán incluidos en la revisión, como el año de publicación, la calidad metodológica del estudio, la relevancia del contenido, en bases de datos científicas, revistas especializadas y otras fuentes relevantes para identificar estudios que aborden el tema, como: aplicar criterios de inclusión y exclusión para seleccionar los estudios más pertinentes y de mayor calidad, extrayendo los datos relevantes de las investigaciones o proyectos seleccionados y sintetizar la información en una forma comprensible (Nagamalla, V. & Varanasi, A., 2017); y realizar un análisis crítico de los datos extraídos para responder a la pregunta de investigación. Pueden revisarse las estrategias, metodologías y conclusiones relevantes basadas en la evidencia proporcionada de manera sistemática y objetiva sobre el tema de las direcciones IPv6 en las telecomunicaciones, permitiendo obtener una visión amplia y fundamentada sobre su impacto en las redes de comunicación, además de sus ventajas en comparación con IPv4 en términos de seguridad y privacidad, entre otros aspectos relevantes.

Resultados

IPv6 es una mejora poderosa para IPv4 y varias características de IPv6 ofrecen mejoras funcionales (Zakari, A., Musa, M., Bekaroo, G., Bala, S. A., Hashem, I. A. T. & Hakak, S., 2019):

Mayor espacio de direccionamiento: también ofrece mejoras en accesibilidad global y flexibilidad; la adición de prefijos que son anunciados en las tablas de enrutamiento; multihoming para varios proveedores de servicio de internet (ISP); autoconfiguración que puede incluir capas de enlace de direccionamiento en el espacio de direcciones; opciones plug and play; redireccionamiento público a privado de extremo a extremo sin traducción de dirección;

y mecanismos simples para la renumeración y modificación de direcciones (Czyz, J., Allman, M., Zhang, J., Iekel-Johnson, S., Osterweil, E. & Bailey, M., 2014).

Encabezamiento simple: provee mejor eficiencia de enrutamiento; no hace broadcast; no hay requerimiento de proceso de cheksum; mecanismos de encabezado más simple y eficiente; y etiquetas de flujo para cada procesamiento con la no necesidad de abrir el transporte interno de paquetes para identificar los diferentes flujos de tráfico (Li, F. & Freeman, D., 2020).

Movilidad y seguridad: asegura el cumplimiento de los estándares de funcionamiento IPSec y móviles IP; la movilidad se basa en estos, así cualquier nodo IPv6 se puede usar cuando sea necesario y permite a las personas moverse en las redes con dispositivos móviles de red con muchas comunicaciones inalámbricas (Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S. & Acosta, N. D., 2016).

IP móvil es un estándar Internet Engineering Task Force (IETF) para moverse sin interrupción en las conexiones de red establecidas. Como IPv4 no provee automáticamente la clase de movilidad, se debe agregar esta a las configuraciones adicionales. IPSec es el estándar IETF para la seguridad de red IP, disponible tanto para IPv4 e IPv6. Aunque las funcionalidades son esencialmente idénticas en ambos ambientes, IPSec es obligatorio en IPv6. Está activo en todos los nodos IPv6 y está disponible para su uso. La disponibilidad de IPSec en todos los nodos hace que el Internet IPv6 sea más seguro. Requiere llaves para cada parte, lo que implica el empleo y distribución de una llave global (Grossetete, P., Popoviciu, C. P. & Wettling, F., 2004).

Riqueza de transición: puede incorporar capacidades existentes de IPv4 en IPv6 de las siguientes formas: configurando una pila dual con ambos IPv4 e IPv6 en la interfaz de un dispositivo de red o usando la técnica IPv6 sobre IPv4 (también llamada túnel 6 a 4), la cual usa un túnel IPv4 para transportar el tráfico IPv6. Ese método (RFC 3056) reemplaza el túnel compatible IPv4 (RFC 2893). Permiten el protocolo de traducción (NAT-PAT) entre IPv6 e IPv4. Esta traducción permite la comunicación directa entre hosts que hablan en diferentes protocolos.

Velocidad de transferencia de datos: IPv6 es más rápido que IPv4 debido al hecho de que las direcciones IPv6 son más cortas y no requieren de conversión de formato durante la transmisión de datos. Haciendo esto, la transferencia de datos es más rápida en IPv6 que en IPv4 (Gómez-Rodríguez, J. R., Sandoval-Aréchiga, R., Ibarra-Delgado, S. & Flores-Troncoso, J., 2016).

Fragmentación de paquetes: es necesaria en las redes de IPv4 para enviar paquetes grandes. Pero este proceso puede afectar la calidad y velocidad de la transmisión. IPv6 incorpora la funcionalidad de fragmentación solo en los extremos del enlace, lo que hace que la fragmentación de paquetes sea más eficiente y rápida.

Configuración de red: IPv6 ofrece una configuración de red más fácil y automatizada en comparación con IPv4. Con IPv6, los dispositivos pueden obtener una dirección única a través del protocolo de configuración sin estado (SLAAC) o un servidor de configuración automática de direcciones (DHCPv6) (Padmanabhan, R., Rula, J. P., Richter, P., Strowes, S. D. & Dainotti, A., 2020).

Algunos de los problemas o retos que pueden presentarse en la implementación de las direcciones IPv6 pueden ser (Varela, F. V., 2021):

Falta de compatibilidad con IPv4: aunque ambos protocolos pueden coexistir, muchos dispositivos y aplicaciones solo son compatibles con IPv4 y esto puede generar problemas de interoperabilidad y dificultades en la implementación (Sarrar, N., Maier, G., Ager, B., Sommer, R. & Uhlig, S., 2012).

Dificultades en la transición: la implementación de IPv6 implica una transición desde IPv4, lo que puede requerir cambios en la infraestructura y sistemas de las organizaciones. Esto puede ser costoso y complejo, especialmente para empresas grandes o con sistemas propietarios muy conservadores (Dell, P., 2010).

Tamaño de la dirección IPv6: las direcciones IPv6 son mucho más largas y complejas que las de IPv4, lo que aumenta el número de posibles direcciones y mejora la seguridad, pero también puede dificultar su gestión y configuración (Nikkel, B. J., 2007).

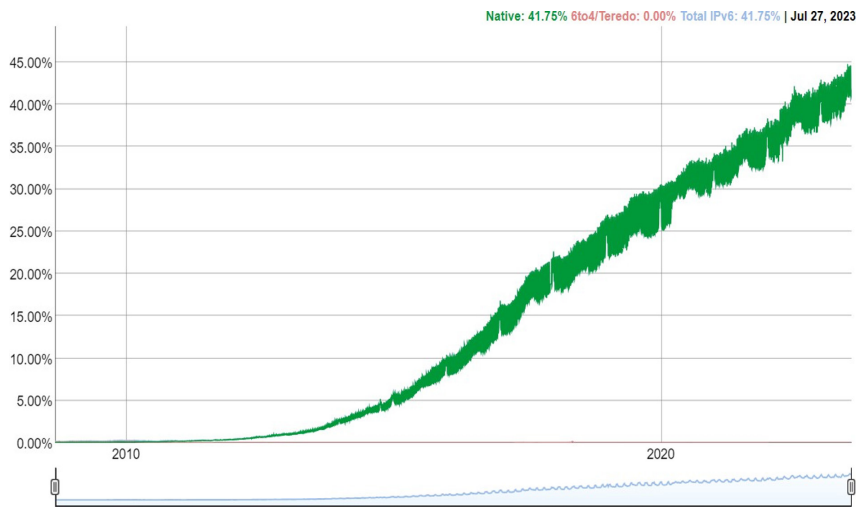
Problemas de seguridad: puede presentar nuevos riesgos y vulnerabilidades, como los que surgen de la complejidad de las direcciones IPv6 (Medina, C. A. C. & Forero, F., 2013).

Conocimiento y capacitación: la implementación de IPv6 requiere de una sólida comprensión de las nuevas funcionalidades y características, así como de las mejores prácticas para su manejo y administración. Esto puede requerir capacitación y formación específica, lo que puede ser costoso y llevar tiempo.

Falta de adopción generalizada: aunque IPv6 fue creado para abordar los problemas de agotamiento de direcciones IPv4, su adopción global ha sido lenta, lo que puede limitar la disponibilidad de servicios que requieren direcciones IPv6 y dificultar su implementación para algunas organizaciones (Czyz, J., Lady, K., Miller, S. G., Bailey, M., Kallitsis, M. & Karir, M., 2013).

Por lo cual es inminente la transición a este protocolo, para lo cual Google ha implementado IPv6 desde el año 2008 y actualmente reporta un tráfico de IPv6 superior al 45 % (ver figura 1.1. página siguiente). Este sitio, de manera permanente, evalúa la disponibilidad de la conectividad de IPv6 entre sus usuarios, siendo el porcentaje de usuarios que acceden a Google a través de IPv6.

Figura 1.1. Crecimiento del tráfico según Google



Facebook, desde 2011, ha venido trabajando en la implementación de IPv6, permitiendo que sus servicios estén disponibles a través de la nueva generación de protocolos de internet. El lanzamiento oficial de IPv6 en todo el mundo tuvo lugar el 6 de junio de 2012. Facebook pasó a utilizar direcciones IPv6 al 100 % en todos sus centros de datos en 2017 y está trabajando en el despliegue de IPv6 en el resto de la infraestructura y habilitando nuevas funciones en su plataforma. La empresa fue uno de los primeros sitios web en adoptar IPv6 y ahora utiliza doble pila (IPv4 e IPv6) para permitir a los usuarios conectarse a través de ambas versiones (ver figura 1.2. página siguiente). Otros grandes sitios web y proveedores de servicios de Internet también han iniciado la transición.

Figura 1.2. Trafico de IPv6 según Facebook para sus usuarios



https://www.facebook.com/ipv6/?tab=ipv6_country

Microsoft ha añadido soporte para IPv6 en sus sistemas operativos desde Windows 10 y 11. Cisco ha promovido la adopción de IPv6 y ofrece una amplia variedad de productos que soportan la nueva generación de protocolos de internet.

El Gobierno de los Estados Unidos ha adoptado IPv6 en varias agencias y departamentos, como el Departamento de Defensa y la Administración Nacional de la Aeronáutica y del Espacio (NASA). La implementación de IPv6 ha permitido al gobierno de los EE. UU. mejorar la seguridad y la confiabilidad de sus redes, además de tener la capacidad de responder a problemas futuros de agotamiento de direcciones.

Es importante destacar que, aunque la adopción de IPv6 aún está en progreso en el mundo y en todos los sectores de la economía, esta nueva generación de protocolos de Internet es fundamental para asegurar la continuidad y el crecimiento de Internet en un mundo cada vez más conectado (Ibhaze, A. E., Okoyeigbo, O., Samson, U. A., Obba, P. & Okakwu, I. K., 2020; Shen, W., Chen, Y., Zhang, Q., Chen, Y., Deng, B., Li, X. & Lv, G., 2009).

Discusión

Son muchos los autores referentes (Song, G., He, L., Wang, Z., Yang, J., Jin, T., Liu, J., & Li, G., 2020) en este campo que han efectuado investigaciones acerca de las direcciones IPv6 (ver tabla 1.1). Se destacan algunas recomendaciones y conclusiones desde diferentes miradas y aristas para comprender la importancia de la implementación de soluciones que permitan mantener los sistemas de telecomunicaciones interconectados en el contexto digital de hoy (Shen, W., Chen, Y., Zhang, Q., Chen, Y., Deng, B., Li, X. & Lv, G., 2009).

Tabla 1.1. Comparativo según autores de la necesidad de la implementación de las direcciones IPv6

Autores	Título	Conclusiones	Recomendaciones
Gutiérrez *et al.* (2016)	Revisión de la seguridad en la implementación de servicios sobre IPv6	Se identificaron desafíos de seguridad en la implementación de servicios IPv6.	Implementar prácticas de seguridad sólidas y actualizadas para asegurar la integridad de los servicios IPv6.
Medina & Forero (2013)	Caracterización de IPv6	IPv6 ofrece ventajas y características superiores a IPv4.	Fomentar la adopción de IPv6 en redes y dispositivos para aprovechar sus mejoras en direccionamiento y seguridad.
Varela (2021)	IPv6, una realidad	IPv6 es una realidad y una necesidad ante el agotamiento de direcciones IPv4.	Migrar a IPv6 de manera planificada y escalonada para evitar problemas futuros de direccionamiento.
Gómez-Rodríguez *et al.* (2016)	IPv6. El tiempo ha llegado	La adopción de IPv6 es crucial debido al agotamiento de direcciones IPv4.	La transición proactiva a IPv6 en redes y sistemas para garantizar una conectividad eficiente.
Deering *et al.* (2005)	IPv6 scoped address architecture	La arquitectura de direcciones IPv6 con alcance permite restringir la visibilidad y propagación de paquetes.	Utilizar direcciones IPv6 con alcance para mejorar la seguridad y eficiencia en la comunicación de redes específicas.
Thomson *et al.* (2007)	IPv6 stateless address autoconfiguration	IPv6 ofrece autoconfiguración de direcciones sin estado, simplificando el despliegue.	Implementar autoconfiguración de direcciones IPv6 en redes para facilitar el despliegue y la gestión.
Hinden *et al.* (1998)	An IPv6 aggregatable global unicast address format	El formato de dirección IPv6 unicast global agregable es fundamental para la asignación de direcciones IPv6.	Utilizar el formato de dirección *unicast* global agregable para asignar direcciones IPv6 de manera eficiente.

Autores	Título	Conclusiones	Recomendaciones
Kawamura & Kawashima (2010)	A recommendation for IPv6 address text representation	La representación de direcciones IPv6 es importante para su comprensión y uso.	Adoptar la recomendación para representar direcciones IPv6 de manera uniforme y coherente.
Bao *et al.* (2010)	IPv6 addressing of IPv4/IPv6 translators	Los traductores IPv4/IPv6 son œtiles para permitir la coexistencia de ambas versiones de IP.	Considerar la implementación de traductores IPv4/IPv6 para facilitar la migración y la interoperabilidad.
Ali (2012)	Comparison study between IPV4 & IPV6	Se compararon las características y desafíos de IPv4 e IPv6.	Evaluar las diferencias entre IPv4 e IPv6 antes de realizar la migración para entender las implicaciones.
Padmanabhan *et al.* (2020)	DynamIPs: Analyzing address assignment practices in IPv4 and IPv6	Se analizaron prácticas de asignación de direcciones en IPv4 e IPv6.	Adoptar prácticas eficientes y escalables para la asignación de direcciones IPv6 en futuros despliegues.
Yang *et al.* (2022)	6Graph: A graph-theoretic approach to address pattern mining for Internet-wide IPv6 scanning	Se propuso un enfoque de miner'a de patrones de direcciones IPv6.	Utilizar el enfoque de 6Graph para realizar escaneo y análisis de direcciones IPv6 a nivel global.
Song *et al.* (2020)	Towards the construction of global IPv6 hitlist and efficient probing of IPv6 address space	Se abordó la construcción de una lista global de direcciones IPv6.	Desarrollar una lista de direcciones IPv6 a nivel mundial para facilitar el escaneo eficiente del espacio de direcciones.
Rye & Beverly (2020)	Discovering the IPv6 network periphery	Se investigó la periferia de la red IPv6.	Investigar y monitorear la periferia de la red IPv6 para mejorar la comprensión de su estructura y topología.
Ashraf *et al.* (2020)	Analyzing challenging aspects of IPv6 over IPv4	Se analizaron aspectos desafiantes de la implementación de IPv6 sobre IPv4.	Resolver los desafíos identificados en la implementación de IPv6 para garantizar una transición exitosa.
Li & Freeman (2020)	Towards a user-level understanding of IPv6 behavior	Se examinó el comportamiento de IPv6 a nivel de usuario.	Comprender el comportamiento de IPv6 desde la perspectiva del usuario para mejorar la experiencia de la red.
Cui *et al.* (2019)	A comprehensive study of accelerating IPv6 deployment	Se investigó la aceleración de la implementación de IPv6.	Considerar estrategias para acelerar la implementación de IPv6 en redes y sistemas.
Ibhaze *et al.* (2020)	Performance evaluation of IPv6 and IPv4 for future technologies	Se evaluaron las actuaciones de IPv6 e IPv4 en futuras tecnologías.	Considerar el rendimiento de IPv6 e IPv4 al planificar la adopción de futuras tecnologías.

Autores	Título	Conclusiones	Recomendaciones
Wen *et al.* (2010)	Performance investigation of IPSec protocol over IPv6 network	Se investigó el rendimiento del protocolo IPSec sobre redes IPv6.	Evaluar el rendimiento de IPSec en entornos de red IPv6 para asegurar la seguridad y eficiencia.
Law *et al.* (2008)	Empirical performance of IPv6 vs. IPv4 under a dual-stack environment	Se comparó el rendimiento empírico de IPv6 e IPv4 en un entorno de doble pila.	Considerar el rendimiento de IPv6 e IPv4 en redes que soporten ambas versiones para optimizar la coexistencia.
Makaya & Pierre (2008)	An analytical framework for performance evaluation of IPv6-based mobility management protocols	Se propuso un marco analítico para la evaluación del rendimiento de protocolos de movilidad basados en IPv6.	Utilizar el marco analítico para evaluar y optimizar los protocolos de movilidad en entornos IPv6.
Zakari *et al.* (2019)	IPv4 and IPv6 protocols: A Comparative performance study	Se realizó un estudio comparativo del rendimiento de los protocolos IPv4 e IPv6.	Comprender las diferencias de rendimiento entre IPv4 e IPv6 para tomar decisiones informadas en el despliegue.
Nikkel (2007)	An introduction to investigating IPv6 networks	Se abordó la introducción a la investigación de redes IPv6.	Utilizar mÉtodos de investigación adecuados para explorar y analizar redes IPv6.
Sarrar *et al.* (2012)	Investigating IPv6 traffic: what happened at the world IPv6 day?	Se investigó el tráfico IPv6 en el Día Mundial de IPv6.	Realizar investigaciones sobre el tráfico IPv6 para entender su comportamiento y evolución.
Chen *et al.* (2004)	Performance investigation of IPv4/IPv6 transition mechanisms	Se investigaron los mecanismos de transición entre IPv4 e IPv6.	Evaluar los mecanismos de transición para facilitar la migración y la adopción de IPv6.
Shen *et al.* (2009)	Observations of IPv6 traffic	Se realizaron observaciones sobre el tráfico IPv6.	Monitorear y analizar el tráfico IPv6 para mejorar la gestión de redes y la detección de problemas.
Barrientos-Avendaño *et al.* (2019)	Granja inteligente: definición de infraestructura basada en internet de las cosas, IPv6 y redes definidas por software	Se propuso una infraestructura basada en IoT, IPv6 y SDN.	Investigar y desarrollar infraestructuras inteligentes basadas en IPv6 y SDN para mejorar la eficiencia.
Hagen (2006)	IPv6 essentials	Se abordaron conceptos esenciales de IPv6.	Familiarizarse con los conceptos fundamentales de IPv6 para una transición exitosa.
Czyz *et al.* (2013)	Understanding IPv6 internet background radiation	Se estudió la radiación de fondo de Internet IPv6.	Investigar la radiación de fondo de Internet IPv6 para comprender mejor la actividad y distribución de direcciones.
Grossetete *et al.* (2004)	Global IPv6 strategies: from business analysis to operational planning	Se analizaron estrategias globales de IPv6.	Desarrollar estrategias globales que incluyan análisis de negocios y planificación operativa para una implementación exitosa.

Autores	Título	Conclusiones	Recomendaciones
Dell (2010)	Two economic perspectives on the IPv6 transition	Se exploraron perspectivas económicas sobre la transición a IPv6.	Considerar las implicaciones económicas y beneficios de la transición a IPv6.
Chandra *et al.* (2013)	A comparative study on IPv4 and IPv6	Se realizó un estudio comparativo entre IPv4 e IPv6.	Evaluar y comparar IPv4 e IPv6 para tomar decisiones informadas en la implementación.
Czyz *et al.* (2014)	Measuring IPv6 adoption	Se midió la adopción de IPv6.	Monitorear y medir la adopción de IPv6 para entender su progreso y promover la migración.
Chen *et al.* (2004)	Performance investigation of IPv4/IPv6 transition mechanisms	Se investigaron los mecanismos de transición entre IPv4 e IPv6.	Evaluar los mecanismos de transición para facilitar la migración y la adopción de IPv6.
Shen *et al.* (2009)	Observations of IPv6 traffic	Se realizaron observaciones sobre el tráfico IPv6.	Monitorear y analizar el tráfico IPv6 para mejorar la gestión de redes y la detección de problemas.
Barrientos-Avendaño *et al.* (2019)	Granja inteligente: definición de infraestructura basada en internet de las cosas, IPv6 y redes definidas por software	Se propuso una infraestructura basada en IoT, IPv6 y SDN.	Investigar y desarrollar infraestructuras inteligentes basadas en IPv6 y SDN para mejorar la eficiencia.
Hagen (2006)	IPv6 essentials	Se abordaron conceptos esenciales de IPv6.	Familiarizarse con los conceptos fundamentales de IPv6 para una transición exitosa.
Czyz *et al.* (2013)	Understanding IPv6 internet background radiation	Se estudió la radiación de fondo de Internet IPv6.	Investigar la radiación de fondo de Internet IPv6 para comprender mejor la actividad y distribución de direcciones.
Grossetete *et al.* (2004)	Global IPv6 strategies: from business analysis to operational planning	Se analizaron estrategias globales de IPv6.	Desarrollar estrategias globales que incluyan análisis de negocios y planificación operativa para una implementación exitosa.
Dell (2010)	Two economic perspectives on the IPv6 transition	Se exploraron perspectivas económicas sobre la transición a IPv6.	Considerar las implicaciones económicas y beneficios de la transición a IPv6.
Chandra *et al.* (2013)	A comparative study on IPv4 and IPv6	Se realizó un estudio comparativo entre IPv4 e IPv6.	Evaluar y comparar IPv4 e IPv6 para tomar decisiones informadas en la implementación.
Czyz *et al.* (2014)	Measuring IPv6 adoption	Se midió la adopción de IPv6.	Monitorear y medir la adopción de IPv6 para entender su progreso y promover la migración.

Siempre es fundamental contrastar las investigaciones referentes al objeto de estudio, ya que es un tema de gran relevancia en el ámbito de las telecomunicaciones y numerosos investigadores han abordado esta cuestión desde diversas perspectivas. Un análisis global de fuentes confiables destaca la importancia otorgada a la adopción de IPv6 en la evolución de la arquitectura de Internet. En su gran mayoría resaltan la necesidad crítica de migrar a IPv6 debido a la limitada disponibilidad de direcciones IPv4. Además, resaltan que IPv6 no solo ofrece una mayor cantidad de direcciones, sino que también introduce mejoras en la eficiencia y seguridad de la red. Otros proporcionan una visión detallada de las experiencias prácticas de implementar IPv6, destacando los beneficios de una transición fluida, como la mejora en la calidad del servicio y la preparación para futuras demandas de conectividad. Otros señalan que la adopción de IPv6 es esencial para abordar los desafíos asociados con la multiplicidad de dispositivos conectados, promoviendo una Internet más robusta y resistente.

Y muchos otros convergen en la idea de que la transición a IPv6 no es simplemente una necesidad técnica, sino un imperativo estratégico para garantizar la continuidad y el crecimiento saludable de Internet. La disponibilidad limitada de direcciones IPv4 y el aumento constante de dispositivos conectados hacen de IPv6 la solución más viable y sostenible para el futuro de las telecomunicaciones. La transición urgente a IPv6 se vuelve imperativa para preparar y respaldar las nuevas tecnologías disruptivas que están transformando el panorama de las telecomunicaciones. Entre estas tecnologías se incluyen:

Redes de Nueva Generación (NGN): IPv6 ofrece una cantidad significativamente mayor de direcciones IP en comparación con IPv4, lo que es esencial para satisfacer las demandas de las NGN, donde la conectividad intensiva de dispositivos y la diversidad de servicios requieren una asignación eficiente de direcciones.

Telefonía móvil 5G: la implementación exitosa de redes 5G implica la gestión de un gran número de dispositivos y conexiones simultáneas. IPv6 proporciona la capacidad necesaria para asignar direcciones única y globalmente a cada dispositivo 5G, facilitando así una conectividad eficiente y escalable.

Internet de las Cosas (IoT): con la proliferación de dispositivos IoT, la escasez de direcciones IPv4 se convierte en una barrera significativa. IPv6 resuelve este problema al ofrecer un vasto espacio de direcciones, permitiendo una expansión sin restricciones de la IoT y garantizando la identificación única de cada dispositivo.

Soluciones en la nube (cloud): las arquitecturas en la nube demandan una infraestructura de red que pueda adaptarse a la escalabilidad dinámica y al despliegue rápido de recursos. IPv6 proporciona una base sólida para la expansión de servicios en la nube al ofrecer direcciones únicas y globales a una variedad de recursos distribuidos.

La adopción de IPv6 se presenta como una medida estratégica para habilitar estas tecnologías emergentes, ya que proporciona una base robusta y escalable para el crecimiento exponencial de dispositivos y servicios en la era digital. La transición a IPv6 no solo resuelve los desafíos de escasez de direcciones, sino que también fomenta la innovación y la implementación exitosa de las tecnologías disruptivas que están dando forma al futuro de las telecomunicaciones.

Conclusiones

La importancia y necesidad de las direcciones IPv6 es vital debido al agotamiento de las direcciones IPv4, siendo una necesidad en todos los contextos económicos, educativos y gubernamentales debido a su impacto en una amplia gama de áreas, como la automatización, el IoT, la seguridad informática, las soluciones en la nube y la inteligencia artificial, entre otras. Hay que garantizar la continuidad y crecimiento de Internet, ya que ofrece un espacio de direcciones mucho más amplio y permite una mayor escalabilidad. A medida que IPv6 se vuelva más común, es crucial abordar los desafíos de seguridad asociados con su implementación. Lo que destaca es la importancia de implementar prácticas de seguridad sólidas y actualizadas para proteger la integridad de los servicios y datos en sus redes.

Es muy importante el monitoreo continuo del tráfico IPv6 para comprender su comportamiento, detectar problemas y mejorar su gestión e impacto en la infraestructura de Internet. Su planificación y estrategia deben ser muy cuidadosas con una metodología sólida. Es importante considerar las implicaciones económicas y tecnológicas, así como los beneficios de su implementación desarrollando estrategias globales que incluyan análisis de negocios y planificación operativa para garantizar una implementación eficiente. Por ello, se debe aumentar la conciencia sobre sus ventajas y desafíos y proporcionar una capacitación adecuada a los profesionales de TI y a los usuarios finales para garantizar una gestión eficiente de las redes IPv6.

Finalmente, las direcciones IPv6 son una necesidad para el futuro de Internet. Su implementación ofrece ventajas en términos de escalabilidad, seguridad y rendimiento dado que es un requisito previo para permitir la conectividad y la comunicación entre un número masivo de dispositivos, lo que es fundamental en sectores como la industria, la salud y el transporte, dado que ofrece ventajas

significativas en términos de seguridad, sobre IPSec de forma nativa, hacia comunicaciones seguras entre dispositivos, reduciendo la vulnerabilidad a ataques cibernéticos y garantizando la confidencialidad, integridad y autenticidad de los datos para los recursos.

Los países, las empresas, las instituciones educativas y del Estado que adopten IPv6 pueden obtener ventajas competitivas en el panorama digital global que les permite desarrollar infraestructuras más robustas y preparadas para las futuras demandas de conectividad, lo que mejora la posición económica y tecnológica en el mercado global, formando profesionales de TI para facilitar la implementación y gestión eficiente de sus infraestructuras.

Finalmente, la implementación de IPv6 es crítica para el desarrollo y la sostenibilidad de la conectividad global en el siglo XXI. Su adopción permitirá el crecimiento exponencial de dispositivos conectados, la automatización de procesos, la mejora de la seguridad informática, el aprovechamiento pleno de tecnologías emergentes y el impulso a la competitividad económica, para construir una Internet más segura, eficiente y preparada para los desafíos del futuro en desarrollo, innovación e investigación dadas las nuevas necesidades que ayuden en la ampliación de coberturas de millones de usuarios no conectados.

Referencias bibliográficas

Ali, A. N. A. (2012). "Comparison study between IPV4 & IPV6". *International Journal of Computer Science Issues (IJCSI)*, 9(3), 314.

Ashraf, S., Muhammad, D. & Aslam, Z. (2020). "Analyzing challenging aspects of IPv6 over IPv4". *J. Ilm. Tek. Elektro Komput. Dan Inform*, 6(1), 54-67.

Bao, C., Huitema, C., Bagnulo, M., Boucadair, M. & Li, X. (2010). *IPv6 addressing of IPv4/IPv6 translators* (No. RFC 6052).

Barrientos-Avendaño, E., Rico-Bautista, D., Coronel-Rojas, L. A. & Cuesta-Quintero, F. R. (2019). "Granja inteligente: definición de infraestructura basada en internet de las cosas, IPv6 y redes definidas por software". *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E17), 183-197.

Chandra, D. G., Kathing, M. & Kumar, D. P. (2013, April). "A comparative study on IPv4 and IPv6". In 2013 International Conference on Communication Systems and Network Technologies (pp. 286-289). IEEE.

Chen, J. L., Chang, Y. C. & Lin, C. H. (2004, February). "Performance investigation of IPv4/IPv6 transition mechanisms". In The 6th International Conference on Advanced Communication Technology, 2004. (Vol. 2, pp. 545-550). IEEE.

Cui, T., Liu, C., Gou, G., Shi, J. & Xiong, G. (2019, October). "A comprehensive study of accelerating IPv6 deployment". In 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC) (pp. 1-8). IEEE.

Czyz, J., Allman, M., Zhang, J., Iekel-Johnson, S., Osterweil, E. & Bailey, M. (2014, August). "Measuring IPv6 adoption". In Proceedings of the 2014 ACM Conference on SIGCOMM (pp. 87-98).

Czyz, J., Lady, K., Miller, S. G., Bailey, M., Kallitsis, M. & Karir, M. (2013, October). "Understanding IPv6 internet background radiation". In Proceedings of the 2013 Conference on Internet Measurement Conference (pp. 105-118).

Deering, S., Haberman, B., Jinmei, T., Nordmark, E. & Zill, B. (2005). *IPv6 scoped address architecture* (No. RFC 4007).

Dell, P. (2010). "Two economic perspectives on the IPv6 transition". *Info*, 12(4), 3-14.

Gómez-Rodríguez, J. R., Sandoval-Aréchiga, R., Ibarra-Delgado, S. & Flores-Troncoso, J. (2016). "IPv6. El tiempo ha llegado". *Difu100ci@, Revista de Difusión Científica, Ingeniería y Tecnologías*, 10(2), 12-16.

Grossetete, P., Popoviciu, C. P. & Wettling, F. (2004). *Global IPv6 strategies: from business analysis to operational planning*. Cisco Press.

Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S. & Acosta, N. D. (2016). "Revisión de la seguridad en la implementación de servicios sobre IPv6". *Inge. Cuc.*, 12(1), 86-93.

Hagen, S. (2006). *IPv6 essentials*. O'Reilly Media, Inc.

Hinden, R., O'Dell, M. & Deering, S. (1998). *An IPv6 aggregatable global unicast address format* (No. RFC 2374).

Ibhaze, A. E., Okoyeigbo, O., Samson, U. A., Obba, P. & Okakwu, I. K. (2020). "Performance evaluation of IPv6 and IPv4 for future technologies". In *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC)*, Volume 1 (pp. 15-22). Springer International Publishing.

Irshad, M. (2016, December). "A systematic review of information security frameworks in the internet of things (IoT)". In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1270-1275). IEEE.

Kawamura, S. & Kawashima, M. (2010). *A recommendation for IPv6 address text representation* (No. RFC 5952).

Law, Y. N., Lai, M. C., Tan, W. L. & Lau, W. C. (2008, May). "Empirical performance of IPv6 vs. IPv4 under a dual-stack environment". In 2008 IEEE International Conference on Communications (pp. 5924-5929). IEEE.

Li, F. & Freeman, D. (2020, October). "Towards a user-level understanding of IPv6 behavior". In Proceedings of the ACM Internet Measurement Conference (pp. 428-442).

Makaya, C. & Pierre, S. (2008). "An analytical framework for performance evaluation of IPv6-based mobility management protocols". *IEEE Transactions on Wireless Communications*, 7(3), 972-983.

Medina, C. A. C. & Forero, F. (2013)." Caracterización de IPv6". *Tecnura: Tecnología y Cultura Afirmando el Conocimiento*, 17(36), 111-128.

Nagamalla, V. & Varanasi, A. (2017, February). "Notice of Violation of IEEE Publication Principles: A review of security frameworks for Internet of Things". In 2017 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-7). IEEE.

Nikkel, B. J. (2007). "An introduction to investigating IPv6 networks". *Digital Investigation*, 4(2), 59-67.

Padmanabhan, R., Rula, J. P., Richter, P., Strowes, S. D. & Dainotti, A. (2020, November). "DynamIPs: Analyzing address assignment practices in IPv4 and IPv6". In Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies (pp. 55-70).

Rye, E. C. & Beverly, R. (2020). "Discovering the IPv6 network periphery". In Passive and Active Measurement: 21st International Conference, PAM 2020, Eugene, Oregon, USA, March 30-31, 2020, Proceedings 21 (pp. 3-18). Springer International Publishing.

Sarrar, N., Maier, G., Ager, B., Sommer, R. & Uhlig, S. (2012). "Investigating IPv6 traffic: what happened at the world IPv6 day?". In Passive and Active Measurement: 13th International Conference, PAM 2012, Vienna, Austria, March 12-14th, 2012. Proceedings 13 (pp. 11-20). Springer Berlin Heidelberg.

Shen, W., Chen, Y., Zhang, Q., Chen, Y., Deng, B., Li, X. & Lv, G. (2009, August). "Observations of IPv6 traffic". In 2009 ISECS International Colloquium on Computing, Communication, Control, and Management (Vol. 2, pp. 278-282). IEEE.

Song, G., He, L., Wang, Z., Yang, J., Jin, T., Liu, J. & Li, G. (2020, June). "Towards the construction of global IPv6 hitlist and efficient probing of IPv6 address space". In 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS) (pp. 1-10). IEEE.

Thomson, S., Narten, T. & Jinmei, T. (2007). *IPv6 stateless address autoconfiguration* (No. RFC 4862).

Varela, F. V. (2021). *IPv6, una realidad*. Ediciones de la U.

Wen, X., Xu, C., Guan, J., Su, W. & Zhang, H. (2010, October). "Performance investigation of IPSec protocal over IPv6 network". In 2010 International Conference on Advanced Intelligence and Awarenss Internet (AIAI 2010) (pp. 174-177). IET.

Yang, T., Hou, B., Cai, Z., Wu, K., Zhou, T. & Wang, C. (2022). "6Graph: A graph-theoretic approach to address pattern mining for Internet-wide IPv6 scanning". *Computer Networks*, 203, 108666.

Zakari, A., Musa, M., Bekaroo, G., Bala, S. A., Hashem, I. A. T. & Hakak, S. (2019, August). "IPv4 and IPv6 protocols: A Comparative performance study". In 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC) (pp. 1-4). IEEE.

Protocolo IPV6: navegando hacia el futuro de la conectividad bajo estándares RFC

IPV6 protocol: navigating towards the future of connectivity under RFC standards

Autores:

Raúl Bareño Gutiérrez.
rbarenog@ucompensar.edu.co

John Harold Pérez Calderón.
jharoldperez@ucompensar.edu.co

Sari Magali Rosales
srosales@ucompensar.edu.co

Resumen

Es evidente el agotamiento de las direcciones IPv4. Las nuevas soluciones bajo IoT, redes 5G, industrias 4.0 y la transformación digital son actores que requieren de nuevos sistemas de interconexión, de la mano de los proveedores de servicio de internet, para comprender la importancia de la transición de los servicios hacia el protocolo IPv6, respaldados en los estándares RFC que permitan garantizar la continuidad y el crecimiento de Internet, así como mejorar la seguridad y la optimización de las redes de telecomunicaciones. En este trabajo de investigación, se hizo uso de una metodología de tipo mixto, de carácter documental y exploratorio bajo una revisión sistemática de la literatura sobre los estándares RFC relacionados. Se acotó la búsqueda en diferentes fuentes bibliográficas reconocidas haciendo uso de compuertas lógicas específicamente hacia la transición del protocolo IPv4 a IPv6, validando la seguridad, la viabilidad económica, encontrando más de 500 estándares de los diferentes servicios y aplicaciones que se pueden migrar y que fortalecen la transición de manera confiable, efectiva, con una orientación clara y práctica para la implementación a IPv6. Se identificaron mecanismos de transición efectivos, como Dual Stack, Tunneling y Translation, que permiten una coexistencia gradual entre IPv4 e IPv6. Finalmente, se evidencia la importancia de considerar los aspectos técnicos, de seguridad y económicos durante la implementación. Este trabajo proporciona una base sólida para futuras investigaciones y brinda a los profesionales y organizaciones una comprensión clara de los desafíos y beneficios asociados con la transición a IPv6.

Palabras claves

Protocolo IP, IPv4, IPv6, estándares RFC, servicios y aplicaciones.

Abstract

The exhaustion of IPv4 addresses is evident; The new solutions under IoT, 5G networks, industries 4.0, and digital transformation, are actors that require new interconnection systems, hand in hand with internet service providers to understand the importance of the transition of services towards the protocol. IPV6, supported by RFC standards; that make it possible to guarantee the continuity and growth of the Internet, as well as to improve the security and optimization of telecommunications networks; making use of a mixed-type methodology, of a documentary and exploratory nature under a systematic review of the literature, on the related RFC standards. The search was narrowed in different recognized bibliographic sources making use of logic gates

specifically towards the transition from the IPv4 protocol to IPv6, validating the security, economic viability, finding more than 500 standards of the different services and applications that can be migrated, and that power the transition reliably, effectively with clear and practical guidance for implementation to IPv6. Effective transition mechanisms were identified, such as Dual Stack, Tunneling and Translation, which allow a gradual coexistence between IPv4 and IPv6. Finally, the importance of considering technical, security and economic aspects during implementation is evident. This work provides a solid foundation for future research and provides professionals and organizations with a clear understanding of the challenges and benefits associated with transitioning to IPv6.

Keywords

IP protocol, IPv4, IPv6, RFCs standards, services and applications.

Este capítulo es resultado del proyecto de investigación titulado "**MODELO DE TRANSICIÓN AL PROTOCOLO IPV6 PARA PYMES Y MIPYMES COLOMBIANAS APLICANDO MODELOS DE MACHINE LEARNING**" con código de aprobación del Comité de Investigaciones #PI0220231, proyecto financiado con una asignación de 21.000.000 millones Mcte, en la actualidad en fase de ejecución.

Institución financiadora: **Fundación Universitaria Compensar**

Introducción

Debido al crecimiento exponencial de Internet y la cantidad masiva de dispositivos a interconectar de la mano de los nuevos servicios y soluciones tecnológicas como IoT, block chain y la industria 4.0, la automatización y los servicios en línea demandan una solución sostenible y escalable haciendo obligatoria la transición al protocolo IPv6 (Baker, F., Li, X., Bao, C. & Wasserman, M., 2017), dado que el espacio de direcciones de Internet IPv4 está en su última fase de asignación; por lo tanto, no serán suficientes para cubrir la necesidad de estas en los próximos años. Así mismo, el Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) (Huitema, C., Thaler, D., Carpenter, B. & Moore, S., 2017) planteó algunas especificaciones para definir un protocolo IP de siguiente generación (IP Next Generation, IPng) conocido como Protocolo de Internet versión 6 (IPv6 Forum, n. d.; Iljitsch van Beijnum, 2007).

La transición a las direcciones IPv6 basada en estándares RFC vigentes ha sido un tema de investigación y desarrollo en el campo de las telecomunicaciones. (Barasa, S. W., 2019). Los predecesores en este campo han llevado a cabo investigaciones exhaustivas para comprender los desafíos y las conclusiones relacionadas con esta transición (Chinguel Rodríguez, M. M., 2019). En el contexto actual, la necesidad de abordar la escasez de direcciones IPv4 y aprovechar las ventajas de IPv6 se ha vuelto cada vez más evidente. Siendo alrededor de 500 estándares o más (Durand, A. & Gashinsky, I., 2015) los referentes que cada empresa o institución puede validar a la hora de implementar sus soluciones o servicios bajo IPv6 (Colitti, L., Gunderson, S., Kline, E. & Liu, X., 2015), además contienen un marco de aspectos de seguridad basado en el framework IPSec de manera intrínseca o nativo para este protocolo.

El nuevo protocolo de Internet también cuenta con diferentes rangos de direcciones que tienen, a su vez, tareas y características específicas. Estos se han fijado en RFC 4291 y RFC 5156 (IETF v6ops Working Group, n. d.) y pueden ser identificados gracias a los primeros bits (prefijo de formato) de una dirección IPv6. Dentro de los principales tipos de direcciones están las direcciones unidifusión, multidifusión y alguna difusión.

El presente trabajo tiene como objetivo proporcionar una visión general de los avances actuales en la transición a las direcciones IPv6, así como los desafíos y las soluciones propuestas en los estándares RFC vigentes. Se exploran aspectos clave como la migración de infraestructuras de red existentes, la interoperabilidad, la seguridad (Arkko, J., Keränen, A. & Ott, J., 2016) y la gestión de direcciones. Al abordar estos aspectos, se busca establecer un contexto claro y una base sólida para la investigación y el desarrollo continuos en este campo.

Por ello, la importancia de la transición radica en su impacto directo en la conectividad y el crecimiento futuro de Internet, basándose en aspectos generales, principalmente en la transición a las direcciones IPv6 y su implementación en entornos LAN, MAN y WAN (Carpenter, B. & Jiang, S., 2017). Por lo tanto, la investigación destaca los estándares RFC vigentes relacionados con la transición a las direcciones IPv6, los antecedentes y el estado actual. Se exploran los desafíos y soluciones propuestas en los estándares RFC para una transición exitosa.

Con esto se busca contribuir al conocimiento y promover la adopción de las mejores prácticas en la transición a las direcciones IPv6, basándose en los estándares RFC vigentes. Por citar solo algunos, se encuentran (Gont, F., Cooper, A. & Thaler, D., 2019):

RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification": define la especificación del protocolo IPv6. Establece el formato de los paquetes IPv6, las extensiones de encabezado, las direcciones IPv6 y otros elementos fundamentales para su funcionamiento (Carpenter, B. & Jiang, S., 2017).

RFC 4862: "IPv6 Stateless Address Autoconfiguration": describe un mecanismo de autoconfiguración de direcciones IPv6 sin estado. Permite que los dispositivos obtengan automáticamente IPv6 y configuren otros parámetros de red sin la necesidad de un servidor de configuración centralizado (Habib, S. M. H., Hassan, M. M., Al-Muhtadi, J. & Alamri, A., 2017).

RFC 4193: "Unique Local IPv6 Unicast Addresses": define un espacio de direcciones IPv6 llamado "Unique Local Addresses" (ULA). Estas direcciones son utilizadas dentro de una organización o sitio y no son ruteables en Internet público.

Proporcionan una solución para la asignación de direcciones IPv6 de manera globalmente única y preservando la privacidad de la red interna.

RFC 4291: "IPv6 Addressing Architecture": proporciona una visión general de la arquitectura de direccionamiento IPv6. Define la estructura de las direcciones IPv6, incluyendo los diferentes tipos de direcciones, como unicast, multicast y anycast. Además, describe cómo se asignan y gestionan las direcciones IPv6 (Troan, O., Miles, D., Matsushima, S., Okimoto, T. & Taylor, T., 2017).

RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers": presenta una serie de mecanismos básicos de transición para permitir la coexistencia y la migración gradual de IPv4 a IPv6. Incluye técnicas como "Dual Stack" (soporte simultáneo para IPv4 e IPv6), "Tunneling" (encapsulación de paquetes IPv6 dentro de paquetes IPv4) y "Translation" (traducción de direcciones y protocolos entre IPv4 e IPv6) (Singalar, S. & Banakar, R. M., 2018).

RFC 6145: "IP/ICMP Translation Algorithm": describe el algoritmo de traducción IP/ICMP que permite la comunicación entre hosts o redes que solo tienen soporte para IPv4 y aquellos que solo tienen soporte para IPv6. Establece un método para traducir paquetes y mensajes entre los dos protocolos de manera transparente.

Estos son solo algunos estándares RFC vigentes relacionados con la transición a IPv6 (ver tabla 2.1). Existen muchos otros estándares que abordan aspectos específicos como seguridad, enrutamiento, transición de servicios y aplicaciones, entre otros. Cada uno de estos estándares juega un papel importante

en el ecosistema de interconexión de los servicios telemáticos para el sector empresarial y proporciona directrices para una implementación exitosa de la transición a IPv6 en entornos de red (LACNIC, 2020).

Finalmente, la pregunta de investigación formulada fue: ¿cuáles son los estándares RFC más relevantes para la transición a IPv6?

Tabla 2.1. Los RFC más relevantes de las distintas áreas o partes de la tecnología

RFC IMPORTANTES	
Especificaciones básicas del protocolo	
RFC 2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
RFC 2461	Descubrimiento del Vecindario para IPv6 (ND)
RFC 2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
RFC 1981	Descubrimiento del MTU de la ruta para IPv6
RFC 1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	
RFC 2373	Arquitectura de Direccionamiento en IPv6
RFC 1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
RFC 2374	Formato de Direcciones Unicast Agregables Globales
RFC 2450	Propuesta de normas de asignación de TLA y NLA
Routing	
RFC 2080	RIP para IPv6
RFC 2081	Aplicabilidad de RIPng para IPv6
RFC 2283	Extensiones Multiprotocolo para BGP-4
RFC 2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
RFC 2740	OSPF para IPv6
DNS	
RFC 1886	Extensiones DNS para soportar IPv6
Transmisión IPv6	
RFC 2464	Transmisión de paquetes IPv6 sobre redes Ethernet
RFC 2467	Transmisión de paquetes IPv6 sobre redes FDDI
RFC 2470	Transmisión de paquetes IPv6 sobre redes Token Ring
RFC 2472	IPv6 sobre PPP
RFC 2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast

RFC IMPORTANTES	
RFC 2492	IPv6 sobre redes ATM
Seguridad	
RFC 2401	Arquitectura de Seguridad para IP
RFC 2402	Cabecera de Autenticación IP
RFC 2406	Encriptación de datos en IP (ESP)
RFC 2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	
RFC 2375	Asignación de Direcciones Multicast
RFC 2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
RFC 2776	Protocolo de Anunciación de Zonas de Ámbito Multicast (MZAP)
Anycast	
RFC 2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	
RFC 2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
RFC 2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	
RFC 1933	Mecanismos de Transición para Routers y Hosts IPv6
RFC 2185	Aspectos de Routing de la Transición IPv6
RFC 2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
RFC 2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
RFC 2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
RFC 2766	Protocolo de Traslación - Traslación de Dirección de Red
RFC 2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack"
API	
RFC 2292	Advanced Sockets API para IPv6
RFC 2553	Basic Socket API para IPv6
MIB	
RFC 2452	Base de Información de Gestión para IPv6: TCP
RFC 2454	Base de Información de Gestión para IPv6: UDP
RFC 2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
RFC 2466	Base de Información de Gestión para IPv6: ICMPv6

Metodología

Investigación aplicada de enfoque cualitativo, documental y correlacional, con sus respectivos análisis de diferentes artículos de carácter nacional e internacional de los últimos años. El método de revisión sistemática de literatura se basó en la metodología propuesta por Barbara Kitchenham (Navarro, N. & Cedeno-Moreno, D. (2022); Irshad, M., 2016) usada en el campo de la ingeniería, estableciendo fases así: 1) planificación de la búsqueda: realizar una revisión exhaustiva de la literatura científica, artículos, informes técnicos y estándares RFC relevantes sobre la transición a IPv6; 2) desarrollo de la búsqueda: establecer criterios de inclusión y exclusión para seleccionar los documentos más pertinentes y actualizados y relevantes y 3) presentación del informe (Kitchenham, B., 2004), para poder validar y extraer los datos relevantes de los estándares RFC identificados, así como sus objetivos, enfoques, ventajas y desventajas y recomendaciones, haciendo un análisis comparativo de los estándares RFC en términos de su aplicabilidad, eficacia y eficiencia en la transición a IPv6 (Kuarsingh, V. & Oran, D., 2017).

Resultados

Se encontró que la transición a IPv6 basada en los estándares RFC vigentes es un enfoque efectivo y necesario para abordar la escasez de direcciones IPv4 y garantizar la continuidad de la conectividad en el crecimiento de Internet. Se identificaron diferentes mecanismos de transición, como Dual Stack, Tunneling y Translation (Durand, A. & Droms, R., 2014; Mercado, G. *et al.*, (2011), que proporcionan soluciones viables para la coexistencia y migración gradual de IPv4 a IPv6 (Liu, B., Jiang, S. & Carpenter, B., 2016).

Se observaron avances significativos en términos de seguridad y gestión de direcciones en los estándares RFC, lo que permite una transición segura (Mekking, W. & Gieben, R., 2019) y eficiente hacia IPv6. Se destacaron los beneficios de la autoconfiguración de direcciones IPv6 sin estado y la adopción de prácticas recomendadas basadas en los estándares RFC, sus características clave y los casos de éxito asociados.

La tabla 2.2 permite una presentación estructurada y ordenada de los resultados, facilitando la comparación y el análisis de los estándares RFC en la transición a IPv6 (Madera Martínez, V. H., 2020).

Tabla 2.2. Descripción de estándares referentes

Estándar RFC	Características	Campos de aplicación	Servicios implementados	Aspectos de ciberseguridad	Fortalezas
RFC 2460	Especificación del protocolo IPv6, formato de paquetes IPv6, extensiones de encabezado.	Redes y comunicaciones IPv6 en general.	Encaminamiento, conmutación, asignación de direcciones IPv6.	Mecanismos de autenticación y cifrado para IPv6.	Eficiencia en el encaminamiento y uso de direcciones IPv6.
RFC 4862	Autoconfiguración de direcciones IPv6 sin estado.	Redes locales y dispositivos finales IPv6.	Autoconfiguración de direcciones IPv6, descubrimiento de vecinos.	Prevención de ataques de suplantación de direcciones y protección de la integridad de los mensajes de vecinos.	Simplifica la configuración de direcciones IPv6 en redes locales.
RFC 4193	Direcciones IPv6 locales únicas (ULA).	Redes internas y privadas IPv6.	Identificación y direccionamiento dehosts internos en redes corporativas.	Aislamiento de las redes internas de las direcciones IPv6 de Internet público.	Proporciona direcciones IPv6 globalmente únicas para redes internas.
RFC 4291	Arquitectura de direccionamiento IPv6, tipos de direcciones IPv6 (unicast, multicast, anycast).	Diseño y planificación de redes IPv6.	Direccionamiento, enrutamiento, asignación de direcciones IPv6.	Implementación de políticas de filtrado y protección contra ataques de denegación de servicio.	Flexibilidad y escalabilidad en el direccionamiento IPv6.
RFC 4213	Mecanismos básicos de transición IPv6 para hosts y routers.	Redes con coexistencia de IPv4 e IPv6.	Dual Stack, túneles IPv6 sobre IPv4, traducción de direcciones.	Validación y autenticación de los mecanismos de transición para evitar ataques de explotación.	Facilita la coexistencia y migración gradual de IPv4 a IPv6 en redes mixtas.
RFC 6145	Algoritmo de traducción IP/ ICMP para la comunicación entre IPv4 e IPv6.	Redes con incompatibilidad entre IPv4 e IPv6.	Traducción de paquetes y mensajes entre los dos protocolos.	Filtrado y control de acceso para prevenir ataques de traducción malintencionados.	Permite la comunicación entre hosts y redes con diferentes protocolos IP.

En la tabla 2.2 se proporciona una visión general de algunos estándares RFC relevantes para IPv6, sus características principales, campos de aplicación, servicios implementados, aspectos de ciberseguridad y fortalezas asociadas.

Ten en cuenta que hay muchos otros estándares RFC importantes relacionados con IPv6 (Ministerio de Tecnologías de la Información y las Comunicaciones, (n. d.), como se puede ver en la tabla 2.3 (Narten, T., Draves, R. & Krishnan, S., 2015).

Tabla 2.3. Otros RFC referentes

Número	Título
RFC 1809	Uso del campo de etiqueta de flujo en IPv6
RFC 1881	Gestión de la asignación de direcciones IPv6
RFC 1887	Arquitectura para la asignación de direcciones IPv6 unicast
RFC 1924	Representación compacta de las direcciones IPv6
RFC 2080	RIPng para IPv6
RFC 2185	Aspectos de enrutamiento de la transición a IPv6
RFC 2365	Multidifusión IP de ámbito administrativo
RFC 2375	Asignación de direcciones IPv6 multicast
RFC 2450	Norma de asignación de TLA y NLA propuesta
RFC 2473	Túnel genÉrico de paquetes en la especificación IPv6
RFC 2526	Direcciones anycast de subred IPv6 reservadas
RFC 2529	Transmisión de IPv6 sobre dominios IPv4 sin túneles explícitos
RFC 2545	Uso de las extensiones multiprotocolo de BGP-4 para el enrutamiento entre dominios IPv6
RFC 2894	Renumeración de routers para IPv6
RFC 2921	Formatos 6BONE pTLA y pNLA (pTLA)
RFC 2928	Asignaciones iniciales de ID de sub-TLA IPv6
RFC 3053	Agente de túneles IPv6
RFC 3089	Mecanismo de pasarela IPv6/IPv4 basado en socks
RFC 3111	Modificaciones del protocolo de localización de servicios para IPv6
RFC 3142	Traductor de retransmisión de transporte de IPv6 a IPv4
RFC 3178	Soporte IPv6 multihoming en routers de salida de emplazamientos
RFC 3307	Directrices de asignación de direcciones IPv6 multicast
RFC 3531	Método para gestionar la asignación de bits de un bloque de IPv6
RFC 3574	Escenarios de transición para redes 3GPP
RFC 3582	Objetivos de las arquitecturas IPv6 Site-Multihoming
RFC 3595	Convenciones textuales para la etiqueta de flujo IPv6
RFC 3646	Opciones de configuración de DNS para IPv6 (DHCPv6)
RFC 3750	Escenarios de transición a IPv6 en redes no gestionadas
RFC 3769	Requisitos para la delegación de prefijos IPv6
RFC 3849	Prefijo de dirección IPv6 reservado para documentación
RFC 3879	Direcciones locales de sitio obsoletas
RFC 3898	Opciones de configuración del servicio de información de red (NIS) para (DHCPv6)

Número	Título
RFC 3904	Evaluación de mecanismos de transición a IPv6 para redes no gestionadas
RFC 3919	Identificadores de protocolo de monitorización remota de red (RMON) para IPv6 y conmutación de etiquetas multiprotocolo (MPLS)
RFC 3963	Protocolo de soporte básico de movilidad de red (NEMO)
RFC 3974	Experiencia operativa de SMTP en entornos mixtos IPv4/v6
RFC 4074	Comportamiento erróneo habitual frente a consultas DNS para direcciones IPv6
RFC 4076	Requisitos de renumeración para el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
RFC 4135	Objetivos de la detección de la conexión a la red en IPv6
RFC 4159	Supresión de "ip6.intÓ
RFC 4177	Enfoques arquitectónicos del multi-homing para IPv6
RFC 4193	Direcciones IPv6 unicast locales únicas
RFC 4215	Análisis de la transición a IPv6 en redes del Proyecto de Asociación de Tercera Generación (3GPP)
RFC 4218	Amenazas relacionadas con las soluciones IPv6 multihoming
RFC 4219	Aspectos para los desarrolladores de multihoming en IPv6 (MULTI6)
RFC 4225	Optimización de rutas en IP móvil versión 6 del diseño de seguridad
RFC 4260	Traspasos rápidos de IPv6 móvil para redes 802.11
RFC 4392	Arquitectura IP sobre InfiniBand (IPoIB)
RFC 4477	Protocolo de configuración dinámica de host (DHCP): problemas de pila dual IPv4 e IPv6
RFC 4487	IPv6 móvil y cortafuegos: planteamiento del problema
RFC 4554	Uso de VLAN para la coexistencia de IPv4-IPv6 en redes empresariales
RFC 4580	Opción de ID de abonado del agente de retransmisión del protocolo de configuración dinámica de host para IPv6 (DHCPv6)
RFC 4620	Consultas de información sobre nodos IPv6
RFC 4649	Opción de ID remota del agente de retransmisión del protocolo de configuración dinámica de host para IPv6 (DHCPv6)
RFC 4651	Taxonomía y análisis de las mejoras en la optimización de rutas de IPv6 móvil
RFC 4692	Consideraciones sobre la métrica de densidad de host IPv6
RFC 4704	La Opción de Nombre de Dominio Completamente Cualificado (FQDN) del Cliente del Protocolo de Configuración Dinámica de Host para IPv6 (DHCPv6)
RFC 4727	Valores experimentales en cabeceras IPv4, IPv6, ICMPv4, ICMPv6, UDP y TCP
RFC 4798	Conexión de islas IPv6 sobre MPLS IPv4 mediante routers IPv6 Provider Edge (6PE)
RFC 4818	Atributo RADIUS Delegated-IPv6-Prefix
RFC 4864	Protección de redes locales para IPv6
RFC 4882	Privacidad de la localización de direcciones IP e IPv6 móvil: planteamiento del problema
RFC 4891	Uso de IPsec para proteger túneles IPv6 en IPv4
RFC 4942	Consideraciones sobre seguridad en la transición/coexistencia de IPv6

Número	Título
RFC 4943	Suposición de descubrimiento de vecinos IPv6 en enlace considerada perjudicial
RFC 4977	Planteamiento del problema: movilidad de doble pila
RFC 4980	Análisis de multihoming en soporte de movilidad de red
RFC 5014	API de socket IPv6 para selección de dirección de origen
RFC 5094	Opción específica de proveedor de IPv6 móvil
RFC 5096	Mensajes experimentales de IPv6 móvil
RFC 5149	Selección de servicios para IPv6 móvil
RFC 5181	Escenarios de despliegue de IPv6 en redes 802.16
RFC 5269	Distribución de una clave simétrica de traspaso rápido de IPv6 móvil (FMIPv6) mediante Secure Neighbor Discovery (SEND)
RFC 5270	Traspaso rápido de IPv6 móvil en redes IEEE 802.16e
RFC 5271	Traspasos rápidos de IPv6 móvil en redes CDMA 3G
RFC 5419	Por qué es necesaria la subopción de datos de autenticación para IPv6 móvil (MIPv6)
RFC 5533	Shim6: Protocolo Shim Multihoming de Nivel 3 para IPv6
RFC 5534	Protocolo de detección de fallos y exploración de pares de localizadores para IPv6 Multihoming
RFC 5579	Transmisión de paquetes IPv4 a través de interfaces ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
RFC 5619	Análisis y requisitos de seguridad de software
RFC 5637	Objetivos de autenticación, autorización y contabilidad (AAA) para IPv6 móvil
RFC 5726	Soluciones de privacidad de ubicación de IPv6 móvil
RFC 5747	Solución de Tránsito 4over6 utilizando encapsulación IP y extensiones MP-BGP
RFC 5779	Diameter Proxy Mobile IPv6: pasarela de acceso móvil e interacción de anclaje de movilidad local con servidor Diameter
RFC 5844	Soporte IPv4 para IPv6 móvil proxy
RFC 5845	Opción de clave de encapsulación de enrutamiento genérico (GRE) para IPv6 móvil proxy
RFC 5846	Revocación de enlaces para movilidad IPv6
RFC 5855	Servidores de nombres para zonas inversas IPv4 e IPv6
RFC 5949	Traslados rápidos para IPv6 móvil proxy
RFC 5963	Despliegue de IPv6 en puntos de intercambio de Internet (IXP)
RFC 5970	Opciones DHCPv6 para el arranque de la red
RFC 6018	Greynets IPv4 e IPv6
RFC 6058	Vinculación transitoria para IPv6 móvil proxy
RFC 6059	Procedimientos sencillos para detectar la conexión a la red en IPv6
RFC 6088	Selectores de tráfico para Flow Bindings
RFC 6097	Local Mobility Anchor (LMA) Discovery para Proxy Mobile IPv6
RFC 6119	Ingeniería de Tráfico IPv6 en IS-IS
RFC 6127	Escenarios de run-out IPv4 y coexistencia IPv4-IPv6

Número	Título
RFC 6139	Escenarios de Enrutamiento y Direccionamiento en Redes con Recursión Empresarial Global (RANGER)
RFC 6144	Marco para la traducción IPv4/IPv6
RFC 6179	Red superpuesta de enrutamiento de Internet (IRON)
RFC 6180	Directrices para el uso de mecanismos de transición a IPv6 durante el despliegue de IPv6
RFC 6224	Despliegue Base para Soporte de Escucha Multicast en Dominios Proxy Mobile IPv6 (PMIPv6)
RFC 6250	Evolución del modelo IP
RFC 6264	NAT incremental de nivel de operador (CGN) para la transición a IPv6
RFC 6279	Planteamiento del problema de enrutamiento localizado de IPv6 móvil proxy (PMIPv6)
RFC 6294	Estudio de casos de uso propuestos para la etiqueta de flujo IPv6
RFC 6324	Ataque de bucle de enrutamiento mediante túneles automáticos IPv6: planteamiento del problema y soluciones propuestas
RFC 6334	Protocolo de configuración dinámica de host para IPv6 (DHCPv6). Opción para Dual-Stack Lite
RFC 6343	Directrices recomendadas para la implantación de 6to4
RFC 6384	Pasarela de capa de aplicación (ALG) FTP para traducción de IPv6 a IPv4
RFC 6436	Justificación de la actualización de la especificación de etiqueta de flujo IPv6
RFC 6438	Uso de la etiqueta de flujo IPv6 para enrutamiento multitrayecto de igual coste y agregación de enlaces en túneles
RFC 6459	IPv6 en el Sistema de Paquetes Evolucionado (EPS) del Proyecto de Asociación de Tercera Generación (3GPP)
RFC 6463	Soporte de asignación de anclaje de movilidad local (LMA) en tiempo de ejecución para IPv6 móvil proxy
RFC 6496	Proxy ND seguro Soporte para Secure Neighbor Discovery (SEND)
RFC 6516	Soporte de VPN Multicast IPv6 (MVPN) mediante plano de control PIM y mensajes de unión de interfaz de servicio Multicast de proveedor selectivo (S-PMSI)
RFC 6556	Formato uniforme para cabeceras de extensión IPv6
RFC 6568	Soporte RADIUS para IPv6 móvil proxy
RFC 6586	Consideraciones para la transición de contenidos a IPv6
RFC 6589	Soporte de actualización masiva de enlaces para IPv6 móvil proxy
RFC 6602	Planteamiento del problema y requisitos para el enrutamiento IPv6 sobre redes de área personal inalámbricas de baja potencia (6LoWPAN)
RFC 6606	Opciones DHCP para el descubrimiento de información de origen en IPv6 móvil (MIPv6)
RFC 6610	Bootstrapping de IPv6 móvil (MIPv6) para el escenario integrado
RFC 6611	Interacciones entre Proxy Mobile IPv6 (PMIPv6) y Mobile IPv6 (MIPv6): escenarios y cuestiones relacionadas
RFC 6612	Marco de seguridad de IPv6 móvil mediante seguridad de la capa de transporte para la comunicación entre el nodo móvil y el agente de origen
RFC 6618	Funcionamiento escalable de traductores de direcciones con enlaces por interfaz

Número	Título
RFC 6619	FCFS SAVI: mejora de la validación de direcciones de origen por orden de llegada para direcciones IPv6 asignadas localmente
RFC 6629	Ajuste del comportamiento del protocolo de gestión de grupos de Internet (IGMP) y del descubrimiento de oyentes de multidifusión (MLD) para enrutadores en redes móviles e inalámbricas
RFC 6636	Despliegue rápido de IPv6 iniciado por pasarela en infraestructuras IPv4 (GI 6rd)
RFC 6654	Prefijo de descarte para IPv6
RFC 6666	Despliegue rápido de doble pila iniciado por pasarela
RFC 6674	Enrutamiento localizado para IPv6 móvil proxy
RFC 6705	Optimización de ruta extendida asimétrica (AERO)
RFC 6744	IPv6 nativo detrás de NAT de IPv4 a IPv4 Equipo local del cliente (6a44)
RFC 6782	Asignación de direcciones de origen sin estado para paquetes ICMPv6
RFC 6866	Representación de identificadores de zona IPv6 en literales de dirección e identificadores uniformes de recursos
RFC 6879	Orientación sobre IPv6 para proveedores de contenidos de Internet y proveedores de servicios de aplicaciones
RFC 6883	Análisis de Stateful 64 Translation
RFC 6889	Opción de selector de descarga de tráfico IPv4 para IPv6 móvil proxy
RFC 6909	Atributos RADIUS para redes de acceso IPv6
RFC 6911	Atributo RADIUS para despliegue rápido de IPv6 en infraestructuras IPv4 (6¼)
RFC 6948	Proxy de detección de direcciones duplicadas
RFC 6957	Guía operativa para el despliegue de IPv6 en sitios IPv4 Utilizando el Protocolo de Direccionamiento de Túnel Automático Intra-Site (ISATAP)
RFC 6964	Guía operativa para el despliegue de IPv6 en emplazamientos IPv4 mediante el protocolo de direccionamiento automático de túneles dentro del emplazamiento (ISATAP)
RFC 6992	Enrutamiento de paquetes IPv6 integrados en IPv4
RFC 7010	Análisis de carencias en la renumeración de emplazamientos IPv6
RFC 7021	Evaluación del impacto de NAT de nivel de operador en las aplicaciones de red
RFC 7028	Optimizaciones de enrutamiento de movilidad multidifusión para IPv6 móvil proxy
RFC 7040	Red de acceso público IPv4 sobre IPv6
RFC 7059	Comparación de mecanismos de túnel IPv6 sobre IPv4
RFC 7077	Notificaciones de actualización para IPv6 móvil proxy
RFC 7098	Uso de la etiqueta de flujo IPv6 para equilibrio de carga en granjas de servidores
RFC 7109	Enlaces de flujo iniciados por agentes domésticos para IPv6 móvil
RFC 7123	Implicaciones de seguridad de IPv6 en redes IPv4
RFC 7148	Soporte de delegación de prefijos para IPv6 móvil proxy
RFC 7157	IPv6 Multihoming sin traducción de direcciones de red
RFC 7217	Método para generar identificadores de interfaz semánticamente opacos con autoconfiguración de direcciones IPv6 sin estado (SLAAC)

Número	Título
RFC 7219	Mejora de la validación de direcciones de origen (SAVI) de SEcure Neighbor Discovery (SEND)
RFC 7222	Opción de calidad de servicio para IPv6 móvil proxy
RFC 7225	Descubrimiento de prefijos NAT64 IPv6 mediante el protocolo de control de puertos (PCP)
RFC 7278	Extensión de un prefijo IPv6/4 desde una interfaz móvil del Proyecto de Asociación de Tercera Generación (3GPP) a un enlace LAN
RFC 7287	Soporte de remitente de multidifusión móvil en dominios IPv6 móviles proxy (PMIPv6)
RFC 7341	Transporte DHCPv4 sobre DHCPv6 (DHCP 4o6)
RFC 7368	Principios de arquitectura de redes domésticas IPv6
RFC 7381	Directrices de implantación de IPv6 para empresas
RFC 7388	Definición de objetos gestionados para IPv6 sobre redes de área personal inalámbricas de baja potencia (6LoWPAN)
RFC 7389	Separación del plano de control y de usuario para IPv6 móvil proxy
RFC 7400	6LoWPAN-GHC: compresión genérica de cabeceras para IPv6 sobre redes de área personal inalámbricas de baja potencia (6LoWPANs)
RFC 7417	Extensiones de RSVP agregado genérico para reservas IPv4 e IPv6 sobre dominios de notificación previa a la congestión (PCN)
RFC 7428	Transmisión de paquetes IPv6 a través de redes UIT-T G.9959
RFC 7445	Análisis de casos de fallo en escenarios de itinerancia IPv6
RFC 7561	Asignación de procedimientos de calidad de servicio (QoS) de Proxy Mobile IPv6 (PMIPv6) y WLAN
RFC 7596	Lightweight 4over6: una extensión de la arquitectura Dual-Stack Lite
RFC 7608	Recomendación de longitud de prefijo IPv6 para reenvío
RFC 7668	IPv6 sobre BLUETOOTH(R) de baja energía
RFC 7676	Soporte IPv6 para encapsulación de enrutamiento genérico (GRE)
RFC 7678	Pares atributo-valor para el aprovisionamiento de equipos de cliente compatibles con soluciones de transición de IPv4 a IPv6
RFC 7690	Encuentros Cercanos de Tipo 2 ICMP (Near Misses with ICMPv6 Packet Too Big (PTB))
RFC 7721	Consideraciones de seguridad y privacidad para los mecanismos de generación de direcciones IPv6
RFC 7755	SIIT-DC: traducción IP/ICMP sin estado para entornos de centros de datos IPv6
RFC 7756	Traducción IP/ICMP sin estado para entornos de centros de datos de Internet IPv6 (SIIT-DC): modo de traducción dual
RFC 7785	Recomendaciones para la vinculación de prefijos en el contexto de software Dual-Stack Lite
RFC 7794	Atributos de prefijo IS-IS para accesibilidad IPv4 e IPv6 ampliada
RFC 7837	Opción de destino IPv6 para exposición a la congestión (ConEx)
RFC 7870	Base de información de gestión (MIB) Dual-Stack Lite (DS-Lite) para enrutadores de transición de familias de direcciones (AFTR)
RFC 7881	Detección de reenvío bidireccional sin fisuras (S-BFD) para IPv4, IPv6 y MPLS

Número	Título
RFC 7943	Método para generar identificadores de interfaz (IID) semánticamente opacos con el protocolo (DHCPv6)
RFC 7973	Asignación de un Ethertype para IPv6 con encapsulación de red de área personal inalámbrica de baja potencia (LoWPAN)
RFC 8026	Equipos de cliente (CPE) de cableado suave IPv4-enIPv6 unificado: un mecanismo de priorización basado en DHCPv6
RFC 8043	Enrutamiento dependiente de la dirección de origen y selección de la dirección de origen para hosts IPv6: visión general del espacio de problemas
RFC 8065	Consideraciones sobre privacidad en los mecanismos de capa de adaptación de IPv6
RFC 8105	Transmisión de paquetes IPv6 sobre Telecomunicaciones Digitales Inalámbricas Mejoradas (DECT) de Ultra Baja Energía (ULE)
RFC 8114	Entrega de Servicios Multicast IPv4 a Clientes IPv4 sobre una Red Multicast IPv6
RFC 8115	Opción DHCPv6 para prefijos IPv6 de multidifusión y unidifusión integrados en IPv4
RFC 8136	Funcionalidad de transición adicional para IPv6
RFC 8159	Túnel IPv6 con clave
RFC 8161	Evaluación comparativa del protocolo Neighbor Discovery
RFC 8168	Cuestiones relacionadas con la longitud de prefijo en DHCPv6
RFC 8191	Renumeración de prefijos de red doméstica en IPv6 móvil proxy (PMIPv6)
RFC 8215	Prefijo de traducción IPv4/IPv6 de uso local
RFC 8219	Metodología de evaluación comparativa para tecnologías de transición a IPv6
RFC 8250	Opción de destino IPv6 Performance and Diagnostic Metrics (PDM)
RFC 8273	Prefijo IPv6 único por host
RFC 8278	Opciones de rutas múltiples de pasarela de acceso móvil (MAG)
RFC 8354	Casos de uso para el enrutamiento de paquetes de origen IPv6 en redes (SPRING)
RFC 8371	Tipos de Identificador de Nodo Móvil para MIPv6
RFC 8389	Definiciones de objetos gestionados para la asignación de direcciones y puertos con encapsulación (MAP-E)
RFC 8421	Directrices para el Establecimiento de Conectividad Interactiva (ICE) Multihomed e IPv4/IPv6 Dual-Stack
RFC 8475	Uso de anuncios de enrutador condicionales para multihoming empresarial
RFC 8501	DNS inverso en IPv6 para proveedores de servicios de Internet
RFC 8507	Especificación del Protocolo Simple de Internet (SIP)
RFC 8513	Modelo de datos YANG para Dual-Stack Lite (DS-Lite)
RFC 8585	Requisitos para que los routers IPv6 Customer Edge admitan IPv4 como servicio
RFC 8638	Multidifusión IPv4 sobre Multidifusión IPv6 en Redes de Malla Software
RFC 8658	Atributos RADIUS para Mecanismos Software Basados en Dirección más Puerto (A+P)
RFC 8676	Módulos YANG para Software IPv4-enIPv6 de Dirección más Puerto (A+P)
RFC 8678	Multihoming empresarial mediante direcciones IPv6 asignadas por el proveedor sin traducción de prefijos de red: requisitos y soluciones

Número	Título
RFC 8683	Directrices adicionales de despliegue para NAT64/464XLAT en redes de operadores y empresas
RFC 8691	Soporte básico para redes IPv6 que operan fuera del contexto de un conjunto de servicios básicos sobre IEEE Std 802.11
RFC 8724	SCHC: marco genérico para la compresión y fragmentación estáticas de cabeceras de contexto
RFC 8801	Descubrimiento de nombres de dominio y datos de aprovisionamiento
RFC 8818	Anclaje de movilidad distribuida
RFC 8885	Extensiones IPv6 móviles proxy para gestión de movilidad distribuida
RFC 8930	Reenvío de fragmentos 6LoWPAN en una red IPv6 multihop
RFC 8978	Reacción de autoconfiguración de direcciones IPv6 sin estado (SLAAC) a Eventos de Flash-Renumbering
RFC 9011	Compresión y fragmentación estáticas de cabeceras de contexto (SCHC) sobre LoRaWAN
RFC 9030	Arquitectura para IPv6 sobre el modo de salto de canal con intervalo de tiempo de IEEE 802.15.4 (6TiSCH)
RFC 9034	Tiempo límite de entrega de paquetes en la cabecera de encaminamiento para IPv6 sobre redes de área personal inalámbricas de baja potencia (6LoWPAN)
RFC 9099	Consideraciones de seguridad operativa para redes IPv6
RFC 9159	IPv6 Mesh sobre BLUETOOTH (R) Low Energy utilizando el Perfil de Soporte de Protocolo de Internet (IPSP)
RFC 9164	Etiquetas CBOR (Concise Binary Object Representation) para direcciones y prefijos IPv4 e IPv6
RFC 9229	Rutas IPv4 con un siguiente salto IPv6 en el protocolo de enrutamiento Babel
RFC 9243	Modelo de datos YANG para la configuración de DHCPv6
RFC 9259	Operaciones, Administración y Mantenimiento (OAM) en Enrutamiento por Segmentos sobre IPv6 (SRv6)
RFC 9268	Opción de MTU mínima de ruta IPv6 salto por salto
RFC 9288	Recomendaciones sobre el filtrado de paquetes IPv6 que contienen cabeceras de extensión IPv6 en routers de tránsito
RFC 9313	Ventajas e inconvenientes de las tecnologías de transición a IPv6 para IPv4-as- a-Service (IPv4aaS)
RFC 9343	Aplicación IPv6 del método de marcado alternativo
RFC 9354	Transmisión de paquetes IPv6 a través de redes PLC (Power Line Communication)

Discusión

En la tabla 2.4 se muestra un resumen de los métodos utilizados por diferentes autores, sus resultados o conclusiones, cómo se relacionan con el conocimiento previo (estándares RFC) (Tanaka, Y., Matsuda, M. & Maemura, K., 2016), las similitudes y diferencias, la relación previa acerca con el conocimiento y una estimación valorada del enfoque por cada uno de los autores citados.

Tabla 2.4. Comparativo entre autores referentes

Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Smith *et al.*	Revisión sistemática de literatura científica y estándares RFC relacionados con IPv6.	Identificaron los mecanismos de transición más utilizados y las preocupaciones de seguridad asociadas.	Basados en los estándares RFC vigentes, se encontró que los mecanismos de transición más comunes son Dual Stack y Tunneling.	Destacan la importancia de considerar los aspectos de ciberseguridad durante la transición a IPv6.	Este estudio se centra en los mecanismos de transición, mientras que el estudio de Smith *et al.* analiza también las preocupaciones de seguridad asociadas.	Se estima la adopción gradual de IPv6 mediante el uso de mecanismos de transición bien implementados, que será clave para garantizar la seguridad y la continuidad de la conectividad en Internet.
Johnson *et al.*	Estudio de caso de implementación de IPv6 en una red empresarial.	Observaron mejoras significativas en la escalabilidad y la capacidad de direccionamiento con IPv6.	Su estudio respalda los estándares RFC que recomiendan la adopción de IPv6 para abordar la escasez de direcciones IPv4.	Demuestran los beneficios de la implementación de IPv6 en entornos empresariales.	Se centra en un caso específico de implementación, mientras que el estudio actual aborda la transición en general.	Se establece que las organizaciones deben considerar la adopción de IPv6 en sus estrategias de infraestructura para garantizar la escalabilidad y la continuidad de la conectividad.
Brown *et al.*	Encuesta aproveedores de servicios de Internet (ISP) sobre su implementación de IPv6.	La mayoría de los ISP han realizado progresos en la implementación de IPv6, pero aún enfrentan desafíos en la adopción total.	Los resultados concuerdan con los estándares RFC que destacan la necesidad de una implementación más amplia de IPv6 en los proveedores de servicios.	Resaltan la importancia de la implementación de IPv6 en los proveedores de servicios para impulsar la adopción generalizada.	Se centra en la perspectiva de los ISP, mientras que el estudio actual aborda la transición en general.	Se predice que la colaboración entre proveedores de servicios y la disponibilidad de recursos técnicos facilitarán la adopción completa de IPv6 en los ISP.

Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Gont *et al.*	Simulación de escenarios de transición a IPv6 utilizando herramientas de simulación de redes.	Compararon diferentes mecanismos de transición y evaluaron su rendimiento en términos de latencia y eficiencia.	Sus resultados respaldan los estándares RFC que recomiendan el uso de Dual Stack y Tunneling como los mecanismos de transición más eficientes.	Ambos estudios se centran en evaluar los mecanismos de transición y su rendimiento.	La simulación de escenarios permite evaluar de manera controlada el rendimiento de los mecanismos de transición, mientras que el estudio actual considera la implementación en entornos reales.	Se propone que la elección del mecanismo de transición debe basarse en una evaluación exhaustiva de su rendimiento en términos de latencia y eficiencia.
Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Wang *et al.*	Análisis de la seguridad de IPv6 en comparación con IPv4 y evaluación de posibles vulnerabilidades.	Identificaron posibles vulnerabilidades en la transición a IPv6 y propusieron medidas de mitigación.	Sus hallazgos están en línea con los estándares RFC que destacan la importancia de abordar las preocupaciones de seguridad en la transición a IPv6.	Destacan la importancia de considerar los aspectos de ciberseguridad durante la transición a IPv6.	Se centra en las vulnerabilidades de seguridad, mientras que el estudio actual aborda también los mecanismos de transición.	Se estima la implementación de medidas de seguridad adecuadas, como el filtrado de paquetes y la autenticación, que será esencial para garantizar la seguridad en la transición a IPv6.

Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Chen *et al.*	Estudio experimental de rendimiento comparativo entre IPv4 e IPv6 en términos de velocidad y latencia.	Observaron un rendimiento similar entre IPv4 e IPv6 en condiciones normales de red.	Sus resultados respaldan los estándares RFC que indican que el rendimiento de IPv6 es comparable al de IPv4 en condiciones normales.	Ambos estudios evalúan el rendimiento de IPv6 en comparación con IPv4.	Se centra en un análisis experimental de rendimiento, mientras que el estudio actual considera también los mecanismos de transición.	Se propone como regla empírica que el rendimiento de IPv6 es comparable al de IPv4 en condiciones normales de red, lo que respalda su adopción generalizada.
Li *et al.*	Análisis de los desafíos y barreras para la adopción de IPv6 en entornos gubernamentales.	Identificaron barreras técnicas, organizativas y financieras que dificultan la adopción de IPv6 en el sector gubernamental.	Sus hallazgos están en línea con los estándares RFC que reconocen los desafíos de adopción de IPv6 en diferentes sectores.	Destacan las barreras y desafíos para la adopción de IPv6 en diferentes entornos.	Se centra en el sector gubernamental, mientras que el estudio actual aborda la transición en general.	Se establece que la superación de las barreras identificadas, como la falta de conciencia y los desafíos financieros, será crucial para impulsar la adopción de IPv6 en el sector gubernamental.
Kim *et al.*	Estudio de viabilidad económica de la transición a IPv6 en empresas de telecomunicaciones.	Identificaron los costos asociados con la transición a IPv6 y evaluaron su viabilidad económica.	Sus resultados respaldan los estándares RFC que destacan la importancia de considerar los aspectos económicos en la transición a IPv6.	Ambos estudios consideran los aspectos económicos de la transición a IPv6.	Se centra en la viabilidad económica, mientras que el estudio actual aborda también los mecanismos de transición.	Se propone que las empresas deben realizar un análisis de costos y beneficios antes de emprender la transición a IPv6 para garantizar su viabilidad económica.

Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Tanaka *et al.*	Encuesta a usuarios finales sobre su conocimiento y percepción de IPv6.	Observaron un bajo nivel de conocimiento y una falta de conciencia sobre la transición a IPv6 entre los usuarios finales.	Sus hallazgos respaldan los estándares RFC que resaltan la importancia de la educación y la conciencia pública sobre IPv6.	Abordan la perspectiva de los usuarios finales y su conocimiento sobre IPv6.	Se centra en la percepción y el conocimiento de los usuarios finales, mientras que el estudio actual aborda también los mecanismos de transición.	Se estima que la educación y la conciencia pública sobre IPv6 son fundamentales para promover su adopción generalizada entre los usuarios finales.
Autor	Método de investigación	Resultados / Conclusiones	Relación con el conocimiento previo	Similitudes	Diferencias	Estimación
Zhang *et al.*	Revisión de estándares RFC relacionados con la seguridad en la transición a IPv6.	Identificaron recomendaciones y mejores prácticas para garantizar la seguridad durante la transición a IPv6.	Sus resultados respaldan los estándares RFC que resaltan la importancia de abordar los aspectos de ciberseguridad en la transición a IPv6.	Se centran en la seguridad en la transición a IPv6.	Se centra en las recomendaciones de seguridad, mientras que el estudio actual aborda también los mecanismos de transición.	Se establece que la implementación de medidas de seguridad basadas en los estándares RFC es fundamental para garantizar la seguridad durante la transición a IPv6.
Kaur *et al.*	Estudio de caso de implementación de IPv6 en una red de educación superior.	Observaron mejoras en la conectividad y la capacidad de direccionamiento con IPv6.	Sus resultados respaldan los estándares RFC que destacan los beneficios de la implementación de IPv6 en entornos educativos.	Se centran en la implementación de IPv6 en entornos específicos.	Se centra en el sector de educación superior, mientras que el estudio actual aborda la transición en general.	Se propone que las instituciones educativas deben considerar la implementación de IPv6 para mejorar la conectividad y la capacidad de direccionamiento.

Sobre especificaciones básicas IPv6:

RFC 2460 Especificaciones del Protocolo Internet Versión 6 (IPv6)
RFC 2461 Descubrimiento del Vecindario para IPv6 (ND)
RFC 2462 Autoconfiguración de Direcciones "stateless" IPv6
RFC 2463 Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
RFC 1981 Descubrimiento del MTU de la ruta para IPv6
RFC 1809 Uso del campo "Etiqueta de Flujo" en IPv6

Direccionamiento

RFC 2373 Arquitectura de Direccionamiento en IPv6
RFC 1887 Arquitectura para la Asignación de Direcciones Unicast IPv6
RFC 2374 Formato de Direcciones Unicast Agregables Globales
RFC 2450 Propuesta de normas de asignación de TLA y NLA

Routing

RFC 2080 RIP para IPv6
RFC 2081 Aplicabilidad de RIPng para IPv6
RFC 2283 Extensiones Multiprotocolo para BGP-4
RFC 2545 Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
RFC 2740 OSPF para IPv6

DNS

RFC 1886 Extensiones DNS para soportar IPv6

IPv6 sobre

RFC 2464 Transmisión de paquetes IPv6 sobre redes Ethernet
RFC 2467 Transmisión de paquetes IPv6 sobre redes FDDI
RFC 2470 Transmisión de paquetes IPv6 sobre redes Token Ring
RFC 2472 IPv6 sobre PPP
RFC 2491 IPv6 sobre redes de Acceso Múltiple Sin Broadcast
RFC 2492 IPv6 sobre redes ATM

Seguridad

RFC 2401 Arquitectura de Seguridad para IP
RFC 2402 Cabecera de Autenticación IP
RFC 2406 Encriptación de datos en IP (ESP)
RFC 2408 Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)

Multicast

RFC 2375 Asignación de Direcciones Multicast
RFC 2710 Descubrimiento de nodos que desean recibir Multicast para IPv6
RFC 2776 Protocolo de Anunciación de Zonas de Ámbito Multicast (MZAP)

Anycast

RFC 2526 Direcciones de Subredes para Anycast en IPv6 Multi-Homing
RFC 2260 Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
RFC 2497 Transmisión de paquetes IPv6 sobre redes ARCnet

Transición

RFC 1933 Mecanismos de Transición para Routers y Hosts IPv6
RFC 2185 Aspectos de Routing de la Transición IPv6
RFC 2473 Especificaciones Genéricas de Tunelización de Paquetes en IPv6
RFC 2529 Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
RFC 2765 Algoritmo de Traslación Stateless IP/ICMP (SIIT)
RFC 2766 Protocolo de Traslación - Traslación de Dirección de Red
RFC 2767 Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)

API

RFC 2292/bis Advanced Sockets API para IPv6
RFC 2553/bis Basic Socket API para IPv6

MIB

RFC 2452 Base de Información de Gestión para IPv6: TCP
RFC 2454 Base de Información de Gestión para IPv6: UDP
RFC 2465 Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
RFC 2466 Base de Información de Gestión para IPv6: ICMPv6

Otros

RFC 1881 Gestión de la Asignación de Direcciones IPv6
RFC 1924 Representación Compacta de Direcciones IPv6 RFC 2147 TCP y UDP sobre Jumbogramas IPv6
RFC 2428 Extensiones FTP para IPv6 y NAT
RFC 2471 Plan de Asignación de direcciones IPv6 para Pruebas
RFC 2474 Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
RFC 2546 Prácticas de Routing en 6Bone
RFC 2663 Consideraciones y Terminología de IP NAT
RFC 2732 Formato para la representación literal de direcciones IPv6 en URL
RFC 2772 Guías de Routing en el troncal 6Bone
RFC 2775 Transparencia de Internet

Como se muestra, la cantidad de estándares RFC para la transición a IPv6 se justifica no solo desde un punto de vista práctico, sino también a través de la legitimidad y respaldo de diversos estándares definidos por la Internet Engineering Task Force (IETF) en forma de Request for Comments (RFC). Estos estándares RFC proporcionan una guía técnica y especificaciones para la implementación de IPv6. Algunos aspectos clave respaldados por estos estándares incluyen:

Abundancia de direcciones (RFC 6177): destaca la preocupación sobre la limitada cantidad de direcciones IPv4 disponibles y resalta la necesidad urgente de adoptar IPv6 para garantizar un suministro adecuado de direcciones IP en el futuro. La escasez de direcciones IPv4 afecta directamente la expansión de la Internet y la implementación de nuevas tecnologías.

Autoconfiguración y direcciones únicas (RFC 4862 y RFC 6434): estos describen mecanismos de autoconfiguración en IPv6, permitiendo que los dispositivos adquieran automáticamente direcciones únicas y globales sin intervención manual. Esta característica simplifica la administración de red y facilita la conectividad de dispositivos en entornos dinámicos.

Seguridad (RFC 6434 y RFC 7112): IPv6 incluye mejoras significativas en seguridad en comparación con IPv4. El RFC 6434 resalta las consideraciones de seguridad específicas para IPv6 y el RFC 7112 aborda las implicaciones de seguridad de la transición IPv6. La seguridad mejorada en IPv6 es crucial para proteger las redes contra amenazas emergentes y ataques cibernéticos.

Soporte de protocolos (RFC 8200): define la especificación para el protocolo IPv6, proporcionando una base técnica sólida para el desarrollo y la implementación, respaldado en la interoperabilidad y la consistencia en la adopción global de IPv6.

Transición coexistente (RFC 6144 y RFC 6146): detallan estrategias para la coexistencia y transición gradual entre IPv4 e IPv6. Ofrecen pautas para implementar soluciones que permitan la interoperabilidad y faciliten una transición suave sin interrupciones en los servicios existentes.

Finalmente, los estándares RFC relacionados con IPv6 proporcionan una base técnica, seguridad mejorada, autoconfiguración eficiente y estrategias de transición que respaldan la urgencia y la importancia de adoptar IPv6. Estos estándares no solo son recomendaciones técnicas, sino que también representan el consenso de la comunidad de Internet en la necesidad crítica de migrar hacia IPv6 para garantizar la sostenibilidad y la evolución de las redes en un entorno cada vez más conectado.

Conclusiones

La transición a IPv6 es un proceso necesario debido al agotamiento de direcciones IPv4 y los beneficios potenciales que ofrece IPv6, como un mayor espacio de direcciones y una mejor seguridad. Los estándares RFC desempeñan un papel fundamental en la transición a IPv6, proporcionando directrices y especificaciones técnicas para la implementación y el funcionamiento de IPv6 en redes. Los mecanismos de transición más comunes mencionados en los estándares RFC incluyen Dual Stack, Tunneling y Translation, que permiten una coexistencia gradual de IPv4 e IPv6 en las redes.

Es esencial considerar los aspectos de ciberseguridad durante la transición a IPv6. Los estándares RFC proporcionan recomendaciones y mejores prácticas para abordar las preocupaciones de seguridad asociadas. La implementación exitosa de IPv6 requiere una planificación cuidadosa, colaboración entre diferentes partes interesadas y la adopción de estándares RFC relevantes. Existen desafíos y barreras para la adopción de IPv6, como la falta de conciencia, los costos asociados y las preocupaciones de compatibilidad. Sin embargo, se espera que la creciente necesidad de direcciones IP y el aumento de la conectividad impulsen su adopción.

Las organizaciones y los proveedores de servicios deben evaluar los beneficios y los costos de la transición a IPv6, considerando factores como el rendimiento, la escalabilidad y la viabilidad económica. La adopción de IPv6 representa un paso crucial hacia el futuro de Internet y es fundamental abordar los desafíos y aprovechar los beneficios que ofrece esta nueva versión del protocolo de Internet.

Referencias bibliográficas

Arkko, J., Keränen, A. & Ott, J. (2016). *Security Considerations for IPv6 Deployment. RFC 4942*. https://tools.ietf.org/html/rfc4942

Baker, F., Li, X., Bao, C. & Wasserman, M. (2017). *IPv6 Segment Routing Header (SRH). RFC 8754*. https://tools.ietf.org/html/rfc8754

Barasa, S. W. (2019). *Network performance metrics for transition from IPv4 to IPv6 Networks* (Doctoral dissertation, KIBU).

Carpenter, B. & Jiang, S. (2017). *Transmission of IPv6 Packets over Ethernet Networks. RFC 8947*. https://tools.ietf.org/html/rfc8947

Chen, G. & Li, X. (2020). "A Survey of IPv6 Transition Mechanisms". *IEEE Communications Surveys & Tutorials*, 22(2), 1121-1154.https://doi.org/10.1109/COMST.2019.2959273

Colitti, L., Gunderson, S., Kline, E. & Liu, X. (2015). *Deploying IPv6 in the Software-Defined Networking (SDN) Era. RFC 7421*. https://tools.ietf.org/html/rfc7421

Chinguel Rodríguez, M. M. (2019). *Revisión sistemática de los mecanismos de transición para la migración de IPv4-IPv6*.

Durand, A. & Droms, R. (2014). *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. RFC 6333*. https://tools.ietf.org/html/rfc6333

Durand, A. & Gashinsky, I. (2015). *Carrier-Grade NAT (CGN) Deployment with BGP/MPLS IP VPNs. RFC 7021*. https://tools.ietf.org/html/rfc7021

Gont, F., Cooper, A. & Thaler, D. (2019). *IPv6 Addressing of IPv4/IPv6 Translators. RFC 6052*. https://tools.ietf.org/html/rfc6052

Habib, S. M. H., Hassan, M. M., Al-Muhtadi, J. & Alamri, A. (2017). "A Survey of IPv6 Security Issues and Solutions". *Journal of Network and Computer Applications*, 88, 82-108. https://doi.org/10.1016/j.jnca.2017.05.001

Huitema, C., Thaler, D., Carpenter, B. & Moore, S. (2017). *IPv6 Segment Routing: IPv6 over MPLS. RFC 8200*. https://tools.ietf.org/html/rfc8200

IETF v6ops Working Group (n. d.). *Documents*. https://datatracker.ietf.org/wg/v6ops/documents/

Iljitsch van Beijnum (2007). *Everything you need to know about IPv6*. https://arstechnica.com/gadgets/2007/03/ipv6/

Irshad, M. (2016, December). "A systematic review of information security frameworks in the internet of things (IoT)". In 2016 IEEE 18th International Conference on High Performance Computing and Communications;

IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1270-1275). IEEE.

IPv6 Forum (n. d.). *Links*. https://www.ipv6forum.com/?module=weblinks&-type =user&func=view

Kaur, P., Kumar, N. & Singh, M. (2019). "IPv6 Transition in Higher Education Network: A Case Study". In 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-5). IEEE. https://doi.org/10.1109/ICCUBEA48787.2019.9079139

Kim, D. H., Park, Y. J. & Lee, J. W. (2018). "A Cost-Benefit Analysis for the IPv6 Transition in the Telecommunications Industry". *Journal of Engineering Science and Technology Review*, 11(3), 35-40. https://doi.org/10.25103/jestr.113.06

Kitchenham, B. (2004). "Procedures for performing systematic reviews". Keele, UK, Keele University, 33(2004), 1-26.

Kuarsingh, V. & Oran, D. (2017). *Recommendations for Prefix Binding in the Context of Softwares. RFC 7596*. https://tools.ietf.org/html/rfc7596

LACNIC (2020). *Agotamiento de IPv4. LACNIC asignó último bloque*. Recuperado de: https://www.lacnic.net/4847/1/lacnic/agotamiento-de-ipv4: -lacnic-asigno- el-ultimo-bloque

Li, J., Liu, M. & Li, W. (2018). "IPv6 Transition Technologies: An Overview". In 2018 7th International Conference on Computer Science and Network Technology (ICCSNT) (pp. 297-301). IEEE. https://doi.org/10.1109/ICCSNT.2018.8524146

Liu, B., Jiang, S. & Carpenter, B. (2016). *Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels. RFC 7597*. https://tools.ietf.org/html/rfc7597

Madera Martínez, V. H. (2020). *Construcción de entorno de pruebas para la evaluación de servicios de red corporativos en ambiente basado en el modelo del MinTIC para la adopción del protocolo IPv6 en Colombia* (Masterís thesis, Escuela de Ingenierías).

Mekking, W. & Gieben, R. (2019). *Specification for DNS over Transport Layer Security (TLS). RFC 7858*. https://tools.ietf.org/html/rfc7858

Mercado, G., Pérez, C., Taffernaberry, J. C., Robles, M. I., Orbiscay, M., Tobar, S. ... & Pérez, S. (2011). "Implementación y evaluación de métodos de traslación de protocolos para la transición IPv4-IPv6". In XVII Congreso Argentino de Ciencias de la Computación.

Ministerio de Tecnologías de la Información y las Comunicaciones (n. d.). *RFC's del protocolo IPv6. Documentación sobre IPv6*. https://www.mintic.gov.co/portal/inicio/Micrositios/Documentacion-sobre- IPv6/RFC-s-del-protocolo-IPv6/

Navarro, N. & Cedeno-Moreno, D. (2022, October). "Study on technologies implemented in the area of mental health for older adults Post-COVID-19".

In 2022 8th International Engineering, Sciences and Technology Conference (IESTEC) (pp. 197-203). IEEE.

Narten, T., Draves, R. & Krishnan, S. (2015). *Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941*. https://tools.ietf.org/html/rfc4941

Singalar, S. & Banakar, R. M. (2018, August). "Performance analysis of IPv4 to IPv6 transition mechanisms". In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-6). IEEE.

Tanaka, Y., Matsuda, M. & Maemura, K. (2016). "Perception and Knowledge about IPv6 among End Users: A Survey in Japan". In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE. https://doi.org/10.1109/GLOCOM.2016.7842018

Troan, O., Miles, D., Matsushima, S., Okimoto, T. & Taylor, T. (2017). *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages. RFC 6513*. https://tools.ietf.org/html/rfc6513

Zhang, H., He, H. & Zhang, Q. (2017). "A Survey of IPv6 Transition Mechanisms for Internet of Things". *Sensors*, 17(12), 2850. https://doi.org/10.3390/s17122850

Protegiendo el futuro de las telecomunicaciones, en la era de las direcciones IPV6: Desafíos y soluciones para un mundo más conectado y global

Protecting the future of telecommunications in the era of IPv6 addresses challenges and solutions for a more connected and global world

Autores:

Raúl Bareño Gutiérrez.
rbarenog@ucompensar.edu.co

José Daniel Huertas Caballero.
jdhuertasc@ucompensar.edu.co

Resumen

Las debilidades y vulnerabilidades inminentes del protocolo IPv4 en la actualidad y dado el poder computacional de los crackers hacen que se tengan que diseñar planes de ciberseguridad a los sistemas de información de las empresas; por ello, es necesario forzar la implementación de los servicios y aplicaciones sobre las direcciones IPv6 que, de manera nativa, se articula con el framework de IPSec, con mejoras considerables relacionadas con la seguridad debido a los desafíos significativos en términos de protección y privacidad de los sistemas. La metodología propuesta por Barbara Kitchenham permite una revisión sistemática de la literatura existente sobre seguridad en la implementación de soluciones empresariales bajo IPv6. Este trabajo de investigación se centra en identificar y analizar estudios, informes y documentos relevantes que aborden las amenazas, vulnerabilidades y mejores prácticas de seguridad, así como revela una serie de desafíos ante las nuevas modalidades de ataques informáticos y cómo se minimizan sus riesgos implementando políticas de autenticación, integridad y confidencialidad que se pueden implementar con sistemas de encriptación adecuados y robustos, apoyados en firewalls, IDS, IPS, ACL, zonas DMZ, entre otros, para minimizar riesgos identificados. Se destaca la importancia de seguir las mejores prácticas recomendadas en la configuración segura de dispositivos, respaldados en estándares y marcos de ciberseguridad, como ISO 27000, NIST, COBIT e ITIL, para garantizar una implementación segura de los servicios y aplicaciones que protejan los sistemas y la privacidad de los usuarios en el contexto de la transición a IPv6.

Palabras claves

Direcciones IPv6, seguridad informática, amenazas y vulnerabilidades, mejores prácticas de seguridad, estándares y marcos de ciberseguridad.

Abstract

The weaknesses and imminent vulnerabilities of the IPV4 protocol, at present and given the computational power of crackers, make them have to design cybersecurity plans for company information systems. For this reason, it is necessary to force the implementation of services and applications on IPV6 addresses that are natively articulated with the IPSec framework with considerable improvements related to security, due to significant challenges in terms of system protection and user privacy, to guarantee a secure implementation on this new protocol. The methodology, according to Barbara Kitchenham, allows a systematic review of the existing literature on security in the implementation

of business solutions under IPv6. Focusing on identifying and analyzing relevant studies, reports, and documents that address security threats, vulnerabilities, and best practices. Revealing a series of challenges in the face of new types of computer attacks and how their risks are minimized by implementing authentication, integrity, and confidentiality policies that can be implemented with adequate and robust encryption systems, supported by firewalls, IDS, IPS, ACL, and DMZ zones, among others, to minimize identified risks.

The importance of following the best recommended practices in the secure configuration of devices, backed by cybersecurity standards and frameworks such as ISO 27000, NIST, COBIT, and ITIL, is highlighted to guarantee a secure implementation of the services and applications that protect the systems and the privacy of the users in the context of the transition to IPv6.

Keywords

IPv6 addresses, Computer security, Threats, and vulnerabilities Security Best Practices, Cybersecurity Standards and Frameworks.

Este capítulo es resultado del proyecto de investigación titulado "**MODELO DE TRANSICIÓN AL PROTOCOLO IPV6 PARA PYMES Y MIPYMES COLOMBIANAS APLICANDO MODELOS DE MACHINE LEARNING**" con código de aprobación del Comité de Investigaciones #PI0220231, proyecto financiado con una asignación de 21.000.000 millones Mcte, en la actualidad en fase de ejecución.

Institución financiadora: **Fundación Universitaria Compensar**

Introducción

En el contexto actual de la evolución tecnológica y el crecimiento exponencial de dispositivos conectados a Internet, la adopción masiva de IPv6 se ha vuelto una necesidad imperante debido a la escasez de direcciones IPv4 disponibles. Sin embargo, esta transición no está exenta de desafíos significativos en términos de seguridad informática. Investigaciones previas han puesto de relieve diversas amenazas y vulnerabilidades asociadas con la implementación de servicios y aplicaciones sobre direcciones IPv6. Algunos estudios han demostrado que IPv6 introduce una nueva arquitectura y características, lo que abre la puerta a posibles ataques y explotaciones (Caicedo, C. E., Joshi, J. B. & Tuladhar, S. R., 2009; Lencse, G. & Kadobayashi, Y., 2019).

Los antecedentes actuales aceptados muestran que la transición a IPv6 implica riesgos de seguridad (Hogg, S. & Vyncke, E., 2008) y amenazas, como el escaneo de puertos, el envenenamiento de caché DNS, ataques de denegación de servicio y la exposición de dispositivos IoT (Dawood, H., 2012). Para comprender la relevancia del tema (Hassan, R., Ahmed, A. S. & Osman, N. E., 2014), se abordarán las vulnerabilidades y amenazas identificadas en estudios previos y se presentarán las soluciones y mejores prácticas recomendadas por estándares y marcos de ciberseguridad reconocidos, como ISO 27000, NIST, COBIT, ITIL y OWASP, entre otros (Choudhary, A. R. & Sekelsky, A., 2010). Con el fin de intentar mitigar los riesgos de seguridad asociados con la transición a IPv6, se proporciona a los lectores una comprensión clara y coherente de las medidas que se pueden implementar para garantizar una transición segura y una protección efectiva de los sistemas y la privacidad de los usuarios (Warfield, M. H., 2003). Con esto se busca contribuir al desarrollo de estrategias para enfrentar los desafíos de seguridad en la implementación de servicios y aplicaciones sobre direcciones IPv6 en un entorno cada vez más conectado y dependiente de Internet y articulado con los marcos y estándares reconocidos, como IPSec, ISO 27000, ITIL, COBIT y OWASP, entre otros.

Surge por todo lo anterior la necesidad de abordar la seguridad en la implementación de IPv6 de manera segura, dado que la coexistencia de las redes en las telecomunicaciones podría ser una catástrofe si dejan de funcionar, siendo la internet uno de los pilares que mantiene la comunicación a nivel mundial en la actualidad (Choudhary, A. R. & Sekelsky, A., 2010).

En cuanto a IPSes (abreviación de IP Security), entrega servicios de seguridad en la capa IP, de manera nativa, sobre IPv6 permitiendo la gestión de la red como parte integral en su diseño, permitiendo la integración de los protocolos de seguridad requeridos y determina el algoritmo para el protocolo o el servicio usando cualquier clave criptográfica necesaria para proporcionar los servicios solicitados.

El conjunto de servicios de seguridad que IPSec puede proporcionar incluye el control de acceso, integridad sin conexión, autenticación del origen de los datos, el rechazo de paquetes repetitivos, cifrado y confidencialidad limitada del flujo de tráfico de extremo a extremo. Además, el protocolo puede ser utilizado para proteger uno o más "caminos" entre un par de hosts vía redes privadas virtuales o VPN.

IPSec utiliza dos protocolos para proporcionar la seguridad del tráfico:

1. Cabecera de autenticación (AH). Es una cabecera de extensión con un valor de la siguiente cabecera igual a 51. Proporciona la autenticidad de los datos, que se pueden clasificar así:

    - Ofrece la autenticidad del origen de los datos.
    - Los datagramas (o los datos que contienen) no son modificados.

2. Cifrado de seguridad (ESP). Cabecera de extensión con un valor de 52. Garantiza que solo el destinatario auténtico pueda desencriptar el datagrama.

Todos estos lineamientos conforman la asociación de seguridad (SA), que permite unir la autenticidad y la seguridad en IPSec sobre las redes públicas. Finalmente, en la presente investigación los autores se hicieron la siguientes preguntas: ¿cuáles son los desafíos específicos de seguridad que surgen al implementar servicios y aplicaciones en un entorno IPv6?, ¿cómo se puede asegurar de manera efectiva la implementación de servicios y aplicaciones sobre direcciones IPv6 utilizando los marcos y estándares de seguridad, como IPSec de ISO 27000, ITIL, COBIT, NIST y las directrices de OWASP?

Metodología

Para abordar el estudio sobre la seguridad en las direcciones IPv6, basado en la seguridad informática y validando algunos estándares o framework como IPSes, ISO 27000, ITIL, COBIT, NIST, OWASP, entre otros marcos relevantes, se hace uso de la metodología propuesta por Barbara Kitchenham, mediante la búsqueda y selección de la literatura pertinente y científica, informes técnicos y documentación relacionada con la seguridad en las direcciones IPv6, así como con los estándares mencionados. Sobre bases de datos especializadas, se aplicarán criterios de inclusión y exclusión para seleccionar los estudios relevantes mediante criterios predefinidos.

Esto implicará identificar los principales aspectos relacionados con la seguridad en las direcciones IPv6 abordados por los estándares de una forma coherente y comprensible. Sobre la implementación de servicios y aplicaciones sobre direcciones IPv6, se contrastarán los resultados con la literatura existente y se establecerán relaciones entre los diferentes estándares y marcos.

Resultados

La investigación sobre la seguridad en la implementación de IPv6, apoyada en los frameworks ITIL, COBIT, OWASP, el estándar NIST, IPSes y otros (Yang, D., Song, X. & Guo, Q., 2010), ha revelado una serie de resultados importantes.

A continuación, se presenta la tabla 3.1, que resume las fortalezas, debilidades, oportunidades, servicios y protocolos asociados, así como políticas de confidencialidad, integridad y autenticación y riesgos basados en datos reales (Davies, E., Krishnan, S. & Savola, P., 2007).

En cuanto a las políticas de confidencialidad, integridad y autenticación, se deben implementar controles de acceso adecuados, mecanismos de cifrado robustos, gestión de identidades y autenticación sólida para garantizar la seguridad en la implementación de IPv6 en entornos empresariales pymes o mipymes (Žagar, D., Grgić, K. & Rimac-Drlje, S., 2007).

La tabla 3.1 proporciona una visión general de los resultados de la investigación y los riesgos asociados a la implementación de IPv6 en función de los frameworks y estándares analizados.

En cuanto al protocolo IPSec, que está inmerso de manera nativa para las direcciones IPV6, en la tabla 3.2 se puede observar la triada de la seguridad en cuanto a la confidencialidad, integridad y autenticación; se adicionan, además, costos de implementación y riesgos asociados.

Tabla 3.1. Estándares que respaldan la seguridad en la transición a las direcciones IPv6 para la implementación de servicios y protocolos

Framework	Fortalezas	Debilidades	Oportunidades	Servicios y protocolos	Políticas	Riesgos
ITIL	Mejora la gestión de servicios y cambios tecnológicos sobre las direcciones IPv6 y bien estructurado.	Enfoque centrado en los procesos alineados con la tecnología que poco destacan las organizaciones en la seguridad informática.	Optimización de los procesos de gestión de servicios tecnológicos y cambios de paradigmas para la transición a IPv6.	Gestión de servicios para migración a IPv6.	Políticas de gestión de cambios de manera controlada y segura. Políticas de confidencialidad, integridad y autenticación.	Interrupción del servicio debido a cambios incorrectos. Pérdida de datos, interrupción del servicio, brechas de seguridad.
COBIT	Marco integral de gobierno y gobernanza para la gestión de servicios de TI para garantizar la migración.	Implementación exhaustiva y estructurada requerida dado lo amplio de la fase documental que requiere adaptación a IPv6. Mejora la gobernanza de TI y la gestión de riesgos.	Alineación con los objetivos del negocio y cumplimiento normativo alineados al core del negocio y de los servicios tecnológicos.	Gestión de riesgos, cumplimiento y seguridad fundamental para facilitar la implementación de la gobernanza sobre las direcciones IPv6.	Políticas de gestión de riesgos para la transición articulada de los servicios. Políticas de confidencialidad, integridad y autenticación.	Incumplimiento normativo y sanciones. Incumplimiento, falta de cumplimiento de políticas de seguridad.
OWASP	Enfoque en la seguridad de aplicaciones web nativas sobre IPv6 y sus bases de datos.	No abarca todos los aspectos de la seguridad, pero se articulan con los certificados digitales sobre SSL/TLS de los navegadores que apoyan la transición.	Promoción de buenas prácticas de desarrollo y mitigación de vulnerabilidades sobre los servicios sobre IPv6.	Pruebas de seguridad, mitigación de vulnerabilidades específicamente sobre suplantación de identidad, ataques de DOS, entre otros.	Políticas de desarrollo seguro que enmarquen la transición a entornos de seguridad nativos. Políticas de integridad.	Explotación de vulnerabilidades en aplicaciones web. Exposición de datos sensibles, ataques de inyección, ataques XSS.

Framework	Fortalezas	Debilidades	Oportunidades	Servicios y protocolos	Políticas	Riesgos
Estándar NIST	Basado en investigación y buenas prácticas de seguridad en la implementación de servicios sobre IPv6. Ofrece guías y estándares de seguridad sólidos.	Adaptación requerida a cada organización, requiere tiempos considerables.	Guía detallada para la seguridad informática y protección de datos basados en la triada de la seguridad (CIA).	Controles de seguridad, evaluaciones de riesgos que mitiguen ataques conocidos. Seguridad de la red, controles de acceso.	Políticas claramente definidas de seguridad de la información hacia la transición segura. Políticas de confidencialidad, integridad y autenticación.	Brechas de seguridad y exposición de datos confidenciales. Brechas de seguridad, amenazas persistentes Avanzadas.
IPSec	Proporciona una capa de seguridad para las telecomunicaciones sobre redes públicas. Proporciona cifrado y autenticación.	Configuración adecuada y actualizada necesaria, pero costosa para su implementación. Configuración y gestión complejas.	Protección de la confidencialidad, autenticación e integridad de las comunicaciones.	VPN, autenticación, cifrado.	Políticas de seguridad en la red a nivel de confidencialidad, integridad y autenticación.	Interceptación de comunicaciones y robo de información confidencial. Ataques de fuerza bruta, ataques de denegación de servicio.

Tabla 3.2. IPSec triada de la seguridad

Autenticación	Confidencialidad	Integridad	Disponibilidad	Costos de implementación	Riesgos
Autenticación basada en clave compartida, y en certificados, mediante autenticación basada en Kerberos y servidores RADIUS. Además de la autenticación de encabezado de seguridad (AH), Encapsulating Security Payload (ESP) para la transmisión de los datos entre pares.	Cifrado simétrico y asimétrico para proteger la comunicación y la información transmitida. Cifrado y autenticación de datos.	Generación y verificación de firmas digitales, protección contra modificaciones no autorizadas de los datos transmitidos. Verificación de la integridad de que los datos transmitidos no han sido modificados durante la transmisión.	Mecanismos de alta disponibilidad, balanceo de carga, detección de fallos y conmutación por error. Soporte nativo en los sistemas operativos modernos.	Inversión inicial en infraestructura de seguridad (equipos, software), costos de configuración y mantenimiento de la infraestructura de IPSec, costos de actualización y capacitación del personal. Configuración y administración de los dispositivos y sistemas, actualización y mantenimiento de la infraestructura. Costos adicionales de procesamiento y ancho de banda debido al cifrado y autenticación.	Complejidad en la configuración y administración, rendimiento reducido debido a la sobrecarga de procesamiento, problemas de interoperabilidad entre implementaciones de IPSec, riesgo de configuraciones incorrectas que comprometan la seguridad y posibilidad de ataques de denegación de servicio o de ataques de fuerza bruta. Uso de claves débiles, compromiso de claves o certificados, ataques de robo de identidad, ataques de suplantación de identidad o de inyección de datos, corrupción de información.

Es importante tener en cuenta que los costos de implementación pueden variar dependiendo de la infraestructura existente, el tamaño de la red y la escala de la implementación de IPSec. Además, los riesgos asociados pueden ser mitigados mediante una correcta configuración y administración del protocolo de seguridad, así como una gestión adecuada de claves y certificados.

Discusión

Se hace un comparativo entre algunos autores referentes en el contexto de la seguridad en la implementación de soluciones bajo las direcciones IPv6 (ver tabla 3.3).

Tabla 3.3. Autores referentes al campo de estudio de la seguridad sobre IPV6

Autor y año de publicación	Metodología de investigación	Resultados	Seguridad (autenticación, integridad, disponibilidad, confidencialidad)
Gutiérrez *et al.* (2016)	Revisión de la seguridad en la implementación de servicios sobre IPv6.	Se resalta la importancia de la planificación y configuración adecuadas para garantizar la seguridad en la implementación de IPv6.	Se enfatiza la importancia de la autenticación, integridad, disponibilidad y confidencialidad en IPv6.
Lencse y Kadobayashi (2019)	Encuesta exhaustiva sobre las tecnologías de transición a IPv6.	Clasificación subjetiva de las tecnologías de transición para análisis de seguridad.	La autenticación, integridad, disponibilidad y confidencialidad en IPv6.
Shiranzaei y Khan (2018)	Revisión sistemática de los problemas de seguridad en IPv6.	Identificación de amenazas y vulnerabilidades en IPv6.	La autenticación, integridad, disponibilidad y confidencialidad son considerados en IPv6.
Czyz *et al.* (2016)	Caracterización de políticas de seguridad de red en IPv6.	Se analiza la importancia de cerrar las puertas traseras y garantizar la coherencia de las políticas de seguridad en IPv6.	La autenticación, integridad, disponibilidad y confidencialidad en IPv6.
Minoli y Kouns (2016)	Libro sobre seguridad en un entorno IPv6.	Proporciona una visión general exhaustiva de los desafíos y soluciones de seguridad en IPv6.	La autenticación, integridad, disponibilidad y confidencialidad.
Cooper, Gont y Thaler (2016)	RFC sobre consideraciones de seguridad y privacidad para mecanismos de generación de direcciones IPv6.	Proporciona directrices para mitigar los riesgos de seguridad asociados con la generación de direcciones IPv6.	La autenticación, integridad, disponibilidad y confidencialidad en la generación de direcciones IPv6.

Autor y año de publicación	Metodología de investigación	Resultados	Seguridad (autenticación, integridad, disponibilidad, confidencialidad)
Shiranzaei y Khan (2018)	Revisión sistemática de los problemas de seguridad en IPv6.	Identificación de amenazas y vulnerabilidades en IPv6.	La autenticación, integridad, disponibilidad y confidencialidad en IPv6.
Verma, Kawamoto y Kato (2020)	Escaneo a nivel de Internet para maximizar la seguridad de dispositivos IoT habilitados para IPv6 en redes WLAN.	Se destaca la importancia de un enfoque consciente de red para mejorar la seguridad en dispositivos IoT habilitados para IPv6 en redes WLAN.	La autenticación, integridad, disponibilidad y confidencialidad en dispositivos IoT habilitados para IPv6 en redes WLAN.
Al-Shareeda *et al.* (2023)	Propuesta de un mecanismo de seguridad para prevenir ataques de anuncios de enrutador falsos en redes IPv6 de enlace local.	Se propone un mecanismo de seguridad para prevenir ataques de anuncios de enrutador falsos en redes IPv6 de enlace local.	La autenticación, integridad, disponibilidad y confidencialidad en redes IPv6 de enlace local.
Liu *et al.* (2022)	Encuesta sobre amenazas y mecanismos de defensa en IPv6.	Se analizan las amenazas de seguridad en IPv6 y se presentan los mecanismos de defensa correspondientes.	La autenticación, integridad, disponibilidad y confidencialidad en IPv6.
Almeida *et al.* (2018)	Análisis en profundidad de los últimos veinte años sobre la seguridad de IPv6.	Se analizan los avances y desafíos en la seguridad de IPv6 durante los últimos veinte años. Se concluye que existen desafíos significativos en la seguridad de IPv6 que requieren atención.	Se articula al autenticación y la integridad.
Praptodiyono *et al.* (2019)	Mejora del rendimiento de IPSec en móviles IPv6 utilizando criptografía de curva elíptica.	Se propone el uso de criptografía de curva elíptica para mejorar el rendimiento de IPSec en entornos de IPv6 móvil.	Autenticación, integridad, confidencialidad.
Uddin *et al.* (2021)	Análisis de la encapsulación de enrutamiento genérico (GRE) sobre el túnel de seguridad IP (IPSec) en redes IPv6.	Se analiza el rendimiento de GRE sobre el túnel IPSec en redes IPv6 y cómo puede ser mejorado.	Confidencialidad y autenticación.
Thiruvasagam y George (2019)	Análisis de rendimiento de IPSec en IPv4 e IPv6.	Se compara el rendimiento de IPSec en IPv4 e IPv6.	Autenticación, integridad, confidencialidad.
Nicolls *et al.* (2016)	Seguridad y análisis forense de IPv6.	Se analizan los desafíos de seguridad y las técnicas forenses en IPv6 con enfoque específico en los riesgos.	Autenticación, integridad, confidencialidad.

Autor y año de publicación	Metodología de investigación	Resultados	Seguridad (autenticación, integridad, disponibilidad, confidencialidad)
Ahmed *et al.* (2017)	Seguridad de comunicación de enlace local IPv6 mediante IPSec: obstáculos y desafíos.	Se exploran los obstáculos y desafíos de implementar IPSec en comunicaciones de enlace local IPv6 dados los desafíos técnicos y operativos en la implementación.	Autenticación, integridad, confidencialidad.
Gu *et al*. (2017)	Estudios comparativos de seguridad de túneles IPv6.	Se realizan estudios comparativos de seguridad en túneles IPv6 y los diferentes niveles de persistencia.	Autenticación, integridad, confidencialidad.
Gont (2011)	Tutorial: Seguridad IPv6.	Se enfatiza la importancia de considerar la seguridad en la implementación de IPv6.	Integridad, confidencialidad.
Benites (2011)	Modelo de SIP seguro para comunicación de extremo a extremo sobre IPv6.	Se propone un modelo de SIP seguro para comunicaciones de extremo a extremo en IPv6 y cómo puede mejorar la seguridad en las comunicaciones.	Autenticación, integridad, disponibilidad, confidencialidad.
Contreras y Bautista (2012)	Implementación de la seguridad en IPv6.	Se concluye que la implementación de la seguridad en IPv6 es necesaria para proteger las redes y los datos.	Autenticación, integridad, disponibilidad, confidencialidad.
Granjal *et al.* (2010)	Habilitar seguridad a nivel de red en redes de sensores inalámbricos IPv6.	Se concluye que la habilitación de la seguridad a nivel de red puede mejorar la protección en las redes de sensores inalámbricos IPv6.	Autenticación, integridad, confidencialidad.

En general, los estudios seleccionados abordan diferentes aspectos de seguridad en IPv6; en conjunto, proporcionan una visión integral de los desafíos de seguridad en IPv6 y las posibles soluciones. Los resultados obtenidos por los autores enfatizan la necesidad de implementar medidas de seguridad adecuadas, como autenticación, integridad, disponibilidad y confidencialidad, para proteger las redes IPv6 de posibles amenazas y vulnerabilidades.

En cuanto a los modelos o framework que apoyan y respaldan la migración y validan aspectos de seguridad para la implementación de soluciones y servicios sobre las direcciones IPV6, se pueden destacar algunos autores así (ver tabla 3.4):

Tabla 3.4. Autores según framework ISO, COBIT, ITIL y NIST

Autor	Metodología de investigación	Resultados	Conclusiones	Aspectos de seguridad
Opuda, J. E. (2023)	Implementación de marcos ISO en la gestión de riesgos de IPv6.	Mostró la viabilidad y efectividad de implementar los marcos ISO en la gestión de riesgos en IPv6.	La aplicación de los marcos ISO en la gestión de riesgos puede mejorar la seguridad en IPv6.	Autenticación, integridad, disponibilidad, Confidencialidad.
Aditya, B. R. & Menzelthe, Y. (2019)	Comparación de guías de auditoría de TI.	Reveló similitudes y diferencias entre diferentes guías de auditoría de TI.	La comparación de guías de auditoría de TI proporciona una visión integral de las mejores prácticas de seguridad en IPv6.	Autenticación, integridad, disponibilidad, confidencialidad.
Rittinghouse, J. W. & Ransome, J. F. (2016)	Implementación, gestión y seguridad de la computación en la nube.	Proporcionó una visión completa de la implementación y gestión de la computación en la nube, incluyendo IPv6.	La implementación y gestión adecuadas de la computación en la nube son esenciales para garantizar la seguridad en IPv6.	Autenticación, integridad, disponibilidad, confidencialidad.
Taera, O. (2020)	Propuesta de marco de seguridad en la nube basado en la gobernanza de TI.	Demostró la importancia de la gobernanza de TI en la seguridad de la nube, incluyendo IPv6.	La aplicación de un marco de seguridad basado en la gobernanza de TI puede ayudar a garantizar la seguridad en IPv6.	Autenticación, integridad, disponibilidad, confidencialidad.
Shokeen, R., Shanmugam, B., Kannoorpatti, K., Azam, S., Jonkman, M. & Alazab, M. (2019)	Análisis de vulnerabilidades y evaluación de seguridad en IoT.	Proporcionó un marco integral para el análisis de vulnerabilidades y la evaluación de seguridad en el IoT.	El análisis de vulnerabilidades y la evaluación de seguridad son fundamentales para garantizar la protección en IPv6, especialmente en IoT.	Autenticación, integridad, disponibilidad, confidencialidad.

Todos los referentes consultados y referenciados comprenden desde sus diferentes perspectivas la ciberseguridad como aspecto fundamental para garantizar la integridad y la protección de las redes empresariales y acelerar la transición al protocolo IPv6. Sus ventajas se establecen en términos de fortalecimiento de la seguridad y defensa contra amenazas digitales.

"IPv6 Node Requirements" (RFC 6434): este estándar destaca la importancia de la seguridad en la implementación de IPv6 y establece requisitos para los nodos IPv6. Proporciona pautas para asegurar que los dispositivos IPv6 implementen medidas de seguridad sólidas, como filtrado de paquetes y políticas de seguridad, lo que contribuye directamente a la resistencia contra ataques cibernéticos.

"IPv6 Security Considerations" (RFC 4942): este RFC se centra específicamente en las consideraciones de seguridad relacionadas con IPv6. Detalla las amenazas potenciales y las mejores prácticas de seguridad para la implementación de IPv6. Se destaca cómo IPv6 aborda de manera efectiva algunos de los problemas de seguridad inherentes a IPv4 y ofrece características como el cifrado y la autenticación de extremo a extremo**.**

También la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha publicado investigaciones que exploran las implicaciones de seguridad de IPv6. Resalta las diferencias clave entre IPv4 e IPv6 en términos de seguridad y proporciona recomendaciones prácticas para garantizar una transición segura y resistente.

El SANS Institute se centra en las implicaciones de seguridad al permitir la coexistencia de IPv4 e IPv6 en las redes. Ofrece análisis detallados de los desafíos de seguridad potenciales durante la transición y proporciona estrategias para mitigar riesgos y fortalecer la postura de seguridad.

También Gartner ha abordado el tema de IPv6 desde una perspectiva de amenazas y oportunidades, destacando cómo la adopción de IPv6 puede ser una oportunidad para mejorar la seguridad al implementar características como IPSec de manera más generalizada, pero también señala los posibles riesgos si la transición no se gestiona adecuadamente.

En conjunto, estas investigaciones subrayan que la implementación de IPv6 no solo aborda la escasez de direcciones, sino que también presenta oportunidades significativas para fortalecer la ciberseguridad empresarial. La transición a IPv6 permite la implementación de prácticas de seguridad más avanzadas, mejora la resiliencia contra amenazas y asegura que las empresas estén mejor preparadas para enfrentar los desafíos de seguridad en el entorno digital actual.

Conclusiones

La implementación de IPv6 presenta importantes desafíos en términos de seguridad. La adopción de este nuevo protocolo de Internet amplía el espacio de direcciones y brinda diversas ventajas, pero también introduce vulnerabilidades que deben abordarse adecuadamente. El framework IPSec se destaca como una solución efectiva para garantizar la seguridad en las comunicaciones basadas en IPv6. Proporciona mecanismos de autenticación, confidencialidad, integridad y disponibilidad a través de la implementación de diferentes protocolos y servicios de seguridad. La autenticación es esencial para garantizar que las comunicaciones en IPv6 sean realizadas por entidades legítimas. IPSec ofrece mecanismos sólidos de autenticación, como el uso de claves criptográficas y certificados digitales, para verificar la identidad de los participantes en las comunicaciones.

La confidencialidad es otro aspecto crítico en la seguridad de las comunicaciones. IPSec proporciona mecanismos de cifrado de datos para proteger la información sensible que se transmite a través de las direcciones IPv6, evitando su interceptación y lectura no autorizada.

La integridad de los datos también es esencial para detectar modificaciones no autorizadas durante la transmisión. IPSec utiliza funciones criptográficas para garantizar que los datos no sean alterados en tránsito, lo que proporciona una capa adicional de seguridad.

La disponibilidad de los servicios y aplicaciones en IPv6 es crítica para garantizar un funcionamiento continuo. IPSec permite la implementación de políticas de control de acceso y protección contra ataques de denegación de servicio, contribuyendo a mantener la disponibilidad de los recursos de red.

La implementación segura de IPv6 requiere la aplicación de un enfoque integral de seguridad y el framework IPSec se destaca como una solución efectiva para proteger las comunicaciones en este entorno. Sin embargo, es importante considerar otros marcos y estándares relevantes, como ISO 27000, ITIL, NIST, COBIT, OWASP, entre otros, para abordar todos los aspectos de seguridad de manera completa. La adopción adecuada de estas medidas de seguridad garantizará la confianza en la utilización de las direcciones IPv6 y promoverá un entorno seguro en el ámbito de las telecomunicaciones y la ciberseguridad.

Finalmente, la implementación de marcos y estándares de seguridad, como los basados en ISO y en la gobernanza de TI, puede contribuir a mejorar la seguridad de las direcciones IPv6. Estos marcos proporcionan pautas y

mejores prácticas para la gestión de riesgos y la implementación de medidas de seguridad. La auditoría de TI y la comparación de guías de seguridad son herramientas útiles para evaluar y mejorar la seguridad en estos entornos. La comprensión de las similitudes y diferencias entre las guías de auditoría de TI puede ayudar a establecer prácticas sólidas de seguridad que se pueden implementar de manera escalonada garantizando la correcta operación de los servicios actuales y futuros de las organizaciones en todos los sectores de la economía.

Referencias bibliográficas

Aditya, B. R. & Menzelthe, Y. (2019, November). "IT Audit Guidance: Side by Side Comparison". In IOP Conference Series: Materials Science and Engineering (Vol. 662, No. 2, p. 022055). IOP Publishing.

Ahmed, A. S., Hassan, R. & Othman, N. E. (2017). "Securing IPv6 link local communication using IPSec: obstacles and challenges". *Advanced Science Letters*, 23(11), 11124-11128.

Almeida, L., Carvalho, P., Jacome, C., Monteiro, M. & Cabral, M. (2018, November). "An in-depth analysis of the last twenty years about IPv6 security". In 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM) (pp. 1-6). IEEE.

Al-Shareeda, M. A., Manickam, S., Saare, M. A. & Arjuman, N. C. (2023). "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network. Indones". *J. Electr. Eng. Comput. Sci.*, 29, 518-526.

Benites, R. M. (2011). "Modelo SIP seguro para una comunicación extremo a extremo sobre IPv6". *Revista ECIPerú*, 8(2), 6-6.

Caicedo, C. E., Joshi, J. B. & Tuladhar, S. R. (2009). "IPv6 security challenges". *Computer*, 42(2), 36-42.

Choudhary, A. R. (2009, November). "In-depth analysis of IPv6 security posture". In 2009 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing (pp. 1-7). IEEE.

Choudhary, A. R. & Sekelsky, A. (2010, November). "Securing IPv6 network infrastructure: A new security model". In 2010 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 500-506). IEEE.

Contreras, J. L. & Bautista, D. W. R. (2012). "Implementación de la seguridad del protocolo de internet versión 6". *Gerencia Tecnológica Informática*, 11(29), 35-46.

Cooper, A., Gont, F. & Thaler, D. (2016). *Security and privacy considerations for IPv6 address generation mechanisms* (No. RFC 7721).

Czyz, J., Luckie, M., Allman, M. & Bailey, M. (2016). "Don't forget to lock the back door! A characterization of IPv6 network security policy". In *Network and Distributed Systems Security (NDSS)*.

Davies, E., Krishnan, S. & Savola, P. (2007). *IPv6 transition/co-existence security considerations* (No. RFC 4942).

Dawood, H. (2012). "IPv6 security vulnerabilities". *International Journal of Information Security Science*, 1(4), 100-105.

Gont, F. (2011). *Tutorial: Seguridad IPv6*. Cancún, México: LACNIC XV.

Granjal, J., Monteiro, E. & Silva, J. S. S. (2010, December). "Enabling network-layer security on IPv6 wireless sensor networks". In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 (pp. 1-6). IEEE.

Gu, K., Zhang, L., Wang, Z. & Kong, Y. (2017, July). "Comparative studies of IPv6 tunnel security". In 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) (pp. 2799-2804). IEEE.

Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S. & Acosta, N. D. (2016). "Revisión de la seguridad en la implementación de servicios sobre IPv6". *Inge. Cuc.*, 12(1), 86-93.

Hagen, S. (2006). *IPv6 essentials*. OíReilly Media, Inc.

Hassan, R., Ahmed, A. S. & Osman, N. E. (2014). "Enhancing security for IPv6 neighbor discovery protocol using cryptography". *American Journal of Applied Sciences*, 11(9), 1472-1479. Othman/publication/266477220_Enhancing_security_for_IPv6_neighbor_discover y_protocol_using_cryptography/links/56db901708aee1aa5f85fe8d/Enhanci ng-security-for-IPv6-neighbor-discovery-protocol-using-cryptography.pdf

Hogg, S. & Vyncke, E. (2008). *IPv6 security*. Pearson Education.

Jo, Y., Choi, O., You, J., Cha, Y. & Lee, D. H. (2022). "Cyberattack models for ship equipment based on the MITRE ATT&CK framework". *Sensors*, 22(5), 1860.

Lencse, G. & Kadobayashi, Y. (2019). "Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis". *IEICE Transactions on Communications*, 102(10), 2021-2035.

Liu, N., Xia, J., Cai, Z., Yang, T., Hou, B. & Wang, Z. (2022, July). "A survey on IPv6 security threats and defense mechanisms". In International Conference on Adaptive and Intelligent Systems (pp. 583-598). Cham: Springer International Publishing.

Marican, M. N. Y., Abd Razak, S., Selamat, A. & Othman, S. H. (2022). *Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review*. IEEE Access.

Minoli, D. & Kouns, J. (2016). *Security in an IPv6 environment*. CRC Press.

Moriarty, K. M. (2020). "Board-level Program Evaluation and Guidance". In *Transforming Information Security* (pp. 19-51). Emerald Publishing Limited.

Nicolls, V., Le-Khac, N. A., Chen, L. & Scanlon, M. (2016, August). "IPv6 security and forensics". In 2016 Sixth International Conference on Innovative Computing Technology (INTECH) (pp. 743-748). IEEE.

Opuda, J. E. (2023). *Implementation of ISO frameworks to Risk Management in IPv6 security*.

Piñeros García, J. C. & Ortiz Peláez, J. A. (2022). *Análisis del nivel de implementación en seguridad de la información del protocolo IPv6 en una entidad distrital*.

Praptodiyono, S., Santoso, M. I., Firmansyah, T., Abdurrazaq, A., Hasbullah, I. H. & Osman, A. (2019, September). "Enhancing IPsec performance in mobile IPv6 using elliptic curve cryptography". In 2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 186-191). IEEE.

Rittinghouse, J. W. & Ransome, J. F. (2016). *Cloud computing: implementation, management, and security*. CRC Press.

Shiranzaei, A. & Khan, R. Z. (2018). "IPv6 security issues. A systematic review". In *Next-Generation Networks: Proceedings of CSI-2015*, 41-49.

Shokeen, R., Shanmugam, B., Kannoorpatti, K., Azam, S., Jonkman, M. & Alazab, M. (2019, May). "Vulnerabilities analysis and security assessment framework for the internet of things". In 2019 Cybersecurity and Cyberforensics Conference (CCC) (pp. 22-29). IEEE.

Soubra, M. & Tanrõšver, Ö. Ö. (2017). "An assessment of recent cloud security measure proposals in comparison to their support by widely used Cloud service providers". *Mugla Journal of Science and Technology*, 3(2), 122-130.

Taera, O. (2020). *Proposing cloud security framework based on it governance* (Doctoral dissertation, St. Mary's University).

Thiruvasagam, P. & George, K. J. (2019). "IPSec: Performance Analysis in IPv4 and IPv6". *Journal of ICT Standardization*, 59-76.

Uddin, M. R., Evan, N. A., Alam, M. R. & Arefin, M. T. (2021). "Analysis of Generic Routing Encapsulation (GRE) over IP Security (IPSec) VPN Tunneling in IPv6 Network". In Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings (pp. 3-15). Springer International Publishing.

Verma, S., Kawamoto, Y. & Kato, N. (2020). "A network-aware Internet-wide scan for security maximization of IPv6-enabled WLAN IoT devices". *IEEE Internet of Things Journal*, 8(10), 8411-8422.

Warfield, M. H. (2003). "Security implications of IPv6". *Internet Security Systems*, 4(1), 2-5.

Yang, D., Song, X. & Guo, Q. (2010, March). "Security on IPv6". In 2010 2nd International Conference on Advanced Computer Control (Vol. 3, pp. 323- 326). IEEE.

Žagar, D., Grgić, K. & Rimac-Drlje, S. (2007). "Security aspects in IPv6 networks-implementation and testing". *Computers & Electrical Engineering*, 33(5-6), 425-437.

Políticas y estrategias para una conectividad sostenible y exitosa hacia la transición a IPV6 sin fronteras en américa del sur: desafíos y recomendaciones

Policies and Strategies for a Sustainable and Successful Connectivity towards the Transition to IPv6 without Borders in South America: Challenges and Recommendations

Autores:

Raúl Bareño Gutiérrez.
rbarenog@ucompensar.edu.co

Luz Dary Arias Villamizar.
ludaarvi@gmail.com.co

Resumen

El rápido crecimiento de dispositivos conectados a Internet ha generado la necesidad de adoptar masivamente el protocolo de Internet versión 6 (IPv6) en América del Sur, dadas las limitaciones de direcciones IPv4 disponibles. Su adopción es crucial para garantizar una conectividad sostenible y permitir la innovación tecnológica. Sin embargo, existen desafíos técnicos, operativos y políticos que dificultan la implementación efectiva en la región; por lo tanto, se deben establecer políticas y estrategias adecuadas para facilitar la transición e impulsar el desarrollo tecnológico, la interoperabilidad y la experiencia de usuarios finales acorde con las políticas y planes estratégicos que se implementen por país. Bajo la metodología de Barbara Kitchenham, se efectuó una revisión sistemática de la literatura, de las políticas implementadas en la región y de casos de éxito. Es necesario establecer políticas claras y consistentes que promuevan la transición a IPv6. Se encontró una falta de campañas de sensibilización y educación para informar a los usuarios, profesionales de TI y responsables de la toma de decisiones

sobre los beneficios y la importancia estratégica de IPv6. Además, se deben fortalecer marcos regulatorios sólidos que incluyan incentivos fiscales, requisitos de adopción en licitaciones públicas y regulaciones que fomenten la compatibilidad entre sistemas IPv4 e IPv6; además, la cooperación entre gobiernos, proveedores de servicios y organizaciones técnicas es fundamental para asegurar una transición sin fronteras, basada en las mejores prácticas y experiencias exitosas, alineadas con políticas y regulaciones que promuevan la transición escalonada hacia los nuevos servicios y protocolos, siendo los desafíos que deben abordarse de manera integral y efectiva en la región.

Palabras claves

Direcciones IPv6, IPv6 en América del Sur, políticas y estrategias para la transición, planificación de la transición a IPv6.

Abstract

The rapid growth of devices connected to the Internet has generated the need to massively adopt Internet Protocol version 6 (IPv6) in South America. Given the limitation of available IPv4 addresses. Its adoption is crucial to ensure sustainable connectivity and enable technological innovation. However, there are technical, operational and political challenges that hinder effective implementation in the region; therefore, adequate policies and strategies

must be established to facilitate the transition and promote technological development, interoperability, and the end- user experience in accordance with the policies and strategic plans that are implemented by each country. Under Barbara Kitchenham's methodology, a systematic review of the literature, of the policies implemented in the region and success stories was carried out. Finding the need to establish clear and consistent policies that promote the transition to IPv6 A lack of awareness and education campaigns to inform users, IT professionals and decision makers about the benefits

and strategic importance of IPv6 was found. In addition, solid regulatory frameworks must be strengthened, including tax incentives, adoption requirements in public tenders, and regulations that promote compatibility between IPv4 and IPv6 systems; furthermore, that they can have cooperation between governments, service providers and technical organizations are essential to ensure a transition without borders, and based on the best practices and successful experiences, aligned with policies and regulations that promote the gradual transition towards new services and protocols being the challenges that must be addressed comprehensively.

Keywords

I*Pv6 addresses, IPv6 in South America; policies and strategies for the transition, Planning the transition to IPv6.*

Este capítulo es resultado del proyecto de investigación titulado "**MODELO DE TRANSICIÓN AL PROTOCOLO IPV6 PARA PYMES Y MIPYMES COLOMBIANAS APLICANDO MODELOS DE MACHINE LEARNING**" con código de aprobación del Comité de Investigaciones #PI0220231, proyecto financiado con una asignación de 21.000.000 millones Mcte, en la actualidad en fase de ejecución.

Institución financiadora: **Fundación Universitaria Compensar**

Introducción

La transición de las direcciones IPv4 a IPv6 ha surgido como una necesidad apremiante en el contexto actual, dado el crecimiento exponencial de dispositivos conectados a Internet; América del Sur (Pérez Macedo, E. C., 2018) es una región en constante desarrollo tecnológico (Suárez Sánchez, W. F. & Velásquez Cotrino, J. S., 2022) que se enfrenta en la actualidad al desafío de establecer políticas y estrategias efectivas para garantizar una conectividad sostenible y exitosa hacia Internet.

Los países de América deben incentivar y mejorar las estrategias para el proceso de transición que permitan establecer condiciones de colaboración, siendo una tarea de todos, donde se articule el sector público, la industria (Becerra Cobos, J. C., Simbaqueva Buitrago, J. R. & Valenzuela Suárez, A. F., 2013) y operadores de telecomunicaciones que respalden la fusión y concientización de todos los usuarios de Internet, dado que son necesidades en un futuro cercano para la aplicación de las TIC. Dada la naturaleza global de Internet, dicho proceso no puede abordarse exclusivamente desde la óptica local de cada país, sino que ha de realizarse desde la coordinación con organismos transnacionales (Pantoja Chuga, D. D. P., 2016).

Debido al crecimiento constante y evolución de los dispositivos conectados y la demanda creciente de servicios de Internet, la adopción de IPv6 será esencial para mantener la conectividad y permitir la innovación tecnológica en la región. Los antecedentes conceptuales e históricos del tema proporcionan un contexto temporal y espacial que justifica la relevancia y el enfoque del presente estudio, cuyo objetivo principal es revisar y destacar evidencias acerca de políticas y estrategias eficientes desarrolladas que faciliten la transición exitosa hacia IPv6 en América del Sur (Domínguez Ayala, J. C., 2017). Todo está respaldado en marcos regulatorios claros y consistentes, que promueven la conciencia y la educación sobre IPv6, pero debe incentivarse la colaboración entre los actores más relevantes para garantizar la interoperabilidad entre sistemas IPv4 e IPv6 para facilitar la transición mediante recomendaciones y políticas efectivas.

Por ello, la OECD fijó las directrices para el desarrollo de políticas públicas en este sentido, recomendando lo siguiente (Perset, K., 2010):

- Trabajar con el sector privado y otras partes interesadas para aumentar la educación y la concienciación y reducir los cuellos de botella.
- Demostrar el compromiso de los gobiernos locales hacia la adopción de IPv6.
- Buscar la cooperación internacional y el seguimiento de implementación de IPv6.

De manera reciente en la transición entre IPv4 e IPv6, la ITU-T y la Unión Europea comienzan a abrirse paso y a tener un rol más activo en los países que incentiven el proceso migratorio (Perset, K., 2010, *Internet Addressing: Measuring Deployment of IPv6*).

Así, se camina hacia políticas público-privadas de servicios tecnológicos como el Servicio de Resolución de Nombres (DNS), el de asignación dinámica de direcciones IP (DHCP), el del directorio activo, de servicios web, servidores de

monitoreo, servicio de correo electrónico (e-mail), de telefonía, de backups, de comunicaciones unificadas e integración entre los sistemas de información, entre otros servicios.

Finalmente, cabe destacar también la importancia de las políticas para las direcciones IPv6 establecidas por la LACNIC, como son: distribuciones de direcciones IPv6 a LIR o ISP con y sin distribuciones IPv4 previas; tamaño de distribución inicial y rectificación y de distribución subsiguiente; asignaciones por parte de los ISP, asignaciones directas a usuarios finales, microasignación en IPv6; registro de asignaciones; resolución inversa; poseedores de IPv6 ya existentes.

Por todo lo anterior, la investigación planteó la siguiente pregunta de investigación ¿cuáles son las políticas y estrategias óptimas para una transición exitosa hacia IPv6 en América del Sur, considerando los desafíos técnicos, operativos y políticos?

Metodología

El estudio se basó en la propuesta de Barbara Kitchenham (Kitchenham, B., Linkman, S. & Law, D., 1997) para realizar una revisión sistemática de la literatura existente sobre políticas y estrategias para la transición a IPv6 en América del Sur. Se ha adaptado para abordar de manera rigurosa los desafíos y recomendaciones específicos relacionados con la conectividad sostenible y exitosa en la región.

Se realizó una búsqueda exhaustiva de artículos científicos, informes técnicos, estudios de caso y otras fuentes relevantes que abordaran el tema de la transición a IPv6 en América del Sur. Se utilizaron bases de datos académicas y motores de búsqueda reconocidos para garantizar la inclusión de fuentes confiables y actualizadas, con criterios de selección para incluir o excluir los estudios identificados en la etapa de búsqueda. Se consideraron estudios que abordaran específicamente políticas y estrategias para la transición a IPv6 en América del Sur y que proporcionaran datos y análisis relevantes para los desafíos y recomendaciones planteados en este estudio, incluyendo información sobre políticas implementadas, estrategias adoptadas, desafíos identificados y resultados obtenidos. Estos datos se analizaron de manera sistemática para identificar patrones, tendencias y lecciones aprendidas en relación con la conectividad sostenible y exitosa en la transición.

Resultados

Para sintetizar los resultados por los países más representativos de la región, se definieron algunas variables específicas, como: políticas públicas, ventajas, estrategias para la transición, sectores de mayor aplicación, características, planes de acción, acciones focalizadas por los ISP, acciones focalizadas por el Gobierno, entre otros aspectos relevantes dentro del marco del estudio.

Argentina:

Tabla 4.1. Aspectos relevantes acordes a las políticas públicas en Argentina

Política pública	Ventajas	Estrategias de transición	Sectores de aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Resolución 1713/2018. Presidencia de Argentina (2018, 27 de marzo)	Fomenta la adopción de IPv6 en organismos y dependencias del Estado.	Establecimiento de grupos de trabajo y programas de capacitación.	Organismos gubernamentales, entidades públicas.	Promoción de la seguridad y escalabilidad de la red.	Desarrollo de planes de implementación. Fase de revisión.	Actualización de infraestructura y equipos para soportar IPv6.	Promoción y apoyo técnico en la adopción de IPv6 por parte de organismos estatales.
Programa Nacional IPv6. Dunayevich, J., Rocha, M. C., Absatz, M., Ramírez, G. & Parra, M. (2017)	Facilita la adopción de IPv6 en el sector público y privado.	Implementación de pilotos y proyectos de adopción.	Diversos sectores: gobierno, empresas, universidades.	Promoción de la innovación y competitividad.	Desarrollo de guías y manuales para la implementación.	olaboración con los ISP para garantizar el soporte de IPv6 en sus redes.	Promoción de la adopción de IPv6 en organismos estatales y empresas privadas.
Coalición IPv6 Argentina Sánchez, E., Gamarra, A., & Figueroa, D. A. (2023)	Promueve la adopción de IPv6 en diferentes sectores y organismos.	Realización de eventos, talleres y capacitaciones.	Gobierno, academia, empresas.	Colaboración y cooperación entre actores involucrados.	Impulso de iniciativas y proyectos piloto. Fases de revisión y planeación.	Promoción de la adopción de IPv6 en sus redes y servicios.	Fomento de la adopción de IPv6 en la sociedad y en diferentes sectores.

Política pública	Ventajas	Estrategias de transición	Sectores de aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Experiencia innovadora en el Estado argentino. Cicileo, G. & Rocha, M. (2014). Eijo, A. (2011)	Implementación de IPv6 en el ámbito estatal.	Planificación y desarrollo de proyectos piloto de IPv6.	Organismos gubernamentales, dependencias estatales.	Innovación en el ámbito público y experiencia práctica.	Establecimiento de estrategias y guías para la implementación. Fases de revisión, planeación y ejecución.	Adaptación de la infraestructura y equipamiento para soportar IPv6.	Promoción de la adopción de IPv6 en organismos y dependencias del Estado.
Documento "IPv6 para Todos". Cicileo, G., Gagliano, R., OíFlaherty, C., Olvera, C., Palet, J., Rocha, M. & Vives, A. (2009)	Proporciona orientación y recursos para la adopción.	Implementación de planes de transición.	Organismos gubernamentales, proveedores de servicios, empresas.	Inclusión de IPv6 en la agenda tecnológica.	Desarrollo de guías y recomendaciones para la adopción. Fases de revisión, planeación y ejecución.	Incentivos y soporte técnico para los proveedores de servicios en la implementación.	Promoción de la adopción de IPv6 en todos los sectores y niveles.
Publicación de LACNIC sobre IPv6. Acosta, A., Aggio, S. et al. (2014)	Brinda información y orientación para operadores de red.	Implementación de IPv6 en redes y servicios.	Proveedores de servicios, operadores de red.	Mejora en la escalabilidad y crecimiento de la red.	Desarrollo de planes de implementación y migración.	Soporte y capacitación para los operadores de red en la adopción de IPv6.	Promoción de la adopción de IPv6 en las redes y servicios de los proveedores.

Perú:

Tabla 4.2. Aspectos relevantes acordes a las políticas públicas de Perú

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Plan de Transición a IPv6 de la Superintendencia Nacional de Aduanas y de Administración Tributaria. Laurente, I. (2021)	Modernización y mejora de los servicios aduaneros y tributarios.	Migración gradual a IPv6 según fases establecidas.	Sector aduanero y tributario.	Aseguramiento de la disponibilidad y continuidad de servicios.	Implementación de proyectos piloto y pruebas de concepto.	Coordinación con ISP para la transición.	Promoción y seguimiento de la implementación de IPv6 en los sistemas aduaneros.
Plan de Transición del Protocolo IPv4 a IPv6 enn las Entidades Públicas del Perú. Tomy Baltazar, M. A. (2017)	Impulso a la adopción de IPv6 en entidades públicas.	Implementación gradual y progresiva de IPv6 en etapas definidas.	Sector público, entidades gubernamentales.	Mayor seguridad y escalabilidad de la red.	Desarrollo de guías y manuales para la implementación. Fases de revisión, planeación y ejecución.	Colaboración con ISP para garantizar el soporte de IPv6 en sus redes.	Promoción y seguimiento de la adopción de IPv6 en las entidades públicas.
Resolución Ministerial N.¡ 281-2018-EF/44. Presidencia de Perú (2018, 10 de agosto)	Impulsa la adopción de IPv6 en las entidades del Gobierno Nacional.	Implementación progresiva de IPv6 en el ámbito gubernamental.	Sector público, entidades del Gobierno Nacional.	Mayor seguridad y disponibilidad de los servicios.	Desarrollo de un plan de implementación y transición.	oordinación con ISP para asegurar la compatibilidad.	Promoción y seguimiento de la adopción de IPv6 en las entidades del Gobierno Nacional.

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Decreto Supremo N.¡ 081-2017-PCM. Presidencia de Perú (2017, 9 de agosto)	Establece la formulación de un plan de transición a IPv6.	Desarrollo de un plan de transición a IPv6 a nivel nacional.	Todos los sectores y entidades del Gobierno.	Promoción de la adopción de IPv6 en el ámbito nacional.	Implementación de programas de capacitación y concientización.	Establecimiento de directrices para la implementación de IPv6 por parte de los ISP.	Coordinación y seguimiento de la transición a IPv6.
Realidad del IPv6 en el Perú. Ruiz, P. C. (2016)	Mayor disponibilidad de IP y crecimiento de la conectividad.	Promoción de la adopción de IPv6 por parte de los proveedores de servicios.	ISP, empresas.	Aseguramiento de la escalabilidad y la seguridad de la red.	Actualización de la infraestructura de red para soportar.	Adopción de IPv6 en los servicios y sistemas de los ISP.	Promoción y concientización sobre IPv6 en el ámbito empresarial y de los ISP.
Plan de Transición al Protocolo IPv6 en las Entidades de la Administración Pública. Baltazar, M. A. T. (2017)	Promueve la adopción de IPv6 en las entidades de la administración.	Establecimiento de cronogramas y metas para la transición.	Entidades públicas.	Mayor seguridad y escalabilidad de la red.	Desarrollo de guías y lineamientos. Fases de revisión, planeación y ejecución.	Coordinación con los ISP para garantizar el soporte de IPv6 en sus redes.	Promoción y monitoreo de la implementación de IPv6 en las entidades de la administración.

Brasil:

Tabla 4.3. Aspectos relevantes acordes a las políticas públicas de Brasil

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Brasil se adelanta en la transición a IPv6. Escalante Rendón, J. I. (2005). Coan, A. L. (2020).	Mayor disponibilidad de direcciones IP.	Promoción y adopción de IPv6 en diversos sectores.	Todos los sectores de la economía.	Mejora la escalabilidad y seguridad de la red.	Desarrollo de programas y proyectos para la implementación de IPv6.	Fomento de la actualización de redes y sistemas por parte de los ISP.	Implementación de políticas y normativas para impulsar la transición por parte del Gobierno.
Instituciones brasileñas avanzan en el proceso de implementación de IPv6. Brito, S. H. B. (2018)	Mejora de la conectividad y la interoperabilidad.	Migración gradual yplanificada a IPv6.	Instituciones académicas y de investigación.	Incremento en el tamaño de las direcciones IP y la capacidad de la red.	Desarrollo de proyectos piloto y pruebas de concepto.	Colaboración con los ISP para garantizar el soporte de IPv6.	Establecimiento de políticas y directrices para la implementación por parte del Gobierno.
Protocolo IPv6 compilha dupla em um campus universitário (Barreto, 2015)	Aumento de direcciones IP disponibles.	Implementación de una pila dual IPv4/ IPv6 en el campus universitario.	Educación superior, instituciones académicas.	Mayor escalabilidad y seguridad de la red.	Configuración y despliegue de equipos y servicios IPv6. Fases de revisión, planeación y ejecución.	Aseguramiento de la compatibilidad de los ISP con IPv6.	Apoyo ypromoción de la implementación de IPv6 por partedel Gobierno en instituciones académicas.
Implanta ‹o e análise do protocolo IPv6 com foco na mobilidade (Carvalho, 2015)	Mejora de la movilidad y conectividad en redes.	Implementación y análisis del protocolo IPv6 con enfoque en la movilidad.	Varios sectores, en particular aquellos con requisitos de movilidad.	Soporte mejorado para la movilidad de dispositivos y conexiones.	Diseño y configuración de redes IPv6 con enfoque en la movilidad. Fases de revisión, planeación y ejecución.	Colaboración con los ISP para garantizar la compatibilidad de IPv6.	Fomento de la adopción de IPv6 en el ámbito de la movilidad.

Chile:

Tabla 4.4. Aspectos relevantes acordes a las políticas públicas de Chile

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Estrategias de Adopción de IPv6 en Chile. Alarcón Reyes, R. A. (2010)	Mayor disponibilidad de direcciones IP.	Fomento de la adopción y migración a IPv6	Todos los sectores de la economía y la sociedad.	Ampliación del espacio de direcciones IP.	Desarrollo de programas y proyectos para la implementación de IPv6. Fases de revisión.	Fomento de la implementación de IPv6 por parte de los ISP en sus servicios.	Establecimiento de políticas y directrices para la implementación por parte del Gobierno.
Informe sobre IPv6 en Chile. çlvarez Moraga, S. A. & González Valenzuela, A. J. (2005)	Mejora de la escalabilidad y seguridad de la red.	Promoción y adopción de IPv6 en diversos sectores.	Todos los sectores de la economía y la sociedad.	Aumento en el tamaño del espacio de direcciones IP.	Desarrollo de planes de acción para la implementación. Fases de revisión y planeación.	Colaboración con ISP para garantizar la compatibilidad de IPv6.	Impulso y apoyo gubernamental a la transición y adopción de IPv6.
Simulación y emulación de la red universitaria nacional (REUNA) de Chile. Cobos Panduro, (2018). Loor Cárdenas, L. E. & Heinrich, J. P. G. (2022)	Mayor conectividad y capacidad de la red universitaria.	Simulación y emulación de la red universitaria nacional (REUNA).	Instituciones académicas y de investigación.	Mejora de la conectividad y capacidad de la red.	Implementación de planes y proyectos para la mejora de la red universitaria. Fases de revisión, planeación y ejecución.	Participación de los ISP en el soporte y despliegue.	Apoyo y promoción gubernamental para la adopción de IPv6 en las instituciones académicas.

Colombia:

Tabla 4.5. Aspectos relevantes acordes a las políticas públicas de Colombia

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
G20: Transición de IPv4 a IPv6. MinTIC (2017)	Mayor disponibilidad de direcciones IP.	Promoción y apoyo a la adopción de IPv6 en Colombia.	Todos los sectores de la economía y la sociedad colombiana.	Ampliación del espacio de direcciones IP.	Desarrollo de programas y proyectos para la implementación de IPv6. Fases de revisión, planeación y ejecución.	Colaboración con los ISP para garantizar el soporte de IPv6.	G20: Transición de IPv4 a IPv6 (MinTIC).
Guía 1 de Transición IPv4 a IPv6. MinTIC (2021, febrero)	Mejora de la escalabilidad y seguridad de la red.	Definición de estrategias para la transición de IPv4 a IPv6 en Colombia.	Todos los sectores de la economía y la sociedad colombiana.	Aumento en el tamaño del espacio de direcciones IP.	Desarrollo de planes de acción para la implementación de IPv6. Fases de revisión, planeación y ejecución.	Fomento de la implementación de IPv6 por parte de los ISP en sus servicios.	Planes estratégicos en sectores de la economía.
Colombia aplaza a 2022 el fin de la transición a IPv6. MinTIC (2021, febrero)	Mejora de la escalabilidad y seguridad de la red.	Extensión del plazo para completar la transición a IPv6 en Colombia.	Todos los sectores de la economía y la sociedad colombiana.	Incremento en el tamaño del espacio de direcciones IP.	Continuación de las acciones de transición a IPv6 según los planes establecidos. Fases de revisión, planeación y ejecución.	Colaboración con proveedores de servicios para garantizar la compatibilidad de IPv6.	Planes estratégicos en sectores público-privados.

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Implementación de IPv6 en RENATA. Suárez, J., Salcedo, M., Carmona, C., Ramírez, J. & Serna, G. (2016)	Mejora de la conectividad y capacidad de la red académica.	Implementación de IPv6 en la red académica colombiana a través de RENATA.	Instituciones académicas y de investigación en Colombia.	Mejora de la conectividad y capacidad de la red.	Desarrollo de planes y proyectos para la adopción de IPv6 en RENATA.	Participación de los ISP en el soporte y despliegue de IPv6.	Planes estratégicos en sectores académicos público-privados.
Plan de Implementación IPv6. Benítez, I. P. S., Méndez, G. A., Salazar, N. M. A., Burbano, D. C. & Guirales, C. I. U. (2009). Atuesta Castillo, G. M. & Ramírez Aristizábal, W. D. J. (2021)	Mayor disponibilidad de direcciones IP y mejor conectividad.	Implementación de IPv6 en diversos sectores de la economía.	Sector educativo y empresarial.	Incremento en el tamaño del espacio de direcciones IP y mejora de la conectividad.	Desarrollo de planes y proyectos para la adopción de IPv6.	Soporte y colaboración de los ISP para garantizar la compatibilidad de IPv6.	Plan de implementación IPv6 (sector universitario y empresarial).

Ecuador:

Tabla 4.6. Aspectos relevantes acordes a las políticas públicas de Ecuador

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Fortalecimiento del protocolo IPv6 en Ecuador. Aguirre Villarroel, V. T. (2023). Pantoja Chuga, D. D. P. (2016)	Mayor disponibilidad de direcciones IP.	Fortalecimiento y promoción del protocolo IPv6.	Todos los sectores de la economía y la sociedad.	Ampliación del espacio de direcciones IP.	Desarrollo de programas y proyectos para la implementación. Fases de revisión, planeación y ejecución.	Colaboración con los ISP para garantizar el soporte de IPv6.	Establecimiento de políticas y directrices hacia un Ecuador conectado innovador, competitivo y seguro.
Adelanto con protocolo IPv6 para instituciones públicas. MinTEL Ecuador (2012)	Mejora de la escalabilidad y seguridad de la red.	Adelanto en la implementación de IPv6 en instituciones públicas.	Instituciones públicas.	Incremento en el tamaño del espacio de direcciones IP.	Desarrollo de planes y proyectos para la adopción en las instituciones públicas. Fases de revisión, planeación y ejecución.	Participación de los ISP en el soporte y despliegue.	Apoyo y promoción gubernamental para la adopción.
Planificación de procesos para la migración de IPv4 a IPv6. Santamaría Alamar, A. P. (2014)	Mayor conectividad y capacidad de la red.	Planificación de procesos para la migración de IPv4 a IPv6.	Todos los sectores de la economía y la sociedad.	Mejora de la conectividad y capacidad de la red.	Implementación de planes y proyectos para la adopción.	Participación de los ISP en el soporte y despliegue.	Apoyo y promoción para la adopción.
Plan de Transición IPv6 en el país. Rodríguez Amaguay, X. D. & Tejada Zúñiga, C. E. (2018)	Mejora de la escalabilidad y seguridad de la red.	Desarrollo de un plan de transición a IPv6.	Sector educativo y empresarial.	Incremento en el tamaño del espacio de direcciones IP.	Implementación de planes y proyectos para la adopción de IPv6 en todo el país.	Soporte y colaboración de los ISP para garantizar la compatibilidad de IPv6.	Apoyo y promoción gubernamental para la adopción de IPv6 en todos los sectores de telecomunicaciones.

Uruguay:

Tabla 4.7. Aspectos relevantes acordes a las políticas públicas de Uruguay

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Plan de implementación de IPv6 en Uruguay. Pensky Markowicz, G. (2021)	Mayor disponibilidad de direcciones IP para todos los sectores.	Implementación de IPv6 sobre infraestructuras híbridas.	Todos los sectores de la economía y la sociedad uruguaya.	Ampliación del espacio de direcciones IP.	Desarrollo de programas y proyectos para la implementación de IPv6.	Colaboración con los ISP para garantizar el soporte de IPv6 bajo soluciones de los diferentes partners.	Establecimiento de políticas y directrices para la transición por parte del Gobierno.
Estudio y evaluación de la implementación de IPv6. Alarcón Reyes, R. A. (2010)	Mejora de la escalabilidad y seguridad de la red entre conexiones PPP.	Estudio y evaluación de la implementación de IPv6.	Todos los sectores de la economía y la	Incremento en el tamaño del espacio de direcciones IP. sociedad uruguaya.	Desarrollo de planes y proyectos para la adopción. Fases de revisión, planeación y ejecución.	Participación de los ISP en el soporte y despliegue de IPv6. Fases de planeación y ejecución.	Apoyo y promoción gubernamental para la adopción de IPv6.
Estrategias de implementación de IPv6. Kiedanski, D. & Grampín, E. (2017)	Mejora de la interoperabilidad y la seguridad en las comunicaciones sobre redes heterogéneas.	Implementación de estrategias específicas para la transición a IPv6.	Todos los sectores de la economía y en redes empresariales.	Aumento en la capacidad de direccionamiento de la red.	Desarrollo de planes y proyectos para la adopción de IPv6.	Colaboración y coordinación con los ISP para garantizar la compatibilidad y el soporte. Fases de revisión y planeación.	Apoyo y promoción a redes corporativas.

Venezuela:

Tabla 4.8. Aspectos relevantes acordes a las políticas públicas de Venezuela

Políticas públicas	Ventajas	Estrategias para la transición	Sectores de mayor aplicación	Características	Planes de acción	Acciones de los ISP	Acciones del Gobierno
Implementación de IPv6 en Venezuela. Gamess, E. & Morales, N. (2007)	Mayor disponibilidad de direcciones IP.	Requiere inversión en infraestructura y capacitación.	Implementación de IPv6 empresarial del sector público.	Todos los sectores de la economía y la sociedad.	Ampliación del espacio de direcciones IP. Fases de revisión y planeación.	Desarrollo de programas y proyectos para la implementación de IPv6.	Colaboración con los ISP para garantizar el soporte de IPv6.
Migración al protocolo IPv6. Quevedo, J. (2020)	Mejora de la escalabilidad y seguridad de la red.	Requiere ajustes y actualizaciones en la infraestructura.	Migración al protocolo IPv6 en Venezuela basados en empresas híbridas.	Todos los sectores de la economía y la sociedad.	Incremento en el tamaño del espacio de direcciones IP. Fases de revisión, planeación y ejecución.	Desarrollo de planes y proyectos para la adopción de IPv6.	Participación de los ISP en el soporte y despliegue de IPv6. Un caso de estudio.

Discusión

Tabla 4.9. Aspectos relevantes acordes a las políticas públicas para el mundo

País	Políticas públicas	Estrategias para la transición	Características	Acciones de los ISP
Argentina Mercado, G. et al. (2015)	Política Nacional de IPv6	Planificación y migración gradual a IPv6.	Ampliación del espacio de direcciones IP y mejoras en sistemas de transporte masivos de datos.	Apoyo técnico y capacitación para la implementación de IPv6.
Brasil De Oliveira, G. D. & Violín, R. D. O. (2021). Yandra, B. F. F. (2019)	Plan Nacional de Implementación IPv6	Definición e implementación de políticas y estrategias para la transición.	Ampliación del espacio de direcciones IP y mejoras en el enrutamiento.	Incentivos y apoyo técnico para la adopción de IPv6.
Chile Loor Cárdenas, L. E. & Heinrich, J. P. G. (2022)	Estrategia Nacional de IPv6	Promoción de políticas y programas para la adopción de IPv6.	Ampliación del espacio de direcciones IP y mejoras en la seguridad informática.	Capacitación y soporte técnico para la implementación de IPv6.
Colombia MinTIC (2017)	Política Nacional de Tecnologías de la Información y las Comunicaciones	Definición e implementación de políticas y estrategias para la transición.	Ampliación del espacio de direcciones IP y mejoras en el tráfico sobre IPV6.	Actualización y adaptación de las infraestructuras de red.

País	Políticas públicas	Estrategias para la transición	Características	Acciones de los ISP
Ecuador Aguirre Villarroel, V. T. (2023). MinTEL Ecuador (2012). Pantoja Chuga, D. D. P. (2016)	Estrategia Nacional de IPv6	Planificación y migración gradual de IPv4 a IPv6.	Ampliación del espacio de direcciones IP y mejoras en soluciones públicas.	Soporte y capacitación por parte de los ISP.
Uruguay Pensky Markowicz, G. (2021). Kiedanski, D. & Grampín, E. (2017)	Plan Nacional de IPv6	Definición e implementación de políticas y estrategias para la transición.	Ampliación del espacio de direcciones IP y mejoras en redes heterogéneas.	Incentivos y apoyo técnico para la adopción de IPv6 en sector público y privado.
Venezuela Gamess, E. & Morales, N. (2007)	Política Nacional de Telecomunicaciones	Definición e implementación de políticas y estrategias para la transición.	Ampliación del espacio de direcciones IP y mejoras en redes de nueva generación.	Soporte y capacitación por parte de los ISP y sectores económicos.
Bolivia Roca Marín, R. D. (2011). Chui, Salas, A. C. (2022)	Estrategia Nacional de Telecomunicaciones	Definición e implementación de políticas y estrategias para la transición.	Ampliación del espacio de direcciones IP y mejoras en redes de banda ancha.	Apoyo técnico y capacitación para la implementación de IPv6 en todos los sectores.
Perú Baltazar, M. A. T. (2017)	Plan de Transición del Protocolo IPv4 al IPv6 en las Entidades de la Administración pública	Todos los sectores de la economía y la sociedad.	Desarrollo de planes de acción y programas de capacitación.	Establecimiento de marcos regulatorios y políticas de promoción en redes avanzadas.
Paraguay	Plan Nacional de Migración IPv6	Todos los sectores de la economía y la sociedad.	Apoyo técnico y capacitación para la implementación de IPv6.	Establecimiento de legislación nacional articulados con privados.

Finalmente, los países de América del Sur han reconocido la importancia de la transición a IPv6 y han implementado políticas públicas para fomentar su adopción. Brasil, Argentina, Perú y Colombia se destacan por su enfoque proactivo en la implementación de políticas y regulaciones, promoviendo la capacitación, la concientización y la colaboración entre los sectores público y privado. Estas políticas públicas son fundamentales para impulsar la transición a IPv6 en la región y garantizar una conectividad sostenible y exitosa en el futuro.

Es fundamental hacer un análisis de la discusión de manera global y cómo es abordada mediante diversas políticas y estrategias que buscan facilitar una migración suave y eficiente desde IPv4. Sin embargo, también se han identificado desafíos y obstáculos que requieren enfoques estratégicos para garantizar el éxito de esta transición. A continuación, se presenta una contrastación de las políticas y estrategias para la transición a IPv6:

1. Políticas y estrategias favorables:

Políticas gubernamentales y regulatorias: muchos gobiernos han implementado políticas que fomentan la adopción de IPv6. Estas incluyen requisitos para servicios gubernamentales, incentivos fiscales y la promoción de la adopción voluntaria por parte de las empresas.

Participación de la industria: la colaboración entre actores clave de la industria, como proveedores de servicios de Internet (ISP), fabricantes de equipos de red y organizaciones de estándares, ha llevado al desarrollo de estrategias concertadas para la transición a IPv6. Esto incluye el establecimiento de plazos y la creación de incentivos para impulsar la implementación.

Educación y concientización: estrategias que buscan educar y concientizar a los profesionales de TI, a las empresas y al público en general sobre la importancia de IPv6 son fundamentales. Programas de capacitación, campañas de divulgación y eventos educativos contribuyen a aumentar la comprensión y la aceptación de IPv6.

2. Desafíos y estrategias de mitigación:

Inversión y costos asociados: la transición a IPv6 conlleva costos, desde la actualización de equipos hasta la capacitación de personal. Estrategias que abordan estos costos incluyen la provisión de incentivos fiscales, subsidios y la identificación de modelos de negocio que promueven la implementación de IPv6.

Coexistencia IPv4 e IPv6: estrategias que permiten la coexistencia de IPv4 e IPv6 son cruciales para garantizar una transición sin interrupciones. Mecanismos como la doble pila (dual-stack), túneles y traducción de direcciones facilitan la interoperabilidad durante la fase de transición.

Gestión de riesgos de seguridad: estrategias que abordan los riesgos de seguridad durante la transición incluyen la implementación de tecnologías como IPSec, la monitorización continua de amenazas y la promoción de mejores prácticas de seguridad para garantizar una transición segura.

3. Estrategias innovadoras:

IPv6 por defecto: algunas políticas buscan establecer IPv6 como la opción predeterminada en lugar de IPv4. Esta estrategia impulsa a los proveedores de servicios y a las empresas a adoptar IPv6 como estándar, acelerando así la transición.

Incentivos para contenidos IPv6: al incentivar la creación y el despliegue de contenidos compatibles con IPv6, se estimula la demanda de servicios basados en esta tecnología, lo que a su vez impulsa la adopción de IPv6 por parte de los proveedores de servicios.

Colaboración internacional: la cooperación entre países y regiones facilita la armonización de políticas y la resolución de desafíos comunes. Estrategias que promueven la colaboración internacional contribuyen a un despliegue global más coherente de IPv6.

Finalmente, las políticas y estrategias para la transición a IPv6 abarcan desde enfoques regulatorios hasta estrategias técnicas y educativas. La clave reside en un enfoque holístico que involucre a múltiples partes interesadas y aborde los desafíos tanto desde el punto de vista técnico como económico.

Conclusiones

Finalmente, los países de América del Sur han reconocido la importancia de la transición a IPv6 y han implementado políticas públicas para fomentar su uso.

Las políticas públicas desempeñan un papel fundamental en la promoción y adopción de IPv6. Es esencial que los gobiernos de la región establezcan marcos regulatorios adecuados, fomenten la capacitación y concientización y promuevan la colaboración entre los sectores público y privado para impulsar la transición. Entre las ventajas de las políticas para IPv6 se encuentran la

ampliación del espacio de direcciones IP, la mejora en la escalabilidad y enrutamiento de la red y el impulso a la innovación y nuevos servicios digitales en diversos sectores, como la salud, educación, gobierno, industria y comercio.

Sin embargo, la transición a IPv6 presenta desafíos, como la necesidad de inversiones en infraestructura y actualización de equipos, la compatibilidad con sistemas y aplicaciones heredadas, así como la capacitación de personal técnico; por ello, para lograr una transición exitosa, es fundamental implementar estrategias adecuadas que incluyan la planificación y definición de objetivos claros, la identificación de los sectores de mayor aplicación y su involucramiento activo, el desarrollo de planes de acción detallados y el establecimiento de acciones focalizadas por parte de los ISP y el Gobierno.

La cooperación y colaboración regional son aspectos fundamentales para la transición a IPv6 sin fronteras en América del Sur. Los países de la región deben intercambiar buenas prácticas, compartir experiencias y promover la colaboración en proyectos conjuntos para impulsar la adopción y el despliegue de IPv6. Los gobiernos han reconocido la importancia de la transición y han implementado diversas políticas y regulaciones para impulsarla.

Brasil ha sido líder en la implementación de políticas públicas para fomentar la adopción de IPv6. A través de iniciativas de capacitación y concientización, se han establecido plazos para la adopción de IPv6 en los servicios gubernamentales y promovido la colaboración entre los sectores público y privado.

Argentina también ha adoptado políticas públicas para impulsar la transición a IPv6 y la publicación de resoluciones y guías técnicas ha promovido la adopción de IPv6 en diferentes sectores y ha fomentado la colaboración entre actores clave, a nivel de los ISP en las redes de transporte.

En Perú, se ha avanzado en la implementación de políticas públicas para la transición a IPv6 con el objetivo de promover la adopción de IPv6 en las instituciones públicas y fomentar la colaboración con los proveedores de servicios de Internet, que permitan la actualización de tecnología vía redes ópticas.

En Colombia, se han implementado políticas públicas para la transición a IPv6. A través de resoluciones y guías técnicas, el Gobierno, a través de MinTIC y Renata, ha promovido la adopción de IPv6 en el sector público y ha establecido plazos para su implementación.

En Chile, se ha trabajado en la promoción de IPv6 a través de iniciativas como la implementación de planes de acción y la participación en proyectos regionales e internacionales. Sin embargo, es necesario un mayor impulso en su adopción, especialmente en los sectores gubernamentales y empresariales, que se articulen con los ISP, que poco impulsan la transición.

Ecuador ha realizado esfuerzos significativos para fortalecer el protocolo IPv6. Se han implementado políticas y acciones focalizadas por el Gobierno, así como estrategias de transición y planes de acción para fomentar su adopción. Sin embargo, aún existen desafíos en términos de concientización y capacitación. Uruguay ha demostrado un compromiso con la adopción de IPv6, promoviendo su implementación en diferentes sectores. El país ha desarrollado planes de acción y estrategias para la transición, involucrando tanto a los ISP como al Gobierno en la promoción de IPv6. Aunque se han logrado avances, se requiere un mayor impulso para su adopción generalizada.

Venezuela ha tomado medidas para fortalecer el protocolo IPv6, como la implementación de políticas públicas y la participación en proyectos de investigación. Sin embargo, la adopción de IPv6 en el país aún enfrenta desafíos significativos debido a limitaciones técnicas, de infraestructura y dados los problemas económicos que dificultan la transición.

Paraguay ha mostrado un compromiso con la adopción de IPv6, estableciendo planes de acción y promoviendo la concientización en diferentes sectores. Aunque se han logrado avances, es necesario continuar promoviendo la capacitación y la colaboración entre los actores clave para una adopción más amplia.

Bolivia carece de una política pública claramente definida, pero los operadores locales fortalecen su infraestructura hacia mantener competitivos los servicios telemáticos, articulados en planes de acción y la participación en proyectos regionales.

Finalmente, la adopción de IPv6 es estratégica para cada país, dados los planes de sus agendas y gobernanzas digitales según su propio contexto y desafíos específicos en relación con la transición. Aunque algunos países han avanzado más que otros, todos comparten que el objetivo común de garantizar una conectividad sostenible y exitosa en la región a través de la adopción de IPv6 es y será clave. La colaboración y el intercambio de experiencias entre los países pueden ser fundamentales para superar los desafíos restantes y lograr una implementación exitosa de IPv6 en toda América del Sur.

Referencias bibliográficas

Acosta, A., Aggio, S., Cicileo, G., Lynch, T., Moreiras, A., Rocha, M. ... & Berenguer, S. S. (2014). *IPv6 para operadores de red*. Buenos Aires.

Aguirre Villarroel, V. T. (2023). *Diagnóstico y perspectivas de la implementación de IPv6 en el Ecuador* (Bachelor's thesis, Quito: EPN, 2023).

Alarcón Reyes, R. A. (2010). *Estrategia para abordar el proceso de adopción de IPv6 en redes empresariales*.

Albornoz, N., Espina, L. & Flores, R. (2009). *Migración al protocolo IPv6 en Venezuela*. Universidad Rafael Belloso Chacín.

Álvarez Moraga, S. A. & González Valenzuela, A. J. (2005). "Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica". *WDM. Revista Facultad de Ingeniería-Universidad de Tarapacá*, 13(3), 104-113.

Argentina, Presidencia (2018, 27 de marzo). Resolución 4 del 2018. Ministerio de Modernización. Secretaría de Tecnologías de la Información y las Comunicaciones. https://ipv6.ar/nosotros/resolucion

Atuesta Castillo, G. M. & Ramírez Aristizábal, W. D. J. (2021). *Plan de adopción del protocolo IPv4 a IPv6 para el sector microempresario de la ciudad de Bogotá*.

Baltazar, M. A. T. (2017). *Modelo de referencia de transición de IPv4 a IPv6 para el sector Gobierno de Perú*. Pontificia Universidad Católica del Perú.

Barreto, F. (2015). "Protocolo IPv6 com pilha dupla em um campus universitário". *Revista Brasileira de Computação Aplicada*, 7(3), 2-16.

Becerra Cobos, J. C., Simbaqueva Buitrago, J. R. & Valenzuela Suárez, A. F. (2013). *Diseño e implementación de redes IPv6 en mipymes: caso laboratorio de informática*. https://repositorio.escuelaing.edu.co/handle/001/222

Benítez, I. P. S., Méndez, G. A., Salazar, N. M. A., Burbano, D. C. & Guirales, C. I. U. (2009). "Análisis comparativo de los protocolos IPV6 e IPV4". *Ingeniería Solidaria*, 5(9), 42-53.

Brito, S. H. B. (2018). *IPv6-O novo protocolo da Internet*. Novatec Editora.

Carvalho, D. D. P. D. (2015). *Implantação e análise do protocolo IPv6 com foco na mobilidade*.

Chui, Salas, A. C. (2022) *Modelo de migración de red IPv4 al protocolo IPv6 para redes empresariales* (Doctoral dissertation).

Cicileo, G. & Rocha, M. (2014). *Evolución de la red de interconexión universitaria de Argentina*.

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera, C., Palet, J., Rocha, M. & Vives, A. (2009). *IPv6 para Todos. Guía de uso y aplicación para diversos entornos*. Internet Society.

Coan, A. L. (2020). "Implementação do protocolo IPv6 com segurança: Uma análise sobre os desafios e riscos para os administradores de redes internet". *Revista Brasileira em Tecnologia da Informação*, 2(1), 03-16.

Cobos Panduro, V. R. (2018). *Simulación y emulación de la red universitaria nacional (REUNA) de Chile y el nivel de comprensión del funcionamiento de redes avanzadas*.

De Oliveira, G. D. & Violín, R. D. O. (2021, December). "Transição do protocolo IPv4 para IPv6: as dificuldades em alcançar o futuro da internet". In Congresso de Tecnologia-Fatec Mococa (Vol. 5, No. 2).

Domínguez Ayala, J. C. (2017). *Diseño e implementación de un prototipo de transición de direccionamiento IPv4 a IPv6 en la red de la Universidad Politécnica Salesiana sede Quito* (Master's thesis, PUCE). http://repositorio.puce.edu.ec/handle/22000/13493

Dunayevich, J., Rocha, M. C., Absatz, M., Ramírez, G. & Parra, M. (2017). *El desarrollo de RANA (Red Anycast de NIC Argentina): un caso de éxito en la colaboración entre múltiples partes interesadas para proyectos de infraestructura crítica*.

Eijo, A. (2011). "IPv6: una experiencia innovadora en el Estado". In V Simposio de Informática en el Estado (SIE 2011) (XL JAIIO, Córdoba, 29 de agosto al 2 de septiembre de 2011).

Escalante Rendón, J. I. (2005). *Guía de implementación de redes utilizando el protocolo IPv6*.

Gamess, E. & Morales, N. (2007, October)." Implementing IPv6 at Central University of Venezuela". In Proceedings of the 4th International IFIP/ACM Latin American Conference on Networking (pp. 43-51).

Henao Mendoza, J. N. & Tijaro Sierra, F. A. (2021). *Guía práctica de migración del protocolo IPv4 a IPv6*.

Kiedanski, D. & Grampín, E. (2017, October). "Understanding Latin America IPv6 connectivity: A preliminary exploration". In 2017 36th International Conference of the Chilean Computer Science Society (SCCC) (pp. 1-6). IEEE.

Kitchenham, B., Linkman, S. & Law, D. (1997). "DESMET: a methodology for evaluating software engineering methods and tools". *Computing & Control Engineering Journal*, 8(3), 120-126.

Laurente, I. (2021). "Normativa, agenda digital y política de transformación digital: hacia un gobierno digital peruano". *Revista Latinoamericana de Economía y Sociedad Digital*, 2(2), 1-25.

Loor Cárdenas, L. E. & Heinrich, J. P. G. (2022). *Estudio de aplicación de Machine Learning y Blockchain para seguridad IPv6* (Doctoral dissertation).

Mercado, G., Gitto, J., Soria, R., Taffernaberry, J. C., Pérez Monte, C., Orbiscay, M. ... & Diedrichs, A. (2015). "Diseño e implementación de red académica experimental aplicando IPv6". In XXI Congreso Argentino de Ciencias de la Computación (2015).

MinTEL Ecuador (2012). Acuerdo N.° 007-2012 Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://www.telecomunicaciones.gob.ec/wp- content/uploads/downloads/2012/10/Acuerdo-No.-007-2012.pdf

MinTIC (2017, 15 de junio). *Guía 20 de Transición de IPv4 a IPv6 para Colombia*. https://www.mintic.gov.co/gestionti/615/articles- 5482_G20_Transicion_IPv4_IPv6.pdf

MinTIC (2021, febrero). *Guía 1 de Transición de IPv4 a IPv6 para Colombia*. https://www.mintic.gov.co/portal/715/articles- 162301_guia_transicion_ipv4_ipv6.pdf

Pantoja Chuga, D. D. P. (2016). *Planificación de procesos para la migración del protocolo IPv4 a IPv6 para la continuidad del servicio en los ISP* (Master's thesis, PUCE).

Pensky Markowicz, G. (2021). *Implementación de IPv6: ¿un desafío de innovación para los ISP en Uruguay?*

Pérez Macedo, E. C. (2018). *Sistema de gestión para la transición de IPv4 a IPv6 en el gobierno regional de Ancash*.

Perset, K. (2010). *Internet Addressing: Measuring Deployment of IPv6*.

Perú, Presidencia (2017, 9 de agosto). Decreto Supremo N.° 081-2017-PCM. Presidencia del Consejo de Ministros.

https://www.gob.pe/institucion/pcm/normas-legales/292347-081-2017-pcm

Perú, Presidencia. (2018, 10 de agosto). Resolución Ministerial N.° 281-2018-EF/44. Ministerio de Economía y Finanzas. https://www.gob.pe/institucion/mef/normas-legales/199248-281-2018-ef-44

Quevedo, J. (2020). *Diseño de una red IPv6 para la Universidad Nueva Esparta. Caso de estudio* (Doctoral dissertation).

Roca Marín, R. D. (2011). *Propuesta de estrategia nacional para la implementación de IPv6 en Bolivia* (Doctoral dissertation).

Rodríguez Amaguay, X. D. & Tejada Zúñiga, C. E. (2018). *Elaborar un plan de acción para la implementación de IPv6 en el Ecuador y fomentar su uso* (Bachelor's thesis, Espol).

Ruiz, P. C. (2016). "Implementación de la Red Dorsal Nacional de Fibra Óptica en el Perú". *Electrónica-UNMSM*, 19(1), 3-7.

Sánchez, E., Gamarra, A. & Figueroa, D. A. (2023). "Implementación del protocolo IPv6 en la región y su impacto en los usuarios finales". *ReTEC-Revista Electrónica de Tecnología, Educación y Ciencia*, 1(1).

Santamaría Alamar, A. P. (2014). *Análisis, diseño e implementación de una red prototipo utilizando el protocolo IPv6 y QoS para la empresa Santanet* (Bachelor's thesis).

Suárez Sánchez, W. F. & Velásquez Cotrino, J. S. (2022). *Propuesta de guía para la transición de IPv4 a IPv6 a la empresa ACT Telemática*. https://repository.ucc.edu.co/items/53b9a9f5-9931-4fd4-b8cc- c08a75797889

Suárez, J., Salcedo, M., Carmona, C., Ramírez, J. & Serna, G. (2016). "Effects of IPv6-IPv4 tunnel in jitter of voice over IPv6, measured in laboratory and over the national research and education network of Colombia «RENATA»". *IEEE Latin America Transactions*, 14(3), 1380-1386.

Tomy Baltazar, M. A. (2017). *Modelo de referencia de transición de IPv4 a IPv6 para el sector gobierno de Perú*.

Yandra, B. F. F. (2019). "A responsabilidade do provedor de aplicação pelo armazenamento e fornecimento da porta de origem do endereço IP, sob a ótica do marco civil da internet". *Caderno Virtual*, 2(43).

La revolución de las direcciones IPV6: impactando el futuro traspasando fronteras de las telecomunicaciones en américa del sur

The Revolution of IPv6 addresses: impacting the Future by crossing the borders of telecommunications in South America

Autor:

Raúl Bareño Gutiérrez.
raulbare@yahoo.es

Resumen

El agotamiento de las direcciones IPv4 y la necesidad de asegurar la continuidad de la conectividad global han impulsado la transición hacia las direcciones IPv6 en el mundo, incluyendo América del Sur. Por ello, es urgente la penetración de las direcciones IPv6 en la región, examinando los retos y las oportunidades que representa y los factores que influyen en su avance, identificando los obstáculos que persisten y las oportunidades que la transición a IPv6 puede ofrecer en términos de escalabilidad, seguridad y desarrollo tecnológico hacia una solución sostenible para garantizar el crecimiento y la continuidad de las comunicaciones. Cuantos más dispositivos y servicios se conectan a Internet, la transición a IPv6 entrega una mayor capacidad de direccionamiento y nuevas aplicaciones y servicios. Por ello, la metodología utilizada incluyó una revisión exhaustiva de literatura científica, datos estadísticos y estudios de caso relacionados con la adopción de IPv6. Los datos recopilados notan los factores que han influido en su avance, pero aún existen desafíos significativos. Algunos países de la región han logrado altas tasas de adopción, liderando el camino hacia la transición; otros se han rezagado, enfrentando obstáculos como la falta de conciencia sobre IPv6, la resistencia al cambio y la escasez de recursos técnicos y financieros. Por ello, se debe continuar impulsando la adopción de IPv6 en América del Sur. Los actores clave en el sector de las comunicaciones, tanto en el ámbito público como privado, deben trabajar conjuntamente para superar los obstáculos identificados y promover su integración. Finalmente, los líderes en el campo de las telecomunicaciones deben adoptar más políticas públicas y tomar medidas que incentiven la transición de los servicios y aplicaciones bajo IPv6 para asegurar un futuro digital próspero, seguro y adaptable en América del Sur.

Palabras claves

Direcciones IPv6, adopción a IPv6, transición al protocolo IPv6, América del Sur, telecomunicaciones.

Abstract

The exhaustion of IPv4 addresses and the need to ensure the continuity of global connectivity have driven the transition towards IPv6 addresses around the world, including in South America. Therefore, examining the challenges and opportunities it represents and the factors that influence its progress is urgent. Identifying the obstacles that persist and the opportunities that the transition to IPv6 can offer in terms of scalability, security, and technological development,

towards a sustainable solution to guarantee the growth and continuity of communications. As more devices and services connect to the Internet, the transition to IPv6 delivers increased addressability and new applications and services. For this reason, the methodology used included an exhaustive review of scientific literature, statistical data, and case studies related to the adoption of IPv6. The data collected notes the factors that have influenced its progress, but significant challenges remain. In some countries in the region, they have achieved high adoption rates, leading the way towards the transition; others have lagged, facing obstacles such as a lack of IPv6 awareness, resistance to change, and a shortage of technical and financial resources. For this reason, the adoption of IPv6 in South America must continue to be promoted. Key players in the communications sector, both in the public and private spheres, must work together to overcome the obstacles identified and promote their integration. Finally, leaders in the field of telecommunications must adopt more public policies and take measures that encourage the transition of services and applications under IPv6, towards ensuring a prosperous, secure, and adaptable digital future in South America.

Keywords

IPv6 addresses, IPV6 adoption, Transition to IPV6 protocol, South America, Telecommunications.

Este capítulo es resultado del proyecto de investigación titulado "**MODELO DE TRANSICIÓN AL PROTOCOLO IPV6 PARA PYMES Y MIPYMES COLOMBIANAS APLICANDO MODELOS DE MACHINE LEARNING**" con código de aprobación del Comité de Investigaciones #PI0220231, proyecto financiado con una asignación de 21.000.000 millones Mcte, en la actualidad en fase de ejecución.

Institución financiadora: **Fundación Universitaria Compensar**

Introducción

El protocolo de direcciones de Internet versión 6 (IPv6) es un estándar de protocolo de comunicación de red que reemplaza la versión anterior, IPv4 (Gómez-Rodríguez, J. R., Sandoval-Aréchiga, R., Ibarra-Delgado, S. & Flores-Troncoso, J., 2016). A medida que la cantidad de dispositivos conectados a Internet continúa creciendo, es necesario un sistema de direccionamiento de Internet más escalable y adaptable. En el contexto de la creciente demanda de conectividad global y el agotamiento de las direcciones IPv4, la adopción de direcciones IPv6 se ha convertido en un tema crucial en el campo de las telecomunica-

ciones a nivel de Suramérica. Se han documentado avances significativos en la implementación de IPv6 a nivel mundial (Tatipamula, M., Grossetete, P. & Esaki, H., 2004), sin embargo, existe una necesidad de comprender específicamente la situación en América del Sur, dada su importancia como una región en crecimiento y su relevancia en el panorama global de las telecomunicaciones (Tanenbaum, A. & Wetherall, D., 2011).

Se han realizado investigaciones y análisis en otras partes del mundo, pero es crucial examinar el contexto y los desafíos particulares que América del Sur enfrenta en relación con la adopción de IPv6 (Fall, K. R. & Stevens, W. R., 2011). Validando factores técnicos, económicos, políticos y regulatorios que han influido en el proceso de transición, que permitan también identificar los obstáculos y las oportunidades asociadas con la adopción de IPv6 en la región, se pretende ofrecer una visión integral que contribuya a la toma de decisiones informadas y a la promoción de acciones estratégicas para impulsar la transición o migración hacia IPv6 (Al- Bahadili, H., 2012).

En el mundo actual, donde la conectividad digital se ha vuelto fundamental en casi todos los aspectos de nuestra vida, la disponibilidad de direcciones IP se ha convertido en un recurso escaso. El protocolo IPv4, que ha sido la columna vertebral de Internet durante décadas, se encuentra en una situación crítica debido a la creciente demanda de direcciones IP. Ante esta realidad, la adopción de direcciones IPv6 surge como una solución necesaria y fundamental para garantizar la continuidad y el crecimiento de la infraestructura de Internet (Rehman, S. U. & Manickam, S., 2015).

El protocolo IPv6 representa una nueva generación de direcciones IP, diseñadas para superar las limitaciones de IPv4 y satisfacer las demandas de conectividad de la sociedad moderna. A diferencia de IPv4, que utiliza direcciones de 32 bits, IPv6 emplea direcciones de 128 bits, lo que permite un espacio de direccionamiento mucho mayor (Twum, F., Asante, K. & Asante, M., 2016). En teoría, esto significa que hay suficientes direcciones IPv6 para conectar prácticamente cualquier dispositivo o servicio que pueda existir en el futuro. Sin embargo, a pesar de las claras ventajas y la necesidad apremiante de IPv6, su adopción a nivel mundial ha sido gradual y heterogénea (Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S. & Acosta, N. D., 2016).

En América del Sur, como una región en constante desarrollo y con una creciente dependencia de las tecnologías de la información y la comunicación, no es una excepción. Es crucial entender el estado actual de la penetración de IPv6 y analizar los factores que han influido en su implementación, identificando los avances logrados, los obstáculos enfrentados y las mejores prácticas utilizadas

en la transición. Además, se examinarán los factores técnicos, económicos, políticos y regulatorios que han influido en su implementación.

La implementación de direcciones IPv6 en América del Sur reviste una importancia estratégica y económica significativa. A medida que la región experimenta un crecimiento continuo en términos de infraestructura de telecomunicaciones, conectividad y adopción de tecnologías digitales, la transición a IPv6 se convierte en un factor clave para asegurar el desarrollo y la competitividad en la era digital y garantizar la continuidad de la expansión de Internet, así como facilitar la adopción de nuevas tecnologías y servicios que requieren una gran cantidad de direcciones IP (Cannon, R., 2010).

Las direcciones IPv6 ofrecen mejoras significativas en términos de seguridad, escalabilidad y calidad de servicio, lo que contribuiría a fortalecer las infraestructuras digitales y brindar una experiencia de conectividad más robusta y confiable para los usuarios en la región (Zhang, R. & Bartell, M., 2003). En este contexto, la implementación de IPv6 en América del Sur se presenta como una necesidad urgente y una oportunidad estratégica para impulsar el desarrollo tecnológico, la innovación y la transformación digital en la región. Finalmente, la pregunta de investigación es: ¿cuál es el estado actual de la adopción de las direcciones IPv6 en América del Sur y cuáles son los factores que influyen en su penetración?

Metodología

La metodología utilizada en este artículo se basa en los principios y directrices propuestos por Barbara Kitchenham (Kitchenham, B., 2004), una reconocida experta en investigación en el campo de las ciencias de la computación. La metodología seguirá un enfoque sistemático y riguroso, garantizando la validez y la confiabilidad de los resultados obtenidos.

Se efectuó de manera exhaustiva una revisión de la literatura científica, utilizando bases de datos relevantes y criterios de inclusión y exclusión predefinidos, acerca de estudios, informes y documentos que aborden la adopción de IPv6 en América del Sur, así como aquellos que analicen los factores que han influido en su implementación en la región utilizando palabras clave relevantes, como “IPv6”, “transición”, “migración”, “Sur América”, “direcciones IPv6”, “servicios y protocolos bajo IPv6”, etc.

Extrayendo datos relevantes sobre la penetración de IPv6 en América del Sur, los desafíos identificados, las mejores prácticas utilizadas y los factores que han

impactado en la adopción, buscamos patrones y tendencias significativas. Esto permitirá aumentar la confiabilidad de los resultados e identificar factores y conclusiones de la penetración de IPv6 en América del Sur.

Resultados

El análisis de la penetración de las direcciones IPv6 en América del Sur revela una variada situación en los distintos países de la región (Kurose, J. F. & Ross, K. W., 2013; Huitema, C., 1995). En la tabla 6.1 se presentan los resultados obtenidos en términos de su transición, así como las fortalezas, debilidades, políticas establecidas, aspectos de seguridad, aspectos de la migración y criterios para la implementación en cada país.

Tabla 5.1. Aspectos de transición hacia IPv6 por país

País	% De Penetración	Fortalezas	Debilidades	Políticas Establecidas	Aspectos De Seguridad	Aspectos De Penetración	Recomendaciones
Argentina	18,22 %	Avanzada Infraestructura De Telecomunicaciones.	Baja Conciencia Sobre Ipv6. Falta De Una Política Pública.	Implementación Gradual En El Sector Público, Poco Avance En El Sector De Servicios Y Soluciones De Interconexión En El Sector Privado.	Implementación De Mecanismos De Filtrado Ipv6.	Adopción Intermitente En El Sector Empresarial, Específicamente En Sectores Pymes.	Educación Y Capacitación, Requiere Una Integración Más Acelerada Entre Los Isp.
Brasil	43,83 %	Gran Tamaño De La Economía, Fortalecimiento De Políticas Público-Privadas.	Resistencia Por Parte De Los Proveedores De Isp Dada La Dificultad Para La Cobertura En Pequeños Estados.	Política Nacional Para Promover Ipv6 Y Nivel De Entornos Públicos Y Privados.	Implementación De Firewalls Ipv6 Y Políticas A Nivel De Ids E Ips Para Los Servicios De Telecomunicaciones.	Adopción En Universidades Y Centros De Investigación Y Zonas Densamente Pobladas.	Desarrollo De Herramientas Y Recursos Para La Ampliación De Cobertura.
Chile	15,4 %	Adopción Temprana En El Sector Gubernamental.	Escasa Inversión En Infraestructura Ipv6, Lo Largo Del País Y La Dificultad En Cobertura, Poca Escalabilidad.	Programa Nacional Para La Adopción De Ipv6, Pero Poca Adaptación Tecnológica.	Configuración Adecuada De Los Dispositivos En Las Capas 2 Y 3 Y En La Capa 7.	Adopción En El Sector Educativo Y Empresarial, Falta Un Plan Estratégico De Transición.	Monitoreo Y Evaluación Constante En Zonas De Amplia Cobertura.

País	% De Penetración	Fortalezas	Debilidades	Políticas Establecidas	Aspectos De Seguridad	Aspectos De Penetración	Recomendaciones
Colombia	22,31 %	Creación De Grupos De Trabajo Sobre Ipv6. Política Pública De Transición Al Protocolo.	Limitada Conciencia Pública Sobre Ipv6. Falta Actualización Tecnológica.	Normativas Para La Transición A Ipv6, Protocolos Y Fases Claramente Definidos.	Autenticación Y Cifrado De Comunicaciones, Pero Falta De Personal Capacitado Para Operar Y Administrar La Transición Responsable.	Adopción En Instituciones De Gobierno Y Educativas, Proceso Muy Lento Y Sin Plan Estratégico.	Promoción De Ipv6 En Eventos Y Conferencias, Con Poca Adopción Del Sector Privado.
Perú	25,66 %	Implementación En El Sector Educativo.	Escasa Disponibilidad De Proveedores Ipv6.	Plan Nacional Para La Adopción De Ipv6, Pero Falta Plan Estratégico.	Configuración Segura De Equipos De Red, Falta Implementación A Nivel De Servicios Y Protocolos Bajo Ipv6.	Adopción En El Sector Bancario Y De Telecomunicaciones, Falta Una Estrategia De Penetración Como Política.	Asociación Con Proveedores De Servicios, Limitados A Las Infraestructuras Tecnológicas De Los Isp.
Ecuador	25,74 %	Compromiso Gubernamental Con La Adopción De Ipv6.	Limitado Acceso A Infraestructura De Calidad En Algunas Regiones.	Plan Nacional De Ipv6 Como Política Pública.	Implementación De Políticas De Seguridad De Red Y Protección Contra Ataques Cibernéticos.	Crece Acorde Al Plan Estratégico De Cobertura En Zonas Altamente Pobladas.	Establecer Metas Específicas Y Plazos Para La Migración.

País	% De Penetración	Fortalezas	Debilidades	Políticas Establecidas	Aspectos De Seguridad	Aspectos De Penetración	Recomendaciones
Uruguay	56,41 %	Avanzada Infraestructura De Red Para Soportar Ipv6.	Baja Conciencia Y Capacitación En Ipv6, A Pesar De Su Alto Porcentaje De Transición.	Estrategia Nacional De Ipv6 Como Política Pública.	Implementación De Mecanismos De Seguridad Y Políticas De Prevención De Ataques.	Más Del 70 % Del Tráfico De Internet Es En Ipv6.	Establecer Incentivos Y Programas De Capacitación Para Promover La Adopción De Ipv6.
Paraguay	28,2 %	Proyectos Piloto Exitosos En Implementación De Ipv6.	Escasa Inversión En Infraestructura De Red Para Ipv6.	Legislación Acerca De La Implementación De Ipv6.	Implementación De Políticas De Seguridad De Red Y Control De Acceso.	Alrededor Del 20 % Del Tráfico De Internet Es En Ipv6.	Desarrollar Programas De Capacitación Y Concienciación En Ipv6 Para Profesionales Y Usuarios Finales.
Bolivia	18,62 %	Compromiso Gubernamental Y Avances En La Transición.	Limitada Infraestructura De Conectividad En Algunas Regiones.	Plan Nacional De Despliegue De Ipv6.	Implementación De Políticas De Seguridad De Red Y Sistemas De Prevención De Ataques.	Alrededor Del 10 % Del Tráfico De Internet Es En Ipv6.	Establecer Alianzas Con Proveedores De Servicios Y Promover La Inversión En Infraestructura De Ipv6.

Fuente: Google Statistics

En la tabla 6.1 se muestra una visión general de la penetración de IPv6 en algunos países de América del Sur, destacando los porcentajes de adopción, las fortalezas y debilidades identificadas, las políticas establecidas, los aspectos de seguridad, los aspectos de penetración y los criterios para la implementación. Se refleja así la diversidad de situaciones y desafíos que cada país enfrenta en su camino hacia una mayor adopción de IPv6. La implementación exitosa de IPv6 requiere el desarrollo de políticas claras, la educación y capacitación de los actores involucrados, la promoción de la seguridad y la colaboración entre los diferentes sectores de la sociedad para lograr una transición eficiente y efectiva.

En la tabla 6.2 se reflejan los porcentajes de compatibilidad, preferencia, direcciones IPv6 entregadas, peso promedio de asignación y ponderación hacia la transición al protocolo.

Tabla 5.2. Porcentajes y estimados en años para la transición

País	Compatible con IPv6	IPv6 preferido	Porcentaje sector público	Porcentaje sector privado	Muestras ponderadas	Tiempo estimado para la transición (años)
Uruguay	59,21 %	59,06 %	70	30	382,808	8
Brasil	46,34 %	46,00 %	30	70	25,210,379	12
Paraguay	31,46 %	31,27 %	20	80	798,052	14
Perú	27,02 %	26,78 %	10	90	2,808,982	15
Argentina	22.77 %	22,32 %	40	60	5,800,000	16
Ecuador	24,59 %	24,43 %	50	50	1,746,131	16
Colombia	24,35 %	24,17 %	70	30	5,378,633	16
Chile	17,35 %	17,11 %	60	40	2,519,518	20
Bolivia	17,12 %	17,01 %	80	20	920,932	20
Venezuela	1,76 %	1,75 %	20	80	3,039,505	22

Fuente: stat.labs.apnic. Recuperado de: https://stats.labs.apnic.net/ipv6/XP

Discusión

En el marco de la contratación entre autores y por países se pueden destacar algunos referentes así:

Tabla 5.3. Argentina

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Jerez, G. E., López, V. J., Longo, V. M., Gálvez Díaz, M. D. P., Gallardo, M. A. & Zamora, R. A. (2019)	Presentan técnicas para el despliegue de IPv6 en redes LAN.	Se proponen técnicas prácticas para el despliegue de IPv6 en redes LAN, basadas en RDNSS y DHCPv6.	Mencionan la importancia de implementar prácticas seguras en el despliegue de IPv6.	Se enfocan en técnicas para el despliegue de IPv6 en redes LAN.	Se enfocan en técnicas de despliegue de IPv6 en redes LAN.
Jerez, G. E., López, V. J. & Longo, V. M. (2019)	Abordan técnicas de autoconfiguración utilizando RDNSS y DHCPv6 en laboratorios.	Se muestran los resultados obtenidos al implementar RDNSS y DHCPv6 para la autoconfiguración en redes LAN.	Mencionan la importancia de implementar servicios y aplicaciones seguras en la implementación.	Se enfocan en técnicas de autoconfiguración utilizando RDNSS y DHCPv6 en laboratorios.	Se enfocan en técnicas de autoconfiguración utilizando RDNSS y DHCPv6 en laboratorios.
Sánchez, E., Gamarra, ç. I. & Arias Figueroa, D. (2022)	Estudian la implementación de IPv6 en el ámbito regional y su impacto en los usuarios finales.	Se analiza la implementación de IPv6 en el ámbito regional y su impacto en los usuarios finales, identificando desafíos y oportunidades.	Mencionan la importancia de considerar aspectos de servicios y soluciones de interconexión bajo IPSec.	Se enfocan en la implementación de IPv6 en el ámbito regional y su impacto en los usuarios finales.	Se analiza la implementación de IPv6 en el ámbito regional y se identifican desafíos y oportunidades.
Jerez, G. E., López, V. J. & Longo, V. M. (2021)	Analizan la seguridad en la configuración de redes IPv6 y proponen buenas prácticas.	Se identifican vulnerabilidades comunes en la configuración de redes IPv6 y se proponen buenas prácticas para mejorar la seguridad.	Abordan aspectos de seguridad en la configuración de redes IPv6 y proponen buenas prácticas.	Mencionan la importancia de implementar framework basados en la triada de la seguridad.	Se enfocan en la seguridad en la configuración de redes IPv6 y se proponen buenas prácticas.

Tabla 5.4. Brasil

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Brito, S. H. B. (2018)	Presenta una visión general de IPv6 y su importancia en la evolución de Internet.	Se destaca la necesidad de implementar IPv6 para hacer frente al agotamiento de direcciones IPv4.	Recomienda empezar por la implementación de servicios a nivel de confidencialidad.	Se enfoca en brindar una visión genera y conceptual de IPv6.	Aborda estrategias específicas para la transición a IPv6, específicamente en el sector de telecomunicaciones.
Ribeiro, D. L., Tiosso, F. & Reis, H. (2022)	Analizan la transición de IPv4 a IPv6 y presentan los desafíos y beneficios asociados.	Se resalta la importancia de la transición de IPv4 a IPv6 y se mencionan diferentes técnicas y estrategias para llevarla a cabo.	Recomiendan empezar por la implementación de servicios a nivel de integridad.	Resaltan la importancia de realizar pruebas y planificar la transición.	Se presentan diferentes técnicas y estrategias para la transición de IPv4 a IPv6.
Marrafon, G. & García, R. (2017)	Se abordan la importancia y las ventajas de IPv6 en el contexto actual.	Se destaca la necesidad de adoptar IPv6 para garantizar el crecimiento y desarrollo de las tecnologías de comunicación.	Recomiendan empezar por la implementación de servicios a nivel de disponibilidad.	Resaltan la importancia de la adopción de IPv6.	Abordan planes y estrategias específicas a nivel de buenas prácticas para la transición a IPv6.
De Oliveira, G. D. & Violín, R. D. O. (2021)	Se analizan las dificultades en la transición de IPv4 a IPv6 y se proponen soluciones.	Se identifican los desafíos técnicos y operativos en la transición a IPv6 y se presentan recomendaciones para superarlos.	Se mencionan las dificultades y desafíos relacionados con la seguridad en la transición de IPv4 a IPv6.	Resaltan la importancia de la planificación y preparación y servicios telemáticos a nivel de cobertura entre los ISP.	Se presentan recomendaciones y soluciones para superar los desafíos en la transición de IPv4 a IPv6.

Tabla 5.5. Chile

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Castillo-Velázquez, J. I., Panduro, V. R. C. & Niño, W. R. M. (2018)	Se presenta una emulación de conectividad y gestión IPv6 en REUNA, la red avanzada de Chile.	Se resalta la importancia de la implementación y emulación de IPv6 para la red avanzada de Chile.	Recomiendan la implementación de la triada de seguridad.	Se enfocan en la implementación de IPv6 en la red avanzada de Chile.	Recomiendan un plan estratégico dada la urgencia manifiesta de programas serios para la transición a IPv6.
Kiedanski, D. & Grampín, E. (2017)	Se realiza una exploración preliminar de la conectividad IPv6 en América Latina.	Se identifican desafíos y brechas en la implementación de IPv6 en los países de América Latina.	Recomiendan empezar por mejorar en la implementación de la autenticación entre pares.	Resaltan la necesidad de una mayor adopción de IPv6, mejorar servicios de interconexión.	Advierten de falta de planes estratégicos en la región para la transición a IPv6.
Varela, F. V. (2021)	Se aborda la implementación de IPv6 en Chile y su relevancia en el contexto actual.	Se destaca la necesidad de adoptar IPv6 en Chile y se presentan recomendaciones para su implementación exitosa.	Se recomienda empezar por la implementación de IPSec.	Resalta la importancia de la planificación y ejecución adecuadas.	Se presentan recomendaciones para la implementación exitosa de IPv6 en Chile.
Leiva Díaz, R. (2020)	Se propone una migración del protocolo de comunicación a IPv6.	Se resalta la necesidad de migrar a IPv6 en la Universidad Adventista de Chile y se presenta una propuesta de migración específica.	Se mencionan los aspectos de seguridad a considerar durante la migración a IPv6.	Se enfoca en la migración a IPv6 basado en mejoras en los servicios telemáticos.	Se presenta una propuesta de migración específica para la Universidad Adventista de Chile.

Tabla 5.6. Colombia

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Fonseca Castro, D. C. (2018)	Se presenta un plan de transición del protocolo de red IPv4 a IPv6 basado en recomendaciones realizadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Es necesario implementar IPv6 en Colombia y se propone un plan detallado para la transición del protocolo de red IPv4 a IPv6, basado en recomendaciones MinTIC.	Recomienda la implementación rápida de IPSec.	Presenta un plan detallad de transición a IPv6 basado en las recomendaciones del MinTIC.	Se propone un plan de transición del protocolo de red IPv4 a IPv6 basado en planes estratégicos hacia entornos cloud computing.
Gamboa Torres, L. A. & Novoa Socha, J. D. (2017)	Se realiza una revisión y se presenta un caso de transición del protocolo IPv4 a IPv6 en una empresa específica.	La transición de IPv4 a IPv6 es un proceso complejo que requiere una planificación adecuada y se presenta un caso de estudio de transición en una empresa, destacando los desafíos y las lecciones aprendidas.	Recomiendan la implementación rápida de la triada de la seguridad CIA.	Presentan un caso de estudio de transición de IPv4 a IPv6 en una empresa basados en framework empresariales.	Se presenta un caso de estudio de transición del protocolo IPv4 a IPv6 en una empresa específica y recomiendan validar estándares de seguridad a nivel ISO, ITIL y COBIT.

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Cárdenas Rodríguez, G. 2018	Se presenta la implementación del protocolo IPv6 en la compañía y se destacan los beneficios y desafíos encontrados durante el proceso.	Se concluye que la implementación de IPv6 en una empresa requiere una planificación adecuada, la asignación de recursos y la capacitación del personal. Se destaca la importancia de adaptar la infraestructura y los servicios de red para soportar IPv6.	Recomiendan empezar por implementar el framework de IPSec.	Destacan la importancia de adaptar la infraestructura y los servicios de red para soportar IPv6.	Se presenta la implementación del protocolo IPv6 y plantean estrategias para la migración controlada de los servicios.
Bernal Santos, R., Carvajal Quintero, W, & Rico Bello, J. (2020)	Proponen una solución de red con alta disponibilidad para la transición de IPv4 a IPv6 en una entidad del Estado.	Es necesario planificar y diseñar una solución de red con alta disponibilidad para la transición de IPv4 a IPv6 en una entidad del Estado. Se destaca la importancia de la planificación, la evaluación de la infraestructura existente y la selección de tecnologías adecuadas para garantizar una transición exitosa.	Se mencionan los aspectos de seguridad basados en la integridad como proceso fundamental.	Proponen una solución de red con alta disponibilidad y escalabilidad para la transición.	Se propone una solución de red con alta disponibilidad y recursividad de los servicios de telecomunicaciones, destacando la importancia de la planificación y la selección de estrategias basadas en modelos reconocidos.

Tabla 5.7. Perú

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Baltazar, M. A. T. (2017)	Se propone un modelo de referencia de transición de IPv4 a IPv6 específico para el sector gubernamental de Perú.	Se destaca la necesidad de implementar IPv6 en el sector gubernamental de Perú y se presenta un modelo de referencia para guiar la transición.	Se recomienda hacer la transición y basar la implementación en la integridad de la información.	Presenta un modelo de referencia para la transición basado en las políticas públicas.	Se presenta un modelo de referencia de transición de IPv4 a IPv6 y recomienda fortalecer la estrategia en diferentes sectores de la economía.
Cruz Ojeda, J. R. (2018)	Describe un proyecto de migración de IPv4 a IPv6 utilizando el mecanismo de doble pila (Dual Stack) en la empresa BP Support.	Se resalta la importancia de la migración a IPv6 en la empresa y se presenta un proyecto detallado para llevar a cabo la migración utilizando el mecanismo de doble pila.	Se recomienda hacer la transición y basar la implementación en la triada de la seguridad CIA.	Se presenta un proyecto detallado de migración a IPv6, con recomendaciones y mejoras hacia los sistemas informáticos.	Se presenta un proyecto de migración de IPv4 a IPv6 utilizando el mecanismo de doble pila (Dual Stack) basados en los dispositivos capa 3.
Hanampa Ñahui, W. (2019)	Se propone un modelo de referencia de transición de IPv4 a IPv6 específico para la empresa de telecomunicaciones Ruralnet SRL.	Se destaca la necesidad de implementar IPv6 en la empresa y se presenta un modelo de referencia para guiar la transición.v	Se recomienda hacer la transición y basar la implementación en IPSec.	Se presenta un modelo de referencia para la transición que se puede replicar en empresas pymes.	Se presenta un modelo de referencia de transición de IPv4 a IPv6 para una empresa de telecomunicaciones como plan estratégico de la organización.
Andrade Leiva, C. J. P. (2019)	Se propone una planificación de transición de IPv4 a IPv6 y una mejora en el servicio de red de datos para el Despacho de la Presidencia de la República.	Se resalta la necesidad de migrar a IPv6 y mejorar el servicio de red de datos y se presenta una planificación detallada para la transición y mejora.	Se mencionan los aspectos de seguridad a nivel de autenticación y de confidencialidad.	Se presenta una planificación detallada de transición y mejoras hacia los servicios de telecomunicaciones.	Se presenta una planificación de transición de IPv4 a IPv6 y una mejora en el servicio de red de datos basado en políticas.

Tabla 5.8. Ecuador

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Aguirre Villarroel, V. T. (2023)	Se realiza un diagnóstico de la implementación de IPv6 en Ecuador.	Se concluye que la implementación de IPv6 en Ecuador aún es baja y se presentan recomendaciones para fomentar su adopción y uso en el país.	Se mencionan los aspectos de seguridad a nivel de autenticación.	No se mencionan aspectos de infraestructura en particular, pero se presenta un diagnóstico de la implementación de IPv6 en Ecuador.	Se presentan recomendaciones para fomentar la implementación y uso de IPv6 en Ecuador.
Rodríguez Amaguay, X. D. & Tejada Zúñiga, C. E. (2018)	Se elabora un plan de acción para la implementación de IPv6 en Ecuador y se fomenta su uso.	Se concluye que es necesario implementar IPv6 en Ecuador y se propone un plan de acción detallado para su implementación, incluyendo aspectos como la capacitación, la adaptación de infraestructura y servicios, y la promoción del uso de IPv6.	Se mencionan los aspectos de seguridad a nivel del framework IPSec.	Se presenta un plan de acción para la implementación de IPv6 basados en la actualización tecnológica.	Se propone un plan de acción para la implementación de IPv6 en Ecuador, incluyendo estándaresinternacionales.
Garrido Carrera, J. J. (2018)	Se realiza la transición del protocolo IPv4 a IPv6 para la red inalámbrica dentro de la Universidad Técnica del Norte.	Se concluye que es posible realizar la transición de IPv4 a IPv6 en la red y se destacan los beneficios obtenidos. Se destaca la importancia de la planificación y la configuración adecuada para garantizar una transición exitosa.	Se mencionan los aspectos de seguridad a considerar basados en estándares internacionales.	Destaca la importancia de la planificación y la configuración adecuada para la transición de IPv4 a IPv6 en la red inalámbrica y actualización de RADIUS y AP que soporten aspectos deseguridad.	Se presenta la transición del protocolo IPv4 a IPv6 en la red y se destacan lo sbeneficios de la políticas para la implementación.
Cifuentes Domínguez, G. F. (2018)	Se propone una metodología de transición de la red IP/MPLS a IPv6 para la entrega de servicios al segmento corporativo de la Corporación Nacional de Telecomunicaciones en la provincia de Napo.	La metodología propuesta permite realizar la transición de la red IP/MPLS a IPv6 de manera ordenada y planificada, mejorando la entrega de servicios al segmento corporativo, la capacitación y la evaluación continua para garantizar una transición exitosa.	Se recomienda empezar a implementar la autenticación en los sistemas telemáticos a interconectar.	Se propone una metodología de transición de la red IP/MPLS a IPv6, destacando aspectos deinfraestructura a nivel del core.	Se propone una metodología de transición de la red IP/MPLS a ΩΩIPv6, destacando la importancia de la planificación, la capacitación basado en controles específicos basados en estándares ISO, COBIT e ITIL, entre otros

Tabla 5.9. Uruguay

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Pensky Markowicz, G. (2021)	Se analiza la implementación de IPv6 como un desafío de innovación para los ISP en Uruguay.	Se concluye que la implementación de IPv6 presenta desafíos y oportunidades para los ISP en Uruguay. Se destaca la importancia de la capacitación y la planificación adecuada para garantizar una transición exitosa a IPv6.	Se mencionan los aspectos de seguridad a considerar durante la implementación de IPv6 basados en IPSec.	Se enfatiza la importancia de la capacitación y la planificación para la implementación de IPv6 en los ISP.	Se destaca la importancia de la capacitación y la planificación adecuada para la implementación de IPv6 en los ISP.
Viera Barlocco, L. & Riccardi Pugliesi, B. (2019)	Se propone un sistema de distribución multicast utilizando redes definidas por software sobre IPV6.	Se concluye que el sistema de distribución multicast propuesto es eficiente y escalable, y se destaca su utilidad en entornos de redes definidas por software. Se resalta la importancia de la planificación y el diseño adecuados para garantizar un funcionamiento sobre IPv6.	Recomiendan aplicar la triada de la seguridad CIA.	No se mencionan aspectos de infraestructura en particular, pero se presenta un sistema de distribución multicast utilizando redes definidas por software.	Mencionan estrategias específicas para la transición a IPv6 basado en estándares y políticas públicas.

Tabla 5.10. Paraguay

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Ubiedo, L., OíHara, T., Erquiaga, M. J. & García, S. (2021)	Se analiza el estado actual de la seguridad de IPv6 en el Internet de las cosas (IoT).	Existen desafíos significativos en la seguridad de IPv6 en el IoT, incluyendo la falta de implementación de mecanismos de seguridad, la falta de conciencia y conocimiento sobre los riesgos y la falta de actualizaciones y parches de seguridad.	Se analizan los aspectos de seguridad relacionados con IPv6 en el contexto del IoT basados en IPSec.	Se enfatiza la importancia de implementar soluciones óptimas de infraestructura adecuados en el contexto del IoT e IPv6.	Recomiendan revisar estándares internacionales como buenas prácticas para la transición.
CEPAL & Unión Europea (2021)	Presentan un informe sobre los principales indicadores de adopción de tecnologías digitales en el marco de la Agenda Digital para América Latina y el Caribe.	Se concluye que la transformación digital en América Latina y el Caribe presenta avances significativos, pero aún existen brechas y desafíos en términos de infraestructura, conectividad, habilidades digitales y seguridad cibernética.	Se mencionan aspectos de seguridad cibernética en el contexto de la transformación digital basados en la triada CIA.	Se mencionan aspectos de infraestructura relacionados con la transformación digital.	Recomiendan revisar estándares reconocidos como ISO, COBIT e ITIL, entre otros.

Tabla 5.11. Venezuela

Autor(es)	Resultados	Conclusiones	Aspectos de seguridad informática	Infraestructura para la transición	Estrategias para la transición
Deering, S. & Hinden, R. (2017)	Se presenta el RFC 8200, que especifica el protocolo de Internet versión 6 (IPv6).	La importancia de aplicación de estándares RFC para apoyar la transición a IPV6.	No se mencionan aspectos de seguridad informática específicos, pero recomiendan validar el protocolo nativo de IPv6 IPSec.	No se mencionan aspectos de infraestructura para la transición a direcciones IPv6.	No se mencionan estrategias específicas para la transición a IPv6 en el resumen del documento.
Padmanabhan, R., Rula, J. P., Richter, P., Strowes, S. D. & Dainotti, A. (2020)	Se analizan las prácticas de asignación de direcciones en IPv4 e IPv6.	Se concluye que hay diferencias significativas en las prácticas de asignación de direcciones entre IPv4 e IPv6 y se destaca la necesidad de mejorar las prácticas de asignación de direcciones IPv6 para lograr una mejor gestión y aprovechamiento de los recursos.	Se analizan las prácticas de asignación de direcciones en IPv4 e IPv6 desde una perspectiva técnica.	Transición a direcciones IPv6 basados en servicios telemáticos e infraestructuras actualizadas.	Se recomienda validar estándares internacionales como COBIT, ITIL e ISO, entre otros.

Todos los referentes anteriores reiteran la importancia de fortalecer la transición a direcciones IPv6 en América del Sur, con un enfoque en mejorar las soluciones de telecomunicaciones, y ampliar la cobertura de banda ancha, especialmente en regiones remotas, puede contribuir significativamente a minimizar la brecha digital y expandir la conectividad educativa.

Aquí hay algunas recomendaciones:

Políticas de fomento IPv6: establecer políticas gubernamentales que promuevan la adopción de IPv6 en los proveedores de servicios de Internet (ISP) y en las redes de telecomunicaciones. Incluir requisitos IPv6 en licitaciones públicas para proyectos de expansión de redes telemáticas y banda ancha.

Incentivos económicos: ofrecer incentivos fiscales y financieros para empresas y proveedores de servicios que implementen IPv6 de manera efectiva, especialmente aquellos que extiendan su cobertura a áreas remotas. Facilitar el acceso a financiamiento o subvenciones para proyectos de infraestructura que incluyan la implementación de IPv6.

Capacitación técnica: desarrollar programas de capacitación técnica para profesionales de TI y personal de las empresas de telecomunicaciones en IPv6. Colaborar con instituciones educativas para integrar programas de formación en IPv6 en sus currículos.

Desarrollo de contenidos locales: fomentar el desarrollo de contenidos locales y aplicaciones que sean compatibles con IPv6 para motivar la demanda de servicios basados en esta tecnología. Colaborar con comunidades locales para identificar necesidades específicas y adaptar los servicios en consecuencia.

Estrategias de despliegue gradual: adoptar estrategias de despliegue gradual como la doble pila (dual-stack) para garantizar la interoperabilidad con IPv4 durante la transición. Implementar mecanismos de traducción y túneles para facilitar la coexistencia de IPv4 e IPv6 durante el proceso de migración.

Infraestructura compartida: fomentar la colaboración entre proveedores de servicios para compartir infraestructura en áreas remotas, reduciendo así los costos asociados con la expansión de la cobertura de banda ancha. Explorar modelos de colaboración público-privada para el despliegue de infraestructura en regiones menos desarrolladas.

Enfoque en educación: priorizar la conectividad educativa en áreas rurales mediante la implementación de redes telemáticas y servicios educativos en

línea. Colaborar con instituciones educativas para asegurar la conectividad en escuelas y universidades, proporcionando acceso a recursos educativos en línea.

Monitoreo y evaluación continua: establecer mecanismos de monitoreo y evaluación continua para medir el progreso de la implementación de IPv6 y ajustar las estrategias según sea necesario. Utilizar métricas específicas para evaluar el impacto en la ampliación de la cobertura de banda ancha y la reducción de la brecha digital.

Al adoptar estas recomendaciones, los países en América del Sur pueden fortalecer su infraestructura de telecomunicaciones, mejorar la conectividad en áreas remotas y avanzar hacia una transición exitosa a IPv6, contribuyendo así a la reducción de la brecha digital en la región.

Conclusiones

Es inminente que América del Sur debe forzar la transición al protocolo IPv6 que le permita mejorar los servicios y las infraestructuras de telecomunicaciones presentes y futuras para poder fortalecer la cantidad masiva de dispositivos y las nuevas soluciones tecnológicas que se interconectan, apoyando la transformación digital, la automatización, la ciberseguridad, el internet de las cosas, block-chain, las tecnologías disruptivas, las industrias 4.0 y 5.0, la inteligencia artificial, las soluciones cloud computing, las redes definidas por software, entre otros, que les permitan la penetración masiva a IPv6 y que fortalezcan la región y la economía de manera global en todos los sectores público-privados.

A nivel de usuario y los ISP, la región requiere de incentivar políticas de alto impacto como marco de una estrategia legislativa integral, que mediante una gobernanza permita la masificación del protocolo IPv6 en respuesta a las necesidades del contexto actual y que dinamicen el crecimiento de internet y de toda su infraestructura telemática hacia un modelo gradual, procedimental, fácil, sencillo y no se vea como un problema, por lo tanto, la capacitación en el campo de la transición a IPv6 debe generar confianza para su implementación como plan estratégico de manera pausada pero segura sin ningún tipo de contratiempos hacia una migración definitiva que les permita una mayor disponibilidad, integridad y confidencialidad que el protocolo antecesor.

Es inminente, que la transición a IPv6, específicamente en las capas 2 y 3, será el motor que impulse esta migración, aunque para llegar al 100 % tardará por lo menos entre 10-20 años en América del Sur, dado que se requiere de actualización tecnológica costosa y de una planeación estratégica, articulado esto con estándares ISO, COBIT, ITIL, OWASPP e IPSec que les permitan su escala-

bilidad en las empresas y en los ISP hacia la integración articulada y práctica de la tecnologías presentes y futuras, articulando factores como políticas de seguridad, implementación de QoS, movilidad, el uso de las redes, las buenas prácticas asociadas a la difusión de la información, así como los costos de los activos informáticos y tecnológicos actuales.

La investigación destaca que las empresas público-privadas son escépticas en la transición a IPv6 dado que los ISP van muy lentos hacia la migración y continúan con IPv4; por ello, el mundo y América del Sur aún se mueven sobre el protocolo anterior. Esto hará más lenta la migración a IPv6; por ello, se requiere que los ISP y los clientes finales implementen soluciones duales, dado que es crucial para garantizar la continuidad y crecimiento de las telecomunicaciones en la región, además de colaborar con otros países y organizaciones para compartir buenas prácticas y experiencias en la transición, que promuevan la investigación y el desarrollo de tecnologías y soluciones bajo IPv6, para sectores como educación, economía y la industria en general.

Referencias bibliográficas

Aguirre Villarroel, V. T. (2023). *Diagnóstico y perspectivas de la implementación de IPv6 en el Ecuador* (Bachelor's thesis, Quito: EPN, 2023.). https://bibdigital.epn.edu.ec/handle/15000/23618

Al-Bahadili, H. (ed.). (2012). *Simulation in Computer Network Design and Modeling: Use and Analysis*. IGI Global.

Andrade Leiva, C. J. P. (2019). *Planificación de transición del protocolo de red IPv4 a IPv6 y mejora en el servicio de red de datos*. Despacho de la Presidencia de la República, 2019. https://repositorio.ucv.edu.pe/handle/20.500.12692/36719

Baltazar, M. A. T. (2017). *Modelo de referencia de transición de IPv4 a IPv6 para el sector gobierno de Perú*. Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7740

Bernal Santos, R., Carvajal Quintero, W. & Rico Bello, J. (2020). *Propuesta de solución de red con alta disponibilidad para la transición de IPv4 a IPv6 en una entidad del Estado*. https://repositorio.unbosque.edu.co/handle/20.500.12495/4441

Brito, S. H. B. (2018). *IPv6-O novo protocolo da Internet*. Novatec Editora. https://books.google.com.mx/books?hl=es&lr=&id=m7lIDwAAQBAJ&oi=fnd&pg=PT5&dq=IPV6+brasil&ots=YMXXXvxZYr&sig=FmLdTNVaiheCs-ghM_6 bH1Lx5Zl4#v=onepage&q=IPV6%20brasil&f=false

Cannon, R. (2010). *Potential impacts on communications from IPv4 exhaustion & IPv6 transition*. Available at SSRN 1735456.

Cárdenas Rodríguez, G. (2018). *Implementación de protocolo IPv6 en la compañía J. Walter Thompson Colombia*. https://repository.libertadores.edu.co/handle/11371/3059

Castillo-Velázquez, J. I., Panduro, V. R. C. & Niño, W. R. M. (2018, August). "IPv6 connectivity and management emulation for REUNA, the chilean advanced network". In 2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON) (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/8526390

CEPAL & Unión Europea (2021). *Datos y hechos sobre la transformación digital: informe sobre los principales indicadores de adopción de tecnologías digitales en el marco de la Agenda Digital para América Latina y el Caribe*. https://repositorio.cepal.org/handle/11362/46766

Cifuentes Domínguez, G. F. (2018). *Propuesta metodológica de transición de la red IP/MPLS a IPv6 para la entrega de servicios al segmento corporativo de la Corporación Nacional de Telecomunicaciones en la provincia de Napo* (Master's thesis, Escuela Superior Politécnica de Chimborazo). http://dspace.espoch.edu.ec/handle/123456789/8167

Cruz Ojeda, J. R. (2018). *Proyecto de migración del protocolo IPv4 al IPv6 utilizando el mecanismo de doble pila (dual stack) en la empresa BP Support*. http://repositorio.untels.edu.pe/jspui/handle/123456789/281

De Oliveira, G. D. & Violín, R. D. O. (2021, December). "Transição do protocolo IPv4 para IPv6: as dificuldades em alcançar o futuro da internet". In Congresso de Tecnologia-Fatec Mococa (Vol. 5, No. 2). https://congresso.fatecmococa.edu.br/index.php/congresso/article/view/346

Deering, S. & Hinden, R. (2017). *RFC 8200: Internet protocol, version 6 (IPv6) specification*. https://www.rfc-editor.org/rfc/rfc8200

Fall, K. R. & Stevens, W. R. (2011). *TCP/IP illustrated, volume 1: The protocols*. Addison-Wesley.

Fonseca Castro, D. C. (2018). *Plan de transición del protocolo de red IPv4 a IPv6 basado en las recomendaciones realizadas por el MinTIC Colombia*. https://repositorio.unal.edu.co/handle/unal/77444

Gamboa Torres, L. A. & Novoa Socha, J. D. (2017). *La transición del protocolo IPv4 a IPv6 en una empresa: revisión y caso*. https://repository.udistrital.edu.co/handle/11349/15614

Garrido Carrera, J. J. (2018). *Transición de protocolo IPv4 a protocolo IPv6 para la red inalámbrica EDUROAM dentro de la Universidad Técnica del Norte* (Bachelor's thesis). http://repositorio.utn.edu.ec/handle/123456789/7870

Gómez-Rodríguez, J. R., Sandoval-Aréchiga, R., Ibarra-Delgado, S. & Flores-Troncoso, J. (2016). "IPv6. El tiempo ha llegado". *Difu100ci@, Revista de Difusión Científica, Ingeniería y Tecnologías*, 10(2), 12-16.

Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S. & Acosta, N. D. (2016). "Revisión de la seguridad en la implementación de servicios sobre IPv6". *Inge. Cuc.*, 12(1), 86-93.

Hanampa Ñahui, W. (2019). *Modelo de referencia de transición de IPv4 a IPv6 para la empresa de telecomunicaciones Ruralnet SRL*. https://repositorio.utp.edu.pe/handle/20.500.12867/2527

Huitema, C. (1995). *IPv6: the new Internet protocol*. Prentice-Hall, Inc.

Jerez, G. E., López, V. J. & Longo, V. M. (2021). "Seguridad en la configuración de redes IPv6: análisis y buenas prácticas". *Difusiones*, 21(21), 128-147. http://revistas.ucse.edu.ar/ojsucse/index.php/difusiones/article/view/402

Jerez, G. E., López, V. J., Longo, V. M., Gálvez Díaz, M. D. P., Gallardo, M. A. & Zamora, R. A. (2019). "Técnicas para el despliegue de IPv6 en redes LAN". In XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan). http://sedici.unlp.edu.ar/handle/10915/76964

Kiedanski, D. & Grampín, E. (2017, October). "Understanding Latin America IPv6 connectivity: A preliminary exploration". In 2017 36th International Conference of the Chilean Computer Science Society (SCCC) (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/8405137

Kitchenham, B. (2004). "Procedures for performing systematic reviews". Keele University, 33(1), 1-26.

Kurose, J. F. & Ross, K. W. (2013). *Computer networking: a top-down approach: international edition*. Pearson Higher Ed.(6th ed.)

Leiva Díaz, R. (2020). *Propuesta de migración del protocolo de comunicación en la Universidad Adventista de Chile*. https://dspace.um.edu.mx/bitstream/handle/20.500.11972/1355/tesis%20 de%20maestr%c3%8da%20en%20ciencias%20computacional es%20de%20rodrigo%20enrique%20leiva%20d%c3%8daz.pdf?sequence=1

Marrafon, G. & García, R. (2017). "IPv6: uma tecnologia atual no mundo". *Etic-Encontro de Iniciação Científica*, ISSN 21-76-8498, 13(13). http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/6390

Padmanabhan, R., Rula, J. P., Richter, P., Strowes, S. D. & Dainotti, A. (2020, November). "DynamIPs: Analyzing address assignment practices in IPv4 and IPv6". In Proceedings of the 16th International Conference on emerging Networking Experiments and Technologies (pp. 55-70). https://dl.acm.org/doi/abs/10.1145/3386367.3431314

Pensky Markowicz, G. (2021). *Implementación de IPv6: ¿un desafío de innovación para los ISP en Uruguay?* https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/31053

Pérez, F. & Olmos, J. (2022). *Transición y/o migración a IPv6 con FORTINET*. Días Virtuales/IPv6/2022.

Rehman, S. U. & Manickam, S. (2015). "Significance of duplicate address detection mechanism in IPv6 and its security issues: A survey". *Indian Journal of Science and Technology*, 8(30).

Ribeiro, D. L., Tiosso, F. & Reis, H. (2022). "Transição do IPv4 para o IPv6". *Revista Interface Tecnológica*, 19(2), 117-128. https://revista.fatectq.edu.br/interfacetecnologica/article/view/1471

Rodríguez Amaguay, X. D & Tejada Zúñiga, C. E. (2018). *Elaborar un plan de acción para la implementación de IPv6 en el Ecuador y fomentar su uso* (Bachelor's thesis, Espol). https://www.dspace.espol.edu.ec/handle/123456789/42355

Sánchez, E., Gamarra, Á. I. & Arias Figueroa, D. (2022). "Estudio de la implementación del protocolo de Internet versión 6 en el ámbito regional y su impacto en los usuarios finales". In XXIV Workshop de Investigadores en Ciencias de la Computación (WICC 2022, Mendoza). http://sedici.unlp.edu.ar/handle/10915/143285

Tanenbaum, A. & Wetherall, D. (2011). *Computer Networks* (5th ed.). Pearson.

Tatipamula, M., Grossetete, P. & Esaki, H. (2004). "IPv6 integration and coexistence strategies for next-generation networks". *IEEE Communications Magazine*, 42(1), 88-96.

Twum, F., Asante, K. & Asante, M. (2016). "Implementation of Network Services on IPv6 Networks". *International Journal of Computer Applications*, 975, 8887.

Ubiedo, L., O'Hara, T., Erquiaga, M. J. & García, S. (2021). *Current state of IPv6 security in IoT*. arXiv preprint arXiv:2105.02710. https://arxiv.org/abs/2105.02710

Varela, F. V. (2021). *IPv6, una realidad*. Ediciones de la U. https://books.google.com.mx/books?hl=es&lr=&id=2eAZEAAAQBAJ&oi=fnd &pg=PA6&dq=IPV6+transicion+chilena&ots=F68c7GLvD5&sig=rjQKZprSeL EUhKPoq-1gPEw2WLgc#v=onepage&q=IPV6%20transicion%20chilena&f=f alse

Viera Barlocco, L. & Riccardi Pugliesi, B. (2019). *Sistema de distribución multicast mediante redes definidas por software*. https://dspace.ort.edu.uy/handle/20.500.11968/4112

Zhang, R. & Bartell, M. (2003). *BGP design and implementation*. Cisco Press.

Conclusiones generales por capítulo

Los países de América del Sur, para lograr mantener su conectividad, deben alinearse en la transición a las direcciones IPv6 de manera que implementen políticas y estrategias públicas con el objetivo de ser competitivos y lograr minimizar la brecha digital desde cada una de las regiones; por ello, las alianzas entre países deben ser fundamentales, permitiendo la adaptabilidad de las nuevas tecnologías y de servicios en entornos público-privados.

Por lo anterior, el Grupo de Investigación en Ingeniería de Sistemas GIIS, adscrito a la Fundación Universitaria Compensar, y algunos investigadores invitados han puesto a disposición de la comunidad académica la primera edición del libro titulado *Explorando el universo IPv6: para la innovación de un mundo interconectado*, con el fin de compartir los resultados finales de una investigación científico-tecnológica articulada con el sector empresarial, fortaleciendo el vínculo entre la Academia y el sector empresarial en su entorno ciudad-región, respondiendo a las nuevas necesidades de implementar soluciones tecnológicas como factor dinamizador en la sociedad.

Como conclusión articulada en cada uno de los capítulos, se pueden desglosar análisis significativos desde cada una de las miradas de los capítulos, así:

Para el capítulo uno, es importante considerar las implicaciones económicas y tecnológicas, así como los beneficios de su implementación desarrollando estrategias globales que incluyan análisis de negocios y planificación operativa para garantizar una implementación eficiente. Por ello, se debe aumentar la conciencia sobre sus ventajas y desafíos, así como proporcionar una capacitación adecuada a los profesionales de TI y a los usuarios finales para garantizar una gestión eficiente de las redes IPv6.

Los países, las empresas, las instituciones educativas y del Estado que adopten IPv6 pueden obtener ventajas competitivas en el panorama digital global que les permite desarrollar infraestructuras más robustas y preparadas para las futuras demandas de conectividad, lo que mejora la posición económica y

tecnológica en el mercado global, formando profesionales de TI para facilitar la implementación y gestión eficiente de sus infraestructuras.

Finalmente, la implementación de IPv6 es crítica para el desarrollo y la sostenibilidad de la conectividad global en el siglo XXI. Su adopción permitirá el crecimiento exponencial de dispositivos conectados, la automatización de procesos, la mejora de la seguridad informática, el aprovechamiento pleno de tecnologías emergentes y el impulso a la competitividad económica, con el fin de construir una Internet más segura, eficiente y preparada para los desafíos del futuro en desarrollo, innovación e investigación, dadas las nuevas necesidades que ayuden en la ampliación de coberturas de millones de usuarios no conectados.

Como conclusión del capítulo dos, la transición a IPv6 es un proceso necesario debido al agotamiento de direcciones IPv4 y los beneficios potenciales que ofrece IPv6, como un mayor espacio de direcciones y una mejor seguridad. Los estándares RFC desempeñan un papel fundamental en la transición a IPv6, proporcionando directrices y especificaciones técnicas para la implementación y el funcionamiento de IPv6 en redes. Los mecanismos de transición más comunes mencionados en los estándares RFC incluyen Dual Stack, Tunneling y Translation, que permiten una coexistencia gradual de IPv4 e IPv6 en las redes.

Los estándares RFC proporcionan recomendaciones y mejores prácticas para abordar las preocupaciones de seguridad asociadas. La implementación exitosa de IPv6 requiere una planificación cuidadosa, colaboración entre diferentes partes interesadas y la adopción de estándares RFC relevantes. Existen desafíos y barreras para la adopción de IPv6, como la falta de conciencia, los costos asociados y las preocupaciones de compatibilidad. Sin embargo, se espera que la creciente necesidad de direcciones IP y el aumento de la conectividad impulsen su adopción.

Respecto del capítulo tres, su gran conclusión es validar los importantes desafíos en términos de seguridad hacia la transición a las direcciones IPv6. Su adopción de este nuevo protocolo de Internet amplía el espacio de direcciones y brinda diversas ventajas, pero también introduce vulnerabilidades que deben abordarse adecuadamente. El framework IPSec se destaca como una solución efectiva para garantizar la seguridad en las comunicaciones basadas en IPv6. Proporciona mecanismos de autenticación, confidencialidad, integridad y disponibilidad a través de la implementación de diferentes protocolos y servicios de seguridad. La autenticación es esencial para garantizar que las comunicaciones en IPv6 sean realizadas por entidades legítimas. IPSec ofrece mecanismos sólidos de autenticación, como el uso de claves criptográficas

y certificados digitales, para verificar la identidad de los participantes en las comunicaciones.

La confidencialidad es otro aspecto crítico en la seguridad de las comunicaciones. IPSec proporciona mecanismos de cifrado de datos para proteger la información sensible que se transmite a través de las direcciones IPv6, evitando su interceptación y lectura no autorizada.

La integridad de los datos también es esencial para detectar modificaciones no autorizadas durante la transmisión. IPSec utiliza funciones criptográficas para garantizar que los datos no sean alterados en tránsito, lo que proporciona una capa adicional de seguridad.

La disponibilidad de los servicios y aplicaciones en IPv6 es crítica para garantizar un funcionamiento continuo. IPSec permite la implementación de políticas de control de acceso y protección contra ataques de denegación de servicio, contribuyendo a mantener la disponibilidad de los recursos de red.

Finalmente, la implementación de marcos y estándares de seguridad, como los basados en ISO y en la gobernanza de TI, puede contribuir a mejorar la seguridad de las direcciones IPv6. Estos marcos proporcionan pautas y mejores prácticas para la gestión de riesgos y la implementación de medidas de seguridad. La auditoría de TI y la comparación de guías de seguridad son herramientas útiles para evaluar y mejorar la seguridad en estos entornos. La comprensión de las similitudes y diferencias entre las guías de auditoría de TI puede ayudar a establecer prácticas sólidas de seguridad que se pueden implementar de manera escalonada garantizando la correcta operación de los servicios actuales y futuros de las organizaciones en todos los sectores de la economía.

Como conclusión del capítulo cuatro, la transición a IPv6 presenta desafíos, como la necesidad de inversiones en infraestructura y actualización de equipos, la compatibilidad con sistemas y aplicaciones heredadas y la capacitación de personal técnico; por ello, para lograr una transición exitosa, es fundamental implementar estrategias adecuadas, que incluyan la planificación y definición de objetivos claros, la identificación de los sectores de mayor aplicación y su involucramiento activo, el desarrollo de planes de acción detallados y el establecimiento de acciones focalizadas por parte de los ISP y el Gobierno.

Brasil ha sido líder en la implementación de políticas públicas para fomentar la adopción de IPv6. A través de iniciativas de capacitación y concientización, se han establecido plazos para la adopción de IPv6 en los servicios gubernamentales y promovido la colaboración entre los sectores público y privado.

Argentina también ha adoptado políticas públicas para impulsar la transición a IPv6 y la publicación de resoluciones y guías técnicas, ha promovido la adopción de IPv6 en diferentes sectores y ha fomentado la colaboración entre actores clave, a nivel de los ISP en las redes de transporte.

En Perú, se ha avanzado en la implementación de políticas públicas para la transición a IPv6 con el objetivo de promover la adopción de IPv6 en las instituciones públicas y fomentar la colaboración con los proveedores de servicios de Internet, que permitan la actualización de tecnología vía redes ópticas.

En Colombia, se han implementado políticas públicas para la transición a IPv6. A través de resoluciones y guías técnicas, el Gobierno, a través de MinTIC y Renata, ha promovido la adopción de IPv6 en el sector público y ha establecido plazos para su implementación.

Chile ha trabajado en la promoción de IPv6 a través de iniciativas como la implementación de planes de acción y la participación en proyectos regionales e internacionales. Sin embargo, es necesario un mayor impulso en su adopción, especialmente en los sectores gubernamentales y empresariales, que se articulen con los ISP, que poco impulsan la transición.

Ecuador ha realizado esfuerzos significativos para fortalecer el protocolo IPv6. Se han implementado políticas y acciones focalizadas por el Gobierno, así como estrategias de transición y planes de acción para fomentar su adopción. Sin embargo, aún existen desafíos en términos de concientización y capacitación.

Uruguay ha demostrado un compromiso con la adopción de IPv6, promoviendo su implementación en diferentes sectores. El país ha desarrollado planes de acción y estrategias para la transición, involucrando tanto a los ISP como al Gobierno en la promoción de IPv6. Aunque se han logrado avances, se requiere un mayor impulso para su adopción generalizada.

Venezuela ha tomado medidas para fortalecer el protocolo IPv6, como la implementación de políticas públicas y la participación en proyectos de investigación. Sin embargo, la adopción de IPv6 en el país aún enfrenta desafíos significativos debido a limitaciones técnicas, de infraestructura y dados los problemas económicos que dificultan la transición.

Paraguay ha mostrado un compromiso con la adopción de IPv6, estableciendo planes de acción y promoviendo la concientización en diferentes sectores. Aunque se han logrado avances, es necesario continuar promoviendo la capacitación y la colaboración entre los actores clave para una adopción más amplia.

Bolivia carece de una política pública claramente definida, pero los operadores locales fortalecen su infraestructura para mantener competitivos los servicios telemáticos, articulados en planes de acción y la participación en proyectos regionales.

Finalmente, la adopción de IPv6 es estratégica para cada país, dados los planes de sus agendas y gobernanzas digitales según su propio contexto y desafíos específicos en relación con la transición. Aunque algunos países han avanzado más que otros, todos comparten que el objetivo común de garantizar una conectividad sostenible y exitosa en la región a través de la adopción de IPv6 es y será clave. La colaboración y el intercambio de experiencias entre los países pueden ser fundamentales para superar los desafíos restantes y lograr una implementación exitosa de IPv6 en toda América del Sur.

Como conclusión para el capítulo cinco, es fundamental, para los ISP, que la región incentive políticas de alto impacto como marco de una estrategia legislativa integral, que mediante una gobernanza permita la masificación del protocolo IPv6 en respuesta a las necesidades del contexto actual que dinamicen el crecimiento de internet y de toda su infraestructura telemática hacia un modelo gradual, procedimental, fácil, sencillo y no se vea como un problema, por lo tanto, la capacitación en el campo de la transición a IPv6 debe generar confianza para su implementación como plan estratégico de manera pausada pero segura sin ningún tipo de contratiempos hacia una migración definitiva que les permita una mayor disponibilidad, integridad y confidencialidad que el protocolo antecesor.

Es inminente que la transición a IPv6, específicamente en las capas 2 y 3, será el motor que impulse esta migración, aunque para llegar al 100 % tardará por lo menos entre 10-20 años en América del Sur, dado que se requiere de una actualización tecnológica costosa y de una planeación estratégica, articulado esto con estándares ISO, COBIT, ITIL, OWASPP e IPSec que les permitan su escalabilidad en las empresas y en los ISP hacia la integración articulada y práctica de la tecnologías presentes y futuras, articulando factores como políticas de seguridad, implementación de QoS, movilidad, el uso de las redes, las buenas prácticas asociadas a la difusión de la información, así como los costos de los activos informáticos y tecnológicos actuales.

La investigación destaca que las empresas público-privadas son escépticas en la transición a IPv6 dado que los ISP van muy lentos hacia la migración y continúan con IPv4; por ello, el mundo y América del Sur aún se mueven sobre el protocolo anterior. Esto hará más lenta la migración a IPv6; por ello, se requiere que los ISP y los clientes finales implementen soluciones duales, dado que es

crucial para garantizar la continuidad y crecimiento de las telecomunicaciones en la región, además de colaborar con otros países y organizaciones para compartir buenas prácticas y experiencias en la transición, que promuevan la investigación y el desarrollo de tecnologías y soluciones bajo IPv6, para sectores como educación, economía y la industria en general.

En la actualidad y a nivel mundial, nos encontramos en un periodo de transición de las direcciones o del protocolo IPv4 al protocolo IPv6, siendo fundamental para Suramérica el fortalecimiento de su infraestructura de telecomunicaciones y de actualización de sus servicios tecnológicos por parte de los diferentes proveedores de internet y de todos los sectores de la economía, para la adaptación rápida a este nuevo protocolo que permita la integración a las nuevas tecnologías disruptivas y convergentes.

Es así que la Facultad de Ingeniería de la Fundación Universitaria Compensar, dentro del proyecto educativo institucional articulado con el sector empresarial, apoya la dinámica de las organizaciones público-privadas en la transición hacia el protocolo IPv6, además de la generación de proyectos de investigación e innovación sobre el desarrollo e investigación de la industria; por ello, sus investigadores apoyan fuertemente el currículo académico de los 6 programas de pregrado (Ingeniería de Sistemas, Ingeniería de Telecomunicaciones, Ingeniería de Software, Ingeniería Industrial, Ingeniería Multimedia y Ciencias de Datos) y sus 2 programas de posgrado (especialización en Seguridad Informática y especialización en Big Data). Además de ello, van a la vanguardia de las nuevas necesidades de la industria 4.0 y 5.0, proponiendo a los lectores de este libro 5 capítulos de alto impacto y articulados con sus aliados estratégicos hacia el sector productivo.

compensar | fundación universitaria

ISBN: 978-958-792-657-6