

Análisis y desarrollo del protocolo IPV6 en la red de datos de la Defensoría del Pueblo regional Cesar

Analysis and development of the ipv6 protocol in the data network of the Cesar Regional Ombudsman's Office

Jorge Carlo Jiménez Paredes¹

Iván Camilo Nieto Sánchez²

July Natalia Mora Alfonso³

Néstor Javier Rodríguez García⁴

Universidad Nacional Abierta y a Distancia, Colombia

Resumen

A continuación, se presentan los resultados de la investigación desarrollada para la migración hacia IPv6 en la Defensoría del Pueblo – Regional Cesar, a partir de las fases I y II de la guía del Ministerio de Tecnologías de la Información y las Comunicaciones denominada “Guía de transición de IPv4 a IPv6 para Colombia”. Lo anterior, obedece al agotamiento de las direcciones IPv4 establecido por los Registros Regionales de Internet (RIR), el Centro de Información de Redes de Asia Pacífico (APNIC), el Centro de Coordinación de Redes IP de Europa (RIPE NCC), entre otras, que lleva a las organizaciones a realizar dicha transición para no quedar sin operatividad representada en agotamiento de direcciones para nuevos dispositivos, problemas de compatibilidad con aplicaciones y soluciones de IPv6 nativas, problemas de seguridad asociados a políticas, complejidad en la administración, y otras más que afectan su crecimiento; por lo tanto, al desarrollar la Fase I se identifica el nivel de preparación de la entidad para realizar la migración al protocolo

¹ Ingeniero de Sistemas UNAD, <https://orcid.org/0000-0002-7498-7448> / jcjimenezpa@unadvirtual.edu.co

² Ingeniero electrónico, especialista en Pedagogía para el Desarrollo del Aprendizaje Autónomo, magíster en Ingeniería Electrónica UNAD, <https://orcid.org/0000-0003-2679-7487> / ivan.nieto@unad.edu.co

³ Ingeniera electrónica, especialista en Educación Superior a Distancia, magíster en Sistemas integrados de Gestión, magíster en Tecnología de Información UNAD, <https://orcid.org/0000-0003-0876-1122> / july.mora@unad.edu.co

⁴ Ingeniero electrónico, especialista en Educación Superior a Distancia, magíster en Ciencias de la información y las comunicaciones con énfasis en teleinformática UNAD, <https://orcid.org/0000-0002-5489-4594> / nestor.rodriguez@unad.edu.co

de Internet IPv6, determinado a través de un plan de diagnóstico el porcentaje de compatibilidad de hardware y software, y de esta manera especificar cuáles equipos y servicios deben reemplazarse y/o actualizarse antes de iniciar con el proceso; posteriormente en la Fase II se habilita el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la primera fase y también se configuran los servicios sobre IPv6 de DNS, DHCP, Seguridad, VPN, servicios web, entre otros y de esta manera se valida su funcionalidad y operatividad. Adicionalmente, es necesario coordinar con la ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.

Palabras clave: aplicación de telecomunicaciones, tecnología de información, telemática, transferencia tecnológica, transmisión de datos.

Abstract

The following presents the results of the research conducted on the migration to IPv6 at the Ombudsman's Office – Cesar Regional Office, based on Phases I and II of the Ministry of Information and Communication Technologies' "IPv4 to IPv6 Transition Guide for Colombia." This initiative is driven by the depletion of IPv4 address space, as declared by the Regional Internet Registries (RIR), the Asia-Pacific Network Information Centre (APNIC), and the Réseaux IP Européens Network Coordination Centre (RIPE NCC), among others. Such scarcity compels organizations to adopt IPv6 to maintain operational continuity and to avoid issues such as the exhaustion of addresses for new devices, incompatibility with native IPv6 applications and services, security vulnerabilities linked to policy limitations, increased administrative complexity, and other constraints that hinder organizational growth. Accordingly, during Phase I, the readiness level of the institution for IPv6 migration was assessed. A diagnostic plan was executed to determine hardware and software compatibility rates, thereby identifying which devices and services required replacement and/or upgrades prior to initiating the migration process. In Phase II, IPv6 addressing was enabled for all hardware and software components in accordance with the Phase I diagnostic plan. Additionally, IPv6-based services were configured—including DNS, DHCP, Security, VPN, and Web services, among others—to validate their functionality and operational performance. Furthermore, coordination with the Internet Service Provider (ISP) is required to

establish IPv6 routing and ensure comprehensive external IPv6 connectivity.

Keywords: Data transmission, information technology, technology transfer, telecommunications applications, telematics.

1. Introducción

En la actualidad, las redes de datos son de vital importancia en la cotidianidad del ser humano, siendo un componente esencial para su trabajo, estudio, crear comunidades virtuales con intereses propios, comunicarse en diferentes contextos, fines médicos o científicos, y muchos más. Bajo ese contexto, la necesidad de estar conectados y tener acceso continuo a Internet facilita las acciones de la cotidianidad, como por ejemplo compras en línea a nivel nacional e internacional, formación académica, investigación y desarrollo, entre otros que sin duda alguna contribuyen al bienestar de la humanidad.

Para ello, es necesario que las redes de telecomunicaciones funcionen de la manera esperada, facilitando la comunicación entre origen y el destino, por lo tanto, se requiere de un protocolo que así lo establezca. En ese sentido, IPv4 desde hace más de 3 décadas se viene desempeñando de forma correcta, sin embargo, su capacidad se ha visto limitada por el crecimiento exponencial de equipos que requieren una dirección IP para conectarse y comunicarse con otros dispositivos. Para superar este inconveniente se crea IPv6 como solución, es decir, básicamente pasamos de tener una capacidad de 4.300 millones a 670.000 billones de nuevas direcciones IP.

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, es la entidad encargada de regular la adopción del protocolo IPv6. Para lo cual ha establecido la *Guía de transición de IPv4 a IPv6 para Colombia* que tiene por objetivo principal:

Presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6 en el país (MinTIC, 2017, p. 12).

También, para acompañar este proceso se tiene en cuenta el método *Dual stack* o *pila doble* para tener una transición suave hacia IPv6, y se utilizó un software de simulación como herramienta de apoyo para probar las configuraciones de equipos e interfaces que hacen parte de la red de datos.

Como resultado, se propuso un plan de transición armonizado con la Defensoría del Pueblo Regional Cesar, y se plantea a futuro replicar esta solución a las diferentes regionales de esta institución en el país.

2. Metodología

Esta investigación se realizó bajo una metodología cuantitativa de orden descriptiva, con el fin de caracterizar los parámetros más adecuados de conformidad con la guía de MinTIC para brindar una alternativa adecuada que facilite la migración hacia IPv6 sin generar impactos significativos dentro de la organización. Para ello, la guía menciona 2 fases:

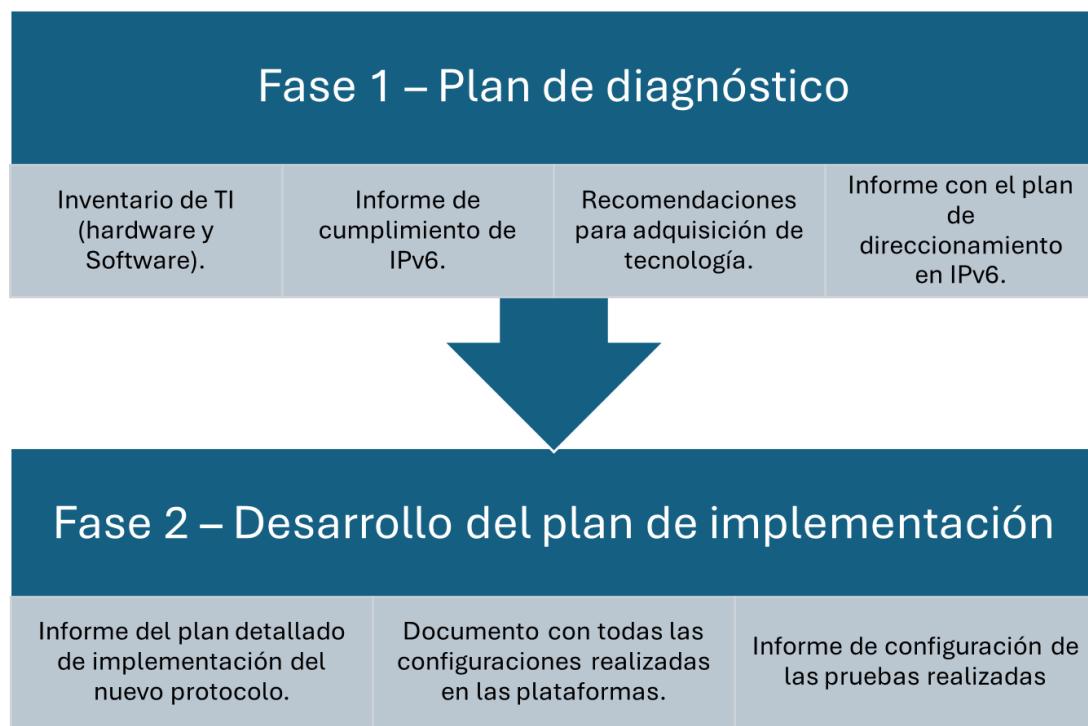


Figura 1. Fases de la Guía de transición de IPv4 a IPv6 para Colombia.

Como lo establece la **iError! No se encuentra el origen de la referencia.**, la Fase 1, se inició con un diagnóstico de la situación actual

de las instalaciones de la Defensoría del Pueblo Regional Cesar, con el ánimo de establecer las necesidades y recomendaciones desde el punto de vista tecnológico para adquirir la tecnología necesaria para que dicha transición se lleve a cabo; posteriormente, en la Fase 2 se realizó una propuesta para ejecutar esta implementación, donde se muestre que la transición es viable desde el punto de vista físico, tecnológico y financiero.

Por otra parte, como estrategia se usó el método Dual stack o pila doble para tener una transición suave hacia IPv6. (Portal IPv6 - LACNIC, s.f). Es decir, la pila doble se utiliza para “rescatar” la IPv4 y de esta manera conectarla con el IPv6. (What is IPv4/IPv6 Dual Stack?, s.f)

3. Resultados

Desde la Fase 1 del plan de migración, se determinó que en la Defensoría del Pueblo Regional Cesar tanto los equipos de comunicación y de cómputo, así como los dispositivos de aplicaciones y servidores cumplen con el soporte del protocolo de comunicaciones IPv6 en un 89 % (ver **iError! No se encuentra el origen de la referencia.**).

Soporte Ipv6 - Defensoría del Pueblo Regional Cesar

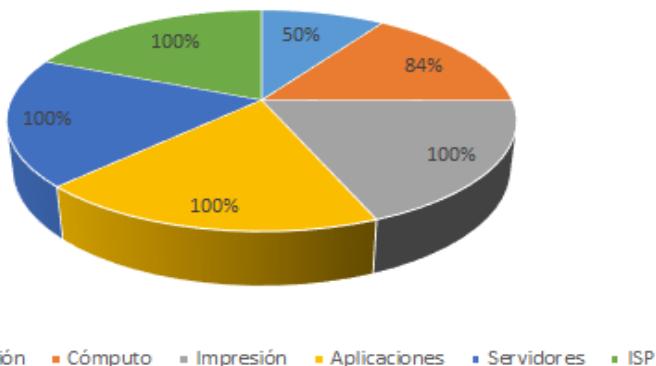


Figura 2. Soporte IP de los dispositivos en la Defensoría del Pueblo Regional Cesar.

En cuanto a la topología actual de la red de datos se tiene:

3.1 Topología en estrella

Red en la cual las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se han de hacer necesariamente a través de él. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí (Molina, s.f.). La topología de red utilizada en la red de datos de la Defensoría del Pueblo – Regional Cesar es en estrella extendida. Es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella (Cisco Networking Academy Program, 2003).

En ese sentido, la **!Error! No se encuentra el origen de la referencia.** muestra la topología actual de la red de datos de la Defensoría del Pueblo Regional Cesar.

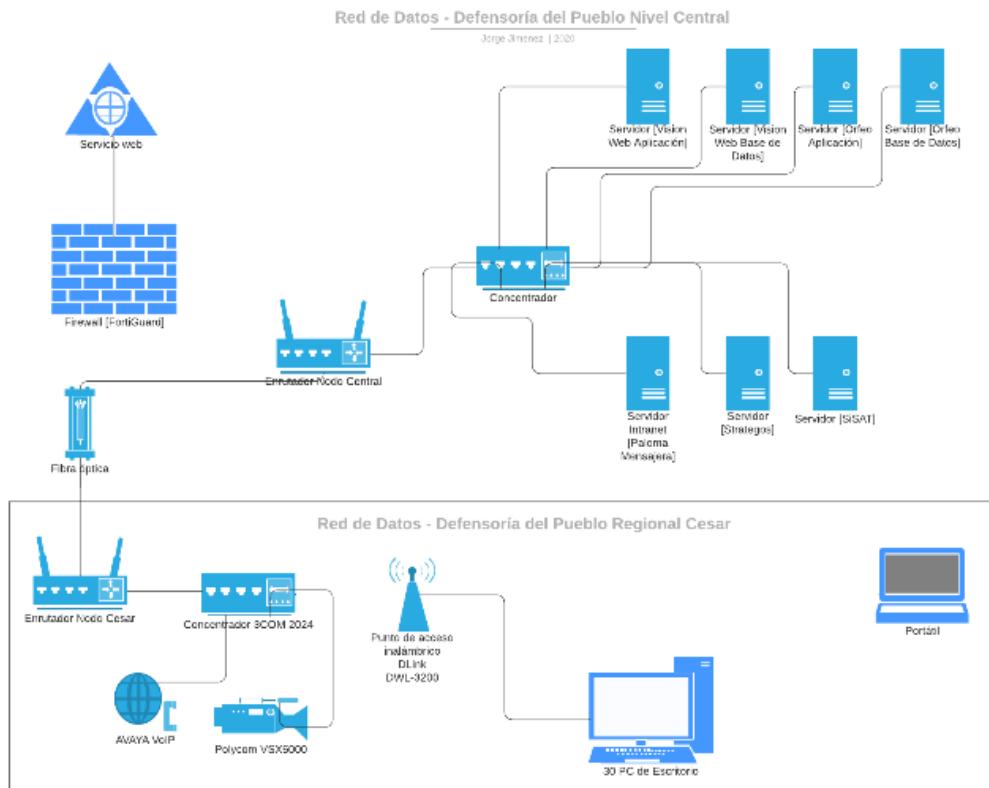


Figura 3. topología actual de la red de datos de la Defensoría del Pueblo Regional Cesar.

En la actualidad, el funcionamiento de la red de datos implica la conexión del segmento de red IPv4 192.168.40.XXX al nodo principal en

el Nivel Central, en la ciudad de Bogotá a través de un canal dedicado con la última milla en fibra óptica que nos brinda la ISP y luego se accede a Internet. En el caso; por ejemplo, de un equipo conectado por medio de una tarjeta de red inalámbrica, la ruta a seguir es:

Usuario → Punto de acceso → Switch → Router (nodo Cesar) → Router (nodo Central) → Switch (Nivel Central) → Firewall → Internet.

Las direcciones IP de la entidad son fijas o estáticas, pero sin una adecuada segmentación.

Se recomienda segmentar la red y establecer subredes acordes a las áreas misionales y la parte administrativa. Teniendo en cuenta para ello lo indicado en el RFC 4291, es decir, que las subredes cuenten con máscara /64.

El diagrama de red a emplear se evidencia a través de la **iError! No se encuentra el origen de la referencia.**, teniendo presente una cantidad N de sedes que acceden al nodo principal y a su vez al servicio de Internet; el cual, debería ser de tipo /48.

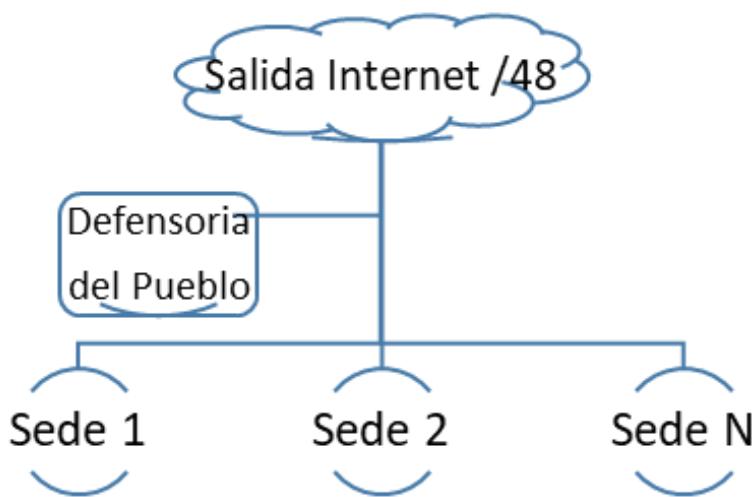


Figura 4. Diagrama de red, TO BE.

Teniendo en cuenta que luego de la adquisición de la membresía y el pago del costo anual de administración a LANIC (Registro de Direcciones de Internet para América Latina y el Caribe) el segmento asignado es, por ejemplo:

Prefijo **2801 : ab12 : abcd**

Certificado del prefijo expedido por LACNIC:

[2001:ab12:abcd /48]

La Tabla 1 presenta la asignación de segmentos de red teniendo en cuenta el prefijo de ejemplo que asigna LACNIC a Nivel Central y en la sede de la Regional Cesar.

Tabla 1. Direccionamiento IPv6

Segmento												Asignación				
2801	:	ab12	:	abcd	:	1000	:	0	:	0	:	0	:	0	/ 48	Salida a Internet
2801	:	ab12	:	abcd	:	1000	:	0	:	0	:	0	:	0	/ 52	Sede Nivel Central
2801	:	ab12	:	abcd	:	1000	:	0	:	0	:	0	:	0	/ 64	Subred Reservada
2801	:	ab12	:	abcd	:	1001	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 1
2801	:	ab12	:	abcd	:	1002	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 2
2801	:	ab12	:	abcd	:	1003	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 3
2801	:	ab12	:	abcd	:	1004	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 4
2801	:	ab12	:	abcd	:	1005	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 5
2801	:	ab12	:	abcd	:	1006	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 6
2801	:	ab12	:	abcd	:	1007	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 7
2801	:	ab12	:	abcd	:	1008	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 8
2801	:	ab12	:	abcd	:	1009	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 9
2801	:	ab12	:	abcd	:	2000	:	0	:	0	:	0	:	0	/ 52	Sede Regional Cesar
2801	:	ab12	:	abcd	:	2000	:	0	:	0	:	0	:	0	/ 64	Subred Reservada
2801	:	ab12	:	abcd	:	2001	:	0	:	0	:	0	:	0	/ 64	Subred Piso No. 1

Posteriormente la Fase 2 del plan de transición resultó con el diseño y la simulación de la red de datos, así como la comunicación entre el nodo central y la Regional Cesar XXXXX, utilizando para ello el programa denominado Cisco Packet Tracer que es un software propiedad de Cisco

System, Inc.®, diseñado para la simulación de redes basadas en los equipos de la citada compañía.

En esta fase se realizaron pruebas para evidenciar el funcionamiento de la red bajo el direccionamiento IPv6. La primera de ellas consistió en realizar una configuración manual en un usuario específico con una IP estática tanto en IPv4 como en IPv6, y posteriormente se comprobó a través de una instrucción “ping”, encontrando respuesta en cada una de las configuraciones; posteriormente se replicó la prueba, pero esta vez usando el puerto WLAN del computador, encontrando respuesta satisfactoria tanto en IPv4 como en IPv6. Finalmente, se realizó una prueba donde se configura únicamente la conexión estática a través de una IPv4 sin necesidad de utilizar la ventana de IPv6 como se evidencia en la **iError! No se encuentra el origen de la referencia..**

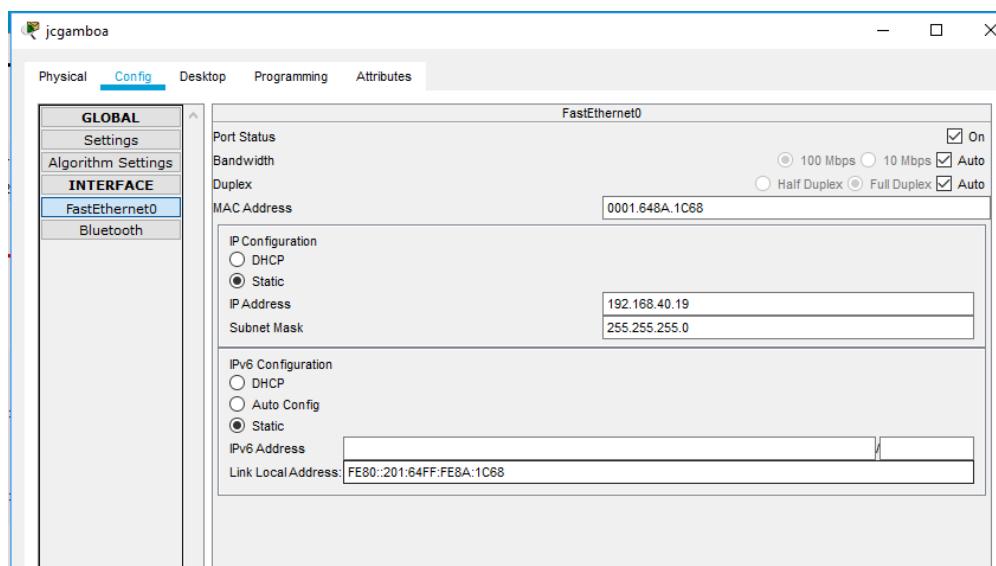


Figura 5. Configuración de host únicamente con la IPv4 estática en un puerto LAN.

Como respuesta, la prueba de “ping” indicó que existe comunicación entre el Pc y el servidor SiSAT utilizando únicamente la dirección IPv4 asignada,

es decir, que la configuración realizada a cada uno de los routers funciona como “doble pila” de manera correcta.

La prueba de “ping” al servidor del aplicativo misional SiSAT, con dirección IPv6 2801:ab12:abcd:1001:0:0:0:4 resulta fallida, pues este Pc no tiene la configuración requerida para dicho acceso a través de IPv6.

4. Conclusiones

En lo que respecta al “Análisis de la nueva topología de la infraestructura actual y su funcionamiento”, se puede concluir que la red de datos estaría organizada con una jerarquía clara, con suficientes direcciones IPv6 disponibles para futuras necesidades y el crecimiento de la entidad.

A través de la “Validación del estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes”, se logró verificar que los servidores y sistemas de cómputo de la institución son compatibles con el nuevo protocolo; y aplicando, los documentos de referencia (RFC) pertinentes para especificar las acciones adecuadas, como lo es el número 6177, el cual recomienda solicitar de manera directa a LANIC el segmento de direcciones, la entidad asegura la transición al nuevo protocolo.

En relación a la Fase II, se sugiere; en el momento de realizar la “Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros”, simular el comportamiento de la red de comunicaciones, ya que al agregar carga, servicios y usuarios finales tanto internos como externos, mediante las pruebas realizadas sobre el procedimiento de IPv6; usando la metodología en doble pila, se logra obtener la configuración adecuada para cada elemento de la interfaz de red. Así mismo se puede supervisar dicho comportamiento de la red.

La elaboración del plan de trabajo sirve como un prototipo para la implementación en la entidad, sugiriendo actividades específicas, utilizando para ello metodologías de levantamiento de información, diagnóstico y determinación de actividades previas.

La planeación adecuada de la transición entre protocolos garantiza el éxito de esta, es por ello por lo que se debe capacitar al personal de TI de la entidad, así como involucrar a la alta gerencia para que entienda y apoye el proyecto de cambio de protocolo.

Con la transición al protocolo IPv6 en la red de datos de la Defensoría del Pueblo Regional Cesar, se consigue el mejoramiento de la conectividad entre equipos y servicios, impactando directamente en la productividad de los servidores públicos y en la calidad de la atención a sus usuarios. En ese sentido, IPv6 como tendencia disruptiva permitirá migrar al Internet de las Cosas y su aplicación hará que el hombre se encuentre conectado en todo momento.

Referencias

- Arafat, M., Ahmed, F. & Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment. *International Journal of Computer Networks & Communications (IJCNC)*, 6(2), 111-126.
- Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera, C., Palet, J., Rocha, M., & Vives A. *IPv6 para todos Guía de uso y aplicación para diversos entornos*. Internet Society.
<http://www.ipv6tf.org/pdf/ipv6paratodos.pdf>
- Cisco (2019). *6lab - The place to monitor IPv6 adoption*.
<https://6lab.cisco.com/index.php>
- Cisco (s.f.). Monitor adopción de IPv6 de Cisco.
<http://6lab.cisco.com/stats/>
- Defensoría del Pueblo. (2018). Organigrama [Figura].
<http://www.defensoria.gov.co/es/public/organigrama>
- Fonseca, D. (2017). *Plan de transición del protocolo de red IPv4 a IPv6 basado en las recomendaciones realizadas por el Min TIC Colombia*. (Tesis de grado). Universidad de Cundinamarca,
<http://fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%20INTEGRADO%20DE%20PLANEACION%20Y%20GESTION/Plan%20de%20Transicion%20del%20Protocolo.pdf>
- NIC México. (s.f.). Mecanismos de transición y RFCs.
<http://www.ipv6.mx/index.php/informacion/rfcs>
- Ministerio de Tecnologías de la Información y las Comunicaciones (2025). ¿Qué es la transición a IPv6?
<http://www.mintic.gov.co/portal/604/w3-article-5893.html>

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.).
Estrategia Gobierno En Línea.
<http://www.mintic.gov.co/portal/604/w3-propertyvalue-7060.html>

Ministerio de Tecnologías de la Información y las Comunicaciones (s.f.).
Resolución 2710 de 2017.
<https://www.mintic.gov.co/portal/604/w3-article-61000.html>

TIC para Servicios - Estrategia GEL. (s.f.).
<http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8011.html>

Vyncke.org. (2019). *Projection of IPv6 %-age of IPv6-Enabled Web Browsers (courtesy Google) in Colombia.* <https://www.vyncke.org/ipv6status/project.php>