



El futuro digital  
es de todos

MinTIC

# Guía 1

Guía de Transición de IPv4 a IPv6 para Colombia

MinTIC – Viceministerio de Transformación Digital  
Dirección de Gobierno Digital  
Abril 2021

# ADOPCIÓN IPv6

- Karen Abudinen Abuchaibe - Ministra de Tecnologías de la Información y las Comunicaciones
- Germán Rueda - Viceministro de Transformación Digital
- Aura María Cifuentes - Directora de Gobierno Digital
- Gersson Jair Castillo Daza – Subdirector de Estándares y Arquitectura de TI
- Fernando Alirio Contreras Sánchez – Equipo IPv6
- Elkin Giovanni Romero Maturana – Equipo IPv6

Versión	Observaciones
1.0.1	Versión inicial del documento
1.0.1	Revisión Jorge Bejarano y Alejandro Becerra
2.0.0	Versión ajustada Fernando Contreras
2.0.1	Versión ajustada Fernando Contreras
2.0.2	Versión ajustada Fernando Contreras
2.0.3	Versión ajustada Fernando Contreras
3.0.0	Versión ajustada Fernando Contreras
4.0.0	Versión ajustada Fernando Contreras
5.0.0	Versión ajustada Equipo IPv6
5.0.1	Erratas y ajustes Equipo IPv6 y Jordi Palet

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:  
[soportecccc@mintic.gov.co](mailto:soportecccc@mintic.gov.co)



Esta guía de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional

# Tabla De Contenido

	<b>PÁG.</b>
1. Derechos de Autor	6
2. Audiencia	7
3. Introducción	8
4. Justificación	10
5. Objetivos Especificos	11
6. Beneficios de la transición	12
7. Fases de transición	14
7.1 Fase I. Planeación de IPv6	14
7.1.1 Entregables de esta Fase	17
7.1.2 Tabla de actividades de la Fase I – Planeación de IPv6	18
7.2 Fase II. Implementación del protocolo IPv6	19
7.2.1 Entregables de esta Fase	20
7.2.2 Tabla de actividades de la Fase II – Implementación de IPv6	21
7.3 Fase III. Pruebas de funcionalidad de IPv6	22
7.3.1 Entregables de esta Fase	22
7.3.2 Tabla de actividades de la Fase III – Pruebas de Funcionalidad de IPv6	22
8. Requerimientos para el proceso de IPv6	24
8.1 Plantillas	25
8.1.1 Modelo de Inventarios de Equipos de Comunicaciones	25
8.1.2 Formato Modelo de Equipos de Cómputo	26
8.1.3 Formato Modelo de Inventario de Aplicaciones de la Entidad	26
8.1.4 Formato Modelo de Inventario de Equipos Servidores de la Entidad	27
8.1.5 Formato Consideraciones de Seguridad	27
9. Lineamientos técnicos en la implementación de IPv6	29
9.1 Servicios	32
9.2 Estructura de Capas de IPv6	32
10. Descripción del plan de trabajo	34
11. Capacitación en IPv6	35
12. Modelo para el proceso de transición	37
13. Fases del proyecto de IPv6	41

14.	Equipo técnico de trabajo IPv6 y porcentaje de dedicación	43
14.1	Dedicación al Proyecto del Equipo de Trabajo	43
15.	Glosario de términos	45
16.	Conclusiones	47
17.	Referencias	48
18.	Bibliografía	50
19.	Anexo 1	51
	Requerimientos de IPv6 para equipos de TIC (LACNOG BCOP 20160127-01)	51
	Best Current Operational Practice (BCOP)	51
18.1	Resumen del BCOP	51
18.2	Trasfondo del BCOP/ Historia	51
18.3	Texto del BCOP	52
18.3.1	Como especificar los requisitos	52
18.3.2	Nota importante para el iniciador de oferta:	53
18.3.3	Texto genérico propuesto para el iniciador de la Licitación	53
18.3.4	Lista de especificaciones técnicas RFC/3GPP obligatorias y opcionales soportadas en variedades de hardware y software	53
18.3.5	IPsec: Obligatorio u opcional	54
18.3.6	Definiciones y descripciones de diferentes tipos de dispositivos	54
18.3.7	Listado de normas RFC/3GPP requeridas para diferentes tipos de hardware	56
18.3.8	Requerimientos para equipo "host"	56
18.3.9	Requerimientos para equipo "enterprise/ISP grade "Layer 2 switch"	57
18.3.10	Requerimientos para equipo "router or Layer 3 switch"	57
18.3.11	Requerimientos para dispositivos móviles	59
18.3.12	Requerimientos para el soporte IPv6 en software	60
18.3.13	Requerimientos de habilidades del integrador de sistemas	61
18.3.14	Declaración de competencia en IPv6	61
20.	Anexo 2	63
19.1	Número de Sistema Autónomo – ASN de IPv6	63
19.2	Administración de políticas de enrutamiento en ASN	63
19.3	Implementación del ASN	64
19.4	Acuerdo de Nivel de Servicio del ASN	64
19.5	BGP (Border Gateway Protocol)	64
19.6	Sistema Autónomo o Número de Sistema Autónomo - ASN	64

# LISTA DE TABLAS

PÁG.

Tabla 1. Actividades de la Fase I.....	<u>18</u>
Tabla 2. Actividades de la Fase II.....	<u>21</u>
Tabla 3. Actividades de la fase III.....	<u>23</u>
Tabla 4. Estructura de Capas de IPv6 .....	<u>31</u>
Tabla 5. Modelo de Procesos de Transición.....	<u>37</u>
Tabla 6. Fases del Proyecto de IPv6.....	<u>40</u>
Tabla 7. Dedicación del Equipo de Trabajo.....	<u>42</u>

# 1. Derechos de Autor

Todas las referencias a los documentos de adopción del protocolo IPv6, cuentan con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Subdirección de Estándares y Arquitectura de Tecnologías de la Información – Dirección de Gobierno Digital.

## 2. Audiencia

Sujetos obligados de las disposiciones contenidas en el Artículo 2 Ámbito de aplicación de la Resolución 2710 de 3 de octubre de 2017, las entidades de que trata el Artículo 2.2.9.1.1.2 del Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que requieran adoptar el protocolo IPv6, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial, la Estrategia de Gobierno Digital y la Subdirección de Estándares y Arquitectura de TI de la Dirección de Gobierno Digital.

# 3. Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En ese orden de ideas, este documento, presenta los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas entidades del Estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país.

Para abordar esta temática se empezará por describir que desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando una mayor demanda de servicios y oportunidades en la red mundial de Internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de Internet que permiten establecer conexiones para cada elemento conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en la actualidad entraron a una fase de agotamiento final, así mismo en el año 1992 la Internet Engineering Task Force IETF<sup>1</sup> a partir de diversos grupos de trabajo, definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo protocolo de conectividad denominado IPv6 o IPng (Next Generation Internet Protocol).

De este modo, el protocolo IPv6, hace posible que todos los dispositivos tecnológicos usados para la conexión a Internet tengan una dirección en IP, la cual facilitará la conectividad en banda ancha, ofreciendo más y mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer oportunidades para el desarrollo tecnológico y la transformación digital a nivel mundial.

Así mismo, para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Resolución 2710 del 3 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.<sup>2</sup>

Para entrar en el proceso de adopción de este nuevo protocolo, las distintas entidades del Estado requieren realizar un inventario de los activos de información, revisar su actual infraestructura de

1 <http://www.ietf.org> - Internet Engineering Task Force

2 Resolución 2710 de 2017: Por la cual se establecen lineamientos para la adopción del protocolo IPv6



computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6 y con base en estas actividades construir el plan de diagnóstico de IPv6, que permita indicar que tan preparada se encuentra la entidad en implementar el nuevo protocolo.

Así mismo, para atender esta necesidad inminente de innovación tecnológica en el país, el MinTIC, mediante este instrumento, desea proyectar los lineamientos para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del estado, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Resolución 2710 de octubre de 2017, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

En todo caso, debe contemplarse, que el objetivo final de esta transición es que toda Internet funcione exclusivamente con IPv6 y la desaparición final de IPv4, manteniendo la coexistencia con ese mientras sea preciso, evitando así costes de nuevas transiciones en el futuro. El IETF ha definido estos mecanismos como "IPv6-only with IPv4aaS" (sólo IPv6 con IPv4 como servicio), permitiendo con ello que, antiguos dispositivos, servicios o aplicaciones que no puedan ser actualizados a IPv6, sigan funcionando de forma transparente con IPv4, aun cuando las redes intermedias sean exclusivamente IPv6, dada la falta de direcciones IPv4.

Finalmente, este mismo documento, será el apoyo al plan guía de acompañamiento, que facilitará las acciones necesarias para la adopción del nuevo protocolo en las entidades del país, partiendo de la fase inicial (Planeación), el cual contiene el plan de diagnóstico de las infraestructuras de TI (Hardware y el Software), hasta la fase intermedia que contempla la implementación y la fase final con las pruebas de funcionalidad del nuevo protocolo.

# 4. Justificación

El Ministerio de las Tecnologías de la Información y las Comunicaciones, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial, la Estrategia de Gobierno Digital y la Subdirección de Estándares y Arquitectura de TI, pone a disposición de las entidades, la siguiente guía, la cual permite a las entidades contar con una línea base para el análisis, desarrollo e implementación del protocolo IPv6, de conformidad con los lineamientos establecidos en la Resolución 2710 de octubre de 2017.

# 5. Objetivos Especificos

Presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las Entidades del Estado 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.

# 6. Beneficios de la transición

Los siguientes puntos representan beneficios a tener presente en un proceso de transición de IPv4 a IPv6, que son importantes tener presente al momento de adoptar el nuevo protocolo con éxito, ellos son:

- La posibilidad de tener un mayor número de equipos de las entidades conectados a la red al ser implementada esta solución.
- Proceso técnicamente transparente para los usuarios de la red de comunicaciones y sus distintos servicios dentro de las entidades.
- La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.
- Mejor control de la seguridad por las características que ofrece el protocolo a nivel de capa de red y en virtud de la arquitectura del nuevo protocolo y sus servicios de cifrado automático.
- Reducción de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores al no implementarse el nuevo protocolo en las entidades.
- Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.
- Gran número de direcciones IP para conexiones a Internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el Internet de las Cosas, las ciudades inteligentes, redes de sensores, blockchain, inteligencia artificial, sistemas de geolocalización entre otras.
- Los Proveedores de Servicio de Internet, tendrán que preparar el proceso de enrutamiento de los prefijos de IPv6, mediante la creación de una troncal o *backbone* con soporte de IPv6 que apoye a los clientes en el enrutamiento de las direcciones IPv6 a fin de garantizar la publicación de servicios y aplicaciones que se consideren pertinentes hacia Internet para todas las entidades del Estado. Ver lineamiento en la Resolución 2710 de 2017<sup>3</sup>

---

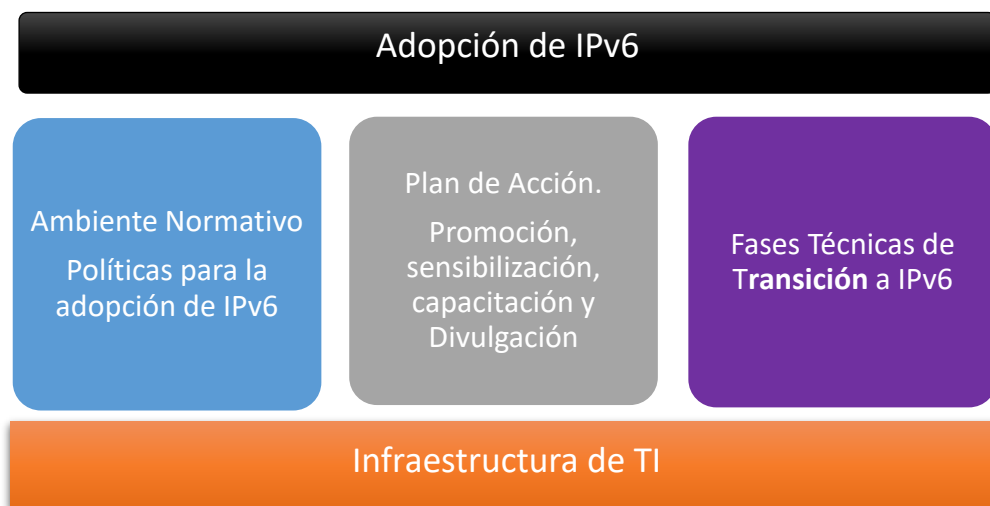
<sup>3</sup> Artículo 2. Ámbito de aplicación, pag.2 de la Resolución 2710 de octubre 3 de 2017

- Para el ciudadano en general, la implementación de IPv6 será un proceso gradual y transparente cuya responsabilidad no será del gobierno, sino directamente del proveedor del servicio de Internet y no deberá generar costos directos.
- Todos los cambios que se realicen deben prever que el futuro es IPv6-only, permitiendo el uso de IPv4aaS (como servicio entre los extremos), de tal forma que cuando no haya tráfico IPv4, eso no suponga costos operacionales o de capital adicionales, y no se requiera una nueva transición para desactivar IPv4.

# 7. Fases de transición

## 7.1 Fase I. Planeación de IPv6

La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con el inventario de activos de información y se consolida con el plan de diagnóstico de las infraestructuras de TI de las Entidades; para ello se recomienda tener en cuenta el modelo de referencia para la adopción de IPv6, de la gráfica 1.



Gráfica 1. Modelo de Referencia para la Adopción de IPv6

Las siguientes son las actividades de esta fase:

- Elaborar y validar el inventario de activos de información de los servicios tecnológicos de las entidades y su interrelación entre ellos, se entiende que la validación de este inventario corresponde a todos aquellos elementos que son susceptibles a tener una dirección IP dentro de los elementos tecnológicos de la entidad. Para esta actividad se requiere tener preparado el inventario de hardware y software, identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6. Para esta etapa se recomienda que para cada elemento del inventario de activos de información se pueda constatar con los fabricantes, y/o los terceros el cumplimiento o no con el nuevo protocolo, para ello se recomienda solicitar hasta donde sea posible una certificación que avale el cumplimiento con el nuevo protocolo en las infraestructuras de TI.

- Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de las entidades del estado con base en lo establecido en el inventario de activos de información; en este documento se recomienda dejar consignado las razones del cumplimiento o no cumplimiento con IPv6 e indicar con fechas y plazos el cumplimiento definitivo del elemento validado. Debe indicar claramente el cumplimiento de IPv6 en modo de doble-pila y de IPv6-only.
- Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en las Entidades; dentro de dicha validación, es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI de las entidades de tal manera que la información recogida de esta tarea, sea insumo para el inicio de la fase II de IPv6.
- Se requiere desarrollar un documento con el plan detallado de la red, en el cual se requiere identificar la topología actual y futura de la red y su funcionamiento dentro de la entidad y con base en esto, proponer el nuevo diseño de red sobre IPv6, tanto con la inclusión de las dos versiones del protocolo IP en aquellas partes de la red que lo requieran (doble-pila), como IPv6-only, en las que no.
- El plan detallado de la red debe contemplar la coexistencia de IPv4 e IPv6, especialmente en las redes de usuarios y otras que lo puedan requerir, así como de IPv6-only en donde se pueda prescindir de IPv4 nativo, a fin de iniciar el proceso de transición de los dos protocolos en la entidad; este documento debe estar basado en el plan de diagnóstico previamente establecido en los anteriores puntos.
- El proceso de transición se planea teniendo en cuenta los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico (Local y/o en la nube), Validación del Servicio de la Central Telefónica, Sistemas Ininterrumpidos de Potencia, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información, Servicios de ambiente colaborativo e IPAM (*IP Address Management*); así mismo se deberán revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC<sup>4</sup> de IPv6.
- Dejar consignadas preferiblemente en el documento plan de diagnóstico, las actividades tendientes a validar el estado actual de los sistemas de información, los sistemas de

<sup>4</sup> RFC: "Request For Comments" Solicitud de Comentarios: para documentar requerimientos técnicos

comunicaciones, los sistemas de almacenamiento y su interacción entre ellos cuando se implemente el protocolo IPv6, tanto en modo doble-pila como IPv6-only.

- Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no pueden soportar IPv6. Dado que IPv6-ready es genérico, es importante detallar los RFC que cada dispositivo debe cumplir, para cumplir correctamente sus funciones de forma segura, dependiendo de su ubicación específica dentro de la red.
- Identificar la configuración y todos los esquemas de seguridad de la red de comunicaciones y sistemas de información.
- Revisar y dejar consignado en el plan de direccionamiento IPv6, las políticas de enrutamiento y las políticas de seguridad y privacidad de IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el firewall respectivo de cada entidad, se recomienda en todo caso revisar los RFC correspondientes a políticas de enrutamiento y seguridad de IPv6, en especial el RFC 7721 y draft-ietf-opsec-v6<sup>5</sup>.
- Definir los mecanismos de asignación de direcciones, teniendo en cuenta características de DHCP, DHCPv6 y SLAAC, y los requerimientos de seguridad y auditoría relacionados con direcciones, y su vinculación con sistemas IPAM, posiblemente relacionados con el DNS y DHCP/DHCPv6.
- Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, equipos de cómputo, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 por cada Entidad.
- Es imprescindible que las pruebas se hagan no sólo desde redes internas o directamente conectadas, sino desde ASNs remotos, contemplando el funcionamiento de usuarios externos tanto con IPv4-only, IPv6-only y doble-pila.
- La ejecución y configuración de las pruebas piloto de IPv6, se deben realizar bajo un proceso metódico que implique inicialmente la creación de una o varias VLAN (Redes de Área Local Virtuales) de prueba, que impactarán sobre el Core de la red. Estas VLAN de prueba deberán incluir diversos equipos y servicios de misión crítica que contemplen entre otros, el análisis del comportamiento de software, el análisis del hardware en cada dispositivo, el análisis y comportamiento de estos en la red de comunicaciones, su comportamiento dentro de los

---

<sup>5</sup> <https://tools.ietf.org/html/rfc7721>



aplicativos de la entidad, el análisis de cada servicio ofrecido y agregación de carga de tráfico de red, teniendo en cuenta que las pruebas realizadas deben estar sujetas a las mejores prácticas y metodologías de transición a IPv6 conservando el criterio técnico de la doble-pila, pero admitiendo y verificando el funcionamiento de dispositivos, aplicaciones y servicios que no puedan ser actualizados a IPv6 (por tanto sean IPv4-only), e incluso de aquellos que puedan ser IPv6-only.

- Una vez se tenga la certeza de que la VLAN de pruebas, ha soportado todo el proceso de pruebas de funcionalidad sobre un ambiente de tráfico controlado, ya será posible propagar este ambiente en toda la red de la entidad y proceder enseguida a las pruebas de funcionalidad, garantizando el funcionamiento del nuevo protocolo en toda la infraestructura de la entidad.
- Preparar una zona controlada para realizar pruebas de funcionalidad del nuevo protocolo IP, teniendo en cuenta en aislar un segmento de red o crear un nuevo segmento de red, el cual debe permitir aceptar cambios y activaciones necesarias para confirmar la funcionalidad de IPv6 sin afectar el ambiente de producción de los usuarios.
- Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el proyecto de transición previo.
- Es necesario preparar a los funcionarios de las Áreas de TI, de conformidad con los planes de capacitación establecidos por cada entidad y establecer la sensibilización a las personas de toda la organización en especial a la Alta Dirección, a fin de dar a conocer el nivel de impacto en la implementación del nuevo protocolo, de conformidad con lo dispuesto en la Resolución 2710 de 2017.
- Las entidades deberán entrar en sincronización y operación con los ISP (Proveedores de Servicios de Internet) y/o los PRST (Proveedores de Redes y Servicios de Telecomunicaciones) con el fin de definir el plan de trabajo que le permita a cada entidad enrutar los prefijos IPv6 sobre una troncal definida previamente por el (los) operador(es), incluso con el uso de BGP cuando haya múltiples proveedores y/o enlaces. Se deberá igualmente permitir el enrutamiento de prefijos de IPv4, incluso con BGP, si fuera el caso.

### *7.1.1 Entregables de esta Fase*

- Plan detallado de trabajo para la adopción de IPv6 en toda la organización.
  - Inventario de TI (Hardware y software) de cada Entidad diagnosticada.

- Plan de diagnóstico de cumplimiento de IPv6 por cada elemento de hardware y software (Red de comunicaciones, sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros), el plan de diagnóstico deberá realizarse con base en los conceptos técnicos de certificación de cumplimiento o no cumplimiento emitidos por los fabricantes de hardware y los terceros que hayan desarrollado software en cada entidad.
  - Recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6 e IPv6-only.
  - Elaboración del plan de direccionamiento en IPv6 (Plan de numeración de IPv6) con base en la topología de la red de comunicaciones de la entidad
  - Plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6 o IPv6-only.
  - Informe de preparación (*Readiness*) de los sistemas de comunicaciones, bases de datos y aplicaciones (Que tan preparada se encuentra la entidad en tema de adopción de IPv6 e IPv6-only).
  - Documento que define los lineamientos de implementación de IPv6 en concordancia con la política de seguridad de información y los controles de seguridad informática de las entidades.
  - Preparación de un plan de contingencias de IPv6.
- Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de las Entidades y plan de sensibilización al total de funcionarios de las Entidades.

### 7.1.2 Tabla de actividades de la Fase I – Planeación de IPv6

Se recomienda a las entidades tener en cuenta la siguiente tabla y diligenciar el tiempo en meses que le lleve desarrollar cada actividad:

Fase I	Actividades Generales	Tiempo en meses de la actividad
<b>Diagnóstico de la Situación Actual</b>	Construcción del plan de Diagnóstico	
	Inventario de TI (Hardware, Software)	
	Análisis de la nueva topología de la infraestructura actual y su funcionamiento	
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de	

	seguridad y coexistencia de los protocolos	
	Planeación de la transición de los servicios tecnológicos de la Entidad. Plan de direccionamiento de IPv6 y plan de contingencia de IPv6	
	Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.	
	Identificación de esquemas de seguridad de la información y las comunicaciones	

*Tabla 1. Actividades de la Fase I*

## 7.2 Fase II. Implementación del protocolo IPv6

La fase de implementación debe cubrir las siguientes actividades:

- Habilitar el plan de direccionamiento IPv6 definido en la Fase I, para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico también definido en la primera Fase del proceso de transición de IPv4 a IPv6, teniendo en cuenta el inventario de los activos de información previo de cada una de las infraestructuras de TI de las Entidades del Estado y teniendo en cuenta el diseño de la red bajo IPv6; todo esto como se ha venido mencionando previamente sobre la base de lo definido en la Fase de Planeación.
- Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs creadas, con un número especial de usuarios que aprovechen la homogeneidad de la red, con servicios de filtrado, los factores críticos en las aplicaciones y servicios, todo esto con el normal funcionamiento de los servicios y aplicaciones de la red.
- Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y

usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en doble-pila e IPv6-only, de conformidad como se ha definido en la Resolución 2710 de 2017; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.

- Aplicar el modelo de transición de IPv6 definido por la Entidad, permitiendo la coexistencia de las aplicaciones, infraestructuras y servicios bajo las dos versiones del protocolo IP, a fin de establecer la modalidad de funcionamiento en doble-pila, garantizando el provisionamiento de mecanismos de transición IPv4-IPv6 para los casos en los que no sea posible el servicio IPv6, y permitiendo al mismo tiempo el acceso cuando sea preciso mediante IPv6-only.
- Aplicar el diseño de la nueva topología de la red con base en los criterios técnicos del nuevo protocolo IPv6 en doble-pila y garantizando la continuidad con IPv6; estas técnicas permiten que tanto los servicios como aplicativos en IPv4 queden funcionando en coexistencia con IPv6 dentro de las Entidades.
- Validar la funcionalidad en IPv6 de los siguientes servicios y aplicaciones de las Entidades sobre IPv6: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servicios Voz sobre IP, Servidores de Monitoreo, Servicios con sistema IPTV, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicios que soporten canales TDT, Servicio de Respaldo, Servicio de Comunicaciones Unificadas, Servicios VPN, Integración entre Sistemas de Información, Sistemas de Almacenamiento, Servicios de Administración de Red, Sistemas en la Nube y Sistema Ininterrumpido de Potencia.
- .
- Activar las políticas de seguridad de IPv6 con modo doble-pila e IPv6-only, en los equipos de seguridad y comunicaciones, por ejemplo, servidores AAA, firewalls, NAC, y equipos perimetrales de conformidad, zonas desmilitarizadas. Al respecto, se recomienda revisar los RFC de seguridad en IPv6, en especial el RFC 7721 y draft-ietf-opsec-v6.
- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer las políticas de enrutamiento del prefijo IPv6 con su propio ASN y establecer la conectividad integral, desde el interior de las redes LAN, hacia el exterior de las redes WAN a fin de garantizar que las entidades puedan generar tráfico de IPv6 en la comunidad de Internet.

### *7.2.1 Entregables de esta Fase*

- Preparación y presentación del Informe del plan detallado de implementación del nuevo protocolo.
- Documentación con todas las configuraciones del nuevo protocolo realizadas en las plataformas

de hardware, software y servicios que se han intervenido durante esta fase, incluyendo las configuraciones realizadas sobre el/(los) canal(les) de comunicaciones con acceso a Internet.

- Informe de configuración de las pruebas pilotos y las definitivas realizadas a nivel de comunicaciones, de aplicaciones y de sistemas de almacenamiento.

### 7.2.2 Tabla de actividades de la Fase II – Implementación de IPv6

Las entidades deberán tener en cuenta la siguiente tabla y diligenciar el tiempo en meses que le lleve desarrollar cada actividad:

Fase II	Actividades Generales	Tiempo en meses de la actividad
<b>Desarrollo del Plan de implementación</b>	Habilitación direccionamiento IPv6 (plan de numeración) para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase.	
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	
	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.	
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	
	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	

Tabla 2. Actividades de la Fase II

## *7.3 Fase III. Pruebas de funcionalidad de IPv6*

Las pruebas de funcionalidad de esta fase deben cubrir las siguientes actividades:

- Realizar las pruebas y monitoreo de funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la Entidad en un ambiente que permita empezar a generar tráfico de IPv6 de la entidad hacia Internet y viceversa.
- Realizar las pruebas de funcionalidad del nuevo protocolo utilizando las políticas de seguridad perimetral, de seguridad en redes locales, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones, equipos de almacenamiento y presentar el informe de las pruebas realizadas.
- Al momento de ejecutar las pruebas de funcionalidad, se debe realizar el afinamiento de las configuraciones de hardware, software y servicios, con base en la información resultante de la fase II.
- Se recomienda elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

### *7.3.1 Entregables de esta Fase*

- Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación.
- Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación.
- Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

### *7.3.2 Tabla de actividades de la Fase III – Pruebas de Funcionalidad de IPv6*

Las entidades deberán tener en cuenta la siguiente tabla y diligenciar el tiempo en meses que le lleve desarrollar cada actividad:

Fase III	Actividades Generales	Tiempo en meses de la actividad
<b>Pruebas de funcionalidad de IPv6</b>	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.	
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	
	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.	

*Tabla 3. Actividades de la Fase III*

# 8. Requerimientos para el proceso de IPv6

Los siguientes son los requerimientos a tener en cuenta en el proceso de transición de IPv4 a IPv6:

- Cumplir con el plan de implementación del protocolo IPv6 en la infraestructura tecnológica de cada Entidad.
- Se requiere asegurar que el servicio suministrado sea de la más alta calidad, sin afectar las operaciones normales de cada Entidad.
- Garantizar el buen funcionamiento y operatividad de los servicios y aplicaciones que se soportarán sobre el nuevo protocolo IPv6, tanto en servicios prestados localmente como servicios en la nube.
- Realizar el seguimiento de cada una de las fases del proceso de transición de IPv4 a IPv6, teniendo en cuenta que cada entidad es responsable del desempeño y la funcionalidad de los servicios y aplicaciones de red, de los equipos intervenidos, del uso de herramientas de administración y monitoreo, necesarias para el afinamiento del nuevo protocolo en las infraestructuras de TI de cada una de las Entidades.
- El Ministerio TIC, prestará a las Entidades el acompañamiento requerido para el cumplimiento del proyecto de transición y adopción de IPv6 en cada Entidad.
- Cada entidad dispondrá del recurso humano idóneo necesario para el desarrollo de cada una de las fases del proyecto de transición a IPv6 en cabeza y coordinación con las Áreas de TI de cada Entidad.
- El Ministerio TIC, recomendará a cada una de las Entidades, la solicitud previa del bloque de direcciones de IPv6 ante LACNIC<sup>6</sup>, con el fin de preparar la implementación con estas direcciones; teniendo en cuenta que esta actividad representa las siguientes ventajas:
  - La Entidad tendrá su propio segmento de direcciones IPv6 (Portabilidad numérica de direcciones IPv6), cuyo tráfico de IPv6 será visible a nivel de la comunidad de Internet, y esto facilitaría identificar el tráfico cursado por la entidad desde cualquier red.
  - La Entidad tendrá total Independencia de su proveedor de servicio de Internet, sin verse

---

<sup>6</sup> LACNIC: Organismo Internacional encargado del registro de direcciones de Internet para América Latina y el Caribe, por sus siglas Latin American and Caribbean Internet Addresses Registry



afectado por el cambio de proveedor y cambio del direccionamiento IPv6, como si ocurre generalmente con el direccionamiento en IPv4.

- .
- Para poder anunciar los prefijos en Internet, también se solicitará a LACNIC su propio ASN.
- cual se dependerá de una lista de espera de LACNIC. Al momento de solicitar el recurso de direcciones IPv6 en LACNIC, se recomienda seguir las políticas establecidas para “Asignaciones directas a Usuarios Finales”<sup>7</sup>. Atendiendo a dichas políticas, cada “sitio” de una Entidad debe tener su propio /48<sup>8</sup>, y por tanto el número de ellos dependerá del número de “sitios”, y del crecimiento previsto si se pudiera prever, de tal forma que se obtenga un bloque de direccionamiento IPv6 agregado en función del número de sitios.
- Atendiendo a las políticas de LACNIC, debe tenerse en cuenta que dichas asignaciones a usuario final son exclusivamente para el uso por parte del solicitante, y por tanto, no permiten la sub-asignación a otras entidades. Por ello, en aquellos casos de entidades que requieran asignar recursos IPv6 a otras organizaciones deberán utilizar las políticas de distribución, ya que frente a LACNIC esas entidades son un LIR (*Local Internet Registry*). De otro modo se estarían incumpliendo las políticas de LACNIC con el consiguiente riesgo de pérdida de los derechos de uso de los recursos y la recuperación de los mismos.

## 8.1 Plantillas

### 8.1.1 Modelo de Inventarios de Equipos de Comunicaciones

Equipo	Marca	Modelo	Sistema Operativo	Puertos Ethernet	Rol	Versión IP

**Equipo:** Descripción del tipo de equipo de comunicaciones, ejemplo, switch, enrutador, firewall, modem, AP, DTE, NAC, etc.

**Marca:** Describir la marca, ejemplo Fortinet, Cisco, Avaya, HP, Huawei, 3M, 3COM, etc.

**Modelo:** Referenciar el modelo del equipo de comunicaciones.

**Sistema Operativo:** Descripción del sistema operativo que soporta el equipo de comunicaciones.

**Puertos Ethernet:** Describir los puertos de Ethernet que soporta, ejemplo E0, S0, FE, FC, PoE, etc.

<sup>7</sup> <https://www.lacnic.net/547/1/lacnic/4-politicas-para-la-distribucion-y-asignacion-de-direcciones-ipv6>

<sup>8</sup> <https://www.rjpe.net/publications/docs/rjpe-690>

**Rol:** El papel que desempeña el equipo de comunicaciones en la red de cada entidad.

**Versión IP:** Versión IPv4 / IPv6

### 8.1.2 Formato Modelo de Equipos de Cómputo

Equipo	Memoria	Procesador	Discos	Sistema Operativo	Versión	Software Instalado	Rol	Versión IP

**Equipo:** Descripción del tipo de equipo de cómputo ejemplo, Computador, Servidor, SAN, Tableta, entre otros.

**Memoria:** Descripción de la memoria RAM.

**Procesador:** Característica del procesador (Intel, AMD, de 32 /64 bits, etc).

**Sistema Operativo:** Descripción del sistema operativo que soporta el equipo de cómputo.

**Rol:** El papel que desempeña el equipo en la red de la Entidad.

**Versión IP:** Versión IPv4 / IPv6.

### 8.1.3 Formato Modelo de Inventario de Aplicaciones de la Entidad

Aplicativo	Característica	Tipo	Lenguaje Programación	Responsable	Componentes	Contrato	Soporte IPv6

**Aplicativo:** Descripción de la característica, tipo de aplicativo y Lenguaje de programación utilizado para el desarrollo del aplicativo.

**Responsable:** Persona responsable del aplicativo, DBA, etc.

**Componentes:** Descripción de las partes que constituyen la aplicación y sus interfaces.

**Contrato:** Descripción del soporte y/o mantenimiento sobre los Aplicativos de la Entidad si existe.

**Soporte IPv6:** Descripción si el aplicativo cumple o no con el protocolo IPv6.

#### 8.1.4 Formato Modelo de Inventario de Equipos Servidores de la Entidad

El siguiente formato describe las características de la infraestructura de servidores y sus correspondientes servicios, aplicaciones y componente de direccionamiento IP.

Tipo de Servidor	Sistema Operativo	Versión Sistema Operativo	Direccionamiento IP	Funcionalidad

**Tipo de Servidor:** Si es un servidor de aplicaciones o de comunicaciones, de Bases de datos.

**Sistema Operativo:** Si es Windows, Linux, Solaris, etc.

**Versión del Sistema Operativo:** Versión del Sistema Operativo y niveles de parcheo.

**Direccionamiento IP:** Direccionamiento IPv4/IPv6.

**Funcionalidad:** El rol que cumple el servidor dentro de la organización.

#### 8.1.5 Formato Consideraciones de Seguridad

La siguiente tabla contempla un ejemplo de cómo las entidades pueden clasificar las reglas de seguridad utilizadas en su firewall tanto para IPv4 como para IPv6, esto debe entenderse únicamente para aquellas entidades que les aplique configurar las reglas en su propio firewall.

Tipo de equipo firewall	Soporte de IPv6	Reglas de Firewall para IPv4	Reglas de Firewall para IPv6	Regla (objeto) en el firewall
Fortinet – Fortigate 30e Generation Network Security	SI	10.50.200.0/24	2801:12:0:100::/64	VPN_P1
		10.50.100.0/27	2801:12:0:200::/64	VLAN_Cont
		10.50.50.0/22	2801:12:0:300::764	USR_NET

**Tipo de equipo Firewall:** Mencionar las características generales del equipo de seguridad a validar

**Soporte de IPv6:** Validar si el equipo de seguridad cumple o no con soporte de IPv6

**Reglas de Firewall para IPv4:** Describir el direccionamiento IPv4 público que estará asociado a la regla de tráfico de IPv4 configurada dentro del Firewall.

**Reglas de Firewall para IPv6:** Describir el direccionamiento IPv6 Global que estará asociado a la regla de tráfico de IPv6 configurada dentro del Firewall.

**Regla (objeto) en el firewall:** Las reglas de tráfico que el firewall tenga configuradas tanto para IPv4 como para IPv6, estarán asociadas a un objeto o grupo de objetos que cumplen una función dentro de la red de la entidad, ya sea para una VLAN, un servicio de aplicaciones, un servicio de VPN o un sistema WAF, entre otros. Es necesario que el firewall tenga clasificadas las reglas por:

- Puertos (Interfaces)
- Aplicaciones
- URLs
- Red

Importante mencionar, que las reglas tanto de IPv4 como de IPv6 deben operar en paralelo entre sí dentro del firewall, teniendo en cuenta que IPv4 trabaja con máscaras de subred, mientras que IPv6 lo hace mediante prefijos en un máximo divisible por /64, que es independiente de las máscaras utilizadas para IPv4.

# 9. Lineamientos técnicos en la implementación de IPv6

- Siempre que sea posible, y especialmente en LANs de usuarios y de servicios, aplicaciones y servidores, utilizar la metodología de transición de IPv4 a IPv6 en doble-pila (*Dual-Stack*), que consiste en permitir la coexistencia de los dos protocolos simultáneamente con el fin de continuar con los servicios y aplicaciones tanto en el ambiente de IPv4 como en el ambiente de IPv6.
- Elaborar el nuevo plan de direccionamiento en IPv6 con la utilizando direcciones GUA (*Global Unicast Address*), es decir direcciones globales.
- Se recomienda contemplar la implementación de un IPAM, que es un método para planificar y administrar recursos de IP, está integrado a los sistemas DNS y DHCP.
- El esquema de enrutamiento debe considerar el bloque de direcciones IPv6 asignado o distribuido por LACNIC para la Entidad. Cada Entidad debe solicitar, una vez, realizado el plan de direccionamiento, su propio bloque IPv6 ante LACNIC<sup>9</sup>, y aun cuando no haya disponibilidad de IPv4, a través de la lista de espera.
- Revisar el pool de direccionamiento IPv4 de cada Entidad y hacer un nuevo plan de direccionamiento, que dadas las características de IPv6 y el número de direcciones, puede no tener que ver con el actual de IPv4, y ser una oportunidad para hacerlo correctamente e incrementar la seguridad frente a *port-scanning*.
- El bloque de direccionamiento IPv6, debe ser solicitarlo ante LACNIC una vez realizado el plan de direccionamiento y antes de la fase de implementación de IPv6. Debe funcionar de manera transparente para los usuarios finales e independientemente del proveedor del servicio de Internet – ISP que se tenga en la Entidad. No se recomienda utilizar direccionamiento del ISP, ni siquiera de forma temporal, porque supondría depender de dicho proveedor, sin posibilidad de *multihoming* y una costosa reenumeración de toda la red al cambiar de proveedor o solicitar su propio prefijo a LACNIC.

---

<sup>9</sup> LACNIC: Organismo Internacional encargado del registro de direcciones de Internet para América Latina y el Caribe, por sus siglas Latin American and Caribbean Internet Addresses Registry.

- La segmentación del bloque de direcciones IPv6 debe establecerse de forma lo más adecuada posible a cada Entidad y cada uno de sus sitios y subredes. Un posible esquema sería por zonas lógicas de seguridad acorde a las necesidades de la red de la organización, contemplando zona de comunicaciones, zona de administración de servidores, zona de aplicaciones, zona de bases de datos, zona de ambiente de pruebas, zona de respaldos y monitoreo, zona WiFi y zona de publicaciones Web.
- Para cada zona lógica debe ser configurada en el firewall y deben contener las políticas de seguridad de acuerdo con la gestión y uso de los servicios prestados en las Entidades.
- Coordinar con los Proveedores de Servicio de Internet - ISP (*Internet Service Provider*) de cada Entidad, las acciones técnicas necesarias para que estos apoyen la implementación del enrutamiento de IPv6, que sean necesarios realizar en las aplicaciones y/o servicios de red con el fin de garantizar la generación de tráfico IPv6 por medio de estos canales; así mismo como se mencionó antes, para esta instancia es recomendable tener el bloque de direcciones IPv6 (prefijo), previamente solicitado ante LACNIC. La solicitud de este bloque de direcciones IPv6 estará fundamentado en que lo mínimo que se puede solicitar para salir a Internet es un /48 (por cada "sitio" de la Entidad), según las políticas de LACNIC<sup>10</sup>.
- Se requiere la definición de un cronograma general para cada una de las fases del proceso de transición a IPv6, a fin de establecer con tiempo, las ventanas de mantenimiento e indisponibilidad cuando se requieran a fin de evitar traumatismos en la continuidad de los servicios.
- Para la fase implementación de IPv6 es importante generar previamente un ambiente de pruebas que simule completamente la topología de red propuesta para IPv6.
- Definir un plan de marcha atrás (Plan de Contingencias de IPv6) en caso de presentarse inconvenientes de indisponibilidad de las aplicaciones y servicios de la Entidad dentro de la fase de Implementación de IPv6, que presenten problemas a la hora de implementar IPv6.
- Evaluar el soporte de IPv6 para los servicios de Directorio Activo, Servicio de DNS, Servicios de Voz sobre IP, Servicios con Sistemas IPTV, Servicio de Correo Electrónico, Servicio de DHCP, Servicios de aplicaciones, Servicios Web, Servicios de Gestión y Servicios en la Nube, Plataformas computacionales, Servicios que soporten canales de acceso a Internet y otros servicios.
- Revisar las políticas y/o reglas de seguridad de los siguientes componentes que cada organización tenga como son: Enrutadores, Equipos de Seguridad (Firewalls), Servidores, Equipos de Conmutación (Switches), Controladoras, Puntos de Acceso (APs), Servidores, Equipos de Almacenamiento de Datos (SAN), Terminales Inteligentes, Controladoras Inalámbricas (WiFi), Controladoras de Gestión de Redes, Centro de Datos (Data Center), Centros de Cableado, Centrales Telefónicas, Sistemas Ininterrumpidos de Potencia (UPS), Sistemas de

<sup>10</sup> <https://www.lacnic.net/547/1/lacnic/4-politicas-para-la-distribucion-y-asignacion-de-direcciones-ipv6>

Aire Acondicionado, Sistemas de Detección y Prevención contra Incendio y Servicios de Impresoras, dispositivos móviles al servicio de la Entidad, entre otros.

- Realizar la evaluación y selección de protocolos de enrutamiento internos y externos que sean necesarios para implementar la solución IPv6 requerida, como es el caso de protocolos IGRP, EIGRP, BGP, IGP, EGP, entre otros.
- Se requiere trabajar en el proceso de transición a IPv6 para las aplicaciones; en coordinación con los proveedores de las mismas a fin de revisar el cumplimiento de las aplicaciones en IPv6 tanto en modalidad de doble-pila como IPv6-only; para esta labor, es indispensable contar con el acompañamiento de Terceros (si es desarrollo externo) que sean los responsables de las aplicaciones, revisar los contratos de soporte y mantenimiento con ellos y realizar la evaluación final sobre que aplicaciones que pueden actualizarse directamente con IPv6 y cuáles requieren cambios para cumplir con el funcionamiento de los aplicativos sobre el nuevo protocolo.
- De acuerdo con el inventario de las aplicaciones y servicios existentes dentro de la Entidad, se requiere clasificar las aplicaciones de acuerdo con el tipo de proveedor que las ha desarrollado, esto permite identificar claramente cada una de ellas y las bases de datos de compatibilidad. Para este punto es recomendable revisar los distintos RFC que indican las recomendaciones a seguir para la adopción de IPv6 en las aplicaciones.<sup>11</sup>
- Definir las acciones necesarias para permitir la correcta operación de las aplicaciones que soporten IPv6 en compatibilidad con IPv4, de acuerdo con un protocolo de pruebas y validaciones establecido por la Entidad y que deberá ser ejecutado por cada uno de los proveedores de las aplicaciones y servicios que se tengan al momento de implementar.
- Realizar la actualización de las versiones de software que requieran aplicarse para los elementos activos de la red, aplicativos, sistemas operativos y demás que se ajusten a los requerimientos funcionales para la implementación IPv6. Lo anterior estará sujeto a los contratos de soporte con el fabricante de los equipos. Cada Entidad deberá suministrar el software y el proveedor deberá encargarse de ejecutar la actualización sobre los equipos a que haya lugar de este proceso.
- Coordinar con el Proveedor de Servicios de Internet de cada Entidad, todas las acciones técnicas necesarias para permitir que todos los servicios y aplicaciones puedan ser enrutados con el protocolo IPv6, desde el interior hacia el exterior con el fin de poder generar tráfico IPv6 desde y hacia sus canales de comunicación.
- Los proveedores de servicio de Internet deberán estar provistos de un sistema de Backbone<sup>12</sup> con soporte de IPv6, que permitan ofrecer y garantizar el enrutamiento de tráfico IPv6 que demanden las entidades corporativas del país.

<sup>11</sup> [www.mintic.gov.co/portal/inicio/Micrositios/IPv6/IPv6-Colombia/](http://www.mintic.gov.co/portal/inicio/Micrositios/IPv6/IPv6-Colombia/)

<sup>12</sup> Backbone: Se refiere a la conexión troncal de Internet compuesta por un gran número de equipos de comunicaciones de gran capacidad para llevar datos a través de la comunidad de Internet en el mundo.

## 9.1 Servicios

Los siguientes son los servicios generales que las Entidades deben revisar y configurar con el nuevo protocolo IPv6:

- DNS
- DHCP/DHCPv6
- Directorio Activo
- Correo electrónico (Local o en Nube)
- Mensajería Instantánea
- Video Conferencia
- Servicio de respaldo
- Servicio telefónico (Voz sobre IP)
- Servicio WiFi
- Servicio de repositorio compartido de archivos
- Servicios en la nube
- Servicio Web y Acceso a Internet
- Herramientas corporativas
- Canal(les) de comunicaciones de Internet (con el ISP de cada entidad)

Las Entidades deberán dejar documentado en los entregables del proyecto, las aplicaciones, elementos de comunicaciones y demás servicios, que no pudieron ser directamente compatibles (Plan de excepciones) con el nuevo protocolo IPv6, de acuerdo con el resultado del plan de diagnóstico de la fase de planeación, indicando las causas del porque no pudieron soportar el nuevo protocolo y cuáles son las acciones que se debe realizar con plazos y tiempos para su cumplimiento de conformidad con lo establecido en la Resolución 2710 de 2017, así como los mecanismos de transición IPv4 a IPv6 a utilizar para resolverlo de forma provisional.

## 9.2 Estructura de Capas de IPv6

Se recomienda tener en cuenta dentro del desarrollo de cada una de las fases del proceso de transición de IPv4 a IPv6 la siguiente estructura:

ESTRUCTURA DE CAPAS DE IPV6		
Capas	Componentes	Actividad en IPv6
<b>USUARIO</b>	Equipos de escritorio, portátiles, tabletas, dispositivos móviles, video cámaras, impresoras, equipos de monitoreo, de	Validación y Activación del nuevo protocolo IPv6



	almacenamiento, equipos de WiFi.	
<b>SERVICIOS Y APLICACIONES</b>	Aplicativos, Web, Correo, DHCP, DNS, Proxys, Directorio Activo, servicios de nube privada, nube pública, sistemas on-premise, sistemas de información, sistemas operativos	Verificación de compatibilidad, configuración de servicios y Aplicativos locales y de nube, así mismo revisión de buenas prácticas.
<b>HARDWARE</b>	Servidores, equipos de almacenamiento, monitoreo, centrales telefónicas, sistemas ininterrumpidos de potencia, cámaras IP	Validación, configuración y activación de IPv6.
<b>COMUNICACIONES Y SEGURIDAD</b>	Switches, Firewall, equipos de filtrado, módems, enrutadores, Control de acceso a la red, equipos de cifrado, zonas perimetrales, servidores AAA, sistemas WAF, Front Door, controladoras Inalámbricas, entre otros.	Configuración del bloque de direccionamiento de IPv6 en el Core, Habilitación IPv6 en Doble Pila.

*Tabla 4. Estructura de Capas de IPv6*

# 10. Descripción del plan de trabajo

El plan detallado de trabajo definido para el proceso de transición de IPv4 a IPv6, debe convertirse en el instrumento de planificación del proyecto que garantice el éxito de la implementación, por lo tanto, debe contener los siguientes puntos:

- Objetivos y alcances del proyecto en la Entidad.
- Descripción del proyecto por cada una de sus fases y sus respectivas actividades.
- Descripción de entregables con fechas específicas de cada actividad.
- Entrega de documentación evidenciando las acciones, recomendaciones y excepciones del cambio tecnológico que facilite la toma de decisiones pertinentes dentro del proceso de adopción del nuevo protocolo.
- Presentación de cada una de las actividades y productos por fases y tiempos de cumplimiento.
- Presentación del resultado final de consolidación de todas las fases del proyecto de transición de IPv4 a IPv6, especificando el logro alcanzado para cada Entidad.
- Entrega de conclusiones, recomendaciones y lecciones aprendidas del proceso de transición de IPv4 a IPv6 desarrollado en cada fase de las entidades.

# 11. Capacitación en IPv6

La capacitación en el protocolo IPv6 es fundamental para el conocimiento previo no solo de la parte técnica de IPv6, sino también de la concientización por parte de las entidades sobre el conocimiento de la normatividad vigente y la importancia de adoptar IPv6 dado que su omisión podría generar un Internet limitado o definitivamente, dejar a las entidades desconectadas de las demás que si realizaron la implementación del nuevo protocolo.

Para la programación de cursos de capacitación en el protocolo IPv6 para las Entidades del gobierno, se recomienda que éstos deben tener como mínimo los siguientes contenidos:

- a. Introducción y aspectos básicos de IPv6
- b. Normatividad de Colombia y lineamientos para adoptar IPv6
- c. Plan de diagnóstico de IPv6
- d. Plan de direccionamiento de IPv6
- e. Modelos de transición y coexistencia
- f. Políticas de enrutamiento en IPv6
- g. Servicios y aplicaciones sobre IPv6
- h. Seguridad en IPv6

Para cada uno de estos temas, se recomienda que los funcionarios capacitados pertenezcan a las áreas de TI de las organizaciones, adquieran los conocimientos que describen la funcionalidad, la aplicabilidad y los componentes técnicos del nuevo protocolo a través de prácticas y procedimientos de configuración en laboratorios destinados para ello; cada uno de estos temas puede corresponder a un curso con una duración de 8 horas semanales.

Se recomienda realizar cursos presenciales de 24 horas de duración, que contenga los conceptos básicos y herramientas tecnológicas para la comprensión del protocolo IPv6 y los elementos necesarios para apoyar a la Entidad en el proceso de diagnóstico, implementación y monitoreo del nuevo protocolo.

Adicionalmente, se requiere sensibilizar a la alta Dirección de las Entidades, sobre la importancia de implementar IPv6 y su impacto dentro de la infraestructura tecnológica de TI y del negocio de cada entidad, y como su implementación puede afectar las operaciones normales de cada Entidad.

Para el proceso de capacitación es necesario tener presente las siguientes recomendaciones:

- Capacitar a las personas de las Áreas de TI que designe cada Entidad para propiciar un nivel de conocimiento adecuado sobre IPv6.
- La capacitación debe describir no solo el componente técnico del protocolo, sino la forma como se debe orientar el proceso de transición de IPv4 a IPv6 para las Entidades.

- La capacitación debe incluir una reseña de los lineamientos establecidos en la Resolución 2710 de 2017 del MinTIC.
- Cada capacitación debe incluir todo el material necesario de los cursos y los temarios a tratar, con el propósito de aclarar suficientemente los aspectos técnicos sobre IPv6.
- Se recomienda garantizar la transferencia de conocimientos de IPv6 en caso de que las personas capacitadas se retiren de las entidades.

# 12. Modelo para el proceso de transición

Se recomienda para cada Entidad, revisar el siguiente modelo de transición desde el punto de vista del recurso humano y recurso técnico a seguir para todo el ciclo de transición hacia IPv6<sup>13</sup>

		Diagnóstico	Planeación	Implementación	Seguimiento	Lanzamiento
Recurso Humano	Gerencia de Proyecto	<p>Revisión de políticas y plan de trabajo.</p> <p>Revisión manuales de procedimientos</p> <p>Requerimientos y necesidades</p>	<p>Determinación de alcance y tiempo, cronograma, obtención presupuesto y recursos</p> <p>Construcción plan de proyecto y planes específicos</p>	<p>Desarrollo del plan detallado de trabajo del proyecto.</p> <p>Desarrollo de planes específicos.</p>	<p>Controles de riesgo. Informes de avance y gestión. Control de alcances, tiempo, costo y calidad. Mediciones de rendimiento, controles de cambios.</p>	<p>Acta de cierre de proyecto y aceptación.</p> <p>Cierre de contratos.</p> <p>Entrega documentación y recomendaciones generales.</p>
	Talento Humano	<p>Evaluación de recurso humano equipo de trabajo</p>	<p>Especificación de roles, perfiles y competencias</p>	<p>Desarrollo del equipo de trabajo</p>	<p>Indicadores de gestión y rendimiento. Gestión de equipo</p>	<p>Cierre de contratos</p>

<sup>13</sup> Tomado de "Modelo de Transición hacia IPv6", Velásquez, Jairo Alberto – Cintel, IPv6 Colombia, 2012

					de trabajo.	
<b>Recurso Técnico</b>	<b>Infraestructura</b>	<p>Inventario de activos de información y servicios</p> <p>Diagramas lógicos de interrelación</p> <p>Ingeniería de detalle solución actual.</p> <p>Banco de configuraciones.</p>	<p>Evaluación requerimientos</p> <p>Ingeniería de detalle, diagramas lógicos y de componentes nueva solución</p> <p>Especificación equipos, plan de integración</p> <p>Protocolo de pruebas.</p> <p>Factores de éxito y aceptación.</p>	<p>Ambiente de coexistencia y pruebas.</p> <p>Conexiones físicas.</p> <p>Gestión de calidad.</p> <p>Control de versiones.</p> <p>Validación de factores de éxito y aceptación.</p>	<p>Controles de cambio, gestión de riesgos, gestión de calidad.</p> <p>Validación factores de éxito y aceptación.</p>	<p>Puesta en producción.</p> <p>Entrega documentación y manuales de usuario.</p> <p>Entrega de configuraciones.</p>

	<b>Aplicaciones</b>	<p>Inventario de aplicaciones</p> <p>Evaluación estado de aplicaciones (Propietario, código fuente, derechos de autor)</p> <p>Mapa de comunicaciones por cada aplicación</p>	<p>Evaluación código fuente, interfaces utilizadas.</p> <p>Evaluación de capacidad, estructuras de datos y lenguajes de programación para soporte de IPV6, convivencia con IPV4.</p> <p>Plan de integración, protocolo de pruebas.</p> <p>Factores de éxito y aceptación.</p>	<p>Ambiente de coexistencia y pruebas.</p> <p>Modificación librerías, APIs, código fuente, etc.</p> <p>Ejecución protocolo de pruebas.</p>	<p>Controles de cambio, gestión de riesgos, gestión de calidad.</p> <p>Validación factores de éxito y aceptación</p>	<p>Puesta en producción.</p> <p>Entrega documentación y manuales de usuario.</p>
	<b>Seguridad</b>	<p>Revisión de políticas de seguridad.</p> <p>Revisión de inventario de activos</p>	<p>Plan de seguridad para la coexistencia de los dos protocolos.</p> <p>Protocolo de pruebas de aceptación.</p>	<p>Aseguramiento de servidores y de servicios.</p> <p>Ejecución de pruebas de seguridad.</p>	<p>Gestión de incidentes de seguridad.</p> <p>Gestión de riesgos de seguridad.</p>	<p>Ajustes a políticas de seguridad.</p> <p>Entrega documentación.</p>

Tabla 5. Modelo del Proceso de Transición

Se recomienda la aplicación de este modelo de transición hacia IPv6, debido a que se esboza todo el ciclo de diagnóstico, planeación, implementación, seguimiento y lanzamiento del nuevo protocolo y las funciones de desempeño por cada uno de los recursos tanto humanos como de infraestructura de TI, que se requieren tener en cuenta para un proceso de transición exitoso.



# 13. Fases del proyecto de IPv6

El proceso de transición a IPv6 debe ser orientado por fases y para cada una de estas fases, es importante indicar cuales productos deben ser entregados y en qué lapso de tiempo (puede variar de acuerdo con las infraestructuras y necesidades de cada Entidad), con respecto a la siguiente tabla:

Producto	Fase	Productos para entregar	Tiempo Entrega
Proceso de Implementación del protocolo de IPv6	Diagnóstico Situación Actual	Plan de trabajo para la adopción de IPv6 Inventario de TI, informe de infraestructura de comunicaciones, recomendaciones de adquisición elementos Hardware/Software, plan de diagnóstico, plan de direccionamiento IP, plan de excepciones, informe de preparación – <i>Readiness</i> , plan de contingencias de IPv6. Documento implementación de seguridad de IPv6 en congruencia con la política de seguridad de las Entidades, plan de contingencias de IPv6 y plan de capacitación en IPv6.	
	Desarrollo del Plan de Implementación	Informe plan detallado implementación de IPv6. Documento configuraciones del nuevo protocolo sobre las plataformas de hardware, software y servicios intervenidos durante esta fase. Informe de aplicación de políticas de seguridad de IPv6. Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.	

	<p>Pruebas de Funcionalidad de IPv6</p>	<p>Documento con cambios detallados de las configuraciones realizadas, según análisis de funcionalidad de la fase II. Acta(s) de cumplimiento a satisfacción de funcionamiento de los servicios y aplicaciones intervenidos durante la fase II. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.</p>	
--	---	--	--

*Tabla 6. Fases del Proyecto de IPv6*

# 14. Equipo técnico de trabajo IPv6 y porcentaje de dedicación

El equipo técnico de trabajo recomendado para desarrollar el proyecto de transición del protocolo de IPv4 a IPv6 debe contener los siguientes perfiles:

Gerente del Proyecto, Ingeniero de Seguridad, Ingeniero de Redes, Ingeniero de Comunicaciones, Ingeniero de Aplicaciones. Un equipo conformado por estas funciones puede abordar proyectos de transición de IPv4 a IPv6 de diferentes procesos de negocio o alcances organizacionales, para desarrollar las actividades que conforman las diferentes fases de cada proceso de transición planteado para la cada Entidad.

## 14.1 Dedicación al Proyecto del Equipo de Trabajo

Dedicación Equipo Técnico de trabajo IPv6		
Personal mínimo requerido	Certificaciones exigidas	Dedicación al proyecto
Gerente de Proyecto	Ingeniero certificado en PMP (Project Management Professional) con Especialización en	60%

	Gerencia de Proyecto	
Ingeniero de Seguridad	Recurso certificado en Seguridad	30%
Ingeniero de Networking	Recurso certificado en Routing y Switching	40%
Ingeniero de Comunicaciones	Ingeniero certificado en Seguridad y Networking.	100%
Ingeniero de Aplicaciones	Ingeniero certificado en ITIL.	100%

*Tabla 7. Dedicación del Equipo de Trabajo*

# 15. Glosario de términos

**DHCPv6 (Dynamic Host Configuration Protocol):** Protocolo de Configuración Dinámica de Hosts para IPv6 con característica cliente-servidor y definido por la RFC 8415 de la IETF, que proporciona una configuración administrada de dispositivos sobre redes IPv6.

**Dirección IPv6:** Es un identificador numérico único configurado en una interfaz de red que provee una conexión entre nodos de una red sobre IPv6, y facilita el enrutamiento de los paquetes entre distintos hosts.

**DNS (Domain Name System):** Sistema de Nombres de Dominio que contiene un sistema de nomenclatura jerárquica para equipos de computación. Los DNS contienen una base de datos que tienen la función de indicar la IP que está asociada a un nombre de un sitio web (Resolución de nombres).

**IPv4aaS IPv4-as-a-Service:** Término aplicado a ofrecer el protocolo IPv4 como un servicio dentro de la infraestructura de red en los extremos

**ICMPv6 (Internet Control Message Protocol for IPv6):** El protocolo de mensajes de control ICMPv6, es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de Internet como el diagnóstico, combina funciones que anteriormente estaban contempladas por varios protocolos tales como ICMP, IGMP y ARP, adicionalmente introduce algunas mejoras.

**IPAM (IP Address Management):** Software de Gestión de direcciones de protocolo de Internet, que emplea un método de planificación, seguimiento y gestión de la información asociada con el espacio de direcciones IP de una red.

**IPv6:** Es la nueva versión del Protocolo de Internet (Internet Protocol - IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90 en el IETF (Internet Engineering Task Force). Hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en sustitución de IPv4.<sup>14</sup>

**Protocolo de Comunicaciones:** Conjunto de convenciones y reglas a procedimientos que permiten el intercambio de la información entre diferentes elementos de red.

---

<sup>14</sup> Fuente: <http://portalipv6.lacnic.net/que-es/>

**RFC (Request For Comments):** Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos aprobadas por el IETF - Engineering Task Force. Describen aspectos técnicos del funcionamiento de Internet y otras redes de comunicaciones, protocolos, procedimientos y comentarios o ideas para clarificar o corregir aspectos técnicos que garanticen buenas prácticas de trabajo.

**Redes Privadas Virtuales – VPN (Virtual Private Network):** Es una tecnología de acceso que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

**SaaS (Software as a Service):** Software como Servicio, se le denomina al modelo de distribución de software donde un proveedor aloja el software en sus servidores y los usuarios acceden a él a través de internet.

**SERVICIOS DE NUBE:** Se conocen a las infraestructuras, plataformas o sistemas de software que los proveedores externos alojan y que se ponen a disposición de los usuarios a través de Internet.

**SNMP (Simple Network Management Protocol):** Es un protocolo Simple de Administración de Red de capa de aplicación, que facilita el intercambio de información de administración entre dispositivos de red, siendo un componente de la suite de protocolos de Internet como se define en la IETF

# 16. Conclusiones

Culminado el proceso de transición de IPv4 a IPv6, las Entidades no tendrán que preocuparse por el agotamiento de las direcciones IP (*Internet Protocol*), pues se garantizará que las infraestructuras de TI seguirán conectadas con los dos protocolos de manera coexistente, ofreciendo a los usuarios múltiples oportunidades de seguir conectados y apuntar a los nuevos mercados, servicios y tecnologías que surgen alrededor de IPv6, como IoT, ciudades inteligentes y sistemas de 5G, entre otros.

El nuevo protocolo IPv6 permitirá a las entidades, introducir nuevas funciones que mejorarán aspectos tales como la seguridad informática, vista desde del escenario del funcionamiento del protocolo mismo, la facilidad para conectar una gran variedad de dispositivos de comunicaciones, de computación y de almacenamiento, produciendo un cambio gradual en el funcionamiento tanto de las redes de comunicaciones como de las aplicaciones que producirá resultados exitosos a mediano plazo en la medida en que este nuevo protocolo se afiance en el medio.

De otro lado, con la adopción del protocolo IPv6 se podrá seguir construyendo códigos de software más robustos y portables, permitiendo que el desempeño de las aplicaciones mejore con su adopción y que la red de comunicaciones y los sistemas de información de las Entidades tengan mejores tiempos de respuesta y se beneficien gradualmente de acuerdo con los lineamientos establecidos en la Resolución 2710 de octubre de 2017 del Ministerio TIC, que establece los lineamientos para impulsar la implementación, aplicabilidad y el despliegue del nuevo protocolo en un ambiente de planificación, y operación cuya finalidad es ofrecer más y mejores servicios con mayor conectividad a todas las zonas del país y acercarnos a la vanguardia de los países con mayor tráfico de IPv6 en la región.

La adecuada planificación con el objetivo de un entorno IPv6-only garantizará un menor costo de todo el proyecto y a mas largo plazo, garantizando al mismo tiempo el soporte de dispositivos, servicios y aplicaciones que por las razones que sean, se mantengan en IPv4, con el concepto "IPv4aaS" (IPv4 como servicio), y por lo tanto garantizando la transparencia para usuarios internos y externos.

# 17. Referencias

<https://www.mintic.gov.co/portal/inicio/Micrositios/IPV6/>

<https://www.mintic.gov.co/portal/inicio/Micrositios/IPV6/Documentacion/5903:Documentos-IPv6>

<http://micrositios.mintic.gov.co/ipv6/control/>

<http://www.lacnic.net/es/web/lacnic/inicio>

<https://stats.labs.lacnic.net/IPv6/ipv6ranking.html>

<https://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption>

<http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion4.pdf>

<http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion3.pdf>

<http://www.ietf.org/rfc/rfc2460.txt>

<http://www.tunnelbroker.net>

<http://www.sixxs.net/tools/aiccu/>

<http://www.lacnic.net/es/web/lacnic/inicio>

<http://www.portalIPv6.lacnic.net>

<http://www.IPv6.es>

<http://www.6deploy.eu>

<http://www.lacnic.net/web/lacnic/IPv6-end-user>

<http://kb.wisc.edu/page.php?id=11691;>

[http://IPv6.niif.hu/m/IPv6\\_apps\\_db](http://IPv6.niif.hu/m/IPv6_apps_db)

<http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>



[http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6\\_Equipos-Red-LACNOG\\_2016.pdf](http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2016.pdf)

<https://www.vyncke.org/ipv6status/project.php?metric=p&timeforward=365&timebackward=365&country=co>

# 18. Bibliografía

- Cicileo, G., Gagliano, R., et al. (2009). IPv6 para todos, 1a ed. - Buenos Aires: Asociación Civil Argentinos en Internet.
- Ciprian, P., (2006). Deploying IPv6 Networks, Cisco Systems.
- Circular: 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones, Recuperado el 29 de julio de 2020, del sitio Web del Mintic <https://www.mintic.gov.co/portal/inicio/5932:Circular-00002-de-2011>.
- Grossetete, P., (2008). Global IPv6 Strategies: From Business Analysis to Operational. Cisco System, Ciscopress.com.Hagen, S., (2006). IPv6 Essentials. (2° ed), O'Reilly Media.
- Internet RFC/STD/FYI/BCP Archiver, Enlaces Web Asociados. Recuperado de la página Web de la Internet Faqs Archives: <http://www.faqs.org/rfcs/>
- Manual de Gobierno en Línea 3.0 y 3.1, 2013.
- Moreno, A., (2009). IPv6 Interoperabilidad y robustez. Recuperado el 11 noviembre 2013 de la página Web <http://www.cs.cinvestav.mx/Estudiantes/TesisGraduados/2004/tesisAxelErnesto.pdf>
- Resolución 2710 de 3 octubre de 2017, del Ministerio de Tecnologías de la Información y las Comunicaciones, Recuperado el 29 de julio de 2017, del sitio Web del MinTIC <https://www.mintic.gov.co/portal/inicio/61000:Resolucion-2710-de-2017>
- Stockebrand, B., (2007). IPv6 in Practice, A. Unixer's Guide to the Next Generation Internet. Springer.
- Zorz, J., (2016). LACNOG BCOP 20160127-01, Requerimientos de IPv6 para equipos de TIC. Recuperado el 30 de mayo de 2017 de la página web [http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6\\_Equipos-Red-LACNOG\\_2016.pdf](http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2016.pdf)

# 19. Anexo 1

## *Requerimientos de IPv6 para equipos de TIC (LACNOG BCOP 20160127-01)<sup>15</sup> Best Current Operational Practice (BCOP)*

### *18.1 Resumen del BCOP*

Para asegurar la inserción suave y rentable de IPv6 en sus redes, es importante que los gobiernos y las grandes corporaciones especifiquen requerimientos de compatibilidad de IPv6 en la búsqueda de ofertas de equipamiento y soporte de TIC (Tecnologías de Información y Comunicaciones). Este documento tiene como objeto proporcionar una “Mejor Práctica Actual” *Best Current Practice* (BCP) y no especifica ninguna norma ni política por sí mismo.

### *18.2 Trasfondo del BCOP/ Historia*

Los certificados IPv6 Ready Logo pueden ser requeridos para cualquier dispositivo. Esta es la forma más fácil para que los proveedores que ofrecen equipos pueden demostrar que cumplen con los requisitos básicos de IPv6. El iniciador de la licitación también proporcionará la lista de RFCs obligatorios y opcionales requeridos con el fin de no excluir a los proveedores que aún no exponen

<sup>15</sup> Extracción parcial del documento LACNOG BCOP 20160127-01, Requerimientos de IPv6 para equipos TIC, Jan Zorz, Documentos de referencia: RIPE-554, Traducción de Azael Fernández Alcántara, Ernesto Pérez Estévez, Ariel Weher, otros, 27/01/2016.  
[http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6\\_Equipos-Red-LACNOG\\_2016.pdf](http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2016.pdf)

sus equipos a la prueba de certificación del programa IPv6 Ready Logo. De esta forma los licitadores públicos no pueden ser acusados de preferir cualquier tipo de proveedor de equipamiento.

Cuando especificamos la lista de RFCs requeridas, debemos enumerar todos los requisitos obligatorios, con excepción de las entradas que comienzan con: "Si [funcionalidad] Se solicita ...". Estas entradas son obligatorias sólo si el iniciador de la licitación requiere cierta funcionalidad. Tenga en cuenta que el iniciador de licitación debe decidir qué funcionalidad se requiere, no el proveedor de equipos.

Algunas de las funciones que se encuentran en la sección "opcional" en este documento pueden ser importantes para su caso y / u organización específica. En tales casos, el iniciador de licitación debe mover el requisito hacia la sección "necesaria" en su solicitud de licitación.

## *18.3 Texto del BCOP*

### *18.3.1 Como especificar los requisitos*

Como se mencionó anteriormente, el programa IPv6 Ready Logo no abarca todo el equipamiento que soporta correctamente IPv6; por lo que declarar esos equipos como no elegibles puede no ser deseable. Este documento recomienda que el iniciador de la licitación especifique que los equipos elegibles serán ya sea certificados bajo el programa IPv6 Ready o serán compatibles con los RFCs apropiados que se enumeran en la sección siguiente.

Acerca del programa "IPv6 Ready Logo":

<http://www.ipv6ready.org/>

Tenga en cuenta que existe el proyecto BOUNDv6 cuyo objetivo es crear un entorno de red permanente de múltiples proveedores conectando laboratorios autorizados donde la comunidad puede probar las aplicaciones y los dispositivos habilitados para IPv6 en escenarios de prueba significativos. Se anima a los iniciadores de licitación a echar un vistazo y también utilizar los resultados de este proyecto.

Acerca de BOUNDv6:

<http://www.boundv6.org/>

### *18.3.2 Nota importante para el iniciador de oferta:*

La certificación “IPv6 Ready Logo” cubre los requisitos básicos de IPv6 y algunas características avanzadas, pero no todas ellas. Si usted requiere alguna característica avanzada que no está cubierta por la certificación IPv6 Ready Logo, por favor solicite una lista de RFCs que cubran esas necesidades específicas, además de las comprendidas por la certificación IPv6 Ready Logo. En las listas siguientes, los RFCs que se tratan en dicha certificación están marcados con \*.

### *18.3.3 Texto genérico propuesto para el iniciador de la Licitación*

En cada licitación, deberá incluirse el siguiente texto:

“Todo el hardware de TIC objeto de esta licitación debe apoyar tanto los protocolos IPv4 e IPv6. Similar comportamiento se debe proporcionar para ambos protocolos de entrada, salida y / o el rendimiento de flujo de datos de rendimiento, la transmisión y el procesamiento de paquetes.

El soporte de IPv6 puede ser verificado y certificado por el certificado IPv6 Ready Logo.

Cualquier software que se comunica a través del protocolo IP debe ser compatible con ambas versiones del protocolo (IPv4 e IPv6). La diferencia no debe ser perceptible para los usuarios.

El equipo que no se ha puesto a través de los procedimientos de pruebas IPv6 Ready deben cumplir con las RFC se enumeran a continuación:”

[lista apropiada de los RFCs obligatorios y opcionales seleccionados de las listas a continuación]

### *18.3.4 Lista de especificaciones técnicas RFC/3GPP obligatorias y opcionales soportadas en variedades de hardware y software*

Los requisitos se dividen por equipos de hardware y soporte del integrador.

Se debe asumir que todo el tráfico de IPv4 migrará a IPv6. Todos los requisitos impuestos a las capacidades de tráfico IPv4 como latencia, ancho de banda y throughput también se debería exigir para el tráfico IPv6.

### 18.3.5 IPsec: Obligatorio u opcional

En el estándar original Requisitos de Nodos IPv6 (RFC4294), IPsec fue listado como un

"DEBE" para ser compatible con los estándares. El RFC actualizado (RFC6434) cambió IPsec a "DEBERÍA" ponerse en práctica. Las razones para el cambio se expresan en este nuevo RFC.

El Grupo de Trabajo RIPE IPv6 ha debatido ampliamente si es necesario hacer el soporte IPsec obligatorio u opcional. Los constituyentes más participativos mostraron apoyo para mover IPsec para las secciones opcionales, que es lo que se refleja en este documento.

Mientras que el consenso de la comunidad era hacer IPsec opcional en la mayoría de los casos, el IETF ahora ha declarado que IPsec 'DEBERÍA' ser implementado en la versión más reciente del estándar Requisitos de Nodos IPv6 (RFC6434). En el contexto del IETF, un 'DEBERÍA' significa que pueden existir razones válidas en circunstancias particulares para ignorar un tema en particular, pero todas las consecuencias deben entenderse y valorarse cuidadosamente antes de elegir un camino diferente.

Las organizaciones que utilizan IPsec o tengan intención de utilizar en el futuro deberían incluir lo siguiente en la sección obligatoria al iniciar su oferta:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] \*

### 18.3.6 Definiciones y descripciones de diferentes tipos de dispositivos

Las siguientes definiciones se utilizarán para clasificar los distintos equipamientos de hardware.

Mientras algún hardware pueda tener funcionalidades superpuestas (por ejemplo, un switch Capa 2 puede operar como un router Capa 3 o un router puede tener algunas capacidades de firewall), se espera que, para cada funcionalidad superpuesta, se combinen los requerimientos de cada dispositivo específico.

Host: Un host es un participante de una red que recibe y envía paquetes, pero no los conmuta en nombre de otros.

Conmutador, Switch, o 'Switch Capa 2': Un conmutador, switch o 'switch Capa 2' es un dispositivo que es usado principalmente para el reenvío de tramas Ethernet basándose en sus atributos. El intercambio de información Ethernet con otros switches Ethernet suele también ser parte de sus funciones.

Enrutador, router or 'Switch Capa 3': Un router o 'switch Capa 3' es un dispositivo que es usado principalmente para realizar el reenvío de paquetes IP basándose en sus atributos. El intercambio de información de ruteo con otros Routers suele también ser parte de sus funciones.

Equipos de Seguridad de Red: Los Equipos de Seguridad de Red son dispositivos cuya función primaria es permitir, denegar y/o monitorear el tráfico entre interfaces con el fin de detectar o prevenir potenciales actividades maliciosas. Estas interfaces además pueden incluir las VPNs (SSL o IPsec). El Equipamiento de Seguridad de Red es a menudo también un Switch Capa 2 o un Router/Switch Capa 3.

Customer Premise Equipment (CPE): Un dispositivo CPE es un router de pequeña oficina o bien un router residencial que es usado para conectar a los usuarios finales hogareños o pequeñas empresas usando una amplia cantidad de configuraciones diferentes. A pesar de que un CPE es usualmente un dispositivo llamado router, los requerimientos son diferentes desde el punto de vista de un Router o Switch Capa 3 en una empresa o ISP, dado que estos suelen ser más complejos al estar compuestos por un hardware y software más avanzado.

Dispositivo Móvil: En el contexto de este documento, un dispositivo móvil es un nodo que se conecta a un sistema 3GPP definido utilizando alguna tecnología de acceso 3GPP específica (tal como 2G, 3G, o LTE). En las situaciones donde la lógica de red se compone únicamente por un dispositivo dedicado A conectado a otro dispositivo B, la especificación se referirá al dispositivo A y no al dispositivo B. Si la lógica de protocolos está distribuida (por ejemplo, una computadora con una interfaz ethernet externa que realiza TCP checksum offloading), el sistema agregado será referido.

Balancedador de Carga: Un balanceador de carga es un dispositivo de red que distribuye la carga de trabajo a través de múltiples computadoras, servidores u otros recursos, con el fin de lograr la utilización óptima o prevista de recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobrecarga.

Las siguientes referencias son de relevancia a este documento BCP. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las referencias son objetos de revisiones; Por lo que los usuarios de este documento BCP deben animarse a investigar la posibilidad de aplicar las ediciones más recientes de las referencias citadas a continuación.

### *18.3.7 Listado de normas RFC/3GPP requeridas para diferentes tipos de hardware*

El equipamiento para TIC está dividido en siete grupos funcionales:

- Host: cliente o servidor
- Conmutador o Switch Capa 2
- Router o Switch Capa 3
- Equipos de seguridad de red (firewalls, IDS, IPS...)
- CPE
- Dispositivo móvil
- Balanceador de carga

Hemos dividido los siguientes requisitos en dos categorías, “obligatorias” y “opcionales”. El equipo debe cumplir con la lista de requisitos de los estándares obligatorios. Los soportes de requisitos opcionales pueden ganar puntos adicionales en la licitación, si esto fuera especificado por el iniciador.

Cualquier hardware que no cumpla con todos los estándares obligatorios debe ser marcados como no apropiado por el evaluador de la licitación.

Las normas que son parte de los procedimientos de prueba del “IPv6 Ready Logo”, y son llevados a cabo típicamente por laboratorios acreditados, están marcados con un asterisco \*.

### *18.3. 8 Requerimientos para equipo "host"*

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] \*
- IPv6 Addressing Architecture [RFC4291] \*
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] \*
- DHCPv6 client [RFC3315] \*
- SLAAC [RFC4862] \*
- Path MTU Discovery [RFC1981] \*
- Neighbor Discovery [RFC4861] \*



- Si se requiere soporte para túneles y doble-pila, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts y Routers” [RFC4213]
- Si se requiere soporte para IPv6 móvil, el dispositivo debe soportar “MIPv6” [RFC6275, RFC5555] y “Mobile IPv6 Operation With IKEv2 y el Revised IPsec Architecture” [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] \*

### 18.3.9 Requerimientos para equipo “enterprise/ISP grade “Layer 2 switch”

Soporte obligatorio:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]
- Router Advertisement (RA) filtering [RFC4862]
- Dynamic “IPv6 Neighbor solicitation/advertisement” inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping y filtering.<sup>16</sup>

### 18.3.10 Requerimientos para equipo “router or Layer 3 switch”

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] \*
- IPv6 Addressing Architecture [RFC4291] \*  
Default Address Selection [RFC3484]  
Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] \*

<sup>16</sup> El IETF Source Address Validation Improvements (SAVI) Working Group está actualmente trabajando en las RFCs que especificarán un marco para la validación de direcciones de origen. Una vez sean publicadas estas RFC, las referencias al filtrado de NUD y DAD serán cambiadas de acuerdo a lo especificado.

- SLAAC [RFC4862] \*
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] \*
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981] \*
- Neighbor Discovery [RFC4861] \*
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] \*
- Si se requiere un “dynamic interior gateway protocol (IGP)” , entonces deben ser soportados RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308].
- La entidad de contratación deberá especificar el protocolo requerido.  
Si se requiere OSPF-v3 , el equipo debe cumplir con  
"Authentication/Confidentiality para OSPF-v3" [RFC4552]
- Si se requiere el protocolo BGP4 , el equipo debe cumplir con RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 y RFC2545
- Soporte para QoS [RFC2474, RFC3140]
- Si se requiere soporte para encapsulamiento y pila dual, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts y Routers” [RFC4213]
- Si se requiere soporte para encapsulamiento y pila dual, el dispositivo debe soportar “Generic Packet Tunneling y IPv6” [RFC2473]
- Si se requiere 6PE, el equipo debe soportar "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- Si se requiere IPv6 móvil, el equipo debe soportar MIPv6 [RFC6275, RFC5555] y "Mobile IPv6 Operation With IKEv2 y el Revised IPsec Architecture" [RFC4877]
- Si se requiere “IS-IS routing protocol” el equipo debe soportar "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]
- Si se requiere funcionalidad MPLS (por ejemplo, BGP-free core, MPLS TE, MPLS FRR) , los PE-routers y route reflectors deben soportar "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]

- Si se requiere funcionalidad "Layer 3 VPN", los PE-routers y route reflectors deben soportar "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC4659]
- Si "MPLS Traffic Engineering" es usado en combinación con "IS-IS routing protocol", el equipo debe soportar "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]

### *18.3.11 Requerimientos para dispositivos móviles*

Soporte obligatorio:

- IPv6 basic specification [RFC2460] \*
- Neighbor Discovery for IPv6 [RFC4861] \*
- IPv6 Stateless Address Autoconfiguration [RFC4862] \*
- IPv6 Addressing Architecture [RFC4291] \*
- ICMPv6 [RFC4443] \*
- IPv6 over PPP [RFC2472]
- Multicast Listener Discovery version 2 [RFC3810] \*
- IPv6 Router Alert Option [RFC2711]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]

Soporte opcional:

- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941]
- Path MTU Discovery for IPv6 [RFC1981] \*
- Generic Packet Tunneling for IPv6 [RFC2473]
- DHCPv6 [RFC3315] \*
- Stateless DHCPv6 [RFC3736]
- DHCPv6 option for SIP servers [RFC3319]
- IPv6 Prefix Options for DHCPv6 [RFC3633]
- Prefix Exclude Option for DHCPv6-based Prefix Delegation [draft-ietf-dhc-pd-exclude]
- Default Address Selection [RFC3484]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] \*

- IKEv2 Mobility y Multihoming Protocol MOBIKE [RFC 4555]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191] Referencias:
- 3GPP
- Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services y Packet Data Networks (PDN) [3GPP TS 29.061]
- GPRS Service Description [3GPP TS 23.060]
- General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access [3GPP TS 23.401]
- Signaling flows for IP multimedia Call control based on SIP y SDP [3GPP TS 24.228]
- IP multimedia call control protocol based on SIP y SDP [3GPP TS 24.229]
- IP Based Multimedia Framework [3GPP TS 22.941]
- Architectural Requirements [3GPP TS 23.221]
- Packet domain; Mobile Stations (MS) Supporting Packet Switching Service [3GPP TS 27.060]
- IPv6 migration guidelines [3GPP TR 23.975]
- IETF
- IPv6 for Some Second y Third Generation Cellular Hosts [RFC3316]
- Recommendations for IPv6 in 3GPP Standards [RFC3314]
- IPv6 in 3rd Generation Partnership Project (3GPP) [RFC6459]

### *18.3.12 Requerimientos para el soporte IPv6 en software*

Todo el software debe soportar IPv4 e IPv6 y ser capaz de comunicarse sobre redes sólo IPv4, sólo IPv6 y doble-pila. Si el software incluye parámetros de red en su configuración de servidor local o remoto este debe, además permitir la configuración de parámetros en IPv6.

Todas las características que se ofrecen sobre IPv4 deben estar disponibles también en IPv6. El usuario no debe experimentar ninguna diferencia notable tanto si el software se comunica por IPv4 o por IPv6 excepto cuando esto provea un beneficio apreciable al usuario.

Se recomienda encarecidamente no utilizar ninguna dirección en el código del software, como está descrito en "Default Address Selection for Internet Protocol version 6" [RFC3484].

### *18.3.13 Requerimientos de habilidades del integrador de sistemas*

...Además, se recomienda que los integradores de sistemas y sus empleados tengan un amplio conocimiento de IPv6 y certificados de IPv6 genéricos fuera de aquellos ofrecidos por los fabricantes de equipamiento. Estos certificados pueden ser obtenidos de sistemas de capacitación independientes. Este conocimiento debe recibir puntuación adicional en el proceso de contratación.

Todos los participantes en el proceso de contratación deben firmar una declaración la cual indicará que la compañía y sus empleados han cursado entrenamientos técnicos para el diseño, construcción e integración de equipamiento de las TIC en redes IPv4 e IPv6.

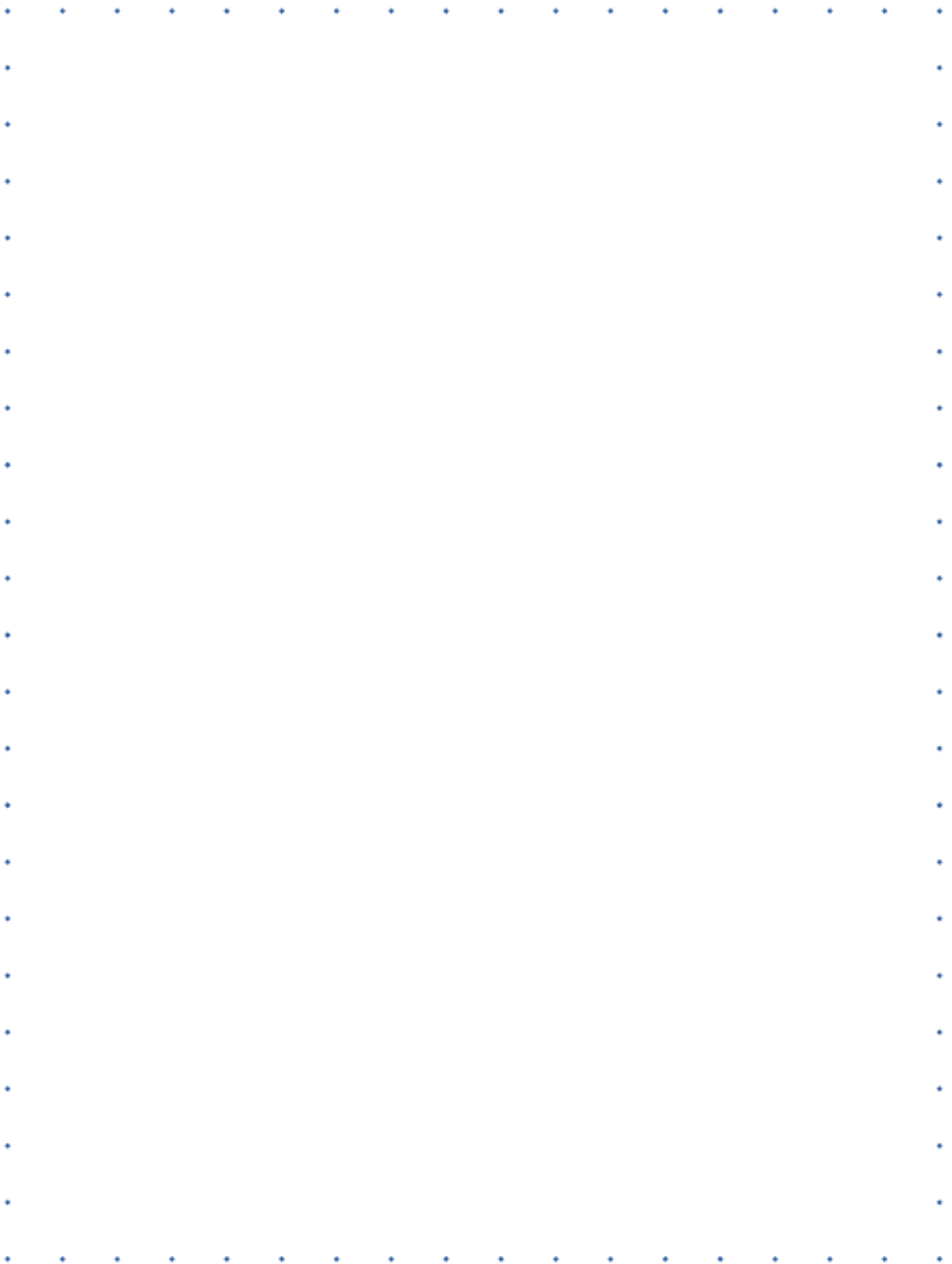
### *18.3.14 Declaración de competencia en IPv6*

Los contratantes deben requerir una declaración de competencias técnicas en IPv6 de parte del suministrador o integrador del equipamiento. Se requiere conocimiento y experiencia en IPv6 como forma de asegurar una apropiada instalación e integración de IPv6 en ambientes de las TIC.

La declaración debe decir que el suministrador de equipamiento o integrador de sistemas declara bajo juramento de ley:

- Que ellos tienen suficiente número de empleados para cumplir con los servicios ofertados.
- Que estos empleados han sido entrenados profesionalmente para su trabajo de diseño, integración y/o construcción de equipamiento de las TIC en ambientes IPv4 e IPv6;
- Que la calidad de los servicios ofertados cumple todos los requerimientos definidos en los documentos de la contratación y que estos requerimientos aplican tanto para IPv4 como para IPv6.

Debe notarse que este tipo de declaraciones pueden variar en dependencia de la legislación local. Por tanto, los traductores y los contratantes deben buscar apoyo legal respecto las palabras y textos a utilizar en estos documentos.



## 20. Anexo 2

### *19.1 Número de Sistema Autónomo – ASN de IPv6*

Las entidades que requieran tener varios servicios en la nube con más de un operador o proveedor de servicios de Internet – ISP, o con más de un enlace, y que utilicen tráfico de IPv6, deben solicitar un ASN propio ante LACNIC, a fin de compartir la misma política de enrutamiento con los demás operadores de manera versátil y ordenada con el fin de generar tráfico IPv6.

Con el ASN, las organizaciones tendrán la oportunidad de que su red sea de fácil reconocimiento en los rastreos de tráfico de IPv6 a nivel mundial.

El ASN permite que cada entidad sea independiente del ASN del proveedor contratado, y por tanto poder publicar su propio segmento de IPv6 recibido de LACNIC y tener la posibilidad de obtener estadísticas de tráfico de IPv6.

### *19.2 Administración de políticas de enrutamiento en ASN*

El ASN permitirá a las entidades una administración coordinada de políticas de enrutamiento y políticas de seguridad.

Se recomienda además el uso de RPKI para incrementar la seguridad del sistema autónomo en BGP.

## 19.3 Implementación del ASN

Para implementar un ASN, es necesario realizar una tarea conjunta entre los proveedores de servicio de Internet y los clientes; consistente en configurar los sistemas de enrutamiento (*routers*), localizados del lado de los clientes y los ubicados del lado de los proveedores (ISPs), el Número de Sistema Autónomo respectivo y hacer la publicación del direccionamiento en Internet.

## 19.4 Acuerdo de Nivel de Servicio del ASN

Si la entidad recibió el ASN, es necesario que los proveedores del servicio de Internet- ISP, entreguen una solución integral de conectividad en donde sus equipos de comunicaciones deben anunciar el nuevo ASN (es decir los enrutadores deben soportar servicios BGP (del inglés, Border Gateway Protocol) que permitan hacer la labor de anunciar el Sistema Autónomo en la red).

Se recomienda revisar con su proveedor de servicio las directrices sobre ASN, que asigna la IANA en los RFC 1930, RFC 5396 y RFC 4893.

## 19.5 BGP (Border Gateway Protocol)

Es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos – ASN.

## 19.6 Sistema Autónomo o Número de Sistema Autónomo - ASN

Se define como un grupo de redes IP que poseen una política de enrutamiento propio e independiente, que permiten una gestión de tráfico propia frente a otros Sistemas Autónomos y que tiene asociado un Número de Sistema Autónomo – ASN, que es el que lo identifica de manera única dentro de la comunidad de Internet. El ASN proporciona la capacidad a la entidad que lo requiera, de tener una alta disponibilidad de servicios de Internet en modo activo – activo, con varios proveedores del servicio, manteniendo siempre un único direccionamiento IPv6 propio e independiente del operador que da acceso a la red.