PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU

Tesis para optar el grado de Magíster en Ingeniería de las Telecomunicaciones que presenta

MARCO ANTONIO TOMY BALTAZAR

Dirigido por

JOSE LUIS MUÑOZ

San Miguel, 2017

“Cada vez que usted planea, se arriesga, fracasa, revalúa o hace ajustes, está disponiendo de otra oportunidad para volver a empezar, sólo que en mejores condiciones que la primera vez.”

John C. Maxwell

A mi madre, Ana Baltazar Alvarado.

AGRADECIMIENTOS

A mi asesor de Tesis el Doctor Jose Luis Muñoz.

Al profesor de Tesis el Doctor Carlos Silva Cárdenas.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

ABSTRACT

Given the imminent exhaustion of the IPv4 addresses, organizations are required to begin the transition of their networks and contents to IPv6. Therefore, the purpose of this thesis is to present a reference model to begin the transition process to IPv6 within the public institutions of the Peruvian government, as at a government level –at the moment of the publication of this thesis work– the public institutions, directly related to the development of the telecommunications and the information technologies in Peru, have not yet considered the development of a methodology and/or technical documents to allow the public institutions to prepare themselves to begin deploying the IPv6 within their networks and contents.

Having a reference model and the necessary technical documents allows boosting the adoption of the new protocol. Evidence can be found by observing the actions made by Argentina, Brazil, Colombia, Chile, United States and Spain, who in addition to defining a national strategy of transition to IPv6, have developed reference models and technical documents of specific support for their public institutions to start the transition towards the new IPv6 protocol.

In that sense, the main contribution of this thesis work is to present a reference model and technical documents which support the beginning of the transition to IPv6 in public institutions within the Peruvian government.

RESUMEN

Ante el inminente agotamiento de las direcciones IPv4, se requiere que las organizaciones inicien la transición de sus redes y contenidos hacia el protocolo IPv6, por lo que la presente tesis tiene como finalidad proponer un modelo de referencia para iniciar el proceso de transición hacia el protocolo IPv6 en las Instituciones Públicas del Gobierno de Perú, debido a que a la fecha de publicado el presente trabajo, a nivel de gobierno, las instituciones públicas que están relacionadas directamente con el desarrollo de las telecomunicaciones y de las tecnologías de información en el Perú, no han considerado la elaboración de una metodología y/o documentos técnicos que permita a las instituciones públicas prepararse para iniciar el despliegue del protocolo IPv6 en sus redes y contenidos.

El contar con un modelo de referencia y los documentos técnicos necesarios permite dinamizar la adopción del nuevo protocolo, esto se evidencia en la revisión de las acciones que vienen realizando diversos países como: Argentina, Brasil, Colombia, Chile, Estados Unidos y España, quienes a parte de definir una estrategia nacional de transición hacia IPv6, han elaborado modelos de referencia y documentos técnicos de apoyo específicos para que sus instituciones públicas puedan iniciar la transición hacia el nuevo protocolo IPv6.

En ese sentido, el aporte principal del presente trabajo es presentar un modelo de referencia y documentos técnicos que sirvan de apoyo para iniciar la transición hacia el protocolo IPv6 en las instituciones públicas a nivel del Gobierno Peruano.

INTRODUCCION

La mayoría de los países a nivel mundial vienen realizando diversas acciones para iniciar la transición hacia el nuevo protocolo IPv6, toda vez que los diferentes Regional Internet Registry - RIR han anunciado el agotamiento de las direcciones IPv4.

La transición hacia el nuevo protocolo (IPv6) es técnicamente posible, ya que los fabricantes de hardware y software han actualizado sus productos en base a los documentos técnicos publicados por la IETF y diversas investigaciones realizadas por los diferentes actores que gobiernan el Internet.

En ese sentido, el presente trabajo tiene como finalidad proporcionar un modelo de referencia y documentos técnicos que permitan a las instituciones públicas del Perú, iniciar su transición hacia el protocolo IPv6.

En el Capítulo I, se realiza un análisis detallado de la problemática actual en relación al agotamiento de las direcciones del protocolo IPv4 y se evidencia las acciones casi nulas que se han realizado a nivel del gobierno de Perú para la adopción del nuevo protocolo en sus redes y contenidos de las instituciones públicas.

En el Capítulo II, se describe el estado del arte de la transición de IPv6 en las instituciones públicas de los países de Argentina, Brasil, Colombia, Chile, Estados Unidos y España, de tal manera nos permita conocer las buenas prácticas para iniciar la transición a nivel de las instituciones públicas.

En el Capítulo III, se describe la situación actual de las acciones realizadas por el gobierno de Perú hacia el protocolo IPv6, específicamente se analiza las instituciones públicas que tienen relación directa con el desarrollo de las telecomunicaciones y con las tecnologías de información a nivel de Perú, a quienes se les ha realizado una encuesta con la finalidad de conocer la importancia del nuevo protocolo y el por que no han iniciado su transición en sus redes y contenidos, evidenciando la carencia de alguna metodología o documentos técnicos que les permitan iniciar la transición hacia el protocolo IPv6 a nivel de instituciones públicas.

En el Capitulo IV, se propone un modelo de referencia para iniciar la transición en las instituciones públicas a nivel de Perú, considerando que las primeras instituciones en adoptar este modelo son aquellas que están directamente relacionadas con el desarrollo de las telecomunicaciones y de las tecnologías de información, de tal manera se genere una curva de aprendizaje del personal técnico y madurez del modelo de transición propuesto, permitiendo su posterior implementación a nivel nacional.

Finalmente se adjuntan como Anexo diversos documentos técnicos que proporcionan conceptos, buenas prácticas y recomendaciones para iniciar la transición en las instituciones públicas.

CAPITULO I: DESCRIPCION DE LA PROBLEMATICA

El presente capítulo describe la problemática del agotamiento de las direcciones IPv4 y el aporte que se propone realizar para dinamizar el despliegue de IPv6 en las instituciones públicas del gobierno peruano.

1.1 Análisis de la Problemática

Internet, llamada la red de redes, desde su concepción, en 1969 [1], ha evolucionado increíblemente, con una expansión a nivel mundial, permitiendo publicar y acceder a diversos contenidos en diferentes formatos (texto, audio y video) y medios (fijo e inalámbrico); así mismo Internet, permitió crear nuevas formas de comunicación como: correo electrónico, mensajería instantánea, voz IP, videoconferencia, entre otros. Este crecimiento inesperado y acelerado, evidencio que uno de sus principales protocolos, del modelo TCP/IP, específicamente el Protocolo de Internet versión 4 (IPv4), no estaba del todo preparada para el futuro, ya que fue diseñado para el contexto de su época.

IPv4 se diseñó para soportar un número limitado de direcciones IP. El tamaño del protocolo es de 32 bits, lo cual permite asignar un máximo de 2^{32} o aproximadamente 4 mil millones de direcciones IP [1]. Esta limitada capacidad de direcciones, se vio reflejada cuando en febrero del 2013, la IANA (Internet Assigned Numbers Authority), entrego a los registros regionales de Internet (Regional Internet Registry - RIR), el último bloque de direcciones IPv4 [2].

Los RIR debido a este agotamiento, han elaborado diversas políticas de asignación de direcciones IPv4 a las organizaciones que la soliciten. Esto con la finalidad de realizar una mejor asignación de sus bloques de direcciones IPv4 restantes.

En la siguiente Tabla 1, se muestra la disponibilidad de direcciones IPv4 en los respectivos RIR a nivel mundial.

Tabla 1 ***Estado de la disponibilidad de IPv4 en los RIR's***

Nº	Regionals Internet Registries – RIR	Direcciones IPv4 disponibles a Diciembre 2015
1	APNIC (Asia/Pacifico)	0.66 /8s [3]
2	ARIN (América del Norte y parte del Caribe)	0.00 /8s [3]
3	AfriNIC (África y parte del océano indico)	2.44 /8s [3]
4	LACNIC (América Latina y parte del Caribe)	0.138 /8s [3]
5	RIPE NCC (Europa, centro y medio de Asia)	1.06 /8s [3]

Fuente: www.nro.net [3]

Ante este inminente agotamiento de direcciones IPv4, que se venia venir desde inicio de los años 90s, la IETF (Internet Engineering Task Force) desarrollo diversas estrategias que permitieron hacer un uso más eficiente de las direcciones IPv4 y extender su tiempo de vida. Estas estrategias permitieron desarrollar el CIDR (Classless Inter-Domain Routing) - RFC 1519[1], NAT (Network Address Translation) - RFC 1631[2], DHCP (Dynamic Host Configuration Protocol) - RFC 1531[3] y la definición de direcciones IP Privadas definida en la RFC 1918 [4].

En paralelo al desarrollo de estas estrategias, diversos organismo mundiales, en la década de los 90s inician la investigación de un nuevo protocolo que permita tener un amplio número de direcciones IP, considerando su crecimiento a futuro; y es en 1995, cuando la IETF, publica oficialmente, la RFC 1883 "Internet Protocol, Versión 6 (IPv6) Specification", dando inicio a la nueva versión del protocolo de Internet [4].

El protocolo IPv6, proporciona un amplio espacio de direcciones, su tamaño de 128 bits, permite alcanzar un total de 2^{128} o aproximadamente 340 sextillones de direcciones IP [4]. Este protocolo proporciona un mejor diseño de direccionamiento, formato de

[1] La RFC 1519 ha sido actualizada por la RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.

[2] La RFC 1631 ha sido actualizada por la RFC 3022 Traditional IP Network Address Translator (Traditional NAT).

[3] La RFC 1531 ha sido actualizada por la RFC 1541 y esta última por la RFC 2131 Dynamic Host Configuration Protocol.

cabecera simplificada, mayor seguridad, calidad de servicio, soporte multicast, entre otras mejoras [4].

Definitivamente la implementación de IPv6, en las redes a nivel mundial, no es una tarea simple. Ante esto, diversas organizaciones que gobiernan Internet, investigan mecanismos de transición de IPv4 a IPv6, con la finalidad de garantizar la coexistencia de ambos protocolos y una migración gradual hacia IPv6 a nivel de Internet. A la fecha, luego de varias investigaciones, la IETF, considera tres (03) técnicas maduras de mecanismos de transición: Pila doble, Túneles/Encapsulamiento y Traducción [5].

Han pasado más de 18 años desde el lanzamiento del protocolo IPv6 y a la fecha de publicado este documento, de acuerdo a la estadística publicada por el RIR RIPE, 22.01% (11,722 de 53,264 ASes) de sistemas autónomos (Autonomous System - AS) a nivel mundial han anunciado un prefijo IPv6 [5]. El gran buscador Google, indica que, 8.24% de usuarios se conectan a su portal usando IPv6 [6].

Estas estadísticas, muestran que el despliegue de IPv6 es relativamente lento en el mundo, considerando que varios de los RIR ya han iniciado la última fase de asignación de sus últimos bloques (prefijo /8s) de direcciones IPv4, por lo que resulta importante dinamizar la implementación del protocolo IPv6.

Haciendo un análisis a nivel local, LACNIC a Diciembre 2015, tiene un 28.87% (1,328 de 4,600 ASes) de ASes que han anunciado un prefijo IPv6 [5]. El Perú, registra 34.62% (9 de 26 ASes) de ASes que han anunciado un prefijo IPv6 [5].

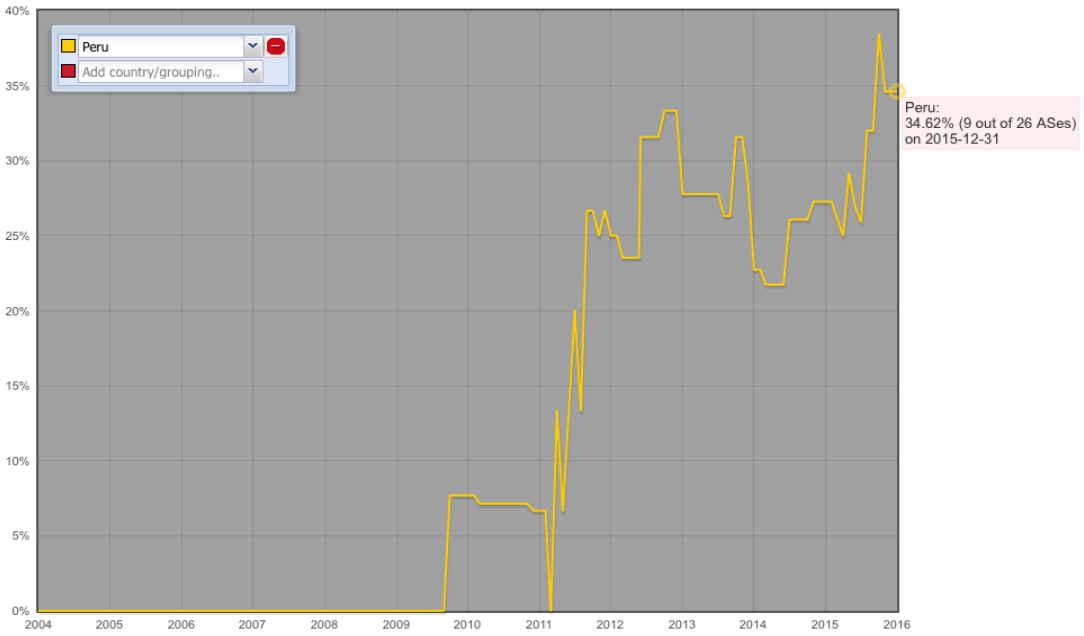


Figura 1 Estado de los ASes que han anunciado prefijo IPv6

Fuente: RIR RIPE [5]

Google, indica que Perú tiene un 15,76% de usuarios que se conectan a su portal usando IPv6 [7]. Este avance en nuestro país (Perú), es liderado por la empresa Telefónica del Perú S.A.A, quien ha desplegado IPv6 en su red de acceso ADSL (clientes del tipo residenciales) [9].

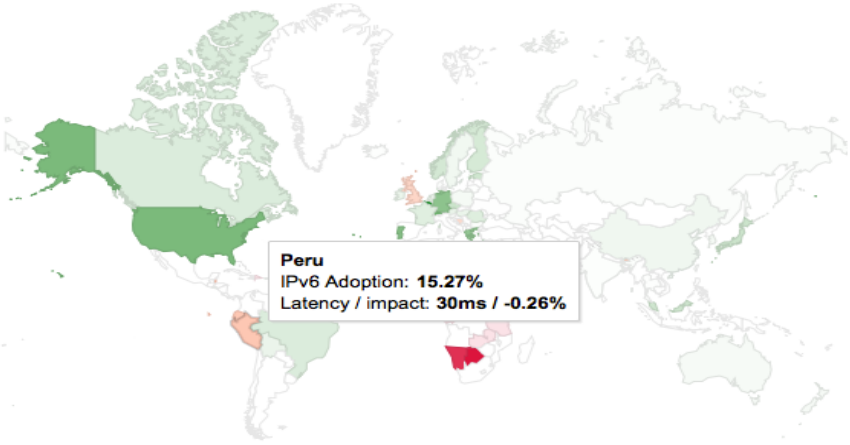


Figura 2 Porcentaje de usuarios de Perú que se conectan a Google utilizando IPv6
Fuente: Google [6]

En relación a los fabricantes de hardware y software de comunicaciones en el mundo, estos han implementado el soporte a IPv6, desde ya varios años. Esto evidencia la estabilidad del protocolo IPv6 a nivel de capa de red y los protocolos que han sido actualizados para su soporte, como ICMPv6, DHCPv6, DNS, RIPng, OSPFv3, BGP para IPv6, entre otros [4]. Asimismo, los principales proveedores de contenidos a nivel mundial como Google, Youtube, Yahoo, Facebook, entre otros; ya han implementado sus contenidos con soporte de IPv6 [36].

De acuerdo a lo descrito, el agotamiento de IPv4 es inminente, y el protocolo IPv6 está listo para su adopción, ya que es un protocolo estable, el cual ha sido mejorado y preparado para el Internet actual y del futuro; por lo que, se considera importante dinamizar el despliegue de IPv6 a través de los principales actores como los Proveedores de Servicio de Internet (Internet Service Provider – ISP), los Proveedores de Contenidos, los Fabricantes, el sector Académico, el Gobierno, entre otros.

El gobierno es un actor que toma mayor importancia, ya que tiene que impulsar el despliegue de IPv6 por parte de los actores privados a nivel país, y liderar su propia adopción del protocolo IPv6 en sus instituciones públicas. Así mismo, una publicación realizada por la ITU (International Telecommunication Union), específicamente la resolución 180 “Facilitating the transition from IPv4 to IPv6”, reconoce que los gobiernos son los actores que pueden desempeñar un papel importante como catalizador para la transición a IPv6 [10].

En ese sentido, siendo considerada de importancia la participación del gobierno para la adopción de IPv6 en un país, estos deben de iniciar acciones conducentes a la adopción del nuevo protocolo en sus redes y contenidos.

Realizando el análisis de manera preliminar a nivel Perú, en Julio del 2011, se aprobó el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0", en la cual se establecieron diversos objetivos al 2015, siendo considerado en uno de los objetivos la inclusión del protocolo IPv6. Específicamente se menciona que para alcanzar su Objetivo Nº 01 "Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la sociedad de la información y del conocimiento", deberá considerarse como estrategia lo siguiente: "Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el protocolo de Internet versión 6 (IPv6)".

De lo definido por el gobierno de Perú, a Enero de 2016, la adopción de IPv6 a nivel de las instituciones públicas del Perú no es muy dinámica, siendo casi nula las acciones conducentes para su adopción, ya que al realizar la consulta en el enlace de la Referencia [88], con los parámetros "Perú" y "Governements", se observa que ninguna de las instituciones públicas del gobierno de Perú, con el dominio ".gob.pe", tiene sus servicios de HTTP, SMTP o DNS configurados con el protocolo IPv6.

A Enero del 2016, de acuerdo a la búsqueda realizada en los portales de los principales actores relacionados a las telecomunicaciones y a las tecnologías de información y comunicación en el estado peruano (MTC[4], ONGEI[5], CONCYTEC[6], OSIPTEL[7] y el INICTEL-UNI[8]), se evidencia que ninguna tiene una iniciativa que permita cumplir con esta estrategia. Así mismo, no se ha encontrado documentos técnicos y estrategias formales a seguir por parte de sus instituciones públicas para la transición de IPv4 a Pv6.

Ante esta situación, resulta importante, que el gobierno peruano como principal actor en nuestro país, cuente con un modelo de referencia, el cual considere aspectos técnicos y estratégicos, que permita a las instituciones públicas, realizar una adopción de manera planificada y progresiva del protocolo IPv6; para lo cual analizaremos los diversos planes de adopción de IPv6 de diferentes países y en base a esto proponer un modelo de referencia para la transición a IPv6 por parte de las instituciones públicas del estado peruano con la finalidad de dinamizar la adopción del protocolo IPv6.

[4] www.mtc.gob.pe
[5] www.ongei.gob.pe
[6] www.concytec.gob.pe
[7] www.osiptel.gob.pe
[8] www.inictel-uni.edu.pe

1.2 Establecimiento de la Hipótesis

Tabla 2 ***Alineamiento de Hipótesis***

Problema	Hipótesis	Objetivo
¿Cómo influye el tener un modelo de referencia de transición de IPv4 a IPv6 en las instituciones públicas a nivel país?	La elaboración de un modelo de referencia de transición de IPv4 a IPv6 para las instituciones públicas dinamiza la adopción del nuevo protocolo.	Elaborar un modelo de referencia de transición de IPv4 a IPv6 para las instituciones públicas del Perú, apoyado de documentos técnicos para su adopción.

Fuente: Elaboración Propia

CAPITULO II: ESTADO DEL ARTE DEL DESPLIEGUE DE IPv6 A NIVEL DE GOBIERNO

El presente capítulo tiene como objetivo describir las experiencias de diferentes organizaciones gubernamentales a nivel internacional en su proceso de transición de IPv4 e IPv6. Describiremos las principales acciones que se han realizado para la adopción del nuevo protocolo a nivel de los gobiernos de: Argentina, Brasil, Chile, Colombia, Ecuador, España y Estados Unidos.

2.1 Argentina

La promoción de la adopción del protocolo IPv6 viene siendo realizada por la fuerza de trabajo denominada Task Force IPv6 Argentina, el cual es una organización independiente sin fines de lucro y esta conformada, de manera general, por las entidades del gobierno, proveedores de acceso a Internet, la academia, y la sociedad civil en general [84].

A nivel de gobierno, desde el 2013, la Oficina Nacional de Tecnologías de Información de la Secretaria de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros, elabora los Estándares Tecnológicos para la Administración Pública (ETAP), en la cual se considera el protocolo IPv6 como requerimiento técnico mínimo para la compra de equipamiento de redes a nivel de LAN [85]. Asimismo, a nivel de seguridad se establece el requerimiento de IPSec [85].

En el ámbito académico, Argentina, a través de la red llamada INNOVARED (Red Nacional de Investigación y Educación Argentina), interconecta a diversas instituciones locales a través del protocolo IPv6 y esta interconectada a las diferentes redes avanzadas a nivel mundial: en América Latina (RedCLARA) [86].

El capitulo Argentino de la Internet Society, denominada ISOC Argentina, tiene un papel muy activo a nivel Latinoamérica, en relación al despliegue de IPv6 en Argentina y en el ámbito de LACNIC [84]. ISOC Argentina, ha publicado dos libros muy importantes, los cuales son: "IPv6 para todos: Guía de uso y aplicación para diversos entornos (2009) [37]" y el libro "IPv6 para operadores de Red (2014)" [59], en los cuales se detalla las buenas practicas y recomendaciones técnicas para el despliegue de IPv6.

En el libro "IPv6 para todos", para un ambiente empresarial, recomienda realizar 3 etapas: Análisis, Planificación y Transición [59]. De manera general, en la etapa de "Análisis", describe la importancia de realizar un estudio de la información del nuevo protocolo IPv6, con la cual se pueda identificar su impacto en la infraestructura (switches, enrutadores, firewall, PBX, etc.), en los servicios de red (DHCP, DNS, Servicios Web, etc.) y en el recurso humano (aprendizaje, mejora de habilidades) [59]. Este análisis permitirá establecer objetivos claros para el despliegue de IPv6 de forma gradual dentro de un ambiente empresarial [59]. En la etapa de "Planificación", se recomienda realizar los siguientes documentos [59]:

- Plan de Direccionamiento.
  - Numeración de Servidores.
  - Numeración de Terminales.
- Plan de Encaminamiento (Si es que se tuviera sucursales).
- Plan de Seguridad.
- Plan de Servicios.

Para la etapa de "Transición", se describe que este es un proceso gradual, por lo que se debe evaluar de acuerdo al análisis de impacto, por donde iniciar el despliegue, manteniendo siempre los servicios activos para el usuario final. El inicio puede partir desde los usuarios finales, luego a la infraestructura, servicios de red y finalmente a los servicios Web o aplicaciones de uso interno/externo.

Otro organismo que es muy dinámico en la adopción de IPv6, es el Network Information Center de Argentina o simplemente NIC Argentina, quienes en febrero del 2015, anunciaron la habilitación del protocolo IPv6 en sus sistemas, incorporándolo en su sistema de nombres de dominio – DNS de forma nativa, por lo que su dominio de primer nivel (ccTLD – country code Tope Level) ".ar" esta preparado para entregar dominios con IPv6 nativo [87].

A la fecha de redactado este documento, las principales instituciones públicas del gobierno de la Argentina, no han publicado el porcentaje de avance del despliegue de IPv6 en sus redes de manera oficial; sin embargo el Task Force Argentina, publica el enlace [88], en donde se muestra que el estado de uso de IPv6 basado en los parámetros de publicación de DNS, servicio de correo electrónico y servicios Web, en las instituciones públicas de la Argentina es todavía nulo [89]. A nivel país el tráfico IPv6, según las estadísticas del buscador Google, Argentina, registra a Diciembre de 2015 una adopción del 0.04% de usuarios con IPv6 que visitan el sitio web de Google [6]; y según el RIR RIPE, se registra que el 14.41% (48 de 333 AS) de AS, en Argentina, han anunciado un prefijo IPv6 [5]; sin embargo esta estadística no representaría la situación real del nivel de adopción en las Instituciones Públicas.

2.2 Brasil

En Setiembre del 2003, se publica el Decreto Nº 4829, en la que se crea el Comité Gestor de Internet en Brasil – CGI.br, para el gobierno de Internet en Brasil [90]. Este comité esta conformado por diversos actores del sector público, privado, académico y la sociedad civil [90]. Entre sus funciones se encuentra la asignación y administración de sistemas autónomos (AS), nombres de primer nivel (ccTLD) ".br" y la asignación del protocolo IP a nivel Brasil [90]. Estas funciones han sido delegadas al NIC Brasil, quien se encarga de su ejecución [91]. El NIC Brasil, cumple las funciones de un LIR en Brasil, y a través del Centro de Estudios e Investigación en Tecnología de Redes y Operaciones – CEPTRO (Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações), se encarga de la difusión del protocolo de IPv6, creando el portal ipv6.br, en donde se difunde todo el material didáctico en portugués del protocolo IPv6, actividades de capacitación, documentos normativos, guías, implementación gratuita de páginas web con IPv6, buenas prácticas y noticias actualizadas del despliegue de IPv6 en Brasil [92].

En mayo del 2012, el CGI.br, emite la Resolución CGI.br/RES/2012/007/p - Recomendação para Implantação do Protocolo IPv6 [93], en la cual recomienda iniciar la transición del protocolo IPv4 a IPv6 en los proveedores de servicio de Internet, en el gobierno, en las universidades, centros de investigación e insta a los fabricantes la inserción de compatibilidad de ambos protocolos (IPv4/IPv6) en sus productos [93].

En abril del 2014, el CGI.br, a través de la Resolución CGI.br/RES/2014/008/p - Recomendação para o suporte ao IPv6 em equipamentos que usam protocolos Internet [94], ratifica la importancia del despliegue de IPv6 en la redes de Brasil y define un conjunto de requerimientos técnicos mínimos a considerar en la compra de equipamiento que hace uso del protocolo IP [94]. Esta Resolución considera que la RFC 2460, RFC 6434, RFC 7066 y la RFC 7084, deben ser requeridos en al compra de equipamiento,

con la finalidad de garantizar el buen funcionamiento e interoperabilidad en la redes de Internet con IPv6 [94]. Asimismo, el NIC Brasil, toma como referencia el documento denominado RIPE 554, el cual es un documento publicado por el RIR RIPE y tiene como alcance establecer los requerimiento técnicos mínimos de IPv6 en la compra de equipamiento de TIC [95]. Esta acción realizada por el NIC Brasil, tiene como objetivo la de servir de guía para la compra de equipamiento TIC en los órganos de gobierno y empresas brasileras [95].

El portal IPv6.br proporciona mucha información relacionada a IPv6; sin embargo no se evidencia de manera pública alguna guía o metodología para el despliegue de IPv6 en una institución de gobierno.

En el ámbito académico, Brasil, a través de la red llamada RNP (Rede Nacional de Ensino e Pesquisa), interconecta a diversas instituciones locales a través del protocolo IPv6 y esta interconectada a las diferentes redes avanzadas a nivel mundial: en América Latina (RedCLARA), América del Norte (Internet2 y ESnet), Europa (GÉANT y Terena), Asia (APAN) y África (UbuntuNet Alliance). Participando activamente en la investigación del protocolo IPv6, entre otras tecnologías [96]. El RNP desde el 2001 viene realizando la implementación de IPv6 en su nodos de interconexión [97]. Durante este tiempo ha creado el proyecto Br6Bone que es un backbone IPv6 virtual, que tiene como objetivo realizar las capacitaciones a los técnicos de la RNP [97].

Según, las estadísticas del buscador Google, Brasil, registra a Diciembre de 2015 una adopción del 1.3% de usuarios con IPv6 que visitan el sitio Web de Google [6]; y según el RIR RIPE, se registra que el 23.84% (676 de 2836 AS) de AS, en Brasil, han anunciado un prefijo IPv6 [5]; sin embargo esta estadística no representaría la situación real a nivel de gobierno.

A la fecha de publicado este documento, Brasil no ha reportado de manera oficial el porcentaje o número de instituciones públicas que tengan implementando IPv6. En el enlace [88] al realizar el filtro “Brasil” y “Gobierno”, se muestra un 0% de uso de IPv6, esto basado en los parámetros de publicación de DNS, servicio de correo electrónico y servicios Web.

El NIC Brasil ha publicado un cronograma de adopción de IPv6 en base a un diálogo con los diferentes actores [98]. Es así que de manera sencilla se establece que primero las operadoras de telecomunicaciones (ISP) deben ofrecer tránsito IP, luego debe migrar el contenido y finalmente los usuarios [98]. En este cronograma se estimo que para Enero del 2014 todo Brasil utilizaría el nuevo protocolo; sin embargo por la información estadística citada no se ha llegado a la meta estimada [98].

2.3 Chile

En Junio del 2009, la Subsecretaria de Telecomunicaciones del Ministerio de Transportes y Telecomunicaciones de Chile, inicia su estrategia de implementación de IPv6, convocando a la presentación de proyectos para el diseño del Plan Estratégico para la implementación temprana de IPv6 en Chile [54]. En dicha convocatoria, se aprueba el proyecto denominado "IP versión 6 para Chile: Desarrollo de Roadmap para la implementación del Protocolo de Internet versión 6 (IPv6) para Chile e instalación del primer Punto de Intercambio de Tráfico (PIT) y laboratorio de experimentación IPv6" [55]. Este proyecto ha sido desarrollado por un consorcio "Publico – Académico – Privado", exactamente cofinanciado por la Corporación de Fomento de la Producción – CORFO y logro reunir a relevantes actores de la academia, la industria de Tecnologías de la Información y del sector público, como la SUBTEL, la Administración Informática de las redes del Estado, NIC Chile Research Labs, los principales proveedores de servicios de acceso a Internet en Chile, proveedores de equipamientos de redes entre otras empresas locales [54] [55]. Este proyecto se estimo en 3 años y tiene como objetivo general lo siguiente [54] [56]:

- "Implementar tempranamente y de manera bien planificada el protocolo IP versión 6 en las redes nacionales de modo de facilitar el desarrollo tecnológico de Internet, fortaleciendo de esta manera, el liderazgo regional de Chile en esta tecnología"

Asimismo, se estableció 4 ejes estratégicos:

- Desarrollar e impulsar un plan de adopción a nivel país de IPv4/IPv6,
- Difundir dentro de la comunidad el nuevo protocolo, el plan propiamente y sus participantes,
- Capacitar y formar técnicamente los recursos humanos en IPv6 y,
- Promover el desarrollo de mercados para productos basados en tecnologías IPv6.

Finalmente se definieron los siguientes resultados que se querían alcanzar [54]:

- Un punto de intercambio de tráfico (PIT) y un laboratorio de experimentación que permitan a los asociados realizar conexiones y probar la tecnología en forma segura sin afectar las redes productivas,
- Una planificación nacional (roadmap) que describe los plazos y actividades que permitirán que en Chile se adopte finalmente IPv6,
- Un curso auto contenido accesible tanto en modalidad de e-learning como sus contenidos, para ser impartidos por instituciones educacionales chilenas con el fin de formar profesionales capaces de afrontar el cambio,
- La formación altamente especializada de los recursos humanos de los asociados al proyecto.

- Información permanente de mercado identificando oportunidades de nuevas aplicaciones, productos y servicios que utilizan IPv6.

Realizando un seguimiento a la ejecución de este proyecto, en el 2011, se publica el documento denominado "Balance de Gestión Integral 2010" de la subsecretaria de telecomunicaciones, en la que se menciona, que en el año 2010, se realizo la implementación del Punto de Intercambio de Tráfico(PIT), ubicado en dependencias del Palacio de La Moneda y se comenzaron las pruebas técnicas de interconexión; así como también el proceso de capacitación al personal técnico involucrado de las empresas asociadas [57].

En junio del 2012 se publica un documento denominado "Estudio, análisis y generación de guía práctica para la aplicación por parte del Estado de Chile del requisito de incorporación de IPv6 en compras públicas" [58]. Este documento, tiene como finalidad, explicar la importancia del rol del estado como dinamizador de la adopción del nuevo protocolo, proponiendo que se impulse a través del organismo de compras del estado, en sus distintas modalidades, la obligatoriedad de cumplimiento del protocolo IPv6, tanto en hardware como en software, por parte de los productos ofertados por las empresas proveedoras [58].

A través del documento de la referencia [58] se encuentra descrita la Hoja de Ruta definida como "Hoja de Ruta para la Activación de IPv6 en el Estado Chileno"; sin embargo no es de manera oficial, ya que no se ha encontrado ningún documento normativo que lo difunda o lo sustente. Esta hoja de ruta, se divide en 3 fases, inicia con el levantamiento de información y compra de equipos, en el período del 2012 – 2014; siguiendo con la, adecuación de redes internas, en el período del 2015 – 2016; y finaliza con la adecuación de servicios a la ciudadanía en IPv6, el cual se inicia el 2017. Asimismo, este documento, tiene como anexo, a manera de extracto, el documento denominado "Plan Técnico de Implementación de IPv6", el cual esta orientado para las instituciones públicas del estado Chileno. Este plan considera 4 etapas:

- Plan de Direccionamiento,
- Plan de Ruteo,
- Plan de Seguridad y el
- Plan de Servicios

Chile, considera estos pasos, basado en el documento publicado por Internet Society Capítulo de Argentina llamado "IPv6 para todos" [59].

En el ámbito académico, Chile, a través de la red llamada REUNA (Red Universitaria Nacional), interconecta a diversas instituciones locales a través del protocolo IPv6 y esta interconectada a las diferentes redes avanzadas a nivel mundial: en América Latina (RedCLARA), América del Norte (Internet2 y Canarie), Europa (GÉANT), Asia

(APAN) y Oceanía (AARNET). Participando activamente en la investigación del protocolo IPv6, entre otras tecnologías [60].

Según, las estadísticas del buscador Google, Chile, registra a Diciembre de 2015 una adopción del 0.05% de usuarios con IPv6 que visitan su sitio Web [6]; y según el RIR RIPE, registra que el 14.29% (19 de 133 AS) de AS, en Chile, han anunciado un prefijo IPv6 [5]; asimismo, al realizar la búsqueda en el enlace [88], filtrando "Chile" y "Gobierno", se muestra un 0% de uso de IPv6, esto basado en los parámetros de publicación de DNS, servicio de correo electrónico y servicios Web; sin embargo esta estadística no representaría la situación real a nivel de gobierno.

A la fecha de publicado este documento, Chile no ha reportado de manera oficial el porcentaje de implementación de IPv6 a nivel de las instituciones públicas del gobierno, así como también no cuenta con un portal activo de monitoreo del despliegue de IPv6 a nivel de sus instituciones públicas del gobierno Chileno.

2.4 Colombia

En Julio del 2011, el Ministerio de Tecnología de la Información y las Comunicaciones – MinTIC, emite un documento, específicamente la Circular 000002, para sus instituciones públicas y la sociedad en general [61]. Este documento, insta a todas las instituciones públicas del estado, a incluir un "Plan de Transición para la Adopción de IPv6 en coexistencia con IPv4" que considere un periodo de 3 años [61]. Este plan debe de considerar los siguientes aspectos: diagnóstico, plan de inversión, cronograma de implementación, formación en IPv6 de los funcionarios del área afín, evaluación de resultados y los aspectos técnicos que permitan la correcta transición de IPv4 a IPv6 en su infraestructura tecnológica, sistemas de información y en los servicios de Internet entre las instituciones de gobierno y hacia el ciudadano [61]. Asimismo, insta a las instituciones públicas realizar sus compras tecnológicas exigiendo el soporte de IPv6 y la compatibilidad con IPv4, y que la industria del país y del sector TIC comercialice tecnología que soporte el protocolo IPv6 con compatibilidad IPv4. Es importante mencionar que este documento se genera con la finalidad de cumplir las metas establecidas en el Plan llamado "Plan Vive Digital 2010 - 2014" [61].

En el 2012, el MinTIC, elabora el documento llamado "Estrategia de Gobierno en línea 2012 – 2015", basado en el Decreto 1152 publicado en el 2008 [62]. Este documento define 8 componentes, de los cuales el primero llamado "Componente de Elementos Transversales", considera 4 actividades, y es la actividad 3 "Implementar un Sistema de Gestión de Tecnologías de la Información", en el que se considera la adopción del Protocolo IPv6 [62]. Esta actividad, define 3 metas: Planeación (1%), Implementación

(3%) y Monitoreo (1%), cada una con un porcentaje de avance a cumplirse en el 2015 [62].

En el ámbito académico, Colombia, a través de la red llamada RENATA (Red Nacional Académica de Tecnología Avanzada), interconecta a diversas instituciones a nivel local, permitiendo integrar a los diferentes actores del Sistema Nacional de Ciencia Tecnología e Innovación, mediante el protocolo IPv6 y estar interconectada con las redes avanzadas de ámbito internacional para la investigación del protocolo IPv6 y otras tecnologías [65].

En el articulo de la referencia [66], el cual no tiene fecha de publicación, se menciona que a través del Convenio 835, RENATA en coordinación con el MinTC iniciaron el proceso de implementación del protocolo IPv6 en 40 instituciones del gobierno Colombiano. La presencia de RENATA en este proceso es considerado importante, ya que es la institución con mas experiencia en el protocolo IPv6 en Colombia.

Según, las estadísticas del buscador Google, Colombia, registra a Diciembre de 2015 una adopción del 0.03% de usuarios con IPv6 que visitan su sitio Web [6]; y según el RIR RIPE, se registra que el 28.41% (25 de 88 AS) de AS, en Colombia, han anunciado un prefijo IPv6 [5]; asimismo, al realizar la búsqueda en el enlace [88], filtrando "Colombia" y "Gobierno", se muestra que solo una institución pública con el dominio "areadigital.gov.co" puede responder consultas DNS sobre IPv6, pero no se puede recibir consultas a correo electrónico y servicios Web sobre IPv6. Estas estadísticas no representan el porcentaje o estado del despliegue de IPv6 en las instituciones públicas de Colombia.

Actualmente, Colombia cuenta con un portal activo y actualizado del proceso de despliegue de IPv6 en su país a nivel de sus instituciones públicas [63]. En Octubre del 2014, Colombia publica a través de su portal de IPv6, que el 92.13% de su infraestructura tecnológica es compatible con IPv6[64]. Asimismo, se menciona también en la citada publicación, que el MinTIC, esta en un proceso de contratación para el análisis, diseño, desarrollo e implementación del plan de transición del protocolo IPv4 a IPv6, el cual considera la parte de hardware y software del MinTIC [63].

2.5 Ecuador

En Enero del 2012, el Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL, emite el documento llamado "Acuerdo Nº007-2012", en donde se describe 4 artículos relacionados al despliegue de IPv6 a nivel de las instituciones públicas del gobierno ecuatoriano [67]. El primer artículo, insta a las instituciones públicas del gobierno a implementar el protocolo IPv6 en sus sitios Web y plataformas de servicios electrónicos [67]. El segundo artículo, designa a la Secretaria Nacional de Telecomunicaciones - SENATEL, que en un plazo de 60 días, a partir de publicado en el

citado documento, realice las gestiones pertinentes para la incorporación y el correcto funcionamiento del protocolo IPv6 en el sistema de nombres de dominio del ecuador (Coutnry Code Top-Level Domain) ccTLD".ec" [67]. Los artículos 3 y 4, encargan al SENATEL, realice las acciones administrativas y normativas con el fin de que los proveedores de servicio de Internet en el ecuador implementen IPv6 en sus redes [67]. Este documento finaliza, precisando que se realizará la elaboración de un plan de compras de equipamiento ICT (Information and Communications Technology) con la finalidad de garantizar la compatibilidad con el protocolo IPv6 [67] en las instituciones públicas.

En Junio del 2012, el MINTEL, emite el documento llamado "Acuerdo Nº 039-2012", en el cual se describe las estrategias a realizarse para la adopción del protocolo IPv6 en el Ecuador [68]. Este documento describe acciones similares al documento que lo precede (Acuerdo Nº007-2012). Este nuevo acuerdo, considera, que el MINTEL incluya el proceso de incorporación y adopción del protocolo IPv6 en el programa llamado "Recursos de Banda Ancha" que forma parte su Plan Nacional de Banda Ancha del Ecuador; asimismo, delega la responsabilidad al MINTEL para realizar diversas acciones relacionadas con la capacitación de IPv6 a nivel nacional [68]. El documento finaliza, precisando que se realizará la primera evaluación sobre la adopción e incorporación del protocolo IPv6 en las instituciones públicas y en las empresas públicas de telecomunicaciones del gobierno de Ecuador [68].

El Plan Nacional de Banda Ancha del Ecuador, considera la transición y coexistencia de los protocolos IPv4-IPv6, específicamente en el objetivo "Masificar el Internet en el país, dando prioridad a las zonas rurales" y esta definido su implementación en el periodo 2012-2017 [69].

Ecuador, desde setiembre del 2009, activo un portal web con la finalidad de informar el estado de implementación de IPv6 en el Ecuador, este portal tiene definido la URL www.ipv6tf.ec y se encuentra certificado con el sello IPv6. Este portal crea una fuerza de trabajo (Task Force) del Ecuador, el cual es de participación abierta, y están involucrados diversos actores de la industria, gobierno, la academia y la sociedad en general; sin embargo, de acuerdo a las publicaciones realizadas en el portal, no esta actualizado desde el 2012 [70].

Otra iniciativa para el despliegue de IPv6 en el Ecuador, es el mencionado en la publicación de noticias, de Junio del 2014, realizada por el MINTEL, en donde se menciona la activación de un portal Web con soporte IPv6, desarrollado en conjunto con la Asociación de Empresas Proveedoras de Servicio de Internet, Valor Agregado, Portadores y Tecnologías de la Información (AEPROVI). El portal tiene como finalidad mostrar toda la información técnica, avances, recopilar opiniones, entre otros, acerca del

protocolo IPv6 en el Ecuador. En la citada publicación, se cita la siguiente URL para este portal, www.itfipv6.ec; sin embargo, no se logro acceder ya que se encuentra inhabilitado.

En el 2014, se publica el documento denominado "Gobernanza de Internet en Ecuador: Infraestructura y acceso", en el cual se menciona los avances descritos con anterioridad en este documento, correspondiente a Ecuador, y no se ha encontrado información mas actualizada [72]. En dicho documento, se hace mención a la necesidad de contar con un plan de implementación del protocolo IPv6 a nivel país y para sus entidades públicas, por lo que se puede deducir que todavía no se cuenta con el plan de implementación o no es de conocimiento público, así como también no se ha encontrado el plan de compras de equipamiento ICT.

En el ámbito académico, Ecuador, a través del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado – CEDIA, que integra las Universidades e Instituciones de Investigación y Desarrollo de Ecuador, participa activamente en el desarrollo y difusión de IPv6. CEDIA, al igual que sus pares de otros países, esta interconectado con las redes avanzadas de ámbito internacional para la investigación del protocolo IPv6 y otras tecnologías [73].

Según, las estadísticas del buscador Google, Ecuador, registra a Diciembre de 2015 un tráfico de 4.05% de usuarios con IPv6 que visitan su sitio Web [6]; y según el RIR RIPE, se registra que el 43.14% (22 de 51 AS) de AS, en Ecuador, han anunciado un prefijo IPv6 [5]; asimismo, al realizar la búsqueda en el enlace [88], filtrando "Ecuador" y "Gobierno", se muestra un 0% de uso de IPv6, esto basado en los parámetros de publicación de DNS, servicio de correo electrónico y servicios Web; sin embargo esta estadística no representaría la situación real a nivel del gobierno ecuatoriano.

A la fecha de publicado este documento, Ecuador no ha reportado de manera oficial el porcentaje de implementación de IPv6 a nivel de las instituciones del estado, así como también no cuenta con un portal actualizado de monitoreo del despliegue de IPv6 a nivel de sus instituciones públicas del gobierno de Ecuador.

2.6 Estados Unidos

En agosto de 2005, la "Office of Management and Budget – OMB", de los Estados Unidos - EEUU, emitió el Memorando M-05-22, con el asunto "Transition Planning for Internet Protocol Version 6 (IPv6)" [28]. En este documento se establece un conjunto de acciones que deben realizar cada una de las agencias de gobierno de los EEUU para el despliegue de IPv6 entre los años 2006 - 2008 [28]. De manera resumida, se menciona alguna de estas acciones previstas hacer realizadas (2006 – 2008) por cada una de las agencias de gobierno de los EEUU [28]:

- Asignación de un responsable para realizar las coordinaciones pertinentes,
- Realizar el inventario del equipamiento informático y de comunicaciones para determinar la compatibilidad con el nuevo protocolo IPv6,
- Análisis de impacto y riesgos para la transición a IPv6,
- Plan de transición IPv6,
- Asegurar en las nuevas adquisiciones de TI (Tecnologías de Información) el soporte de ambos protocolos (IPv4 – IPv6), entre otros que se detallan en la referencia [28].

En el citado memorando, también, se designa a la "National Institute for Standards and Technology – NIST", de ser necesario, para el desarrollo de las normas y ensayos para la implementación del IPv6 en el gobierno federal de EEUU y designa también a la "Federal Acquisition Regulation - FAR", de ser necesario, para el desarrollo de una modificación para el uso por todas las agencias de gobierno [28].

En el 2008, el NIST, publica el documento "A profile for IPv6 in the U.S. Government – Version 1.0", en el cual se recomienda una lista de RFCs y consideraciones técnicas mínimas de seguridad, calidad de servicio, multicast, gestión de red y movilidad para la adquisición de equipamiento (Hosts, routers y dispositivos de seguridad) con IPv6 en las agencias de gobierno [29].

En el 2009, el NIST, publica el documento "USGv6 Test Methods: General Description and Validation", en la cual se establece un programa de pruebas mínimos de IPv6 hacer realizados por laboratorios acreditados con la ISO/IEC 17025 [79]. Estados Unidos, a través de la NIST [80], actualiza continuamente el programa de pruebas para el protocolo IPv6, para lo cual ha firmado memorandos de entendimiento con el programa de prueba "IPv6 Ready Logo", para el uso de sus especificaciones de prueba como base inicial para el programa de pruebas del NIST en relación a IPv6 [79]. Asimismo, considera el uso de los parámetros de pruebas establecido por el Department of Defense - DoD en su programa "The DoD IPv6 Standards Profile for IPv6 Capable Products" [79].

En Mayo del 2009, la agencia federal Chief Information Officers – CIO, en base a las buenas prácticas Público/Privadas, publica el documento denominado "Planning Guide/Roadmap Toward IPv6 Adoption within the US Government Version 1.0" [81], y en Julio del 2012, la misma agencia (CIO), publica la versión 2.0 [31]. En estos documentos se evidencia que las agencias de gobierno, a través de sus oficinas de tecnología, cuentan con una arquitectura empresarial madura (Arquitectura de negocio, Arquitectura de Aplicaciones y Arquitectura Tecnológica), que es soportada por una infraestructura tecnológica que permite la integración, interoperabilidad, seguridad, etc., de los servicios de red entre las agencias de gobierno, con un fin compartido, la de tener

un framework que soporte todos sus servicios de TI de forma estándar, orientándose a llegar a ser un gobierno electrónico [81] [31]. La agencia federal CIO, realiza un análisis del estado actual tecnológico y normativo, para determinar la línea base que les permita establecer las estrategias de transición a una arquitectura empresarial soportada por IPv6, para lo cual, considera tres etapas importantes, basada en la RFC 5211:

- Etapa de preparación,
- Etapa de transición y
- Etapa post-transición.

En ese sentido, Estado Unidos, al tener diversas metodologías maduras de gestión de sus servicios de TI, considera un plan que le permita desplegar IPv6 en cada una de estas metodologías propias para las agencias de gobierno de ese país.

De manera general, se describe los aspectos considerados, para la etapa de preparación, el cual consiste en la elaboración del plan estratégico para realizar la transición hacia IPv6, por parte de las agencias de gobierno [81] [31]:

- Identificación de las prioridades de transición.
- Identificación de las actividades de transición.
- Los hitos de transición.
- Criterios de transición para las capacidades heredadas, actualizadas y nuevas.
- Dependencias.
- Riesgos y estrategias de mitigación.
- Mantenimiento de la interoperabilidad y seguridad durante la transición.
- El uso del USGv6 para expresar requerimientos específicos de las capacidades soportadas de IPv6 en la compra de productos específicos [80].
- Gobierno de la transición:
    - Política.
    - Roles y responsabilidades.
    - Estructura de Gestión.
    - Medición del desempeño.
    - Reportes.
    - Acciones de gestión.
- Entrenamiento.
- Pruebas.

Sumado a estos aspectos, las agencias de gobierno, tienen que elaborar y presentar casos de negocio para la inversión de IPv6 basado en su estrategia de implementación y enfocado en su arquitectura empresarial establecida [81] [31].

En la etapa de transición, la agencia CIO, define las siguientes acciones a realizar por parte de las agencias de gobierno [81] [31]:

- Acelerar del despliegue de IPv6 por parte de las agencias de gobierno.
- Creación de una agencia centralizada de autoridad de direccionamiento.
- Establecer el servicio de nombre de dominio para IPv6 (AAAA).
- Establecer el métodos de asignación de direccionamiento IP.
- Gestión de toda la red.
- Seguridad de IPv6.

Asimismo, consideran tener en cuenta los siguientes potenciales impactos en la redes de las organizaciones [31]:

- IPv6 routing
- IPv6 addressing
- IPv6 multi-homing/business continuity
- IPv6 security (firewall/IDS)
- Telework/remote access
- IPv6 device management
- IPv6 address and network management
- IPv6 SLAs
- DNS support

Por lo comentado, EEUU, expone una transición madura de IPv6 en sus agencias de gobierno, proporcionando guías metodológicas, técnicas y de pruebas, laboratorios de evaluación de equipamiento, normativa y el monitoreo del despliegue de este protocolo en las redes de sus agencias de gobierno. Para el monitoreo, la NIST, a través de la División denominada "Advanced Network Technologies Division", crea el portal de reportes estadísticos del despliegue de IPv6 en las agencias de gobierno [82]. Estas estadísticas, se forman considerando tres aspectos: publicación de DNS, servicio de correo electrónico y servicios Web de las agencias de gobierno [82]. A Diciembre de 2015, a través de su portal Web de monitoreo, indica que 449 agencias de gobierno publican servicios Web con IPv6, 140 tienen sus servicios de correo con IPv6 y 251 DNS han sido publicados con IPv6 [82]. Sin embargo, todavía queda una brecha de 853(Web), 483(mail) y 587 (DNS) agencias [82].

En el ámbito académico, EEUU, a través de la Internet2, que es la red académica y de investigación de EEUU, participa activamente en el desarrollo y difusión de IPv6. Internet2 esta conformado por comunidades de investigación y educación, el gobierno y el sector privado y se comunica a través de IPv6 con otras redes avanzadas a nivel mundial [83].

2.7 España

En Abril del 2011, el Consejo de Ministros de España, aprueba el documento denominado "Plan de Fomento para la Incorporación de Protocolo de Internet IPv6 en España", el cual tiene como objetivo dinamizar la incorporación del protocolo IPv6 [74]. Dicho Plan, a nivel general es impulsado por el Ministerio de Industria, Energía y Turismo - MITYC, y a nivel de la instituciones públicas de España, por el Ministerio de Política Territorial y Administración Pública - MPTYAP [74].

Este Plan considera inicialmente 10 medidas, las cuales están orientadas a la incorporación de IPv6 en los servicios de Internet, iniciando por el MITYC, el portal www.ipv6.es, www.060.es (administracion.gob.es) y en otros 10 portales de instituciones públicas, así como también las siguientes acciones:

- La difusión y capacitación del nuevo protocolo a las instituciones públicas, fomentando la participación público-privada;
- Apoyo en proyectos de implementación de IPv6 en el sector privado;
- Habilitación del protocolo IPv6 en el sistema de nombres de domino de España ccTLD."es";
- Creación de un grupo de trabajo, que reúna a las organizaciones mas representativas tanto público como privadas;
- Elaboración del plan de direccionamiento de la redes nacionales;
- Impulsar la incorporación de IPv6 como requisito de compra pública en productos y servicios de tecnología; y
- Encarga al MITYC y al MPTYAP, realizar el seguimiento y coordinación en el ámbito internacional [74].

En Marzo del 2012, España, publica el documento denominado "Guía para la incorporación de IPv6 como requisito de compra pública", en el cual se realiza una análisis de los requerimiento técnicos a tener en cuenta para la compra de hardware, software, equipo humano, comunicaciones y conectividad en las instituciones públicas de España [75]. El documento recomienda diversas buenas prácticas por cada componentes:

- **Para hardware,** considera el uso de los 7 niveles de clasificación definidos en el RIPE-501bis, definir los RFCs requeridos y la elaboración de cuestionarios que permitan a las empresas proveedoras justificar el cumplimiento del soporte de IPv6 y de las RFC requeridas [75].
- **Para el Software,** se recomienda considerar las buenas practicas definidas por RIPE, los estándares recomendados por el Departamento de Defensa de los Estados Unidos, realizar consultas a bases de datos especializadas en análisis de soporte IPv6 en software (6DISS – IPv6 DISSemination and Explotation, IPv6-

to-Estándar, University of Wisconsin-Madison IPv6 Application Compatibility y National Information Infrastructure Development Institute), generar una lista de RFCs de cumplimiento obligatorio y exigir pruebas de funcionamiento en un ambiente doble pila (IPv4 – IPv6) [75].

- **Para el equipo humano,** se recomienda que este personal disponga de alguna certificación en IPv6 con la participación en otros proyectos de tecnología [75].
- **Para comunicaciones y conectividad,** se diferencia en conectividad a Internet y VPN, para cada uno de estos tipos de conectividad, se recomienda solicitar acuerdos de nivel de servicio independientes del protocolo a usarse, la no utilización de mecanismos de túneles, el 100% de tablas de enrutamiento global con IPv4 e IPv6 (Para una conectividad a Internet), soporte de protocolos BGP, IS-IS, OSPFv3 y RIPng (Para una conectividad VPN), servidores DNS IPv6, realizar un cuestionario de preguntas directas sobre el soporte de IPv6 por parte del ISP (Recomienda utilizar el cuestionario propuesto por CISCO [76]), entre otros según las necesidades de la institución [75].

España desde el año 2002 crea el IPv6 Task Force (www.spain.ipv6tf.org), el cual tiene como objetivo la investigación sobre el nuevo protocolo IPv6 y la implementación de este en España; sin embargo, el MITYC a través del portal de administración electrónica (www.administracionelectronica.gob.es) es el que viene informando sobre la implementación del protocolo IPv6 en las instituciones públicas del gobierno de España.

En la publicación mas reciente, Marzo del 2013, informa que la implementación de IPv6 es del 1% y que el MPTYAP implemento el portal www.060.es (actualmente direccionado a www.administracion.gob.es), el cual es el punto de acceso para los servicios prestados a las administraciones públicas de España.

Este portal es compatible con el protocolo IPv6 y es accedido, por las administraciones públicas, a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que cumple la función de pasarela hacia la infraestructura del www.060.es. SARA es un conjunto de infraestructura de comunicaciones y servicios que conecta las redes de las administraciones públicas de España e Instituciones Europeas, para lo cual el MPTYAP y el Instituto Nacional de Tecnologías de las Comunicaciones – INTECO, vienen elaborando los borradores para la implementación total de IPv6 en la red SARA; así como también un plan de direccionamiento en IPv6 para las administraciones públicas.

En el ámbito académico, España, a través de la RedIRIS, que es la red académica y de investigación de España, participa activamente en el desarrollo y difusión de IPv6. RedIRIS, al igual que sus pares de otros países, esta interconectado con las redes

avanzadas de ámbito internacional para la investigación del protocolo IPv6 y otras tecnologías [73].

La RedIRIS, publica una "Guía para el despliegue de IPv6" en instituciones que tengan un prefijo IPv4, este procedimiento se resume en los siguientes puntos [78]:

- Solicitud de Direccionamiento.
- Solicitar el enrutamiento del prefijo.
- Configurar el DNS y pedir la delegación inversa.
- Definir un plan de direccionamiento para la institución.
- Revisar la política de seguridad.
- Revisar los procedimientos de gestión de la red.
- Actualizar los equipos de comunicaciones troncales.
- Publicar los primeros servicios con doble stack.
- Desplegar doble stack en la intranet de la organización.

Asimismo, implementa un servidor (RedIRIS) para medir y comparar la velocidad de conexión entre protocolos IPv4 e IPv6, el cual puede ser accedido a través del test de velocidad ipv6-test (http://www.ipv6-test.com/speedtest/) [110].

A la fecha, de la elaboración de este documento (Diciembre 2015), podemos obtener las siguientes estadísticas del buscador Google, el cual reporta que España, registra un tráfico del 0.13% de usuarios con IPv6 que visitan su sitio Web [6]; y según el RIR RIPE, se registra que el 20.28% (100 de 493 AS) de AS, en España, han anunciado un prefijo IPv6 [5]. Estas estadísticas son generales, por lo que no representan el estado actual de la transición a nivel de las instituciones publicas en España.

Sobre el despliegue de IPv6 en las instituciones públicas se tiene como única información el publicado en el portal de administración electrónica, el cual precisa que a Marzo 2013 se tiene un 1% de avance en la implementación del protocolo IPv6 [77].

CAPITULO III: ANALISIS SITUACIONAL DE LA ADOPCION DE IPv6 EN LAS INSTITUCIONES PUBLICAS DEL ESTADO PERUANO

El presente capítulo tiene como objetivo describir la situación actual de la estrategia definida por el estado peruano para la adopción de IPv6 y el análisis de la implementación del protocolo IPv6 en las instituciones públicas que tienen participación directa en el desarrollo de las telecomunicaciones y de las tecnologías de la información y comunicación en el Perú, siendo estas instituciones las encargadas de establecer las políticas y las primeras que deberían de adoptar en sus redes el nuevo protocolo (IPv6).

3.1 Estrategia del Gobierno Peruano

De acuerdo al análisis preliminar realizado en el Capitulo I, específicamente en el numeral 1.1 Análisis de la Problemática, se evidencio el liderazgo de Perú en la adopción de IPv6 a nivel del RIR LACNIC; sin embargo, al realizar un análisis mas riguroso, este liderazgo es conseguido por el despliegue de IPv6 realizado por la empresa Telefónica del Perú S.A.A, quien ha sido el primero en anunciar que cerca de 200,000 clientes residenciales con conexión ADSL acceden a Internet utilizando IPv6 desde Junio del 2013 [9]. Sumado a esto, se observa que otros ISP con presencia nacional, tienen asignado un prefijo IPv6 por el LACNIC, como se puede observar en la Tabla 3.

Tabla 3 ***Principales ISP en el PERU con IPv6***

INTERNET SERVICE PROVIDER	SECTOR	PREFIJO ASIGNADO POR LACNIC	FECHA DE ASIGNACION
Telefónica del Perú S.A.A	CORPORATIVO RESIDENCIAL TELEFONIA MOVIL	2001:1388::/32	14/072005
América Móvil Perú S.A.C.	CORPORATIVO RESIDENCIAL TELEFONIA MOVIL	2800:200::/32 2800:4b0::/32	11/04/2008 28/05/2010
OPTICAL TECHNOLOGIES S.A.C.	CORPORATIVO	2800:120::/32	04/06/2007
VIETTEL PERÚ S.A.C.	RESIDENCIAL TELEFONIA MOVIL	2800:cc0::/32	11/01/2012
OLO del Perú S.A.C	RESIDENCIAL MOVIL	2803:4800::/32	24/02/2012
NEXTEL DEL PERU S.A.	CORPORATIVO RESIDENCIAL TELEFONIA MOVIL	2803:7180::/32	10/06/2014

Fuente: LACNIC [102]

La implementación de IPv6 por parte de los ISP, a nivel Perú, no ha sido generada por alguna iniciativa estratégica, regulatoria o documento normativo realizado por el gobierno peruano. Esta iniciativa corresponde al desarrollo del mercado mundial de las telecomunicaciones y principalmente al agotamiento del espacio de direcciones IPv4, lo que ha obligado a los ISP de Perú a estar preparados.

Actualmente, en el Perú, los ISP ofrecen servicios de acceso a Internet con IPv6 a sus clientes residenciales y corporativos, contando con planes estratégicos de migración para sus diferentes servicios, desde los fijos a los inalámbricos.

Estas acciones realizadas por los ISP en el Perú, ha permitido que el Perú sea considerado como uno de los lideres de los países que forman parte del RIR LACNIC, incluso superando en tráfico a países de Europa; sin embargo, este liderazgo es a nivel de trafico cursado, en mayor porcentaje por usuarios residenciales, y no representa el porcentaje de avance real de adopción de IPv6 a nivel país, específicamente por parte de

las instituciones públicas o de gobierno a nivel de su infraestructura tecnológica y contenidos.

Las iniciativas a nivel del gobierno peruano, para promover la adopción del nuevo protocolo, han sido casi nulas. De acuerdo a la búsqueda realizada en los portales web de las instituciones públicas analizadas en el presente estudio, se encontró solo un documento formal en el que se menciona el protocolo IPv6, específicamente, el documento publicado el 26 de Julio del 2011, denominado "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0". En este Plan, se establecen diversos objetivos a cumplirse al 2015, considerado la inclusión del protocolo IPv6. Específicamente se menciona que para alcanzar su Objetivo Nº 01 "Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la sociedad de la información y del conocimiento", deberá considerarse como estrategia lo siguiente: "Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el protocolo de Internet v6 (IPv6)".

A la fecha de elaboración de este documento, Enero 2016, se realizo una búsqueda en los portales de los actores relacionados al desarrollo de las telecomunicaciones y las tecnologías de información y comunicación en el estado peruano (ONGEI, MTC, OSIPTEL, INICTEL-UNI y CONCYTEC) no encontrando ninguna iniciativa que permita cumplir con la estrategia mencionada. Así mismo, no se ha encontrado ningún documento técnico a nivel de gobierno que detalle un modelo de transición de IPv4 a IPv6 a nivel país o específicamente en las instituciones públicas.

De acuerdo a las experiencias de los países analizados en el capitulo II, estos países, a través de sus órganos de gobierno relacionados directamente al desarrollo de las telecomunicaciones y de las tecnologías de información y comunicación, establecieron políticas que fomentan una transición planificada del protocolo IPv4 a IPv6 en sus instituciones públicas u oficinas de gobierno. Se evidencio que los países de Estados Unidos y España, quienes tienen desarrollado planes estratégicos y documentación técnica para la transición al nuevo protocolo, han logrado dinamizar el despliegue de IPv6 en sus instituciones públicas u oficinas de gobierno; y el resto de países quienes vienen realizando diversas acciones que fomentan el uso del protocolo IPv6, como establecer políticas públicas que obligan a considerar el uso del protocolo IPv6 en las compras de gobierno y en la elaboración de planes estratégicos a nivel de gobierno, permiten que estos países realicen una transición al nuevo protocolo de manera planificada, dinamizando el uso del protocolo IPv6 a nivel de instituciones públicas u oficinas de gobierno, algo que todavía en el Perú no se ha iniciado.

Por lo antes descrito, en el Perú no se ha establecido una estrategia de transición a nivel de instituciones públicas; por lo que realizaremos un análisis de manera individual a cada una de las instituciones públicas que tienen relación directa con el desarrollo de las telecomunicaciones y tecnologías de información y comunicación, con la finalidad de conocer su avance de manera aislada en la implementación de este protocolo de IPv6.

3.2 Instituciones Públicas del Gobierno Peruano

Las instituciones públicas identificadas que guardan relación directa con el desarrollo de las telecomunicación y las tecnologías de Información y Comunicación son:

- **Ministerio de Transporte y Comunicaciones – MTC,** a través del subsector Comunicaciones, conduce, ejecuta y supervisa la aplicación de políticas de las telecomunicaciones en el Perú [103].
- **Oficina Nacional de Gobierno Electrónico e Informática – ONGEI,** es el ente rector del Sistema Nacional de Informática en el Perú, y se encarga de la normatividad, desarrollo de proyectos en TIC, capacitaciones entre otras funciones conducentes a la modernización del estado peruano (Gobierno electrónico) [104].
- **Concejo Nacional de Ciencia, Tecnología e Innovación Tecnológica – CONCYTEC,** ente rector del Sistema Nacional de Ciencia y Tecnología e Innovación Tecnológica – SINACYT. Tiene como unas de sus principales funciones la de impulsar el desarrollo de nuevas tecnologías a través de la investigación [105].
- **Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL,** es el ente regulador y supervisor del mercado de los servicios públicos de telecomunicaciones, y tiene como finalidad principal la de garantizar la calidad y eficiencia del servicio de telecomunicaciones a los usuarios y la de proteger el desarrollo de este mercado [106]. El OSIPTEL es miembro activo del LACNIC, siendo categorizados como Miembro Activo B [111].
- **Instituto Nacional de Investigación y Capacitación de Telecomunicaciones – INICTEL-UNI,** tiene como dos de sus principales objetivos la investigación en las Tecnologías de Información y Comunicación – TIC y en la de fortalecer las competencias en TIC de las entidades públicas y privadas que lo requieran [107].

3.2.1 Situación Actual de las Instituciones Publicas Identificadas

Para determinar el grado de avance de implementación o conocer alguna estrategia de manera individual realizada por cada una de las instituciones públicas identificadas, utilizaremos dos fuentes: Portal del Sistema Electrónico de Contrataciones del Estado – SEACE y a través de encuestas. Las encuestas se realizará a los directores de informática o el que haga de sus veces en cada una de las instituciones públicas identificadas.

El SEACE, nos permite acceder a una fuente primaria relevante para determinar si las instituciones públicas en estudio han considerado en sus contratos de servicio de acceso a Internet, el requerimiento de direcciones IPv6.

De la búsqueda realizada, en el SEACE, se tiene la siguiente información:

Tabla 4 ***Contratos de Servicio de Internet – Entidad Públicas***

Nº	INSTITUCIÓN PÚBLICA	PROCESO DE LICITACION	PROTOCOLO IP REQUERIDO
1	Ministerio de Transporte y Comunicaciones – MTC	CP-18-2014/MTC [119]	IPv4
2	Oficina Nacional de Gobierno Electrónico e Informática – ONGEI	CP-004-2014-PCM [121]	IPv4
3	Concejo Nacional de Ciencia, Tecnología e Innovación Tecnológica – CONCYTEC	AMC-028-2013-CONCYTEC-OGA [120]	IPv4
4	Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL	CP-010-2013/OSIPTEL [108]	IPv4/ IPv6 *No se especifica el tamaño del prefijo
5	Instituto Nacional de Investigación y Capacitación de Telecomunicaciones – INICTEL-UNI	CP-002-2015-INICTEL-UNI [109]	IPv4 IPv6/48

Fuente: SEACE [108] [109] [119] [120] [121]

De acuerdo a lo indicado en la Tabla 4, solo 2 instituciones públicas evaluadas, OSIPTEL y el INICTEL-UNI, han considerado la solicitud de un prefijo IPv6 en sus contratos de servicio de acceso a Internet.

Realizaremos pruebas de verificación para conocer si estas instituciones públicas usan el protocolo IPv6 contratado en sus servicios web, correo y DNS. Primero realizamos la consulta, desde una consola UNIX, utilizando el comando "host" con el parámetro "t", consultando los registro de tipo A, quad-A (AAAA), MX y NS para analizar la configuración del protocolo de red.

Al realizar las consultas a las páginas web del OSIPTEL y del INICTEL-UNI, estas no responden a la consulta del registro tipo AAAA, soportando solo registro del tipo A.

```
MMAC:~ root# host -t A www.osiptel.gob.pe
www.osiptel.gob.pe has address 190.12.80.22
MMAC:~ root# host -t AAAA www.osiptel.gob.pe
www.osiptel.gob.pe has no AAAA record
```

Figura 3 Consulta a la página web del OSIPTEL

Fuente: Elaboración propia

```
MMAC:~ root# host -t A www.inictel-uni.edu.pe
www.inictel-uni.edu.pe has address 190.12.75.115
MMAC:~ root# host -t AAAA www.inictel-uni.edu.pe
www.inictel-uni.edu.pe has no AAAA record
```

Figura 4 Consulta a la página web del INICTEL-UNI

Fuente: Elaboración propia

Para consultar el servicio de correo, del OSIPTEL y del INICTEL-UNI, utilizamos el registro del tipo MX, esto nos permite conocer los dominios de sus servidores de correo y de esta manera hacer las consulta de registro tipo A y AAAA. Se obtiene como respuesta solo al registro tipo A para ambas instituciones.

```
MMAC:~ root# host -t MX osiptel.gob.pe
osiptel.gob.pe mail is handled by 10 mail.osiptel.gob.pe.
MMAC:~ root# host -t A mail.osiptel.gob.pe.
mail.osiptel.gob.pe has address 190.12.80.23
MMAC:~ root# host -t AAAA mail.osiptel.gob.pe.
mail.osiptel.gob.pe has no AAAA record
```

Figura 5 Consulta al servicio de correo del OSIPTEL

Fuente: Elaboración propia

```
MMAC:~ root# host -t MX inictel-uni.edu.pe
inictel-uni.edu.pe mail is handled by 20 mailbk.inictel-uni.edu.pe.
inictel-uni.edu.pe mail is handled by 10 mail.inictel-uni.edu.pe.
MMAC:~ root# host -t A mail.inictel-uni.edu.pe
mail.inictel-uni.edu.pe has address 190.12.75.86
MMAC:~ root# host -t A mailbk.inictel-uni.edu.pe
mailbk.inictel-uni.edu.pe has address 190.12.88.12
MMAC:~ root# host -t AAAA mail.inictel-uni.edu.pe
mail.inictel-uni.edu.pe has no AAAA record
MMAC:~ root# host -t AAAA mailbk.inictel-uni.edu.pe
mailbk.inictel-uni.edu.pe has no AAAA record
```

Figura 6 Consulta servicio de correo del INICTEL-UNI

Fuente: Elaboración propia

Para el servicio DNS, utilizamos el registro de tipo NS para hacer la consulta a los dominios del OSIPTEL y del INICTEL-UNI. Se obtiene como respuesta, de ambas instituciones, los servidores de dominio del ISP Optical Technologies S.A.C., comercialmente conocido como "Optical IP". Al pasar el parámetro a los servidores consultados se observa que ninguno de los servidores DNS responde a consultas del registro tipo AAAA.

```
MMAC:~ root# host -t NS inictel-uni.edu.pe
inictel-uni.edu.pe name server ns2.opticalip.com.pe.
inictel-uni.edu.pe name server ns1.opticalip.com.pe.
MMAC:~ root# host -t A ns1.opticalip.com.pe.
ns1.opticalip.com.pe has address 190.12.72.230
MMAC:~ root# host -t AAAA ns1.opticalip.com.pe.
ns1.opticalip.com.pe has no AAAA record
MMAC:~ root# host -t A ns2.opticalip.com.pe.
ns2.opticalip.com.pe has address 190.12.64.102
MMAC:~ root# host -t AAAA ns2.opticalip.com.pe.
ns2.opticalip.com.pe has no AAAA record
```

Figura 7 Consulta del servicio DNS del INICTEL-UNI

Fuente: Elaboración propia

```
MMAC:~ root# host -t NS osiptel.gob.pe
osiptel.gob.pe name server ns1.opticalip.com.pe.
osiptel.gob.pe name server ns2.opticalip.com.pe.
MMAC:~ root# host -t A ns1.opticalip.com.pe.
ns1.opticalip.com.pe has address 190.12.72.230
MMAC:~ root# host -t AAAA ns1.opticalip.com.pe.
ns1.opticalip.com.pe has no AAAA record
MMAC:~ root# host -t A ns2.opticalip.com.pe.
ns2.opticalip.com.pe has address 190.12.64.102
MMAC:~ root# host -t AAAA ns2.opticalip.com.pe.
ns2.opticalip.com.pe has no AAAA record
```

Figura 8 Consulta servicio de DNS del OSIPTEL

Fuente: Elaboración propia

Como segundo método de verificación, realizamos pruebas de accesibilidad de IPv6 a las páginas web del OSIPTEL y del INICTEL-UNIC, utilizando la herramienta web www.ipv6-test.com [100], obteniendo como respuesta que ambos dominios no responden a consultas del registro de tipo AAAA.

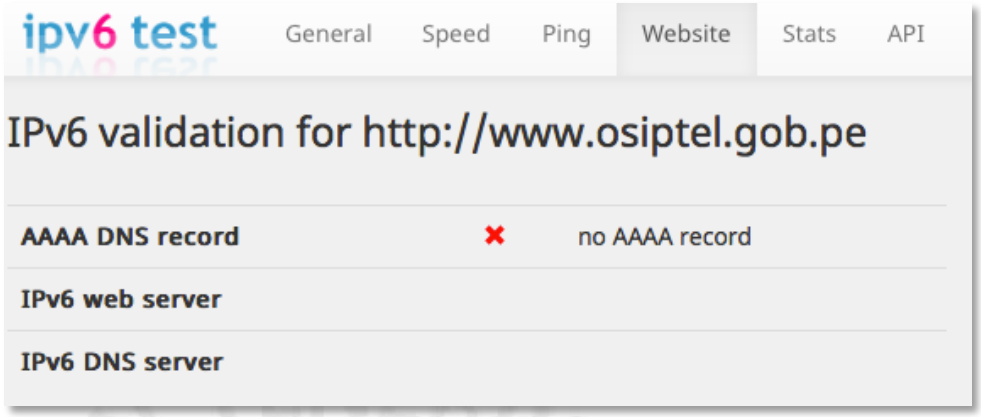


Figura 9 Prueba accesibilidad IPv6 página web OSIPTEL

Fuente: IPv6-Test [100]

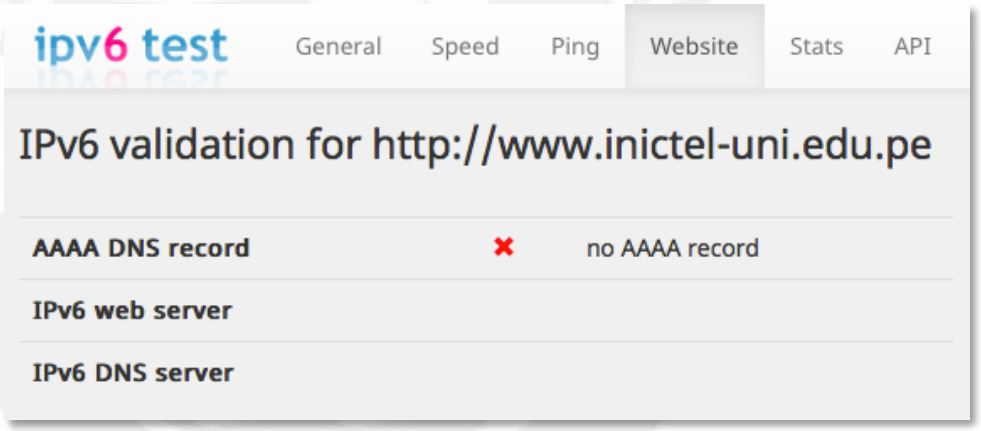


Figura 10 Prueba accesibilidad IPv6 página web INICTEL-UNI

Fuente: IPv6-Test [100]

Como segunda fuente de verificación primaria, para conocer si estas instituciones públicas cuentan con un plan o estrategia interna de despliegue de IPv6 en sus redes, se aplico una encuesta de forma personal a los responsables de las áreas de informática.

ENCUESTA

1. ¿Cómo considera la implementacion de IPv6 en su red y contenidos?
   ___ Extremadamente importante
   ___ Muy importante
   ___ Importante
   ___ Neutral
   ___ Algo importante
   ___ No es importante en lo absoluto

2. ¿Cuenta con un plan o estrategia de transición hacia el protocolo IPv6?
   ___ SI
   ___ NO

3. ¿Cuales son las principales limitaciones de la no activación del protocolo IPv6 en su red y contenidos?
   ___ Recurso humano capacitado.
   ___ Contenidos.
   ___ Modelo de referencia (Buenas prácticas y documentos técnicos).
   ___ Documento normativo de obligatoriedad.
   ___ Otros. Especificar:_____

4. ¿Considera importante tener un modelo de referencia para la transición hacia IPv6 en las instituciones públicas?
   ___ SI
   ___ NO

Figura 11 Encuesta realizada a las Instituciones Públicas de Perú

Fuente: Elaboración propia

Como resultado de la encuesta, se obtuvo los siguientes resultados:

- En relación a la primera pregunta, de la Encuesta, la ONGEI y el MTC consideran "Muy Importante" la implementación del protocolo IPv6 en sus redes. Las otras tres (03) instituciones públicas (OSIPTEL, CONCYTEC y el INICTEL-UNI) consideran "Importante" esta implementación.
- En relación a la segunda pregunta, de la Encuesta, las cinco (05) instituciones públicas no cuentan con un plan de transición o estrategia de transición para habilitación del protocolo IPv6.
- En relación a la tercera pregunta, de la Encuesta, la ONGEI, OSIPTEL y el CONCYTEC indican que las principales limitaciones para iniciar la transición es el personal técnico capacitado, y consideran que contar con una guía de referencia, les permitiría conocer por donde iniciar la transición hacia el nuevo protocolo basado en buenas prácticas. Las otras dos (02) instituciones públicas (INICTEL-UNI y MTC) consideran que una guía de referencia facilitaría la transición hacia el nuevo protocolo.

- En relación a la última pregunta, de la Encuesta, las cinco (05) instituciones públicas encuestadas consideran importante contar con una guía de referencia de buenas prácticas que les permita iniciar una adecuada transición.

3.2.2 Situación Actual de la Red Académica Peruana

De lo analizado en el capitulo II, se evidencio que las redes académicas juegan un papel importante en el desarrollo del protocolo IPv6 en cada país. En el Perú este rol es realizados por la Red Académica Peruana, conocida por sus siglas RAAP, la cual es una organización conformada por un grupo de 5 universidades descritas en la siguiente Tabla [112]:

Tabla 5 ***Miembros de la RAAP Perú***

UNIVERSIDAD	SECTOR	FUNCIÓN
Universidad Nacional Mayor de San Marcos	Público	Presidencia
Universidad Nacional Agraria La Molina	Público	Vice-presidencia
Universidad Peruana Cayetano Heredia	Público	Secretaria
Pontificia Universidad Católica del Perú	Privado	Vocal
Universidad Nacional de Ingeniería	Público	Vocal

Fuente: Página web RAAP [113]

Actualmente viene siendo liderada por la Universidad Nacional Mayor de San Marcos, quien fue elegida para el periodo 2012 – 2016 [112].

De acuerdo a la información publicada en su portal web (www.raap.org.pe), la participación de la RAAP no es muy dinámica, no encontrando documentación técnica relacionada a sus ámbitos de estudio o investigación, específicamente en IPv6 [113]. La última actividad de capacitación registrada es de Julio del 2010, lo cual muestra un estado estático de su participación en el desarrollo de Internet en el Perú, en especial a nivel de las instituciones públicas del Perú [113].

La RAAP tiene asignado el prefijo 2001:13a0::/32, el cual ha sido asignado por el RIR LACNIC [102]. Según el prefijo asignado se realiza el análisis para

conocer si este prefijo IPv6 es utilizado por la RAAP para sus servicios de web, correo y DNS, para lo cual realizaremos las mismas pruebas que se hicieron anteriormente a través de una consola UNIX y realizando el test proporcionado por el portal www.ipv6-test.com [100].

```
MMAC:~ root# host -t A raap.org.pe
raap.org.pe has address 200.16.4.40
MMAC:~ root# host -t AAAA raap.org.pe
raap.org.pe has IPv6 address 2001:13a0:1041::215
```

Figura 12 Consulta a la página web de la RAAP

Fuente: Elaboración propia

```
MMAC:~ root# host -t MX raap.org.pe
raap.org.pe mail is handled by 5 alt1.aspmx.l.google.com.
raap.org.pe mail is handled by 5 alt2.aspmx.l.google.com.
raap.org.pe mail is handled by 1 aspmx.l.google.com.
raap.org.pe mail is handled by 10 aspmx3.googlemail.com.
raap.org.pe mail is handled by 10 aspmx5.googlemail.com.
raap.org.pe mail is handled by 10 aspmx2.googlemail.com.
raap.org.pe mail is handled by 10 aspmx4.googlemail.com.
MMAC:~ root# host -t AAAA ALT1.ASPMX.L.GOOGLE.COM.
ALT1.ASPMX.L.GOOGLE.COM has IPv6 address 2607:f8b0:400c:c06::1a
MMAC:~ root# host -t AAAA alt2.aspmx.l.google.com.
alt2.aspmx.l.google.com has IPv6 address 2800:3f0:4003:c00::1b
MMAC:~ root# host -t AAAA aspmx.l.google.com.
aspmx.l.google.com has IPv6 address 2607:f8b0:4002:c06::1a
MMAC:~ root# host -t AAAA  aspmx3.googlemail.com.
aspmx3.googlemail.com has IPv6 address 2800:3f0:4003:c01::1a
MMAC:~ root# host -t AAAA aspmx5.googlemail.com.
aspmx5.googlemail.com has IPv6 address 2a00:1450:400c:c07::1b
MMAC:~ root# host -t AAAA aspmx2.googlemail.com.
aspmx2.googlemail.com has IPv6 address 2607:f8b0:400c:c06::1b
MMAC:~ root# host -t AAAA aspmx4.googlemail.com.
aspmx4.googlemail.com has IPv6 address 2a00:1450:400b:c02::1b
```

Figura 13 Consulta al servicio de correo de la RAAP

Fuente: Elaboración propia

```
MMAC:~ root# host -t NS raap.org.pe
raap.org.pe name server ns1.raap.org.pe.
MMAC:~ root# host -t A ns1.raap.org.pe.
ns1.raap.org.pe has address 200.16.4.38
MMAC:~ root# host -t AAAA ns1.raap.org.pe.
ns1.raap.org.pe has no AAAA record
```

Figura 14 Consulta al servicio DNS de la RAAP

Fuente: Elaboración propia

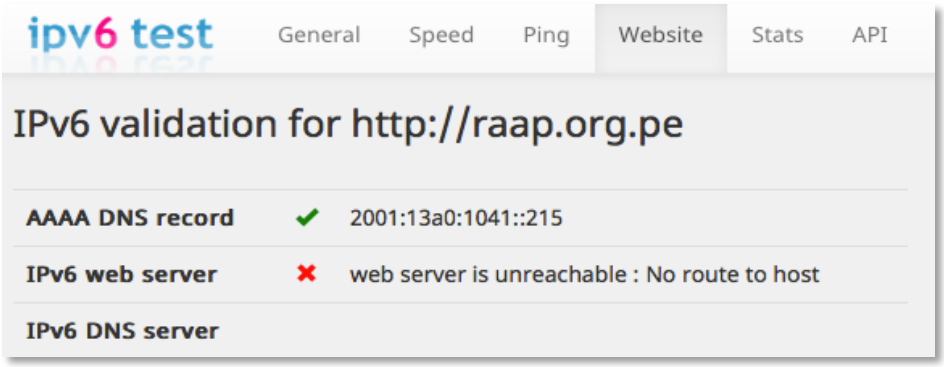


Figura 15 Prueba accesibilidad IPv6 página web RAAP

Fuente: IPv6-Test [100]

Según las pruebas realizadas, se muestra que el portal web de la RAAP es resuelto ante una consulta AAAA, pero su portal web no esta preparado para ser accedido a través de IPv6; la consulta al servicio de correo, nos muestra que este servicio es contratado con el servicio de correo de Google, por lo que al realizar las consultas de resolución se muestra que todos los servidores responden a una resolución AAAA; y en relación al servicio DNS se observa que la RAAP no cuenta con una servidor DNS para el protocolo IPv6.

De lo comentado, se evidencia que la RAAP no tiene, a la fecha de escrito este documento, configurado el protocolo IPv6 a nivel de todos sus servicios de red, lo que suma a su poca participación en el despliegue del protocolo IPv6 a nivel de Perú y el poco aporte en temas de investigación y capacitación. El nivel de participación de la RAAP Perú, es muy poca o casi nula, en comparación con sus pares en los países analizados en el capitulo II, en donde se evidencia que las redes académicas aportan con documentos técnicos, capacitaciones e investigaciones realizadas sobre el protocolo IPv6 para dinamizar el despliegue del nuevo protocolo, especialmente en las instituciones públicas.

3.2.3 Situación Actual del NIC Perú

En el Perú, no existe una organización propiamente conocida como NIC Perú, para la administración del dominio geográfico (country code top-level domain – ccTLD) ".pe" y la operación del DNS a nivel Perú. Estas funciones son realizadas por la Red Científica Peruana – RCP [114].

Al ingresar al portal web de la RCP (www.rcp.net.pe), no se encuentra información técnica o documentación alguna de la estructura de dominios en

Perú o noticias relacionadas a los avances en la administración de los dominios.

Una de las acciones que están realizando actualmente los NIC de los países analizados en el Capitulo II, es que estos soporten de manera nativa el protocolo IPv6 a nivel de ccTLD permitiendo delegar los dominios a nivel geográfico con el nuevo protocolo, sin lugar a duda una tarea que la RCP debe estar considerándolo hacerlo en los próximos años.

La participación activa de los NIC a nivel de los países es importante para el desarrollo del Internet a nivel de sus países, lo cual al parecer es una tarea pendiente de la RCP.

3.2.4 Situación Actual del NAP Perú

La NAP Perú, esta conformado por los principales ISP a nivel nacional, el cual esta conformada por 15 miembros, de los cuales 9 anuncian prefijos IPv4 e IPv6 a nivel del NAP [115].

Tabla 6 *Miembros del NAP Perú*

Nº	Miembro NAP	Versión del Protocolo en sus Prefijos anunciados
1	América Móvil Perú – (Claro)	IPv4/IPv6
2	Americatel Perú	Solo IPv4
3	BT Latam	IPv4/IPv6
4	Internexa	Solo IPv4
5	Level3	IPv4/IPv6
6	Infoductos y Telecomunicaciones del Perú	IPv4/IPv6
7	Media Commerce Perú	IPv4/IPv6
8	Netline Perú	Solo IPv4
9	Optical Networks	IPv4/IPv6
10	Telefónica del Perú	IPv4/IPv6
11	Telefónica Móviles	IPv4/IPv6
12	Telmex Perú	IPv4/IPv6
13	Bitel Perú	Solo IPv4
14	Entel Perú	Solo IPv4
15	Convergía Perú	No anuncia

Fuente: Página web NAP

CAPITULO IV: MODELO DE REFERENCIA PARA LA TRANSICION DE IPv4 a IPv6

El presente capítulo tiene como objetivo presentar un modelo de referencia para la transición del protocolo IPv4 al nuevo protocolo IPv6 en las instituciones públicas del estado peruano, tomando como referencia las acciones realizadas por los países analizados en capitulo II y las recomendaciones realizadas por la ISOC Capitulo Argentina y el LACNIC.

4.1 INSTITUCIONES PUBLICAS EN EL PERU

La implementación del protocolo de IPv6 en las instituciones públicas en el Perú depende directamente de cada una de las Oficinas de Tecnologías de Información y Comunicación (En adelante OTIC) o la que haga de sus veces en cada una de estas instituciones, existiendo estas en las municipalidades, empresas e instituciones del sector público en sus tres niveles de gobiernos (nacional, regional y local); sin embargo, la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI es el ente rector del Sistema Nacional de Informática - SNI, quien establece las políticas y estrategias en gobierno electrónico e Informática y el Ministerio de Transporte y Comunicaciones - MTC, quien a través de el Sub-Sector Comunicaciones, establece políticas y estrategias en Telecomunicaciones.

En ese sentido, la definición de las políticas y estrategias para el despliegue de IPv6 a nivel del sector público parten desde estas dos instituciones públicas, la ONGEI y del MTC.

Existen otras instituciones públicas, las cuales se han analizado en el capitulo III, que también se considera importante su participación para dinamizar el despliegue del protocolo IPv6 a nivel de gobierno. Estas instituciones son las que tiene relación directa con el desarrollo de las telecomunicaciones y tecnologías de información a nivel país, las cuales deben cumplir un rol de acuerdo a sus funciones establecidas normativamente.

En la siguiente Tabla se propone el rol que cada una de estas cumpliría para el modelo que se describirá en el presente documento:

Tabla 7 ***Rol de las Instituciones Públicas***

ROL	INSTITUCIÓN PÚBLICA
Políticas/Estrategias/Supervisión	ONGEI/MTC
Académica/Técnica /Investigación/Innovación	INICTEL-UNI RAAP OSIPTEL RCP
Financiamiento y Fomento en Investigación/Innovación	CONCYTEC
Administración del NIC Perú	RCP
Adquisiciones	OSCE

Fuente: Elaboración propia

A la fecha las OTIC para una adecuada planificación y gestión de su gobierno de Tecnologías de Información y Comunicación deben de elaborar los siguientes documentos de forma obligatoria:

- Plan Operativo Informático – POI.
- Plan Estratégico de Tecnologías de Información - PETI.
- Sistema de Gestión de Seguridad de la Información – SGSI (NTP ISO/IEC 27001:2014).

Estos documentos permiten establecer la planificación y estrategias para las OTIC, y sirven de sustento formal para la programación de adquisiciones de bienes y servicios definidos para el logro de las estrategias que se hayan definido por estas. La planificación de la adopción del nuevo protocolo IPv6 es transversal a estos documentos, lo que permite fortalecer su implementación.

Por otra parte, a nivel país se han establecido diversas estrategias referentes a telecomunicaciones y tecnologías de la información, las cuales permitirían dinamizar el despliegue del protocolo de IPv6 a nivel de las instituciones públicas. Estas estrategias son:

- Ley Nº 29904 "Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica".
- Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0".
- Encuesta Nacional de Recursos Informáticos en la Administración Pública – ENRIAP.
- Política Nacional de Gobierno Electrónico 2013 – 2017.
- Plan de Implementación de la Política Nacional de Modernización de la Gestión Pública 2013 – 2016.

4.2 MODELO DE TRANSICION

El modelo de transición establece una metodología para realizar la activación del protocolo IPv6 en la red de cada una de las Instituciones Públicas o Instituciones de Gobierno (en adelante IG) de forma progresiva a través de un conjunto de métodos y procedimientos.

El modelo de transición propuesto tiene como alcance a todas las IG, indiferentemente del número de computadoras o el tamaño de red que estas tengan.

De manera general establecemos que las IG tienen las siguientes características en relación al uso del protocolo IPv4:

- Equipamiento Core solo con el protocolo IPv4,
- Red nativa a nivel de LAN solo con el protocolo IPv4,
- Red WAN solo con el protocolo IPv4,
- Acceso a Internet solo con el protocolo IPv4,
- Aplicaciones y contenido accesibles solo con el protocolo IPv4.
- Recurso humano con conocimientos del IPv4.

Se define 5 fases que permitirán realizar una transición hacia el protocolo IPv6:

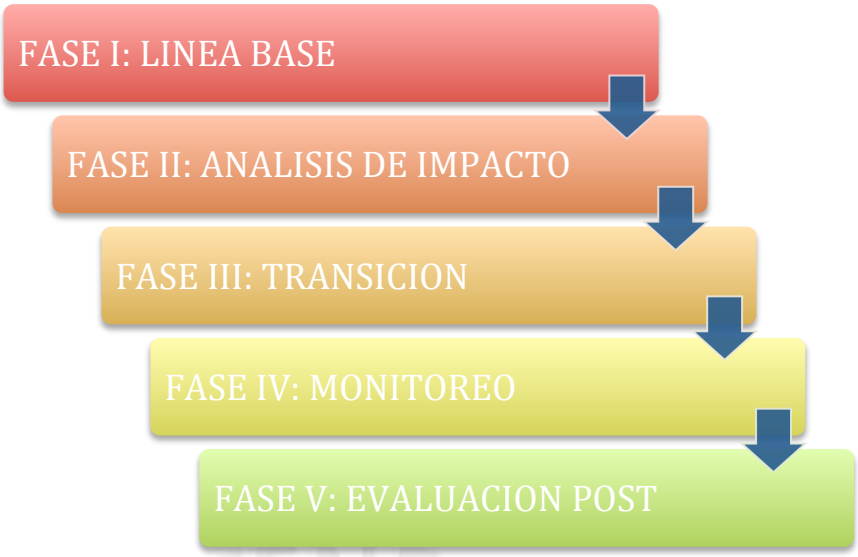


Figura 16 Fases para la transición de IPv4 a IPv6

Fuente: Elaboración propia

4.2.1 Fase I: Línea Base

Esta Fase permitirá conocer la situación actual del equipamiento, software, servicios y recursos humanos relacionados al soporte tecnológico en las IG, para identificar las brechas y definir los indicadores que permitan medir el grado de avance en el proceso de transición al protocolo IPv6.

La principal pregunta a responder en esta fase es ¿Dónde Estoy?, la cual nos llevará a la pregunta ¿Hacia dónde quiero ir?, preguntas que podrán ser absueltas con el desarrollo de esta Fase.

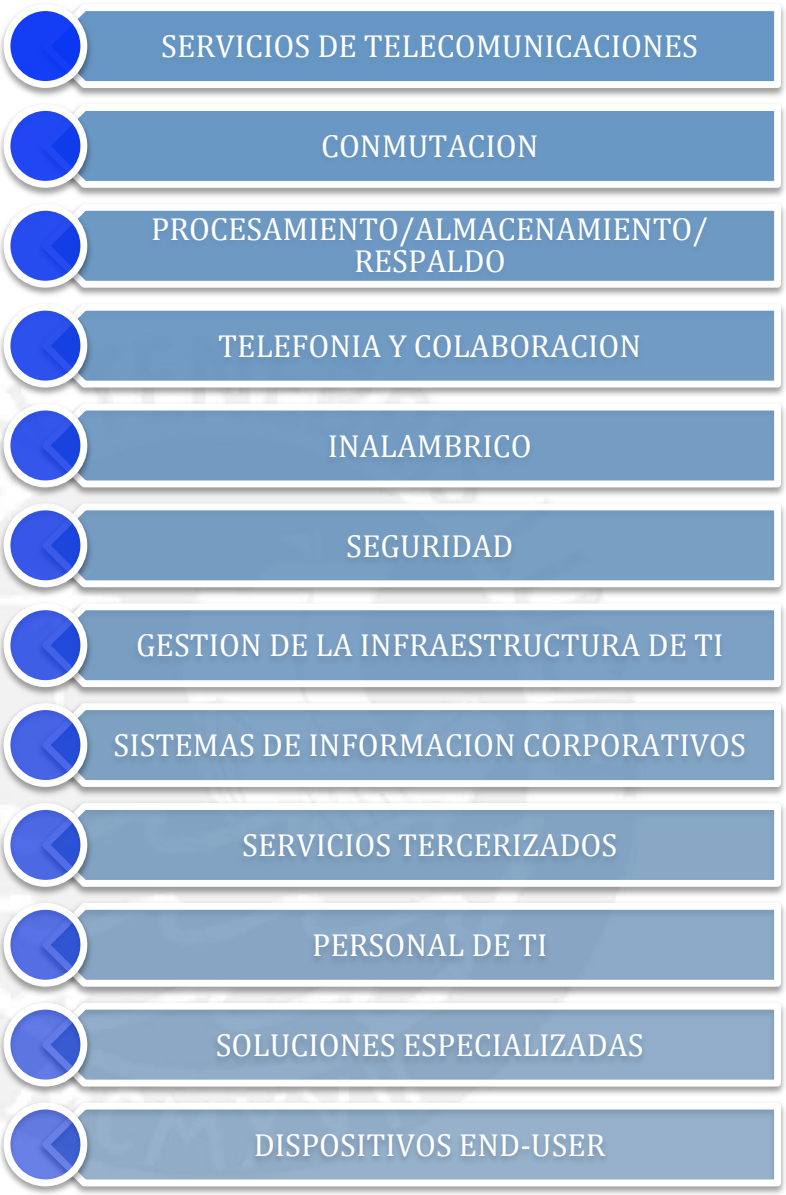
Esta Fase se divide en tres etapas de forma secuencial:

Figura 17 Etapas de la Fase I

Fuente: Elaboración propia

4.2.1.1 Primer Etapa: Situación Actual

Para poder establecer las estrategias es necesario conocer la situación actual, para lo cual se deberá levantar información de los siguientes componentes o sistemas:



Cada uno de estos componentes permitirá conocer la situación actual y establecer las estrategias para una transición progresiva hacia el protocolo IPv6 por parte de las IG.

Tabla 8 ***Formato - Cuadro de Levantamiento de Información***

SERVICIOS DE TELECOMUNICACIONES	▪ Documentar las características de acceso a Internet y/o WAN contratadas, como los datos del ISP, velocidad contratada, tipo de enlace (principal/respaldo), Pull de direcciones públicas IPv4, DNS, datos del contrato, niveles de servicio considerados, etc. ▪ En caso de tener sedes, se deberá de documentar los datos por cada una realizando el diagrama topológico físico y lógico.
CONMUTACION	▪ Realizar el inventario de los equipos de conmutación (switches), detallando las especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, etc.), de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos: switch Core, switch SAN, switch distribución, etc.
PROCESAMIENTO/ ALMACENAMIENTO/ RESPALDO	▪ Realizar el inventario de los equipos/software detallando las especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, servicios DHCP, DNS, FTP, etc.) de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos/software: servidor, storage, Librería de Backup, software de respaldo, Sistema Operativos, etc.
TELEFONIA Y COLABORACION	▪ Este componente hace referencia a los elementos de las comunicaciones unificadas, tanto hardware como software. Se deberá realizar el inventario de los equipos/software detallando las especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, etc.) de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos/sofware: Teléfonos analógicos/digitales/IP, softphone, central IP, Gateways FXS / FXO / Digitales / GSM, videoconferencia, MCU (Multipoint Control Unit), servidores SIP/H323, software de colaboración, comunicaciones multimedia, call manager, etc.

INALAMBRICO	▪ Realizar el inventario de los equipos/software detallando las especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, etc.) de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos: Wireless LAN Controller – WLC, access point, etc.
SEGURIDAD	▪ Realizar el inventario de los equipos/software destinados a la seguridad informática y física, detallando las especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, etc.) de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos: Firewall, IDS/IPS, Antivirus, Web Application Firewall - WAF, Anti – SPAM, Web Content Filter, Proxy, CCTV, controles de acceso, alarmas, etc.
GESTION DE LA INFRAESTRUCTURA DE TI	▪ Las soluciones destinadas a soporte, monitoreo y administración de la red. Estas deberán de ser documentados, con la finalidad de conocer el soporte del protocolo IPv6. ▪ Lista de aplicativos: Software de virtualización, software de gestión y monitoreo de red, software mesa de ayuda, etc.
SISTEMAS DE INFORMACIÓN CORPORATIVOS	▪ Este componente hace referencia a los sistemas de información que son el soporte de los procesos de la organización, incluyendo las bases de datos que lo componen. Es importante elaborar una mapa y la arquitectura de estos sistemas para conocer su interacción. ▪ Es importante identificar los sistemas de información externos con los que se realiza comunicación, identificando el protocolo. Uno de los principales es el SIAF y SIGA, proporcionados por el Ministerio de Economía y Finanzas.
SERVICIOS TERCERIZADOS	▪ Realizar la documentación de los servicios tercerizados, como servicios de housing, hosting, cloud computing, alquileres de equipos, mesas de ayuda externas, centro de datos de respaldo, entre otros. ▪ Los servicios identificados deben de detallarse para analizar su influencia en el proceso de transición, ya que estos servicios también deben usar el protocolo IPv6.

PERSONAL DE TI	▪ Se deberá de identificar al personal de TI, describiendo sus roles y responsabilidades. ▪ Se deberá realizar una evaluación al personal de TI para conocer el grado de conocimiento del nuevo protocolo.
SOLUCIONES ESPECIALIZADAS	▪ Este componente agrupa a todos aquellos equipos que pueden ser controlados y monitoreados, y a las aplicaciones que gestionan estos equipos a través del protocolo IP. ▪ Este componente agrupa a los siguientes equipos: Sistemas de Energía Ininterrumpida (UPS), equipos eléctricos, equipos mecánicos, aplicativos como SCADA, BMS (Building Management System), entre otros que utilicen el protocolo IP.
DISPOSITIVOS END-USER	▪ Este componente agrupa todo el equipamiento y su software que interactúa directamente con el usuario. Se deberá de realizar el inventario de los equipos detallando sus especificaciones técnicas de cada uno de ellos (Sistemas Operativos, protocolos, antigüedad, etc.) de tal manera permita conocer el soporte del protocolo IPv6. ▪ Lista de equipos: Computadoras de escritorio, laptops, impresoras, tablets, teléfonos móviles, etc.

Fuente: Elaboración propia

4.2.1.2 Segunda Etapa: Análisis de Brecha

El análisis de brecha permitirá establecer, a partir de la situación actual, la definición de los objetivos de mejora tecnológica para el proceso de transición hacia el protocolo IPv6.

La Tabla 9, es una propuesta de un formato tipo para establecer los objetivos, en base a las brechas identificadas por cada componente. Por ejemplo, si para el servicio contratado de acceso a Internet, se tiene solo un conjunto de direcciones IPv4 públicas, la brecha seria no contar con direcciones IPv6 del tipo GUA (Global Unicast Address), por lo cual mi objetivo estaría relacionado a la contratación del servicios de acceso a Internet, solicitando la entrega de un prefijo IPv6 o realizar el trámite para solicitud directa al LACNIC de un prefijo IPv6.

Tabla 9 ***Formato - Análisis de Brecha***

Componentes/Sistemas	Elementos Identificados	IPv4	IPv6	Descripción	Brecha	Objetivo
Servicios de Telecomunicaciones	…					
Conmutación						
Procesamiento/ Almacenamiento/ Respaldo						
Telefonía y Colaboración						
Inalámbrico						
Seguridad						
Gestión de la Infraestructura de TI						
Sistemas de Información Corporativos						
Servicios Tercerizados						
Personal de TI						
Soluciones Especializadas						
Dispositivos End-User						

Fuente: Elaboración propia

4.2.1.3 Tercera Etapa: Definición de Indicadores

En esta etapa se deberá de definir los indicadores por componente. Esto permitirá realizar mediciones del avance del proceso de transición hacia IPv6.

Identificados los indicadores, se realizará tres mediciones, al inicio del proceso, que representa la situación actual, a la mitad y al cierre del tiempo estimado para el proceso de transición. Se recomienda un periodo de 3 años de manera inicial.

La definición de indicadores deberá ser definido por el equipo de TI encargado del proceso de transición. En la Tabla 10, se propone el formato para esta etapa.

Tabla 10 ***Formato - Definición de indicadores***

Componentes /Sistemas	Indicador	Cantidad de Equipos	Situación Actual	Punto de Control (Tiempo Medio)	Valor Esperado (3 años)
Conmutación	Ejemplo. % de switches Core con Soporte IPv6	2	0	1	2
	Ejemplo. % de switches Core configurados con IPv6	2	0	1	2
	….				

Fuente: Elaboración propia

4.2.2 Fase II: Análisis de impacto

El análisis de impacto permitirá conocer los riesgos y amenazas que implica la migración hacia el protocolo IPv6, de tal manera se establezca las estrategias necesarias para mitigarlos y disminuir el impacto que esta pueda generar.

La primera pregunta que nos llevará a responder este análisis es ¿Qué pasaría si no adopto IPv6?, pregunta que trata un tema muy importante, que es el "riesgo de no hacer nada". Otro pregunta importante, que esta Fase permitirá absolver es ¿Donde empiezo?, obtener esta respuesta permitirá iniciar la Fase III, que es el proceso de transición.

Es importante realizar este análisis por cada uno de los componentes definidos en el numeral 4.2.1.1, de tal manera permita iniciar el proceso de transición por el componente que menos afecte o impacte a los servicios de TI, especialmente aquellos que son el soporte de los procesos de negocio de la IG.

El primer análisis a realizar es el impacto que generaría el de no adoptar el protocolo IPv6 en la IG, para lo cual la IG, de acuerdo a sus procesos de negocio y a su fin como IG, deberá de identificar el impacto de no hacerlo. Este análisis debe considerar por lo menos una proyección a 10 años.

Las IG para iniciar el proceso de transición, deberán de iniciar por el componente que menos afecte o impacte a los proceso de negocio de la IG, ya que el proceso de transición deberá ser progresivo y es importante iniciar por el componente mas simple o el que requiera cambios no complejos.

El análisis se realiza en base a los Objetivos propuestos en el análisis de Brecha. Esto permitirá conocer el impacto del objetivo propuesto en los proceso de negocio de la IG. En la Tabla 11, se recomienda un formato tipo para este tipo de análisis.

Tabla 11 ***Formato – Análisis de Impacto***

Componentes	**Elementos Identificados**	Objetivo	Riesgo	Amenaza	Impacto	Estrategias de Mitigación
…						

Fuente: Elaboración propia

Siguiendo con el ejemplo descrito en el numeral 4.2.1.2, en el cual se establece como Objetivo "La contratación de servicio de acceso a Internet con prefijo IPv6", se puede considerar como riesgo, "el no acceso de clientes con IPv4 a los servicios a través de Internet que brinda la IG", y como amenaza, "falla en software y sistemas principales o ataques de seguridad a través de IPv6 no controlados", generando un impacto "No aceptable" a nivel de la IG, ya que afectaría a los proceso de negocio que se relacionan directa e indirectamente a los servicios a través de Internet que brinda la IG. A partir de esto, elaborar una lista de estrategias como, la de "contratar el servicio de acceso a Internet con ambas versiones del protocolo IPv4 e IPv6", precisando que el ISP deberá tener implementado algunos de los mecanismos de transición que permitan comunicar ambos mundos (IPv4-IPv6). La selección del mecanismo de transición se detalla en el documento llamado "Mecanismo de Transición Preferido" el cual forman parte de los anexos de la presente tesis.

Se propone la clasificación para la valoración del Impacto, los cuales pueden ser modificados de acuerdo a cada IG.

- **No Aceptable:** Puede afectar seriamente a los proceso de negocio de la IG. El tiempo de recuperación afecta a las operaciones de la IG.
- **Mayor:** Puede afectar seriamente a los servicios de TI. El tiempo de recuperación afecta a las operaciones de la IG.

- **Moderado:** Puede afectar a la operación de ciertas áreas especificas de la IG. El tiempo de recuperación no afecta a los procesos de negocio de la IG.
- **Menor:** No afecta a ninguna de las áreas de la IG. El tiempo de recuperación no afecta a los procesos de negocio de la IG.

Finalizado este proceso de análisis, se deberá de agrupar aquellos objetivos que generen menor impacto, con la finalidad de iniciar la transición por estos, de tal manera permitan al personal iniciar la experiencia y mejorar las habilidades técnicas hacia el nuevo protocolo IPv6.

4.2.3 Fase III: Transición

La transición considera el inicio de las actividades conducentes a la implementación de IPv6. Se deberá crear un documento denominado "Estrategia de Transición" en la cual se establezca un conjunto de actividades, tareas e hitos que permitan la implementación de forma planificada. Estas actividades deberán de ser programadas, estableciendo los roles y responsabilidades de cada uno de los actores identificados que participan en su implementación.

La primera actividad a considerar será la de realizar la capacitación al recurso humano que administra y brinda el soporte tecnológico en las IG, con la finalidad de proporcionar los conocimientos técnicos en IPv6 para iniciar la transición hacia el nuevo protocolo. Esta actividad deberá de ser detallada en el documento de Estrategia.

La recomendación para la implementación de una nueva tecnología es iniciar por el componente o sistema que menos impacte en los procesos de una organización, para lo cual se elaborará una lista resumen del análisis realizado en la Fase II, de tal manera nos permita visualizar los componentes o sistemas que generan menor impacto hasta los que son clasificados como "No Aceptables". Asimismo, esto permitirá establecer un proceso de maduración del personal de TI para afrontar aquellos componentes o sistemas de mayor complejidad.

Se toma como referencia las actividades definidas por el gobierno de Estados Unidos, los cuales deben ser considerados en la estrategia de implementación [31]:

- Actualización de hardware y software para IPv6.
- Actualización de los Sistemas de Información.
- Actualización de los enlaces de acceso a Internet y WAN.

- Identificación de las prioridades de transición.
- Identificación de los principales hitos.
- Seguridad durante la transición.
- Establecer el gobierno de la transición:
    - Políticas.
    - Roles y responsabilidades.
    - Gestión de la transición.
    - Medición de la transición.
    - Reporte de avances.
- Entrenamiento del recurso humano
- Pruebas

La gestión de la transición puede ser realizado considerando buenas prácticas en gestión de proyectos como la propuesta por el Project Management Institute – PMI u otra metodología que sea conocida por el personal de la IG.

La elaboración de la estrategia de transición es particular por cada una de la IG, y varia según la realidad identificada en cada una de las Fases previas. La transición deberá estar acompañada de documentos técnicos, que permitan ser de guía para los especialistas de cada IG al momento de iniciar esta Fase. En la presente tesis se proporciona una serie de recomendaciones para los siguientes puntos:

- Fundamentos Teóricos para la Transición.
- Mecanismo de Transición Preferido.
- Buenas Practicas para la Elaboración del Plan de Direccionamiento IPv6.
- Recomendaciones de Compra con IPv6 en las Instituciones Públicas.
- Metodología para Pruebas de Compatibilidad de IPv6 en Software.

4.2.4 Fase IV: Monitoreo

El monitoreo deberá de realizarse a nivel central, de acuerdo a las competencias de los diferentes actores citados en la Tabla 4, para lo cual deberá de elaborarse una herramienta que permita realizar el seguimiento y control del avance de la implementación por cada una de las instituciones públicas.

Un ejemplo de herramienta a implementar es la desarrollada por el National Institute of Standards and Technology - NIST de los Estados Unidos, en la cual se realiza un monitoreo de los diferentes servicios de red, mostrando

estadísticas en tiempo real del grado de avance de implementación de IPv6 por cada institución de gobierno de los Estados Unidos.

Otra opción, mas inmediata, es utilizar la herramienta disponible publicada por la familia Vyncke-Dehouse Family, quienes son un grupo de profesionales en telecomunicaciones que desarrollaron una herramienta que permite realizar el monitoreo de implementación de IPv6 por cada país, conociendo el nivel de implementación del protocolo IPv6 a nivel DNS, publicación web y SMTP, filtrando por tipo de dominio, en nuestro caso el ".gob.pe". El desarrollo de esta herramienta es liderada por Eric Vyncke, quien es un profesional que trabaja en la IETF y en el IPv6 Council de Bélgica [88]. La herramienta la podemos ubicar en la Referencia [88].

4.2.5 Fase V: Evaluación POST

Se actualizará los indicadores definidos en la Fase I, con la finalidad de conocer el cumplimiento de estas y definir una lista de lecciones aprendidas que permitan mejorar el modelo de transición.

La evaluación se deberá de realizar cada 3 años, considerando que es un tiempo estimado en el cual una institución de gobierno puede realizar la renovación tecnológica.

4.3 PROPUESTAS DE ACCIONES A NIVEL CENTRAL

A nivel de gobierno central, la institución pública de mayor jerarquía institucional es el Ministerio de Transporte y Comunicaciones (MTC), quien a través del Sub-Sector de Comunicaciones, deberá de enviar un documento formal que obligue a cada una de las instituciones de gobierno que están relacionadas directamente con el desarrollo de las telecomunicaciones y las tecnologías de información y comunicación en el Perú, inicien la elaboración de manera conjunta el Plan de Transición hacia el Protocolo IPv6, considerando de manera inicial la metodología propuesta en esta tesis y los documentos técnicos que forman parte de esta, los cuales son una recopilación de buenas prácticas para la transición hacia IPv6.

Estas actividades decantan en la primera Acción a realizar por parte del Gobierno Peruano, la cual la definimos de las siguiente manera:

Acción 1: Formalizar a través de un documento normativo la formación del Comité de Transición hacia IPv6 liderado por el Sub-Sector de Comunicaciones del MTC.

Composición:

- Representante del Sub-Sector Comunicaciones y equipo técnico,

- Representante de la Oficina Nacional de Gobierno Electrónico e Informática y equipo técnico,
- Representante de la Red Académica Peruana y equipo técnico,
- Representante del NIC PERU (Red Científica Peruana y el punto.pe)
- Representante del INICTEL-UNI y equipo técnico,
- Representante del OSIPTEL y equipo técnico,
- Representante del CONCYTEC y equipo técnico y
- Representante del OSCE y equipo técnico.

Funciones Principales:

- Elaborar el Plan de Transición hacia IPv6 a nivel Perú y
- El despliegue e IPv6 en sus redes y servicios, el cual deberá ser monitoreado por el comité.

Las estrategias de nivel país a considerar son:

- Fortalecer a la RAAP, el INICTEL-UNI y la RCP Perú para la elaboración de documentos técnicos sobre IPv6 los cuales deberán estar adaptados a nuestra realidad.
- Mejoramiento de la estructura organizacional del NIC Perú, el cual es asumido por la RCP y el Punto.pe, quienes de acuerdo a los descrito en el Capítulo III, no tienen una participación activa sobre publicaciones de documentos técnicos de acuerdo a su competencia.
- Habilitación del ccTLD para IPv6.
- Fortalecer al IPv6 Council Perú, de tal manera dinamice su participación a nivel Perú.
- Desarrollar una herramienta de monitoreo de avance de la implementación de IPv6 en las instituciones públicas.

Como resultado de la Acción 1, se propone un Acción segunda que permita establecer de manera obligatoria que cada Institución Pública realice su Plan de Implementación hacia IPv6. Esta acción se define de la siguiente manera:

Acción 2: Establecer de obligatoriedad la transición del protocolo IPv6 en todas las instituciones públicas a nivel nacional, instando que las OTIC sean las responsables de su elaboración, implementación y seguimiento. Esta acción puede ser reforzado por un marco normativo. Por ejemplo a nivel de Ley.

CONCLUSIONES

- Cada uno de los países analizados mantiene una estructura bien definida de los roles y responsabilidades de los actores que gobiernan el desarrollo de las telecomunicaciones y de las tecnologías de información en cada uno de ellos. Estos actores tienen una participación muy activa elaborando diversos documentos técnicos y realizando investigaciones que fomentan la adopción del nuevo protocolo en sus redes y contenidos.
- Si bien es cierto el Perú, es uno de los países que tiene mayor porcentaje de tráfico de usuarios que se conectan a IPv6, este tráfico es del tipo residencial en el mayor porcentaje y no representaría el nivel de adopción del nuevo protocolo por parte de las instituciones públicas.
- Las instituciones públicas a nivel de Perú que están directamente relacionadas con el desarrollo de las telecomunicaciones y las tecnologías de información no tienen planes de transición hacia el protocolo IPv6, y su principal limitación de iniciar la transición es no saber por donde empezar (Modelo de Referencia) y capacitación de su recurso humano.
- El modelo de referencia y los documentos técnicos elaborados en la presente tesis permitirá a las instituciones públicas establecer un punto de partida para iniciar sus planes de transición hacia el nuevo protocolo IPv6.
- La presente tesis ha evidenciado que contar con un modelo de referencia a nivel de gobierno permite dinamizar el despliegue del nuevo protocolo, ya que la transición hacia IPv6 no considera solo su activación, sino un conjunto de métodos y procedimientos estructurados que apoyados de documentos técnicos permiten el éxito de la transición.

RECOMENDACIONES

- El gobierno peruano a través del Ministerio de Transportes y Comunicaciones deberá de iniciar la formación de un comité que permita elaborar la estrategia de transición a IPv6 para las instituciones públicas.
- Iniciar el proceso de transición en las Instituciones Públicas de Perú que están relacionadas directamente al desarrollo de las Telecomunicaciones y de las Tecnologías de Información, considerando el modelo y los documentos técnicos propuestos en el presente trabajo.
- Elaborar un gestor de monitoreo que permita realizar el control y seguimiento del proceso de implementación de IPv6 a nivel de las Instituciones Públicas (dominio gob.pe.).
- Incluir en la estructura curricular de los estudio de pre-grado, específicamente en las carreras de ingeniería relacionadas a telecomunicaciones e informática, temas que permitan profundizar los conceptos y aplicaciones del protocolo IPv6 y fomentar la innovación en base a este nuevo protocolo.
- Normar la obligatoriedad de transición a nivel nacional, el cual deberá ser liderado por el comité propuesto en la presente tesis.

BIBLIOGRAFIA

[1] Forouzan, B. A. & Chung, S. F., (2006), *TCP/IP protocol suite – 3rd ed.,* New York, USA: Mc Graw Hill.

[2] ARIN. (2014). Estado de agotamiento de IPv4 en la IANA. Recuperado de https://www.arin.net/resources/request/ipv4_countdown.html. Ultimo acceso: 02 de Diciembre de 2014.

[3] NRO. (2015). Disponibilidad de bloque de direcciones IPv4. Recuperado de https://www.nro.net/wp-content/uploads/NRO_Q3_2015.pdf. Ultimo acceso: 12 de Noviembre de 2015.

[4] Hagen, S. (2014). *IPv6 Essentials*. Disponible en Safari Books Online.

[5] RIPE. (2015). Estado del despliegue de IPv6. Recuperado de http://v6asns.ripe.net/v/6. Ultimo acceso: 31 de Diciembre de 2015.

[6] Google. (2015). Estadísticas IPv6 a nivel mundial. Recuperado de http://www.google.com/intl/es/ipv6/statistics.html. Ultimo acceso: 31 de Diciembre de 2015.

[7] Google. (2015). Estadísticas IPv6 a nivel Perú. Recuperado de http://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption. Ultimo acceso: 31 de Diciembre de 2015.

[8] LACNIC. (2015). Registro de organizaciones que implementan IPv6. Recuperado de http://portalipv6.lacnic.net/quienes-implementan/. Ultimo acceso: 04 de Octubre de 2015.

[9] Telefónica. (2013). Noticia del despliegue de IPv6 en Perú. Recuperado de http://bit.ly/1udljcC. Ultimo acceso: 10 de Enero de 2015.

[10] ITU. (2010). Facilitating the transition from IPv4 to IPv6. Recuperado de http://bit.ly/1w6XetG. Ultimo acceso: 30 de Noviembre de 2014.

[11] IETF. (1995). RFC 1819: Internet Stream Protocol Version 2 (ST2) Protocol Specification - Version ST2+. Recuperado de http://www.rfc-editor.org/rfc/rfc1819.txt. Ultimo acceso: 11 de Julio de 2015.

[12] IETF. (1998) RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. Recuperado de http://www.rfc-editor.org/rfc/rfc2460.txt. Ultimo acceso: 11 de Julio de 2015.

[13] IETF. (1998). RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. Recuperado de http://www.rfc-editor.org/rfc/rfc2474.txt. Ultimo acceso: 12 de Agosto de 2015.

[14] IANA. (2014). Protocol Numbers. Recuperado de http://bit.ly/1w75bPK. Ultimo acceso: 10 de Noviembre de 2015.

[15] IANA. (2014). Internet Protocolo Version 6 (IPv6) Parameters. Recuperado de http://bit.ly/1w9pj2u. Ultimo acceso: 15 de Noviembre de 2015.

[16] IETF. (2005). RFC 4302: IP Authentication Header. Recuperado de http://www.rfc-editor.org/rfc/rfc4302.txt. Ultimo acceso: 12 de Agosto de 2012.

[17] IETF. (2005). RFC 4303: IP Encapsulating Security Payload (ESP). Recuperado de http://www.rfc-editor.org/rfc/rfc4303.txt. Ultimo acceso: 17 de Setiembre de 2015.

[18] IETF. (2006). RFC 4291: IP Version 6 Addressing Architecture. Recuperado de http://www.rfc-editor.org/rfc/rfc4291.txt. Ultimo acceso: 10 de Setiembre de 2015.

[19] IETF. (2010). RFC 5952: A Recommendation for IPv6 Address Text Representation. Recuperado de http://www.rfc-editor.org/rfc/rfc5952.txt. Ultimo acceso: 10 de Setiembre de 2015.

[20] Odom, Wendell. (2008). *CCNA ICND2 Guía Oficial para el examen de Certificación*. España: Pearson Educación.

[21] IETF. (2009). RFC 2526: Reserved IPv6 Subnet Anycast Addresses. Recuperado de http://www.rfc-editor.org/rfc/rfc2526.txt. Ultimo acceso: 16 de Octubre de 2015.

[22] IPv6Portal. (s.f.). Mecanismos de transición. Recuperado de http://bit.ly/1uh3Tgx. Ultimo acceso: 20 de Setiembre de 2015.

[23] IETF. (1998). RFC 2473: Generic Packet Tunneling in IPv6 Specification. Recuperado de http://www.rfc-editor.org/rfc/rfc2473.txt. Ultimo acceso: 21 de Setiembre de 2015.

[24] Portal IPv6 de Brasil. (2015). Centro de Investigación en Tecnología de redes y Operaciones. Recuperado www.ipv6.br. Ultimo acceso: 20 de Noviembre de 2015.

[25] Portal de la Subsecretaria de telecomunicaciones de Chile. (2015). Recuperado de www.subtel.gob.cl. Ultimo acceso: 20 de Noviembre de 2015.

[26] Ministerio de Tecnologías de la Información y Comunicaciones. (2015). Recuperado de www.mintic.gov.co/ipv6. Ultimo acceso: 20 de Noviembre de 2015.

[27] Portal de IPv6 del Ministerio de Industria, Energía y Turismo. (2015). Recuperado de www.ipv6.es. Ultimo acceso: 23 de Noviembre de 2015.

[28] Office of Management and Budget. (2005). "Transition Planning for Internet Protocol Version 6 (IPv6)" (OMB Memorandum M-05-22). Recuperado de http://1.usa.gov/1D4V4Qt. Ultimo acceso: 25 de Noviembre de 2015.

[29] National Institute of Standard san Technology. (2008). A Profile for IPv6 in the U.S. Government – Version 1.0. Recuperado de http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf. Ultimo acceso: 25 de Noviembre de 2015.

[30] Office of Management and Budget. (2005). Transition to IPv6 (Memorandum for Chief Information Officers of Executive Departments and Agencies). Recuperado de http://1.usa.gov/1D4V4Qt. Ultimo acceso: 25 de Noviembre de 2015.

[31] Architecture and Infrastructure Committee, Federal Chief Information Officers Council. (2012). Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government", Version 2.0. Recuperado de http://1.usa.gov/1yz5i3x. Ultimo acceso: 25 de Noviembre de 2015.

[32] FCC's TAC. IPv6 Working Groups. Benchmarking Recommedations. (2011). Recuperado de http://bit.ly/1GgiI8W. Ultimo acceso: 27 de Noviembre de 2015.

[33] IETF. (2003). RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Recuperado de http://www.rfc-editor.org/rfc/rfc3315.txt. Ultimo acceso: 28 de Noviembre de 2015.

[34] IETF. (2003). RFC 3596: DNS Extensions to Support IP Version 6. Recuperado de http://www.rfc-editor.org/rfc/rfc3596.txt. Ultimo acceso: 20 de Setiembre de 2015.

[35] IETF. (2006). RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. Recuperado de http://www.rfc-editor.org/rfc/rfc4443.txt. Ultimo acceso: 20 de Setiembre de 2015.

[36] INTERNET SOCIETY. (s.f.). Yea! LinkedIn Joins Facebook And Google In Permanently Enabling IPv6. Recuperado de http://goo.gl/7lrjwO. Ultimo acceso: 13 de Julio de 2015.

[37] LACNIC. (2014). IPv6 para Operadores de Red. Recuperado de http://goo.gl/5GKS5s. Ultimo acceso: 10 de Setiembre de 2015.

[38] IANA. (2015). IPv6 Multicast Address Space Registry. Recuperado de http://goo.gl/75kd5i. Ultimo acceso: 07 de Agosto de 2015.

[39] IETF. (2005). RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers. Recuperado de http://www.rfc-editor.org/rfc/rfc4213.txt. Ultimo acceso: 20 de Julio de 2015.

[40] IETF. (2000). RFC 2890: Key and Sequence Number Extensions to GRE. Recuperado de http://www.rfc-editor.org/rfc/rfc2890.txt. Ultimo acceso: 20 de Julio de 2015.

[41] CISCO. (2009). Service Provider IPv6 Deployment in the Last Mile. Recuperado de http://goo.gl/9QnglL. Ultimo acceso: 30 de Noviembre de 2015.

[42] IETF. (2007). RFC 4798: Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE). Recuperado de http://www.rfc-editor.org/rfc/rfc4798.txt. Ultimo acceso: 15 de Mayo de 2015.

[43] IETF. (2006). RFC 4659: BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN. Recuperado de http://www.rfc-editor.org/rfc/rfc4659.txt. Ultimo acceso: 15 de Mayo de 2015.

[44] IETF. (2010). RFC 5569: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd). Recuperado de http://www.rfc-editor.org/rfc/rfc5569.txt. Ultimo acceso: 15 de Mayo de 2015.

[45] IETF. (2010). RFC 5969: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) - Protocol Specification. Recuperado de http://www.rfc-editor.org/rfc/rfc5969.txt. Ultimo acceso: 17 de Junio de 2015.

[46] IETF. (2011). RFC 6145: IP/ICMP Translation Algorithm. Recuperado de http://www.rfc-editor.org/rfc/rfc6145.txt. Ultimo acceso: 18 de Junio de 2015.

[47] IETF. (2011). RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Recuperado de http://www.rfc-editor.org/rfc/rfc6146.txt. Ultimo acceso: 19 de Junio de 2015.

[48] IETF. (2011). RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. Recuperado de http://www.rfc-editor.org/rfc/rfc6147.txt. Ultimo acceso: 19 de Junio de 2015.

[49] IETF. (2013). RFC 6877: 464XLAT: Combination of Stateful and Stateless Translation. Recuperado de http://www.rfc-editor.org/rfc/rfc6877txt. Ultimo acceso: 17 de Julio de 2015.

[50] IETF. (2011). RFC 6333: Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. Recuperado de http://www.rfc-editor.org/rfc/rfc6333.txt. Ultimo acceso: 17 de Julio de 2015.

[51] IETF. (2013). RFC 6908: Deployment Considerations for Dual-Stack Lite. Recuperado de http://www.rfc-editor.org/rfc/rfc6908.txt. Ultimo acceso: 17 de Julio de 2015.

[52] IETF. (2015). RFC 7597: Mapping of Address and Port with Encapsulation (MAP-E). Recuperado de http://www.rfc-editor.org/rfc/rfc7597.txt. Ultimo acceso: 17 de Julio de 2015.

[53] IETF. (2015). RFC 7599: Mapping of Address and Port using Translation (MAP-T). Recuperado de http://www.rfc-editor.org/rfc/rfc7599.txt. Ultimo acceso: 18 de Julio de 2015.

[54] SUBTEL. (2009). Chile. Convocatoria Proyecto IPv6. Recuperado de http://goo.gl/yhbuAQ. Ultimo acceso: 20 de Octubre de 2015.

[55] CORFO. (s.f.). Chile. IP versión 6 para Chile: desarrollo de roadmap para la implementación del protocolo de internet versión 6 (IPV6) para Chile e instalación del primer punto de intercambio de tráfico (PIT) y laboratorio de experimentación IPV6. Recuperado de http://goo.gl/NrieFY. Ultimo acceso: 20 de Octubre de 2015.

[56] CORFO. (2009). Chile. IP versión 6 para Chile: desarrollo de roadmap para la implementación del protocolo de internet versión 6 (IPV6) para Chile e instalación del primer punto de intercambio de tráfico (PIT) y laboratorio de experimentación IPV6. Recuperado de http://goo.gl/4GhqEb. Ultimo acceso: 20 de Octubre de 2015.

[57] Dirección de Presupuestos. (2010). Chile. Balance de Gestión Integral. Recuperado de: http://goo.gl/k5kNAN. Ultimo acceso: 21 de Octubre de 2015.

[58] SUBTEL. (2012). Chile. Estudio, análisis y generación de guía práctica para la aplicación por parte del Estado de Chile del requisito de incorporación de IPv6 en compras públicas. Recuperado de: http://goo.gl/vgmF8x. Ultimo acceso: 20 de Octubre de 2015.

[59] ISOC ARGENTINA. (2009). Argentina. IPv6 para Todos. Recuperado de https://goo.gl/JIjRqV. Ultimo acceso: 18 de Noviembre de 2015.

[60] REUNA. (s.f.). Quienes Somos. Recuperado de: http://www.reuna.cl/nosotros/quienes-somos.html. Ultimo acceso: 18 de Noviembre de 2015.

[61] MinTIC. (2011). Colombia. Promoción de la Adopción del IPv6 en Colombia. Recuperado de http://www.mintic.gov.co/portal/604/articles-5932_documento.pdf. Ultimo acceso: 20 de Noviembre de 2015.

[62] MinTIC. (s.f.). Colombia. Estrategia de Gobierno en Línea. Recuperado de http://goo.gl/4fv7w. Ultimo acceso: 20 de Noviembre de 2015.

[63] MinTIC. (s.f.). Colombia. Portal IPv6. Recuperado de http://www.mintic.gov.co/ipv6. Ultimo acceso: 20 de Noviembre de 2015.

[64] MinTIC. (2014). MinTIC es el ejemplo en la implementación del protocolo IPv6. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-7195.html. Ultimo acceso: 21 de Noviembre de 2015.

[65] RENATA. (s.f.). Quienes Somos. Recuperado de: https://www.renata.edu.co/index.php/quienes-somos. Ultimo acceso: 01 de Diciembre de 2015.

[66] MinTIC. (s.f.). 40 instituciones han comenzado el proceso de implementación de IPv6 en Colombia. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-5421.html. Ultimo acceso: 01 de Diciembre de 2015.

[67] Task Force Ecuador. (2012). Acuerdo Ministerial 007-2012. Recuperado de http://www.ipv6tf.ec/descargas/category/7-mintel. Ultimo acceso: 10 de Diciembre de 2015.

[68] Task Force Ecuador. (2012). Acuerdo Ministerial 039-2012. Recuperado de http://www.ipv6tf.ec/descargas/category/7-mintel. Ultimo acceso: 10 de Diciembre de 2015.

[69] Banco de Desarrollo de América Latina. (2013). Sector TIC Ecuador. Recuperado de http://publicaciones.caf.com/media/39689/cartilla_ecuador.pdf. Ultimo acceso: 10 de Diciembre de 2015.

[70] Task Force Ecuador. (s.f.). *Portal web*. Recuperado de http://www.ipv6tf.ec. Ultimo acceso: 11 de Diciembre de 2015.

[71] Ministerio de Telecomunicaciones y Sociedad de la Información. (s.f.). Se agotan dominios IPv4, pero en Ecuador se fortalece protocolo IPv6. Recuperado de http://goo.gl/ZlUkzJ. Ultimo acceso: 11 de Diciembre de 2015.

[72] Gobernanza. (2014). Gobernanza de Internet Ecuador. Recuperado de http://gobernanza.net.ec. Ultimo acceso: 11 de Diciembre de 2015.

[73] CEDIA. (s.f.). Quienes Somos. Recuperado de: https://www.cedia.org.ec/inicio/cedia. Ultimo acceso: 11 de Diciembre de 2015.

[74] Ministerio de la Presidencia. (2011). Aprobación del Plan de fomento para la incorporación del protocolo IPv6 en España. Recuperado de http://www.ipv6.es/es-ES/transicion/Documents/BOE-A-2011-10786.pdf. Ultimo acceso: 12 de Diciembre de 2015.

[75] Ministerio de Hacienda y Administraciones Públicas. (2012). Guía para la incorporación de IPv6 como requisito de compra pública. Recuperado de http://goo.gl/Aw6FPd. Ultimo acceso: 13 de Diciembre de 2015.

[76] CISCO. (s.f.). What To Ask From Your Service Provider About IPv6. Recuperado de http://goo.gl/PVDZPT. Ultimo acceso: 17 de Diciembre de 2015.

[77] Portal de Administración Electrónica. (s.f.). España. La transición a IPv6 en la Administración General del Estado. Recuperado de http://goo.gl/P38GHn. Ultimo acceso: 20 de Octubre de 2015.

[78] RedIRIS. (s.f.). Guía para el despliegue de IPv6. Recuperado de : http://www.rediris.es/actividades/ipv6day/guia_despliegue_ipv6.html.es. Ultimo acceso: 20 de Octubre de 2015.

[79] National Institute of Standards and Technology. (2009). USGv6: Test Methods: General Description and Validation. Recuperado de http://www-x.antd.nist.gov/usgv6/docs/NIST-SP-500-273.v2.0.pdf. Ultimo acceso: 20 de Octubre de 2015.

[80] National Institute of Standards and Technology. (2015). USGv6: A Technical Infraestructure to Assist IPv6 Adoption. Recuperado de http://www-x.antd.nist.gov/usgv6/index.html. Ultimo acceso: 10 de Diciembre de 2015.

[81] Architecture and Infrastructure Committee, Federal Chief Information Officers Council. (2009). Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government" (the "Roadmap"), Version 1.0. Recuperado de http://bit.ly/1wY4HNw. Ultimo acceso: 10 de Diciembre de 2015.

[82] National Institute of Standards and Technology. (2016). Estimating USG IPv6 & DNSSEC External Service Deployment Status. Recuperado de http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov. Ultimo acceso: 12 de Diciembre de 2015.

[83] Internet2. (2015). About us. Recuperado de http://www.internet2.edu/about-us/. Ultimo acceso: 12 de Diciembre de 2015.

[84] Task Force Argentina. (s.f.). Misión, Visión y Objetivos. Recuperado de http://www.ipv6.org.ar/index.php/mision-vision-y-objetivos. Ultimo acceso: 18 de Diciembre de 2015.

[85] Secretaria de Gabinete, Jefatura de Gabinete de Ministros. (s.f.). Estándares Tecnológicos. Recuperado de http://www.jefatura.gob.ar/sgp/. Ultimo acceso: 18 de Diciembre de 2015.

[86] InnovaRed. (s.f.). Quienes Somos. Recuperado de http://www.innova-red.net/acerca-de/quienes-somos. Ultimo acceso: 17 de Diciembre de 2015.

[87] NIC Argentina. (2015). Implementación de IPv6. Recuperado de https://nic.ar/noticias.xhtml?IPv6. Ultimo acceso: 17 de Diciembre de 2015.

[88] VYNCKE ORG. (s.f.). IPv6 Deployment Status. Recuperado de https://www.vyncke.org/ipv6status/detailed.php?country=ar&type=Gov. Ultimo acceso: 18 de Diciembre de 2015.

[89] Task Force Argentina. (s.f.). IPv6 en Argentina. Recuperado de http://www.ipv6.org.ar/index.php/ipv6-en-argentina. Ultimo acceso: 18 de Diciembre de 2015.

[90] Comitê Gestor da Internet no Brasil. (2003). Decreto Nº 4.829. Recuperado de http://cgi.br/pagina/decretos/108. Ultimo acceso: 19 de Diciembre de 2015.

[91] NIC Brasil. (s.f.). Sobre o NIC.br. Recuperado de http://www.nic.br/sobre-nic/nicbr.htm. Ultimo acceso: 19 de Diciembre de 2015.

[92] Portal IPv6 Brasil. (s.f.). Recuperado de http://ipv6.br. Ultimo acceso: 19 de Diciembre de 2015.

[93] Comitê Gestor da Internet no Brasil. (2012). Resolução CGI.br/RES/2012/007/P – Recomendação para Implantação do Protocolo IPv6. Recuperado de http://cgi.br/resolucoes/documento/2012/007. Ultimo acceso: 10 de Enero de 2016.

[94] Comitê Gestor da Internet no Brasil. (2014). Resolução CGI.br/RES/2014/008 – Recomendação para o suporte ao IPv6 em equipamentos que usam protocolos Internet. Recuperado de http://cgi.br/resolucoes/documento/2014/008. Ultimo acceso: 10 de Enero de 2016.

[95] Portal IPv6 Brasil. (s.f.). Requisitos de suporte a IPv6 para equipamentos de TIC. Recuperado de http://ipv6.br/media/arquivo/ipv6/file/63/requisitos-suporte-ipv6-ripe-554-pt.pdf. Ultimo acceso: 10 de Enero de 2016.

[96] Rede Nacional de Ensino e Pesquisa. (s.f.). Alianzas. Recuperado de http://www.rnp.br/es/institucional/alianzas. Ultimo acceso: 10 de Enero de 2016.

[97] Rede Nacional de Ensino e Pesquisa. (2004). IPv6 en la RNP. Recuperado de https://memoria.rnp.br/es/ipv6/rnp.html. Ultimo acceso: 11 de Enero de 2016.

[98] Portal IPv6 Brasil. (s.f.). Cronograma. Recuperado de http://ipv6.br/cronograma/. Ultimo acceso: 12 de Enero de 2016.

[99] Ladid, L. (2015). EU-China FIRE Project: IPv6 best practices. Recuperado de http://www.euchina-fire.eu/about-fire/ipv6-best-practices/. Ultimo acceso: 18 de Octubre de 2015.

[100] IPv6 Test. (s.f.). Recuperado de http://ipv6-test.com/. Ultimo acceso: 16 de Setiembre de 2015.

[101] IETF. (1995). RFC 1752: The Recommendation for the IP Next Generation Protocol. Recuperado de http://www.rfc-editor.org/rfc/rfc7599.txt. Ultimo acceso: 16 de Setiembre de 2015.

[102] LACNIC. (2016). Base de datos de asignación de direcciones IP. Recuperado de ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-latest. Ultimo acceso: 20 de Enero de 2016.

[103] Ministerio de Transportes y Comunicaciones. (2007). Reglamento de Organización y Funciones. Recuperado de http://www.mtc.gob.pe/nosotros/documentos/ROF_MTC2007.pdf. Ultimo acceso: 07 de Octubre de 2015.

[104] Oficina Nacional de Gobierno Electronico. (s.f.). Quienes Somos. Recuperado de http://www.ongei.gob.pe/quienes/ongei_QUIENES.asp. Ultimo acceso: 07 de Octubre de 2015.

[105] Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica. (s.f.). ¿Quiénes somos?. Recuperado de http://portal.concytec.gob.pe/index.php/concytec/quienes-somos. Ultimo acceso: 07 de Octubre de 2015.

[106] Organismo Supervisor de Inversión Privada en Telecomunicaciones. (s.f.). Misión, Visión y Finalidad. Recuperado de https://www.osiptel.gob.pe/categoria/mision-vision-finalidad. Ultimo acceso: 07 de Octubre de 2015.

[107] Instituto Nacional de Investigación y Capacitación de Telecomunicaciones. (s.f.). Objetivos. Recuperado de http://www.inictel-uni.edu.pe/institucional/objetivos. Ultimo acceso: 07 de Octubre de 2015.

[108] Sistema Electrónico de Contrataciones del Estado. (2013). Concurso Público 10-2013/OSIPTEL: Contratación del servicio de acceso a Internet y alojamiento de servidores. Recuperado de http://www2.seace.gob.pe/?_pageid_=3&_contenid_=ca.contentid. Ultimo acceso: 20 de Enero de 2016.

[109] Sistema Electrónico de Contrataciones del Estado. (2015). Concurso Público 02-2015-INICTEL-UNI-1: Servicio de Internet para las instalaciones del INICTEL-UNI. Recuperado de http://prodapp2.seace.gob.pe/seacebus-uiwd-pub/buscadorPublico/buscadorPublico.xhtml. Ultimo acceso: 20 de Enero de 2016.

[110] RedIRIS. (s.f.). Servicio IPv6. Recuperado de: http://www.rediris.es/servicios/conectividad/ipv6/. Ultimo acceso: 20 de Noviembre de 2015.

[111] Organismo Supervisor de Inversión Privada en Telecomunicaciones. (2015). Informe Nº 097-GPP/2015: Renovación de la Membresía del "Registro de Direcciones de Internet para América Latina y el Caribe" – LACNIC.

[112] Red Académica Peruana. (s.f.). Consejo Directivo (2014 - 2016). Recuperado de http://www.raap.org.pe. Ultimo acceso: 15 de Diciembre de 2015.

[113] Red Académica Peruana. (2010). Tercera Jornada Técnica de la RAAP. Recuperado de http://www.raap.org.pe/site/jornada.php. Ultimo acceso: 15 de Diciembre de 2015.

[114] LACNIC. (s.f.). Solicitar IP. Recuperado de http://www.lacnic.net/web/lacnic/solicitar-ip. Ultimo acceso: 20 de Enero de 2016.

[115] National Institute of Standard san Technology. (2014). USGv6 Buyer's Guide. Recuperado de http://www-x.antd.nist.gov/usgv6/testing.html. Ultimo acceso: 19 de Enero de 2016.

[116] IPv6 Ready Logo Program. (2012). Frequently Asked Questions. Recuperado de https://www.ipv6ready.org/?page=faq#q1. Ultimo acceso: 17 de Enero de 2016.

[117] IPv6 Ready Logo Program. (s.f.). IPv6 Ready Logo Program Approved List. Recuperado de https://www.ipv6ready.org/db/index.php/public/?o=4. Ultimo acceso: 18 de Enero de 2016.

[118] RIPE Network Coordination Centre. (2012). Requirements for IPv6 in ICT Equipment. Recuperado de https://www.ripe.net/publications/docs/ripe-554. Ultimo acceso: 18 de Enero de 2016.

[119] Sistema Electrónico de Contrataciones del Estado. (2014). Concurso Público 18-2014/MTC: Acceso a Internet para el MTC. Recuperado de http://www2.seace.gob.pe/?_pageid_=3&_contenid_=ca.contentid. Ultimo acceso: 20 de Enero de 2016.

[120] Sistema Electrónico de Contrataciones del Estado. (2013). Adjudicación Menor Cuantía 028-2013-CONCYTEC-OGA: Contratación del Servicio de Internet. Recuperado de http://www2.seace.gob.pe/?_pageid_=3&_contenid_=ca.contentid. Ultimo acceso: 20 de Enero de 2016.

[121] Sistema Electrónico de Contrataciones del Estado. (2015). Licitación ONGEI Concurso Público – 004 – 2014 – Presidencia de Consejo de Ministros (PCM). Recuperado de http://prodapp2.seace.gob.pe/seacebus-uiwd-pub/buscadorPublico/buscadorPublico.xhtml. Ultimo acceso: 20 de Enero de 2016.

[122] LACNIC. (s.f.). Testingv6. Recuperado de http://www.lacnic.net/web/lacnic/testingv6. Ultimo acceso: 20 de Enero de 2016.