

**UNIVERSIDAD NACIONAL
SANTIAGO ANTÚNEZ DE MAYOLO
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE
INGENIERÍA DE SISTEMAS E INFORMÁTICA**



**“SISTEMA DE GESTIÓN PARA LA TRANSICIÓN DE IPV4 A
IPV6 EN EL GOBIERNO REGIONAL DE ANCASH”**

**TESIS GUIADA
PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS E INFORMÁTICA**

AUTOR:

Bach. EDWIN CHRISTIAN PÉREZ MACEDO

ASESOR:

Ing. JAIME YLIAM MINAYA GONZALEZ

**HUARAZ – PERU
2018**

**PROGRAMA DE TITULACIÓN PROFESIONAL
MODALIDAD TESIS GUIADA 2018**

N° Registro: T067

DEDICATORIA

A mi familia, en especial a mi madre que me brinda su apoyo en todas las etapas de mi vida.

A mis amigos y docentes que me apoyan a crecer cada día más.

Edwin Christian Pérez Macedo

AGRADECIMIENTO

Mi agradecimiento se dirige a quien ha forjado mi camino y me ha dirigido por el sendero correcto.

Sencillo no ha sido el proceso, pero gracias a las ganas de trasmitirme sus conocimientos y dedicación que he logrado importantes objetivos como culminar el desarrollo de mi tesis con éxito.

Edwin Christian Pérez Macedo

PRESENTACIÓN

Señores miembros del jurado les presento la tesis titulada "Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash"

La tesis consta de nueve capítulos, en el Capítulo I se presentan las generalidades de la investigación, el Capítulo II se da a conocer el marco teórico que fundamenta la tesis, en el Capítulo III se detallan los materiales y métodos usados en la investigación, en el Capítulo IV y V se realiza el análisis y diseño de la solución, en el Capítulo VI y VII se plantea los lineamientos que se deben de tener en cuenta para la elaboración del plan de transición de protocolos, el Capítulo VIII presenta los resultados de la investigación y en el Capítulo IX se discuten los resultados obtenidos, finalmente se presentan las conclusiones y recomendaciones de la investigación.

Atentamente

Edwin Christian Pérez Macedo

HOJA DE VISTO BUENO

Ing. César Augusto Narro Cachay
Presidente
Reg. C.I.P. N° 169491

Ing. Erick Giovanni Flores Chacón
Secretario
Reg. C.I.P. N° 89540

Ing. Jaime Yliam Minaya Gonzalez
Vocal
Reg. C.I.P. N° 76963

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.

Palabras Claves: Plan, Transición, IPv6, IPv4.

ABSTRACT

Given the imminent exhaustion of IPv4 addresses, organizations are required to initiate the transition of their networks and content to the IPv6 protocol, so this thesis aims to propose a reference model to start the process of transition to the protocol IPv6 in the Public Institutions of the Government of Peru, due to the fact that at the date of publication of this work, at the government level, public institutions that are directly related to the development of telecommunications and information technologies in Peru, they have not considered the elaboration of a methodology and / or technical documents that allow public institutions to prepare themselves to begin the deployment of the IPv6 protocol in their networks and contents.

Having a reference model and the necessary technical documents allows the adoption of the new protocol to be made more dynamic, this is evidenced in the review of the actions carried out by various countries such as: Argentina, Brazil, Colombia, Chile, the United States and Spain, who In addition to defining a national strategy for the transition to IPv6, they have developed reference models and specific technical support documents so that their public institutions can begin the transition to the new IPv6 protocol. In this sense, the main contribution of this work is to present a reference model and technical documents that serve as support to initiate the transition to the IPv6 protocol in public institutions at the level of the Peruvian Government.

Keywords: Plan, Transition, IPv6, IPv4

ÍNDICE

DEDICATORIA	ii
AGRADECIMIENTO	iii
PRESENTACIÓN	iv
HOJA DE VISTO BUENO	v
RESUMEN	vi
ABSTRACT	vii
CAPITULO I:	1
GENERALIDADES	1
1.1. Realidad problemática	1
1.2. Enunciado del problema	4
1.3. Hipótesis	4
1.4. Objetivos	4
1.4.1. Objetivo general:	4
1.4.2. Objetivo específico:	4
1.5. Justificación	4
1.5.1. Justificación operativa.	4
1.5.2. Justificación tecnológica.	6
1.5.3. Justificación económica	6
1.5.4. Justificación social	6
1.5.5. Justificación legal	7
1.6. Limitaciones	8
1.7. Descripción y sustentación de la solución	8
CAPITULO II:	10
MARCO TEORICO	10
2.1. Antecedentes	10
2.1.1. A Nivel internacional	10
2.1.2. A Nivel nacional	12
2.2. Teorías que sustentan el trabajo	13
2.2.1. Marco teórico	13
2.2.2. Marco conceptual	21
CAPITULO III:	27
MATERIALES Y METODOS	27
3.1. Materiales	27

3.1.1.	Recursos	27
3.1.2.	Materiales, equipos y servicios.....	27
3.1.3.	Población y muestra	28
3.2.	Métodos.	29
3.2.1.	Tipo de investigación	29
3.2.2.	Definición de variables.....	29
3.2.3.	Diseño de la investigación	31
3.3.	Técnicas	33
3.3.1.	Técnicas de procesamiento de la información.....	33
3.4.	Procedimiento	33
CAPITULO IV:		34
ANALISIS		34
4.1.	Análisis de la situación actual.....	34
4.1.1.	Capacidad instalada:	35
4.1.2.	Análisis FODA.....	36
4.2.	Identificación y descripción de requerimientos.....	38
4.3.	Diagnóstico de la situación actual	40
CAPITULO V:		42
DISEÑO DE LA SOLUCION		42
5.1.	Arquitectura tecnológica de la solución.....	42
5.2.	Diseño de estructura de la solución	44
5.2.1.	Base legal.....	44
5.2.2.	Alcance	44
5.2.3.	Diagnostico de la infraestructura tecnológica	44
5.2.4.	Implementación del protocolo IPv6.....	48
5.2.5.	Pruebas.....	51
5.2.6.	Capacitación y sensibilización.....	53
5.2.7.	Presupuesto.....	55
5.2.8.	Anexos	55
5.3.	Diseño de la funcionalidad de la solución	55
CAPITULO VI:		59
CONSTRUCCION DE LA SOLUCION		59
6.1.	Construcción	59
6.1.1.	Base legal.....	62

6.1.2.	Objetivos	64
6.1.3.	Alcance	64
6.1.4.	Diagnóstico de la infraestructura tecnológica	65
6.1.5.	Implementación del protocolo IPv6.....	75
6.1.6.	Pruebas.....	78
6.1.7.	Capacitación y sensibilización.....	80
6.1.8.	Presupuesto.....	81
6.1.9.	Anexos	84
CAPITULO VII:		87
IMPLEMENTACION		87
7.1.	Monitoreo y evaluación de la solución.....	87
7.1.1.	Elementos del monitoreo y evaluación	87
7.1.2.	Plan de monitoreo y evaluación	87
7.2.	Bitácora y puesta a punto	87
CAPITULO VIII:		90
RESULTADOS		90
8.1.	Resultados de acuerdo a los objetivos planteados	90
8.2.	Resultados cuantitativos	91
8.2.1.	Diagnostico e interpretación de resultados.....	91
CAPITULO IX:		96
DISCUSION DE RESULTADOS		96
9.1.	En base a los antecedentes mencionados en la investigación se presentan las siguientes discusiones:	96
9.1.1.	Análisis comparativo con los antecedentes internacionales	96
9.1.2.	Análisis comparativo con el antecedente nacional	97
9.2.	Sobre el impacto del sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Áncash.....	98
CONCLUSIONES		99
RECOMENDACIONES		101
REFERENCIAS BIBLIOGRÁFICAS		102
ANEXOS		104

ÍNDICE DE GRÁFICOS

Gráfico N° 2. 1: Cabecera del protocolo IPv4	15
Gráfico N° 2. 2: Cabecera del protocolo IPv6	16
Gráfico N° 2. 3: Protocolo IPv6 direccionado	19
Gráfico N° 2. 4: Mecanismo de interacción entre protocolo Ipv4 y el Ipv6.....	20
Gráfico N° 2. 5: Mecanismo de interacción entre protocolo Ipv4 y el Ipv6.....	21
Gráfico N° 2. 6: Capas del modelo TCP/IP	22
Gráfico N° 2. 7: Zona DMZ.....	23
Gráfico N° 2. 8: Pilares según ISO 27001:2013	25
Gráfico N° 3. 1: Operacionalización de variables.....	30
Gráfico N° 3. 2: Metodología PHVA.....	32
Gráfico N° 4. 1: Organigrama del Gobierno Regional de Ancash.....	34
Gráfico N° 5. 1: Mantener IPv4 al mundo y tener IPv6 en la red local	43
Gráfico N° 5. 2: Tener IPv6 en el mundo y tener IPv6 en la red local	44
Gráfico N° 6. 1: Carátula del plan de transición al protocolo IPv6	60
Gráfico N° 6. 2: Contenido del plan de transición al protocolo IPv6	61
Gráfico N° 6. 3: Evolución de las capacidades de comunicación.....	66
Gráfico N° 6. 4: Cuadro de resumen de equipos informáticos del GRA.....	69
Gráfico N° 6. 5: Flujograma de sensibilización al personal del GRA	75
Gráfico N° 6. 6: Cronograma de la Fase de Implementación	84
Gráfico N° 6. 7: Cronograma de Fase de Pruebas	85
Gráfico N° 6. 8: Cronograma de la Fase de Capacitación y Sensibilización.....	85
Gráfico N° 8. 1: Resultados de la pregunta 1	92
Gráfico N° 8. 2: Resultados de la pregunta 2.....	93
Gráfico N° 8. 3: Resultados de la pregunta 3.....	94
Gráfico N° 8. 4: Resultados de la pregunta 4.....	95

ÍNDICE DE TABLAS

Tabla N° 3. 1: Personal para el proyecto	27
Tabla N° 3. 2: Equipos para el proyecto	27
Tabla N° 3. 3: Materiales para el proyecto	28
Tabla N° 3. 4: Servicios para el proyecto	28
Tabla N° 4. 1: Análisis FODA	37
Tabla N° 5. 1: Tabla para levantamiento de información de los equipos de computo	45
Tabla N° 5. 2: Tabla para levantamiento de información de los equipos de impresión	46
Tabla N° 5. 3: Tabla para levantamiento de información de los equipos de información	47
Tabla N° 5. 4: Tabla para levantamiento de información de los equipos de aplicativos	47
Tabla N° 5. 5: Modelo de cronograma para la implementación del protocolo IPv6 .	50
Tabla N° 5. 6: Modelo de cronograma para la fase de pruebas en la transición al protocolo IPv6.....	53
Tabla N° 5. 7: Modelo de cronograma para la capacitación y sensibilización del protocolo IPv6.....	54
Tabla N° 6. 1: Inventario de los servidores en el GRA.....	66
Tabla N° 6. 2: Cuadro de resumen de los equipos de comunicación del GRA.....	68
Tabla N° 6. 3: Cuadro de resumen de equipos de impresión del GRA.....	70
Tabla N° 6. 4: Cronograma de transición al protocolo IPv6.....	77
Tabla N° 6. 5: Cronograma de Pruebas.....	79
Tabla N° 6. 6: Cronograma de capacitación y sensibilización	81
Tabla N° 6. 7: Cuadro de Costeo de la implementación	84
Tabla N° 7. 1: Bitácora de proyecto.....	88

Tabla N° 8. 1: Tabulación de la pregunta 1	92
Tabla N° 8. 2: Tabulación de la pregunta 2	93
Tabla N° 8. 3: Tabulación de la pregunta 3	94
Tabla N° 8. 4: Tabulación de la pregunta 4	95

CAPITULO I: GENERALIDADES

1.1. Realidad problemática

Las comunicaciones a través de la red de datos han avanzado considerablemente debido a que hoy en día existe una gran demanda de dispositivos que deben estar conectados de forma permanente. Esto ha generado que el protocolo IPv4 (protocolo de internet versión 4) con 4.3 millones de direcciones ha sido el encargado desde el año de 1981 de las conexiones a través de internet, pero en este momento entró en una fase de agotamiento irreversible ya que su direccionamiento se encuentra saturado y no permite el crecimiento de la infraestructura tecnológica.

Debido a esto en la década de los 90 nace IPv6 (Protocolo de Internet versión 6) que permite sustituir a IPv4, permitiendo así el crecimiento y uso de internet en países densamente poblados, y a su vez la interconexión de más dispositivos. Por otra parte, es de resaltar que los niveles de seguridad presentan mejoras funcionales para el cifrado de datos y autenticación en las comunicaciones, siendo base el modelo de seguridad IPsec que proporciona autenticidad, integridad y confidencialidad de los datos que viajan por la red de extremo a extremo.

Es así que el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC – por sus siglas en inglés) es la organización responsable de la asignación y administración de los recursos de numeración de internet conocidos como IPv4 e IPv6.

LACNIC señala que el agotamiento de las direcciones IPv4 en América Latina y el Caribe se encuentra en su tercera y última fase, debiendo los gobiernos a priorizar el despliegue del protocolo IPv6, quienes deben asegurar que las acciones que se lleven a cabo garanticen que los nuevos recursos TIC cuenten con capacidad IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6, ello conforme con lo dispuesto en la

resolución N° 180 correspondiente a la conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones; se hace necesario que el Perú propicie un entorno que garantice la adopción del protocolo IPv6 por parte de las entidades de la administración Pública ante el inminente agotamiento de las direcciones IPv4, de tal manera que se asegure la comunicación y accesibilidad a dispositivos o servicios que utilizan el sistema de direccionamientos IPv6.

Es así como en base a lo establecido en la ley N° 27658 – Ley del Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; por lo que deviene en necesario mejorar la gestión pública a través del uso de nuevas tecnologías que permitan brindar mejores servicios a los ciudadanos; la Ley N° 29158 – Ley Orgánica del Poder Ejecutivo; el Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, crea el Sistema Nacional de Informática, el cual tiene por finalidad asegurar que sus actividades se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión; teniendo como competencia la instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del Estado; la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Infraestructura, el mismo que busca contar con una red informática que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, bases de datos, entre otros; el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0, aprobada mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo 1, “Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la Sociedad de la Información y del Conocimiento”,

disponiendo a su vez, en su Estrategia 7, “Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el Protocolo de Internet v6 (IPv6)”;

se dicta el Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”; el cual en su alcance señala disponer la formulación de un Plan de Transición al Protocolo IPV6, a implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública; como lo son los Gobiernos Regionales y locales del Perú; indicando los plazos para la aprobación del plan (12, 18, 24 meses según la ubicación en el anexo adjunto del plan), y un plazo máximo de 4 años después de aprobado el plan para la ejecución de este, recayendo la responsabilidad del monitoreo y supervisión en la Secretaria de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, indicándose además que las entidades de la Administración Pública que adquieran hardware o software que reciba, transmita o procese información por medio de protocolo IP, a partir de la fecha de la entrada en vigencia del mencionado Decreto Supremo, deben de asegurar que estos soporten el Protocolo IPv6 con compatibilidad o soporte al protocolo IPv4 .

Con el Decreto supremo mencionado es de prioridad primordial elaborar el plan de Transición al Protocolo IPv6, realizando un análisis situacional de la infraestructura tecnológica y determinar si esta es capaz de soportar el protocolo IPv6, además de definir las etapas para hacer una transición con el menor impacto en los usuarios del servicio tecnológico, todo esto basado en buenas prácticas en la sede central del Gobierno Regional de Ancash y sus dependencias.

Es importante resaltar que los protocolos IPv4 e IPv6 no son compatibles, y la mayor complejidad radica en que se debe mantener esta compatibilidad con IPv4 mientras se migra a IPv6. Teniendo en cuenta toda la problemática descrita anteriormente con el presente documento se pretende implementar el protocolo IPv6 en la infraestructura tecnológica en el Gobierno Regional de Ancash a la

siguiente pregunta. **¿Cómo influye el tener un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash?**

1.2. Enunciado del problema

¿Cómo influye el tener un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash?

1.3. Hipótesis

La elaboración de un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash.

1.4. Objetivos

1.4.1. Objetivo general:

Proponer un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash.

1.4.2. Objetivo específico:

1. Evaluar el decreto supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”, para identificar requerimientos para la elaboración del plan de transición al protocolo IPv6.
2. Identificar las acciones a seguir para hacer la implementación de IPv6 en base a lineamientos, recomendaciones y buenas prácticas a nivel de seguridad.
3. Identificar las pruebas que se deben realizar después de la implementación del protocolo Ipv6.
4. Validar y medir el nivel de satisfacción del personal encargado de elaborar el plan de transición del protocolo IPv4 a IPv6.

1.5. Justificación

1.5.1. Justificación operativa.

IPv4 es el primer protocolo que se creó para el uso de la Internet. Sin embargo, las direcciones IP que emplea se han agotado, lo que limita el crecimiento de diversas conexiones. Por tanto, es difícil su adecuación a las nuevas aplicaciones, más aún cuando a nivel mundial se presenta

el crecimiento continuo de las mismas, las cuales requieren una IP pública única, ejemplo de ello son: los teléfonos con tecnología VoIP, televisión y radio, seguridad, televigilancia, mercados virtuales, juegos, videoconferencia, redes inalámbricas, etc. Sumado a ello las estadísticas evidencian que este tipo de protocolo no permite la asignación de nuevas direcciones IP a los usuarios de diferentes empresas u organizaciones del sector educativo, bancario, industria, entre otros.

En la actualidad, se necesitan protocolos que garanticen unas características adecuadas a los tipos de tráfico de datos, pues cada día crece de forma constante el número de usuarios que acceden a la red desde diversos dispositivos. Esta creciente demanda de conectividad ha hecho que cada vez sean más escasas las IP públicas y se necesiten mejores prácticas para salvaguardar el flujo de información.

En consecuencia, los administradores de redes y servicios han explorado múltiples formas de garantizar la seguridad de los usuarios y la calidad del servicio que reciben, por ejemplo, con el uso de Network Address Translation (NAT). No obstante, lograr este propósito no es fácil y más si se consideran dos factores:

- 1.** La falta de disponibilidad de ancho de banda necesario para soportar los servicios actuales.
- 2.** El uso creciente de internet como plataforma de negocios (E-commerce, EBanking), hace que la seguridad en la red sea necesaria, si se quiere suplir las expectativas de negocio generadas y brindar protección a los distintos actores de los procesos.

Ante el panorama descrito, surge el protocolo IPV6, el cual tiene como objeto subsanar las falencias observadas en el protocolo IPv4, como lo son: el agotamiento de direcciones IP y la seguridad de la información a través del envío cifrado y autenticado de paquetes, lo que permite mantener una transmisión más confiable y segura de la Información. También, posee un sencillo mecanismo de autoconfiguración y

velocidad en la transmisión; además entre sus características más importantes se resaltan la cantidad ilimitada de espacio de direcciones IP y la calidad del servicio.

1.5.2. Justificación tecnológica.

El uso de la TIC's, serán muy importantes para este proyecto, debido a la gran demanda de las direcciones IP, el agotamiento de las direcciones IPv4 disponibles, tablas de enrutamiento de gran tamaño y la falta de funcionalidad para dar seguridad, eficiencia y calidad de servicio en la red del Gobierno Regional de Ancash.

La transición es un proceso de despliegue que se extiende en el tiempo, hoy en día existen muchos servicios que solamente se ofrecen en IPv4 y las soluciones a la transición son temporales porque se vive en función de las direcciones Ipv4. Debido a esto, ambos protocolos deben coexistir y uno de los mecanismos para poder realizar una transición de este tipo es Dual Stack (coexistencia de IPv4 e IPv6 en los mismos dispositivos y redes). Este mecanismo implica la utilización de ambos protocolos en paralelo en los dispositivos.

1.5.3. Justificación económica

En cuanto al desarrollo sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash la propuesta es viable, ya que, al establecer los parámetros de los requerimientos técnicos necesarios y describir la secuencia de acciones para la implementación, lo que conllevará a una reducción en los costos de tercerización.

1.5.4. Justificación social

Las necesidades de los usuarios a conexiones a internet han aumentado exponencialmente, exigiendo nuevas capacidades que la versión IPv4 no proporciona como lo son la seguridad, privacidad, velocidad, VoIP, multimedia, teleconferencias y aplicaciones a gran demanda; es de esta manera se trata de cubrir las necesidades actuales y las futuras necesidades de interconexión que se presentan en el Gobierno Regional de Ancash.

Teniendo en cuenta que la adopción de nuevas tecnologías es sinónimo de desarrollo para cualquier sociedad que quiera estar vigente en el mundo moderno, es importante dar un soporte investigativo que promueva reflexiones comparativas para dar un salto en el camino de la evolución o por lo menos ir a la par con el mundo moderno.

De esta manera se garantiza que a un futuro cuando las necesidades de interconexión en la red de datos incrementen el Gobierno Regional de Ancash esté preparado para la gran demanda que generen los usuarios.

1.5.5. Justificación legal

Legalmente se justifica porque se apoya en las siguientes leyes, decreto supremo:

La ley N° 27658 – Ley del Marco de Modernización de la Gestión del Estado

La Ley N° 29158 – Ley Orgánica del Poder Ejecutivo

El Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, crea el Sistema Nacional de Informática

La Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú.

El Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0, aprobada mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo 1, “Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la Sociedad de la Información y del Conocimiento”, disponiendo a su vez, en su Estrategia 7, “Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el Protocolo de Internet v6 (IPv6)”.

Y basado en todos los anteriores se dicta el Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan

de Transición al Protocolo IPv6 en las entidades de la Administración Pública”.

1.6. Limitaciones

Las limitaciones que se presenta el siguiente proyecto se detalla a continuación:

- La presente tesis en el tiempo solo alcanza o comprende el desarrollo del plan de transición de protocolos de IPv4 a IPv6 en las ejecutoras del Gobierno Regional de Áncash, pero no abarca la implementación.
- El personal que labora en el área de Unidad de tecnologías de la Información del Gobierno Regional de Áncash, son personal con la modalidad de contrato por terceros y el jefe de la unidad como funcionario de confianza, los cuales al no ser personal de planta y/o nombrados corren el riesgo de un cambio sin algún criterio y peligrando así la continuidad del proyecto.

1.7. Descripción y sustentación de la solución

El objetivo de este proyecto es realizar el análisis y diseño de un sistema de gestión para la elaboración del plan de transición del protocolo IPv4 a IPv6 en el gobierno regional de Ancash.

El análisis y el diseño propuesto servirán como base para la futura construcción del plan de transición del Protocolo IPv4 a IPv6 en el gobierno regional de Ancash.

La investigación se sustenta en que el sistema de gestión planteado, cumpla con apoyar a la construcción del plan de transición del protocolo IPv4 a IPv6, en base a los lineamientos descritos en el decreto supremo n° 081-2017-PCM, “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”, y en base a la entrevista (Anexo N° 3) se contempla la siguiente estructura:

Estructura básica del plan de transición al protocolo IPv6

- a. BASE LEGAL**
- b. ALCANCE**
- c. DIAGNOSTICO DE LA INFRAESTRUCTURA TÉCNOLOGICA**
- d. IMPLEMENTACIÓN DEL PROTOCOLO IPV6**
- e. PRUEBAS**

- f. CAPACITACIÓN Y SENSIBILIZACIÓN**
- g. PRESUPUESTO**
- h. ANEXOS**

CAPITULO II: MARCO TEORICO

2.1. Antecedentes

2.1.1. A Nivel internacional

- **MAURICIO SUAREZ MAYORGA y MANUEL ALFONSO ROVIRA SOLANO (2016) en su investigación: DISEÑO, DESARROLLO E IMPLEMENTACION DEL PLAN DE TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 DE LA ENTIDAD FENIX;** Indican que se cumplió a satisfacción con la migración de toda la infraestructura, utilizando el método de DUAL STACK, el cual permito la convivencia de los protocolos IPv4 e IPv6 para que la transición se de manera adecuada hacia una red totalmente IPv6. Demostraron que gran cantidad de los equipos que existían en la empresa Fénix son compatibles con IPv6, lo cual permitió señalar que, para realizar una migración de este tipo, solo es necesario realizar pequeñas configuraciones y algunas actualizaciones a nivel de hardware y software.

Indicaron ser la empresa pionera en la implementación de este tipo de migraciones en el país de Colombia lo cual permitirá ser una guía y un ejemplo para que otras compañías realicen este tipo de migraciones y se preparen para actualizar sus redes hacia a IPv6.

Con la implementación se cumplió con las recomendaciones expuestas con la circular 002 de 2011 del ministerio de las telecomunicaciones y finalmente con la implementación la entidad Fénix se encuentra preparada para el momento de apagón de IPv4.

- **LEIDY JESNETH MELO MORENO (2015) en su investigación: PROPUESTA DE DISEÑO PARA LA TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 (IPV4) AL PROTOCOLO DE INTERNET VERSIÓN (IPV6) EN LA EMPRESA MARKET MIX S.A.S;** se concluyó que con la

elaboración del diseño de red planteado en el trabajo de grado se adecua fundamentalmente a la topología actual que existe en la empresa lo cual le permitirá entrar rápidamente en el mundo IPv6. Esto hace que no sea necesario que los proveedores ISP les den conectividad nativa a IPv6 para poder emplear esta nueva tecnología. Según las características de la estructura de red de la empresa, para poder realizar la transición a IPv6 es preciso realizar la activación de DoubleStack en los equipos de la LAN, logrando con esto una isla IPv6, para posteriormente lograr conectividad con el exterior haciendo uso del mecanismo de transición “6to4” el cual permitirá la enlazar los dos protocolos; concluyendo que los equipos propuestos para la transición se ajustan eficientemente a la topología de la empresa para lograr a futuro la implementación del proyecto.

Es así que para que exista la coexistencia de las dos versiones, se debe mantener la versión actual “IPv4”, ya que la transición total de ésta nueva tecnología será progresiva. IPv6 no es una tecnología aislada, pues implica muchas interacciones con las tecnologías actuales y emergentes.

En el escenario planteado se presenta una solución para lograr que en la empresa fluya tráfico en ambas versiones del protocolo IP (IPv4 – IPv6), mediante los mecanismos DoubleStack y túnel 6to4, permitiendo así la coexistencia de los mismos. Como back up se podrá proponer un escenario en el cual fluya el tráfico en IPv6 se hará uso del túnel 6to4, mientras que cuando el tráfico sea IPv4 se conectará directamente con el ISP. Para así de esa manera tener un respaldo.

- **JOSÉ ALEJANDRO MORENO AGUDELO (2016) en su investigación: TRANSICIÓN DE PROTOCOLOS IPV4 A IPV6, PARA UNA EMPRESA DEL ESTADO, CON APLICACIÓN EN UNA CIUDAD INTERMEDIA;** Observa con preocupación que pese a los esfuerzos y distintos lineamientos /que existen en Colombia, con respecto al tema de la transición del protocolo de IPv4 a IPv6, dicha

transición aún continúa en un proceso muy temprano, en comparación a la adopción efectuada por países de la región.

La transición entre el protocolo IPv4 a IPv6, puede llevarse a cabo de manera efectiva, si se sigue el marco de un modelo procedimental, como el enunciado en este proyecto, de una manera amigable, en donde incluso se buscará una transición gradual, y asentando las bases para una transición definitiva.

Existen diversos mecanismos, que según el análisis definido para la transición del protocolo IPv4 a IPv6, pueden adaptarse para permitir la coexistencia entre Ambos protocolos. Como una etapa posterior sugerida del proyecto, se puede aplicar el modelo procedimental inicial para la adaptación a una empresa del estado en una ciudad intermedia.

2.1.2. A Nivel nacional

- **MARCO ANTONIO TOMY BALTAZAR (2017) en su investigación: MODELO DE REFERENCIA DE TRANSICION DE IPv4 A IPv6 PARA EL SECTOR GOBIERNO DE PERU;** Indica que 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.

Además, indica que 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 dónde empezar (Modelo de Referencia) y capacitación de su recurso humano.

El modelo de referencia y los documentos técnicos elaborados su tesis permite a las instituciones públicas establecer un punto de partida para iniciar sus planes de transición hacia el nuevo protocolo IPv6. de igual manera la tesis evidencia 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.

2.2. Teorías que sustentan el trabajo

2.2.1. Marco teórico

2.2.1.1. Estado del arte

Instituciones públicas y privadas están trabajando mancomunadamente con el fin de (TIC) impulsar la expansión de IPv6, incluyendo Instituciones como la Comisión Europea y el Departamento de Defensa Norteamericano. A nivel de los países de habla Hispana, fue México el precursor en la investigación y experimentación con el protocolo IPv6, seguido de países como España, Chile, Argentina, Uruguay, Brasil, entre otros. En Perú lentamente se está comenzando a surgir en la implementación de IPv6 por iniciativa de la Presidencia del Consejo de Ministro.

La labor de acompañamiento contempla las siguientes actividades:

- Marco de Referencia sobre la importancia de adoptar IPv6, Decreto Supremo N° 022-2017-PCM.

- Divulgación de los últimos anuncios de LACNIC en materia de agotamiento de direcciones IPv4 en países de Latinoamérica y del Caribe.
- Exposición sobre lineamientos para la transición de IPv4 a IPv6.
- Explicación del impacto de implementar o no el nuevo protocolo en las entidades.
- Entrega de documentación y aclaración de dudas o inquietudes.

IPv6 es la actualización del Protocolo de Internet, el cual es fundamental para el funcionamiento de las Redes. Desde que se inició el diseño de IPv6 se previó que tendría que coexistir con IPv4 durante un largo período de tiempo por su lenta implementación. En la actualidad existen millones de dispositivos, aplicaciones y servicios, que requieren de una IP pública. Internet ha llegado a ser una infraestructura de un avance exponencial. (Fedesarrollo, 2011)

Entre los inconvenientes que se presenta al momento de realizar la transición de IPv4 a IPv6 es la incompatibilidad entre los protocolos, por este motivo, IPv6 se ha sido diseñado junto a un conjunto de mecanismos de transición, entre ellas encontramos la doble pila de protocolos o Dual Stack, los cuales permiten la coexistencia de ambos protocolos, IPv4 e IPv6, el tiempo necesario que se lleve a cabo los procesos de transición, de igual manera esto dependerá de diferentes aspectos relacionados con las necesidades propias de las organización y países (Lopez, Gálvez García, & Pedraza, 2010).

Dichos mecanismos de transición contribuyen a la integración de IPv6 en la red Internet que actualmente trabaja con IPv4. IPv6 ha madurado tanto que hoy es posible hacer con esta tecnología de red todo lo que podemos hacer con IPv4 y aun

mucho más, mejorando la calidad y la seguridad de la red. Se pueden anunciar mayores desarrollos y mejoras a los servicios y aplicaciones gracias a la implantación de IPv6.

IPv6 contribuirá a mejorar Internet. En un futuro próximo, veremos toda la red Internet soportando tanto IPv4 como IPv6, e incluso se llegará al punto en que algunas redes dejarán de soportar IPv4. Por supuesto, la comunicación extremo-a-extremo con IPv4 seguirá siendo posible, porque utilizaran mecanismos de transición (Macías, 2004)

2.2.1.2. Características del datagrama en IPV6:

Entre las principales características de IPv6 están:

- Cabecera de longitud fija (40 bytes) conformado por 8 campos.
- Fragmentación de los datagramas sólo es realizada en el host de inicio.
- Eliminación del campo de suma de chequeo.
- La cabecera de extensión, donde se puede implementar nuevas soluciones, está fuera de la cabecera, permitiendo que las aplicaciones puedan ser adaptadas a los nuevos problemas que se presenten.
- Direcciones lógicas o IP de 128 bits, permitiendo disponer 340 sextillones de direcciones IP.

Gráfico N° 2. 1:
Cabecera del protocolo IPv4
Cabecera IPv4

VERS	HLEN	TIPO DE SERVICIO	LONGITUD TOTAL	
IDENTIFICACION		BANDERAS	DESPLAZAMIENTO DE FRAGMENTO	
TIEMPO DE VIDA	PROTOCOLO		SUMA DE VERIFICACION DEL ENCABEZADO	
DIRECCION IP DE LA FUENTE				
DIRECCION IP DEL DESTINO				
OPCIONES (en caso de existir)			RELLENO	

	Nombre del campo se mantiene
	Campo eliminado en IPv6
	Se cambió nombre y ubicación
	Nuevo campo en IPv6

Fuente: Elaboración Propia

En el Gráfico N° 2.1 se muestra cómo se encuentra compuesta la cabecera del protocolo de IPv4 y cada uno de los campos que componen el datagrama.

Gráfico N° 2. 2:
Cabecera del protocolo IPv6
CABECERA IPv6

VERSION	DS	ETIQUETA DE FLUJO
LONGITUD DE CARGA UTIL	CABECERA SIGUIENTE	LIMITE SALTO
DIRECCION DE ORIGE		
DIRECCION DE DESTINO		
CABECERA EXTENSIÓN 1		
CABECERA EXTENSIÓN 2		
:		
CABECERA EXTENSIÓN N		
PDU DE LA CAPA SUPERIOR		

Fuente: Elaboración Propia

En el Gráfico N° 2.2 se muestra como es la nueva composición de la cabecera en IPv6

Al comparar las dos imágenes se puede observar que en el datagrama IPv6 no se introducen los campos de Helen, Banderas, Desplazamiento de fragmentos, Suma de verificación de encabezado, Opciones y Relleno, del protocolo de IPv4, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6 - (Tejedor, 2001)

2.2.1.3. Campos del protocolo IPv6:

- Campo VER (Versión): Este campo tiene una longitud de 04 bits y especifica la versión del protocolo, tomando el valor de 0110. Recordar que el protocolo IPv4 también cuenta con el campo VER y su valor en este caso es de 0100. Hoy en día, los sistemas operativos de los routers soportan ambos protocolos (dual stack) y los routers pueden identificar que versión de protocolo IP llega al router por una de sus interfaces analizando este campo (Blanchet, 2010).

- Campo DS (Differnet Service): Este campo tiene una longitud de 08 bits y de ellos 06 bits definen el nivel de prioridad que presente el protocolo IP, subcampo denominado DSCP (se definen 64 niveles de prioridad). Este campo define la arquitectura de Internet de Servicios Diferenciados o DiffServ (Blanchet, 2010).
- Campo Etiqueta de Flujo: Este campo tiene una longitud de 20 bits y permite que una aplicación asigne un número que identifique a todos los paquetes IPv6 perteneciente a esta aplicación. Antes que se envíen los paquetes IPv6 a red, el host emisor envía a la red el protocolo de señalización RSVP para informar a todos los nodos de la red que reserve recursos para ésta aplicación identificado por el valor del campo Etiqueta de Flujo. Este campo define la arquitectura de Internet de Servicios Integrados o IntServ. (Blanchet, 2010)
- Campo Longitud de carga útil: Este campo tiene una longitud de 16 bits y define el tamaño en bytes de la carga útil (incluyendo la cabecera de extensión). (Blanchet, 2010)
- Campo Cabecera Siguiente: Este campo tiene una longitud de 8 bits y define el tipo de carga útil que encapsula el protocolo IPv6. Existe la posibilidad de que el protocolo IPv6 esté llevando información específica en la región denominado cabecera de extensión; si este es el caso, ésta región cabecera de extensión deberá contener como primer campo cabecera siguiente para indicar que tipo de información corresponde a continuación. (Blanchet, 2010)
- Cabecera Límite de Salto: Este campo tiene una longitud de 08 bits y define la cantidad máxima de saltos que un paquete IPv6 puede transitar antes de que sea considerado que está en un bucle. Cada router disminuye en la unidad el valor de

este campo antes de enviar al router siguiente. Un protocolo IPv6 es eliminado de la red si un router detecta que este campo está en cero. (Blanchet, 2010)

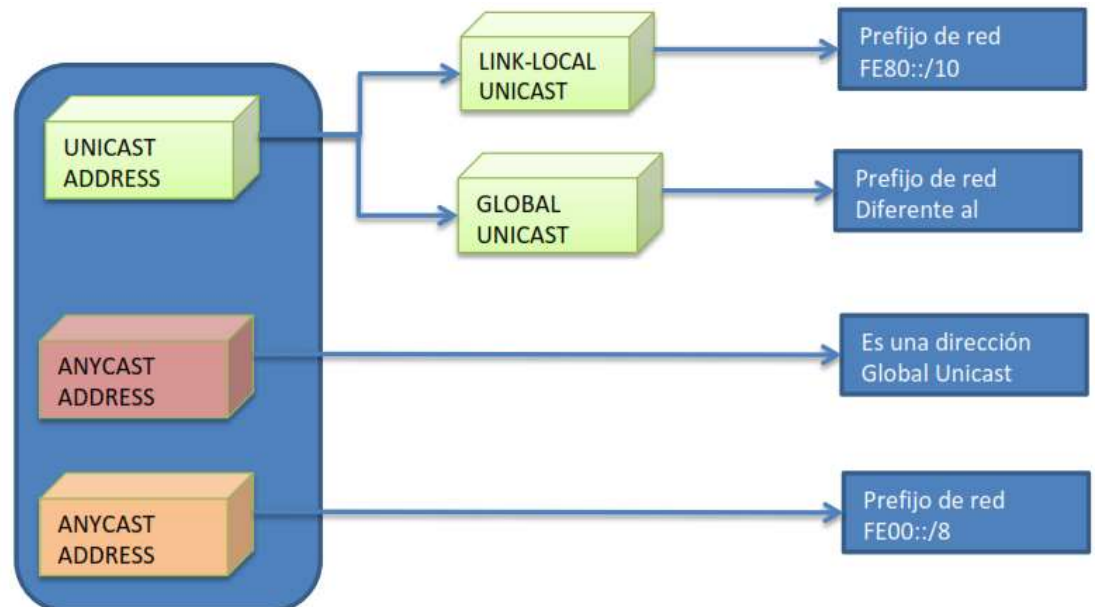
- Campo Dirección IP de origen y Dirección IP de destino: Cada uno de estos campos tiene una longitud de 128 bits y define 2^{128} direcciones IP de origen y 2^{128} direcciones IP de destino. Debido a la longitud de estos campos, se dispone de un número incalculable de direcciones IP; esto permitirá que los diversos nodos y equipos terminales cuenten con direcciones IPv6 públicas, eliminando mecanismos innecesarios como el NAT. (Blanchet, 2010)

2.2.1.4. Tipos de direccionamiento en IPv6

- ✓ Unicast: Identifica a una interfaz y pueden ser de tres tipos. Global unicast que son reconocidas en la Internet; son los equivalentes a las direcciones públicas en IPv4. Site-Local unicast no son reconocidas en la Internet y sirven para asignar una dirección IPv6 a un interfaz dentro de una red LAN; es equivalente a las direcciones privadas en IPv4. Link-Local unicast no son reconocidas en la Internet y sirven para asignar una dirección IPv6 a una interfaz dentro de un segmento de red; es útil para aplicar la autoconfiguración en IPv6. (Lopez, Gálvez García, & Pedraza, 2010).
- ✓ Multicast: Identifica a varias interfaces y son utilizados por algunos protocolos, como RIP y OSPF para IPv6. Se identifica porque los primeros ocho bits de este tipo de direcciones están en uno (FFh).
 - Identifican a un grupo de hosts
 - Un paquete dirigido a una dirección multicast se entrega a todos los hosts identificados con esa dirección.

- Implementan también el tráfico broadcast
- ✓ Anycast: En una dirección que permite identificar a varias interfaces (similar a una dirección multicast) pero se accede a una sola interfaz (similar a una dirección unicast).
 - Identifican a un grupo de hosts.
 - Un paquete dirigido a una dirección anycast se entrega a uno solo de los hosts identificados con esa dirección, normalmente al más cercano, en función de la métrica usada por el protocolo de routing.

Gráfico N° 2. 3:
Protocolo IPv6 direccionado



Fuente: Elaboracion Propia

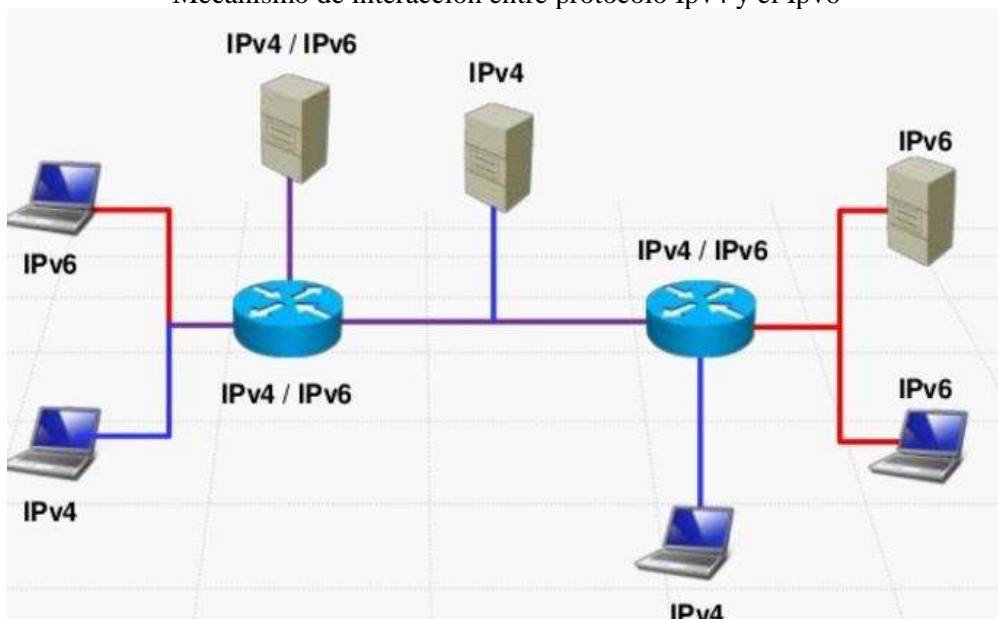
En el Gráfico N° 2.3 se muestra las tres clases posibles en las cuales el protocolo de IPv6 puede ser direccionado.

2.2.1.5. Mecanismos de implementación de redes en IPv6:

- **DUAL STACK:** Una de las maneras conceptualmente más fáciles de introducir IPv6 en una red, es el denominado "mecanismo de pila doble" que se describe en el RFC 2893 (Microsystem, 2000). Por este método un host o un router tendrán ambas pilas de protocolos, IPv4 e IPv6, provistas

directamente como un componente del sistema operativo. Cada nodo, denominado "nodo IPv4/IPv6", se configura con ambas direcciones IPv4 e IPv6. Por consiguiente, las dos pilas envían y reciben datagramas que pertenecen a ambos protocolos y así podrán comunicarse con cada nodo IPv4 e IPv6 en la red. Ésta es la manera más simple y más deseable de coexistencia para IPv4 e IPv6 y es, en general, el próximo paso en la evolución, antes de una transición más profunda, hacia una Internet mundial solo IPv6. No existe un mecanismo de transición real usado en el escenario dual stack, debido a que "Dual Stack" integra en sí mismo el soporte IPv6. Para construir un nodo de pila dual, solo es necesario habilitar en el sistema operativo el soporte IPv6. De esta manera el nodo se convierte en un nodo "híbrido" y dependiendo de la resolución de nombres será el protocolo que usará para cada requerimiento en particular (Blanchet, 2010).

Gráfico N° 2. 4:
Mecanismo de interacción entre protocolo Ipv4 y el Ipv6

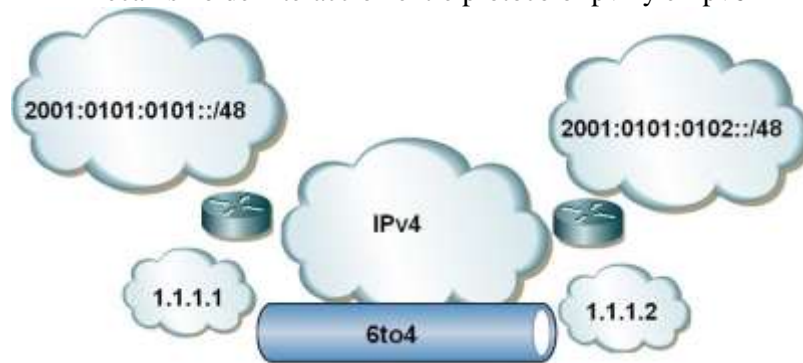


Fuente:Elaboración Propia

En el Gráfico N° 2.4 se muestra el mecanismo de interacción entre protocolo IPv4 y el IPv6, con el fin de interactuar simultanea durante el proceso de transición.

- **Tunelización:** Proporciona una manera de utilizar la infraestructura de IPv4 para llevar el tráfico IPv6, Una de las principales características más importantes es la compatibilidad existente entre los dos protocolos mientras que se puede desplegar completamente IPv6. Se pueden establecer túneles de datagramas IPv6 a través de topologías pertinentes a IPv4 encapsulándolos en datagramas IPv4; Hay dos tipos de tunelización: el automático el cual utiliza la dirección IPv4 incorporada en IPv6 que no tiene ninguna información de IPv4 se deben identificar ambas direcciones en los puntos finales del túnel. (IBM, s.f.)

Gráfico N° 2. 5:
Mecanismo de interacción entre protocolo Ipv4 y el Ipv6



Fuente:Elaboración Propia

En el Gráfico N° 2.5 se muestra el mecanismo de tunelización IPv6 e IPv4.

2.2.2. Marco conceptual

2.2.2.1. TCP/IP (Protocolo de Control de Transporte / Protocolo de Internet)

Este es un conjunto de protocolos de uso extendido y son conocidos como protocolo de control de transmisión / protocolo de Internet o TCP/IP, sirven para conectar redes de todos los

tamaños son valorados por su capacidad para permitir comunicaciones entre diferentes equipos.

TCP/IP muestra una arquitectura de red parecida al modelo de red OSI, pero este no establece tantas distinciones como OSI entre las capas superiores del conjunto de protocolos (Santos Jaimes & Rico Bautista, 2007).

Gráfico N° 2. 6:
Capas del modelo TCP/IP



Fuente: Elaboracion propia

En el Gráfico N° 2.6 se observan las diferentes capas del modelo TCP/IP en donde sus funciones y servicios son variables, cada capa se ocupará de su nivel inferior para solicitar dichos servicios y del nivel superior para devolver los resultados.

2.2.2.2. IPV4 (Protocolo de Internet Versión 4)

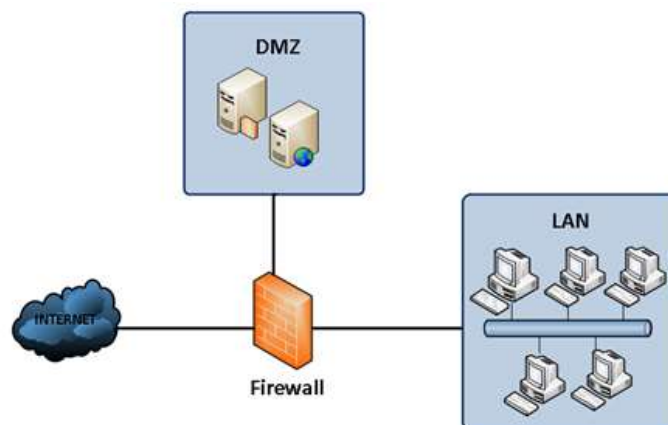
Con el aumento extensivo de internet y los diversos dispositivos interconectados, se ve la necesidad de mejorar el protocolo IP, desarrollándose la versión cuatro de este protocolo (IPV4), el

cual utiliza una dirección única de 32 bits para identificar una máquina y la red a la cual está conectada (Parker, 1995).

2.2.2.3. DMZ (zona desmilitarizada)

De igual manera se observaron problemas de seguridad, para lo cual se implementaron técnicas como el DMZ (zona desmilitarizada) el cual es un diseño conceptual de red cuyo principal objetivo es proteger la red interna de una organización, separando los servicios privados como son servidor Base de Datos, servidor de aplicaciones, de la red pública (internet); así como asegurar la transferencia de datos (Bonilla & González, 2012).

Gráfico N° 2. 7:
Zona DMZ



Fuente: Elaboracion propia

En el Gráfico N° 2.7 se muestra una red donde se tiene un segmento interno que es la LAN de la Organización, y se tiene otro segmento que es la DMZ donde se ubican los servidores de acceso público, al cual se podrá acceder sin exponer la red interna, la cual está protegida por un firewall.

2.2.2.4. Confidencialidad

Cuando se habla de confidencialidad de la Información, se habla de prevenir el acceso no autorizado ya sea en forma deliberada o no intencional a la información.

Se puede perder la confidencialidad de muchas maneras, un ejemplo común es cuando se publica intencionalmente información confidencial de la organización o ente relacionado que es divulgada a personas, entidades o procesos no autorizados.

Por ende esta propiedad de la información asegura el acceso a la información solo a aquellos individuos o grupos que tengan la correspondiente autorización para el uso y tratamiento de dicha información (NTC-ISO, 2013).

2.2.2.5. Integridad

La Integridad de la información es la propiedad que busca asegurar que no se realicen modificaciones a los datos o procesos tanto por personas no autorizadas como por personal autorizado para que estos datos sean consistentes y fidedignos tanto interna como externamente, y así lograr que la información sea exacta, completa y consistente y solo sea modificada cuando sea necesario previa autorización (NTC-ISO, 2013).

2.2.2.6. Disponibilidad

Esta propiedad, característica o cualidad de la Seguridad de la Información busca asegurar que el acceso a la información sea confiable y oportuna y garantizar de manera efectiva que las personas, aplicaciones y entidades autorizadas tengan acceso a la información y sus procesos asociados cuando lo requieran.

Así mismo la disponibilidad debe asegurar que el sistema se mantiene funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo, previniendo la interrupción de los

procesos y actividades, previniendo interrupciones no autorizadas de los recursos informáticos (NTC-ISO, 2013).

Gráfico N° 2. 8:
Pilares según ISO 27001:2013



Fuente: Elaboración propia

La Confidencialidad, Integridad y Disponibilidad son los tres pilares identificados como fundamentales según la norma ISO 27001:2013 para una correcta administración de la Seguridad de la Información (NTC-ISO, 2013).

2.2.2.7. Acuerdos de Nivel de Servicio:

EL modelo de Acuerdo de Nivel de Servicios (Service Level Agreement, SLA) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad (ITIL).

Los principales puntos a cubrir deben ser:

- Tipo de servicio.
- Soporte a clientes y asistencia.
- Provisiones para seguridad y datos.
- Garantías del sistema y tiempos de respuesta.
- Disponibilidad del sistema.

- Conectividad.
- Multas por caída del sistema.

2.2.2.8. RFC (Request for Comments,)

Las RFC (Petición de comentarios) son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general. (IPv6Mx)

2.2.2.9. No repudio

El no repudio es cuando un emisor no puede negar que hizo algún tipo de transacción electrónica, porque el destinatario tiene pruebas suficientes, de que el del origen del envío, lo cual evita que el emisor pueda hacer cualquier tipo reclamación sobre dicha transacción (NTC-ISO, 2013).

2.2.2.10. COBIT: (Objetivos de control de información y tecnologías relacionadas)

Publicado por ITGI, es un modelo aceptado de buen control de la información, las IT y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno sobre IT y mejorar los controles IT. Contiene objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores de éxito críticos y modelos de madurez (COBIT).

2.2.2.11. ISO 27000:

Es un conjunto de estándares desarrollados o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (NTC-ISO, 2013).

**CAPITULO III:
MATERIALES Y METODOS**

3.1. Materiales

3.1.1. Recursos

Personal

El personal involucrado en el presente proyecto son los detallados en la siguiente tabla.

Tabla N° 3. 1:
Personal para el proyecto

Personal Disponible	
Cargo	Nombre
Autores del Proyecto	Pérez Macedo Edwin Christian
Asesor del proyecto	Ing. MINAYA GONZALEZ, Jaime Yliam

Fuente: Elaboración propia

3.1.2. Materiales, equipos y servicios

Los materiales a utilizar son los descritos en la siguiente tabla:

Tabla N° 3. 2:
Equipos para el proyecto

Código	Recurso	Características	Unidad	Cantidad
0001	Laptop	<ul style="list-style-type: none"> • Memoria de 8 Gb. • Procesador: AMD A10, 2.10 GHz. • Tipo de Sistema: Sistema de 64 bits. 	Und.	1
0002	Pendrive	<ul style="list-style-type: none"> • Marca: HP • Capacidad: 8gb 	Und.	1

Fuente: Elaboración propia

Los equipos a utilizados son los descritos en el cuadro siguiente:

Tabla N° 3. 3:
Materiales para el proyecto

Código	Descripción	Cantidad	Unidad
0001	Folder manila tamaño A4	10	Und.
0002	Papel	2	Millares
0003	Lapiceros	20	Und.
0004	Corrector liquido	1	Und.
0005	Cuaderno	1	Und.
0006	Clips	1	Caja
0007	Grapas	1	Caja

Fuente: Elaboración propia

Los servicios que se necesitan para el inicio de la investigación, son los descritos en el cuadro siguiente:

Tabla N° 3. 4:
Servicios para el proyecto

Código	Descripción	Cantidad	Unidad
0001	Pasajes y gastos de transporte	100	Soles
0002	Suministro de energía eléctrica	12	Meses
0003	Telefonía móvil	12	Meses
0004	Internet	12	Meses
0005	Impresiones	500	Hojas
0006	Fotocopias	100	Hojas
0007	Espiralados	5	Und.
0008	Enmicados	5	Und.

Fuente: Elaboración propia

3.1.3. Población y muestra

3.1.3.1. Población

La población de estudio está conformada por el personal que labora en el gobierno regional de Ancash; 350 personas.

3.1.3.2. Muestra

Personal del Área de Unidad de Tecnologías de la Información del Gobierno Regional de Ancash (Sede Central) – 3 personas – Jefe de UTI, personal encargado de la seguridad de la información y coordinador de la infraestructura de la red de datos.

3.1.3.3. Unidad de análisis

Plan de transición del protocolo IPv4 al protocolo IPv6.

3.1.3.4. Tipo de muestreo

No probabilístico, los sujetos de estudio se eligieron por conveniencia, al ser el área de la Unidad de Tecnologías de la información de la sede central del gobierno Regional de Ancash el encargado de velar por la implementación del plan de transición.

3.2. Métodos.

3.2.1. Tipo de investigación

- **De acuerdo a la orientación:**

Investigación aplicada, por qué parte de un marco teórico nacional e internacional que es la guía fundamental de éste trabajo para formular teorías en base a nuestra realidad local. Estas fuentes serán ejes principales para lograr elaborar un modelo de referencia.

- **De acuerdo a la técnica de contrastación:**

Investigación descriptiva, tomada de la realidad del país y de la localidad con respecto a entidades que realizaron planes de transición de protocolos de comunicación.

3.2.2. Definición de variables

- **Variable independiente**

X= Sistema de gestión para la transición de IPv4 a IPv6.

- **Variable dependiente**

Y= Plan de transición del protocolo IPv4 al protocolo IPv6.

Gráfico N° 3. 1:
Operacionalización de variables

VARIABLE	DIMENSIÓN	DEFINICIÓN OPERACIONAL	INDICADORES	INSTRUMENTO	ÍTEM	ESCALA
VI= Sistema de gestión para la transición de IPv4 a IPv6	Gestión del proceso de elaboración de la estructura del plan	Eficiencia con la que se identifica los requerimientos básico que tiene que contener el plan	Estructura básica del plan de transición	Encuesta	Entrevista a los trabajadores de la unidad de tecnologías de información, Pregunta 1.	De no cumplieron mis expectativas a superaron mis expectativas
	Gestión del proceso de etapas de para la transición a IPv6	Eficiencia con la que se identifica las etapas necesarias para el inicio de la transición a IPv6	Secuencia de acciones en el proceso de transición	Encuesta	Entrevista a los trabajadores de la unidad de tecnologías de información, Pregunta 2.	De no cumplieron mis expectativas a superaron mis expectativas
	Gestión del proceso de pruebas en la transición a IPv6	Eficiencia con la que se identifica las pruebas necesarias durante la transición a IPv6	Pruebas para validar el proceso de transición	Encuesta	Entrevista a los trabajadores de la unidad de tecnologías de información, Pregunta 2,3.	De no cumplieron mis expectativas a superaron mis expectativas
VD= Plan de transición del protocolo IPv4 al protocolo IPv6.	Gestión del proceso de elaboración del plan para la migración a IPv6	Validación del nivel de satisfacción para la elaboración del plan de transición en base al sistema de gestión planteado	nivel de satisfacción en la elaboración del plan de transición	Encuesta	Entrevista a los trabajadores de la unidad de tecnologías de información, Pregunta 4.	De no cumplieron mis expectativas a superaron mis expectativas

Fuente: Elaboración propia

3.2.3. Diseño de la investigación

- **Diseño general:**

Esta investigación se caracteriza por ser descriptiva y no experimental por lo cual el diseño de la investigación planteada es el diseño descriptivo simple, puesto que consiste en seleccionar determinada muestra sobre una realidad cualquiera y ejecutar sobre ella observaciones y descripciones, se usa para buscar y recoger información con respecto a un objeto de estudio.

$$X \rightarrow Y$$

Donde:

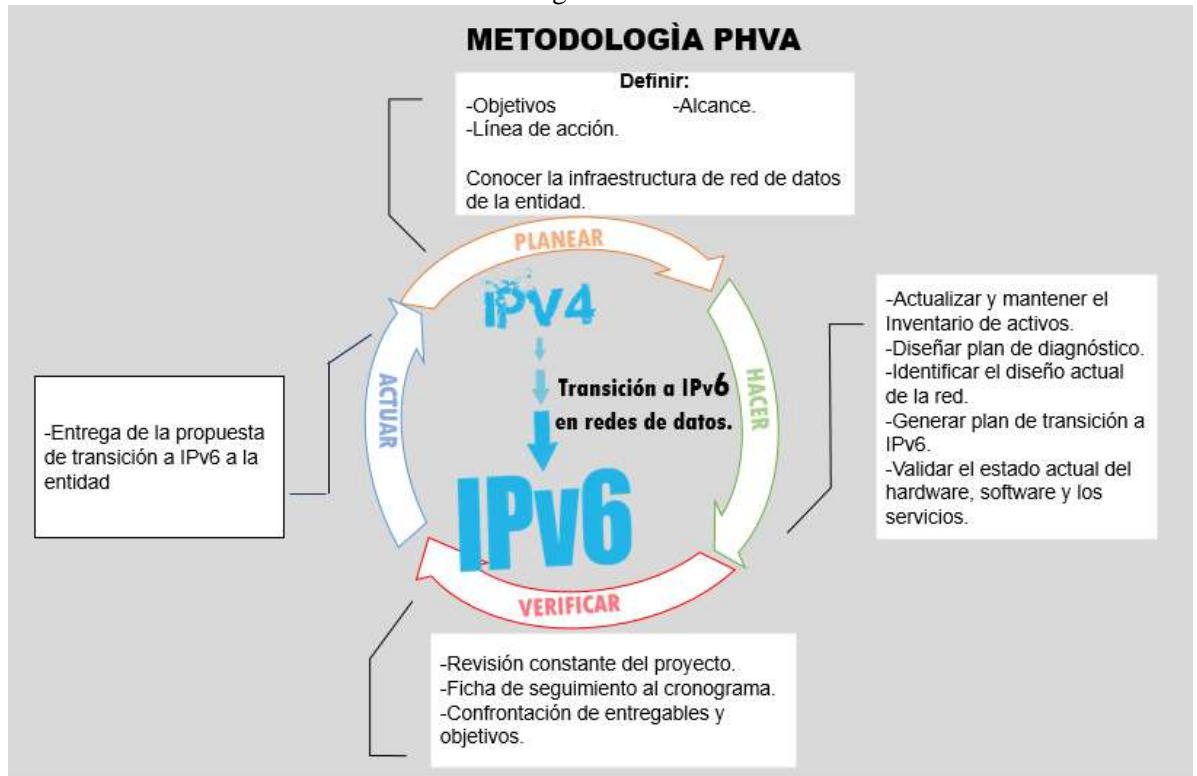
X= Sistema de gestión para la transición de IPv4 a IPv6

Y= Plan de transición del protocolo IPv4 al protocolo IPv6.

- **Diseño metodológico**

La metodología utilizada es el ciclo continuo PDCA, o en español PHVA, normalmente este proceso se utiliza en procedimientos técnicos y gerenciales para hacer cumplir los requisitos de calidad de una empresa ya que permite el mantenimiento y mejora continua dentro de cualquier organización.

Gráfico N° 3. 2:
Metodología PHVA



Fuente: Elaboracion propia

Se vio la aplicabilidad de la metodología PHVA en el sistema de gestión para elaborar el plan de transición a IPv6 porque desarrolla la mejora continua de servicios a través de un proceso cíclico en el que se ven las fases de Planear, Hacer, Verificar y Actuar, lo que haría que el proceso de transición tenga una mayor efectividad al realizarse la revisión de las actividades que se planearon de acuerdo con la definición previa del problema y los objetivos a alcanzar, para finalmente dar una solución concreta y mejorada.

En el Gráfico N° 3.1 se pueden observar las actividades generales que se determinaron para el proceso de planeación de la transición a IPv6, teniendo en cuenta que más adelante se desglosaría cada una de ellas en el cronograma de actividades, siempre definiendo las fases de Planear, Hacer, Verificar y Actuar.

3.3. Técnicas

3.3.1. Técnicas de procesamiento de la información

Las técnicas utilizadas en el presente trabajo de investigación son:

- ✓ **Entrevista:** Consiste en que una persona calificada (entrevistador) hace las preguntas al entrevistado y anota las respuestas, es decir aplica un cuestionario al personal de TI del Gobierno Regional de Ancash (Ver anexo N° 2).
- ✓ **Encuesta:** consiste en una serie de preguntas, abiertas o cerradas, respecto de una o más variables a medir. Serán dirigidos al personal de TI del Gobierno Regional de Ancash (ver anexo N° 3).
- ✓ **Ficha de observación:** es un documento en el que se **anotan** las observaciones realizadas en un experimento. En la presente investigación se usará para anotar las poblaciones de los indicadores.
- ✓ **Inventario de activos informático (hardware y software):** Se clasificarán los activos como Activos de soporte o activos primarios basado en la norma técnica ISO 27000 y el soporte que estos poseen con el protocolo IPv6 (Ver tablas N° 5.1, 5.2, 5.3 y 5.4).

3.4. Procedimiento

Las técnicas de procesamiento de información serán:

- Encuestas dirigidas al personal que labora en el área de Unidad de tecnologías de la Información del Gobierno Regional de Ancash.
- Análisis de las entrevistas realizadas, así como también de los documentos, libros y guías que se estén empleando para la realización de este proyecto.
- Análisis de las observaciones realizadas durante la recopilación de información.

En base a éstas técnicas de procesamiento de información, se establecerá la situación actual del Gobierno Regional de Ancash en la elaboración del sistema de gestión para la elaboración del plan de transición del protocolo IPv4 al protocolo IPv6.

En el Gráfico N° 4.1 se puede apreciar el organigrama del Gobierno Regional de Ancash

En la tesis se establece como unidad de análisis al jefe de la Unidad de Tecnologías de la Información perteneciente a la Sub Gerencia de Desarrollo Institucional de la Gerencia regional de Planeamiento Presupuesto y acondicionamiento Territorial pues es la persona encargada de la elaboración del plan de transición del protocolo IPv4 al protocolo IPv6.

Puesto que esta unidad es la encargada de realizar el plan de transición de protocolos en la sede central, así como también es responsable del monitoreo de la implementación de este plan en todas las unidades ejecutoras dependientes del Gobierno Regional de Ancash.

4.1.1. Capacidad instalada:

Se realiza en base a los recursos de TI que plantea COBIT 5; las aplicaciones, la información, la infraestructura y las personas.

4.1.1.1. Las aplicaciones

Actualmente el Gobierno Regional de Ancash cuenta con aplicaciones de software para diversos procesos de diferentes áreas, entre los que resaltan principalmente los sistemas administrativos como son: el Sistema Integrado de Administración Financiera (SIAF-MEF), Sistema Integrado de Gestión Administrativa (SIGA-MEF), Sistema de Gestión Documentaría (SISGEDO). También se cuenta con otras aplicaciones de uso específico en diversas áreas. Cabe recalcar que al elaborar el plan de transición del protocolo ipv4 a ipv6 se tienen que tener en cuenta el impacto que tendrá en estos aplicativos ya que son de vital importancia para el desarrollo de las funciones dentro del gobierno regional de Ancash.

4.1.1.2. La infraestructura.

Se puede evaluar la infraestructura que posee el Gobierno Regional en taninos de:

- Hardware: se dispone de equipos de cómputo modernos computadoras que van desde Pentium IV hasta i7, impresoras, escáneres, etc.
- Redes: El cableado estructurado está compuesto por un cableado vertical de categoría 6a y el cableado horizontal en categoría 6, 5e, switch en capa 2 y capa 3 y servidores de última generación.

Se tiene que realizar un inventario exhaustivo de toda la infraestructura tecnológica para su análisis y determinar su compatibilidad con el protocolo ipv6

4.1.1.3. Las personas

El personal que actualmente labora en el Gobierno Regional de Ancash cumple una función determinada, pero es claramente apreciable que el personal tiene un promedio de edad bastante alto aproximadamente de 45 años de edad, esto implica que su capacidad de uso de TIC es reducida, lo que demuestra la presencia de una brecha digital, por lo que hay una alta resistencia al cambio y a la actualización tecnológica.

Siendo este un factor importante a tener en cuenta en la elaboración del plan de transición y contemplar acciones las cuales no afecten en demasía las labores realizadas por el personal que labora en la institución.

4.1.2. Análisis FODA

El análisis FODA es una herramienta que permite conformar un cuadro de la situación actual del Gobierno Regional de Ancash, permitiendo de esta manera obtener un diagnóstico preciso de la situación actual de la Institución, desde una perspectiva de lo interno y externo. Para lo cual se utilizó el análisis FODA.

Tabla N° 4. 1:
Análisis FODA

Fortalezas	Debilidades
F1 Crecimiento de la disponibilidad presupuestal para la ejecución del plan de transición de protocolos.	D1 Insuficiente personal profesional y técnico calificado para cumplir con los objetivos institucionales.
F2 Predisposición para alianzas estratégicas con instituciones públicas y privadas.	D2 Débil cultura de cumplimiento a los documentos de Gestión que normalizan los procedimientos.
F3 Tecnología informática adecuada en el Gobierno Regional de Áncash.	D3 Ausencia de cultura organizacional y control interno.
Oportunidades	Amenazas
O1 Decreto Supremo N° 081-2017-PCM.	A1 Falta de cultura de planeamiento estratégico en el sector publico
O2 Nuevas tecnologías que fortalecen las actividades.	A2 Cambios inesperados de responsables de la elaboración y ejecución del plan de transición al protocolo IPv6.
O3 Ofertas de programas de capacitación.	
O4 Presencia de la gran minería.	

Fuente: Elaboración Propia

El análisis FODA del Gobierno regional de Áncash revela que la entidad tiene solvencia para costear la transición al protocolo ipv6; para paliar las debilidades se debe de contratar personal con contrato fijo en el área de TI que será los encargados de la implementación del plan de transición de protocolo

El Gobierno regional de Ancash también debe de enfatizar sus esfuerzos contra las amenazas de la falta de cultura de planeamiento y tener una política para el cambio de funcionarios y personal responsable de la elaboración y desarrollo del plan de transición de protocolos

El Gobierno Regional de Ancash puede esperar mejor rendimiento al tratar de manera efectiva estos factores estratégicos identificados en su análisis FODA.

Los factores críticos de éxito:

- Apoyo de la alta dirección
- Sostenibilidad del equipo humano de la unidad de tecnologías de la Información - GRA
- Capacitación permanente
- Intercambio de experiencias con otras instituciones
- Involucramiento de todas las unidades orgánicas / direcciones del Gobierno Regional de Ancash.

4.2. Identificación y descripción de requerimientos

En esta sección se describirá los requerimientos funcionales y no funcionales identificados para la formulación del plan de transición, basándose en el Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”.

Contenido mínimo que debería tener el plan de transición según el Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”:

- **ALCANCE:**

Al delimitar el alcance se debe de tener bien claro cuáles son los servicios y equipos que se va a exponer a IPv6, determinando si estos vienen a ser toda la red, todos los servicios de la red o solo los servicios que la entidad expone a internet.

- **DIAGNOSTICO DE LA INFRAESTRUCTURA TÉCNOLOGICA**

Cuando se realiza el inventario y posterior análisis de la infraestructura tecnológica (hardware, software y servicios); se debe determinar en el caso de hardware si estos soportan versión IPv6, cuales equipos no soportan y elaborar un cronograma de cambio con otros equipos que si soporten el protocolo IPv6.

En el tema de software de igual manera se debe de verificar si son compatibles con el protocolo IPv6, si los software son propios se debe de tener en cuenta

un plan para la adecuación al protocolo de ipv6 en caso de software de terceros se debe de realizar la consulta con la entidad dueña del código si estos softwares están contemplados a actualizar a la nueva versión del protocolo ipv6 (por ejemplo en aplicaciones necesarias para cualquier entidad del estado como son el SIGA-MEF y SIAF-MEF); en caso los softwares de terceros no estén contemplados en la actualización al nuevo protocolo realizar un acta de riesgo y delimitar las acciones que se adoptaran para el uso normal de estos sistemas.

- **IMPLEMENTACIÓN DEL PROTOCOLO IPV6**

En esta etapa se destinará los cronogramas de la implementación del protocolo IPv6, indicando las fechas de las compras (en caso sea necesario) de nuevo equipo informático, software y/o actualización de los mismos.

Así mismo se debe de elegir que método de transición se va a utilizar para realizar la transición.

- **PRUEBAS**

Realizar la verificación de las configuraciones, para determinar posibles fallas y/o inconvenientes que podrían suscitarse en el proceso de transición del protocolo ipv4 al protocolo ipv6

- **CAPACITACIÓN Y SENSIBILIZACIÓN**

Se debe prever una capacitación al personal que no sea del área de TI, puesto que es muy importante hacer de conocimiento a todo el personal y así estén preparados por si sucede alguna contingencia y esta interrumpa en la función normal de las labores del personal.

- **PRESUPUESTO**

Se debe de tener un presupuesto aproximado contemplando costos que generara la transición de protocolos, por ejemplo: la contratación de personal especializado, compra de equipos necesarios para la transición del protocolo pv4 al protocolo ipv6, adquisición de software para la transición de protocolos y demás gastos en los que se va a incurrir al momento de realizar la transición de protocolos.

- **ANEXOS**

Identificar los anexos que van a acompañar al plan de transición, ya sea normativas en las que se basa el plan de transición (Decreto Supremo N° 081-2017-PCM), si la entidad no cuenta con alguna política, norma, procedimiento de carácter administrativo, procedimiento de carácter técnico que indique algo sobre ipv6, generar las mismas con las áreas y/o gerencias competentes encargadas de generar estos documentos.

4.3. Diagnóstico de la situación actual

De acuerdo al análisis realizado, se evidencio el liderazgo de Perú en la adopción de IPv6 a nivel del RIR LACNIC; sin embargo, al realizar un análisis más 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. Sumado a esto, se observa que otros ISP con presencia nacional, tienen asignado un prefijo IPv6 por el LACNIC.

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 transición 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 líderes 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, empiezan a partir del Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública “en el cual se detalla que todas las entidades públicas desde ministerios, Gobiernos Regionales, municipalidades, etc. tienen que contar con un plan de transición de protocolos en el cual se le piden que tenga ciertos requisitos básicos; así es como el gobierno peruano a través de la Secretaría de Gobierno Digital trata de emular a los países líderes en la adopción del protocolo ipv6.

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 evidenció 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.

CAPITULO V:

DISEÑO DE LA SOLUCION

5.1. Arquitectura tecnológica de la solución

El proceso de transición de IPv4 a IPv6 no es una tarea fácil, por este motivo se debe mantener una comunicación entre la versión actual y el protocolo IPv6, ya que tarde o temprano se deberá llevar a cabo un cambio completo de IPv4 a IPv6 sin la necesidad de afectar los servicios y aplicaciones de la red actual del Gobierno Regional de Ancash.

El objetivo de la transición no es remplazar los servicios IPv4 existentes, lo único que se trata de hacer es buscar diferentes escenarios para la transición ya que las instituciones modernas necesitan implementar lo último en tecnología con el fin de obtener mecanismos estables para que se puedan transmitir los datos y demás aplicaciones tanto en IPv4 como en IPv6.

A continuación, presentamos una descripción de los escenarios para la transición a IPv6 en el Gobierno Regional de Ancash:

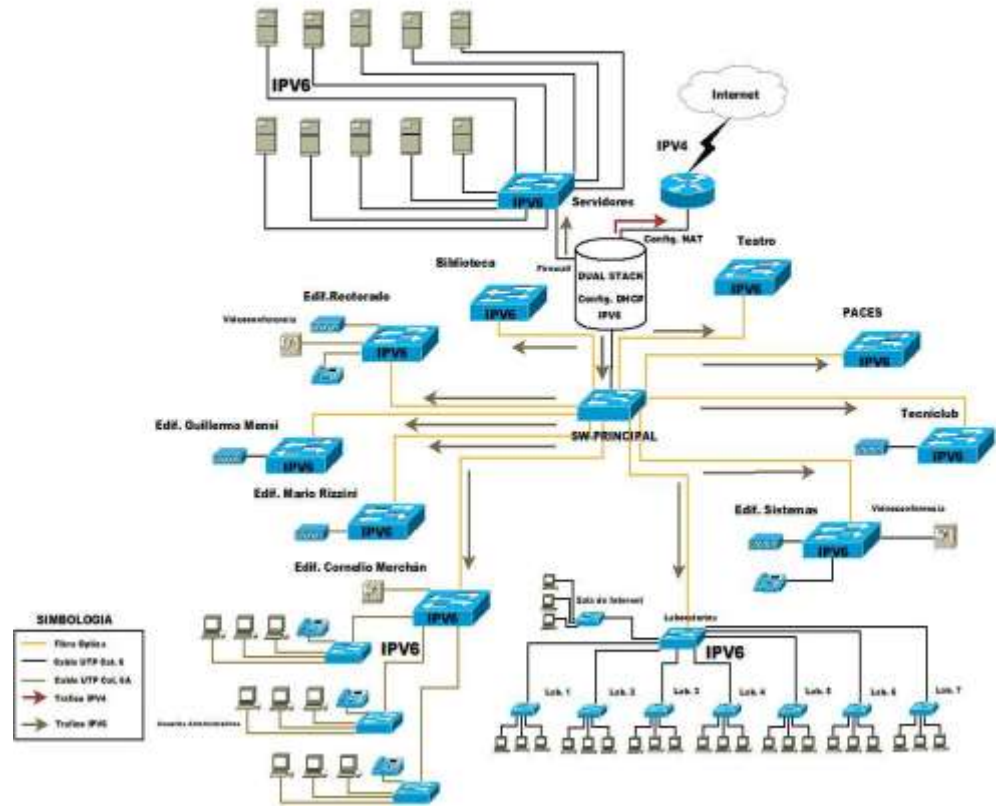
Primer escenario: Mantener IPv4 al mundo y tener IPv6 en la red local.

El esquema que se propone permite activar la configuración IPv6 por medio de DHCP en todos los equipos de red que se encuentran conectados al Switch principal y al Switch servidores hasta la conexión con el Firewall.

Dentro del Firewall CISCO ASA 5510 se establece la configuración del mecanismo de transición Dual Stack para permitir la comunicación de la red local de IPv6 a IPv4, además se debe realizar la configuración de NAT para permitir la traducción de las direcciones IPv4/IPv6.

A continuación, se presenta el diagrama del Primer Escenario para la transición a IPv6:

Gráfico N° 5. 1:
Mantener IPv4 al mundo y tener IPv6 en la red local



Fuente: Elaboracion Propia

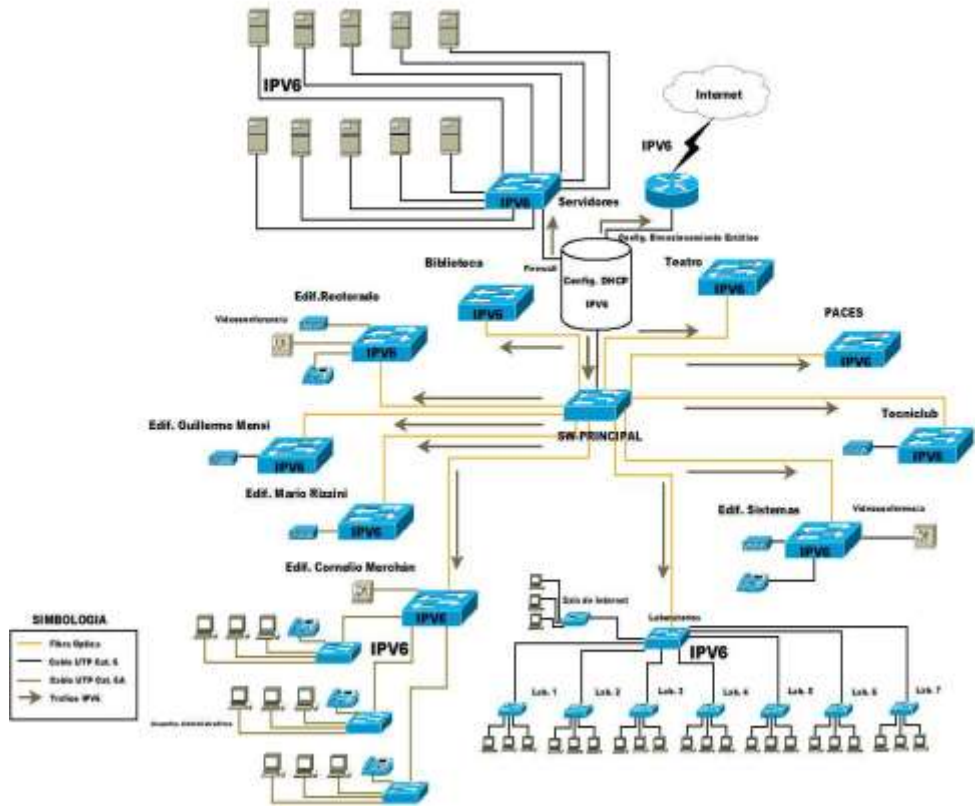
Segundo escenario: Tener IPv6 en el mundo y tener IPv6 en la red local

El esquema que se propone es similar al primer escenario en donde tenemos que activar la configuración IPv6 por medio de DHCP en todos los equipos de red que se encuentran conectados al Switch principal y al Switch servidores hasta la conexión con el Firewall.

En este escenario estamos asumiendo que el mundo ya se encuentra funcionando completamente en IPv6, debido a esto para acceder al Internet desde nuestra red local, lo único que tenemos que hacer es configurar el Firewall utilizando un direccionamiento estático para IPv6.

A continuación se presenta el diagrama del Segundo Escenario para la transición a IPv6:

Gráfico N° 5. 2:
Tener IPv6 en el mundo y tener IPv6 en la red local



Fuente: Elaboracion Propia

5.2. Diseño de estructura de la solución

5.2.1. Base legal

Se incluye todas las normas legales en las cuales se basa la elaboración del plan de transición al protocolo IPv6

5.2.2. Alcance

Se debe de delimitar el alcance de la implementación del plan, si va a ser toda la red de la institución los que se expongan al protocolo IPv6, si va a ser solo los servicios que brinda la entidad los que se expongan a internet.

5.2.3. Diagnostico de la infraestructura tecnológica

Elaborar y validar el inventario de activos de información de servicios tecnológicos de las entidades y su interrelación entre ellos. Para esta actividad se requiere tener preparado el inventario de hardware y

software, identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6. Para esta etapa se recomienda que para cada elemento del inventario de activos de información se pueda constatar con los fabricantes, y con los terceros si ha lugar, el cumplimiento de IPv6, a través de la certificación que avale el soporte del nuevo protocolo en las infraestructuras de TI; se recomienda realizar los inventarios en grupos como se muestra a continuación para un mejor diagnóstico.

a) Equipos de cómputo

Se recomienda realizar un inventario utilizando la siguiente tabla.

Tabla N° 5. 1:
Tabla para levantamiento de información de los equipos de cómputo

N°	Nombre Usuario	Oficina	Equipo	Marca	Tamaño de memoria	Procesador	Sistema Operativo	Soporte Ipv6
-----------	-----------------------	----------------	---------------	--------------	--------------------------	-------------------	--------------------------	---------------------

Fuente: Elaboración Propia

De la elaboración de la tabla anterior se debe de tener en cuenta la mayor parte de los sistemas operativos, desde el año 2001 aproximadamente, tienen algún tipo de soporte de IPv6. Es cierto que, en algunos casos, inicialmente no se trataba de un soporte “comercial”, sino versiones de prueba, aunque se incorporaban a sistemas operativos de “producción”. Tal es el caso del soporte de IPv6 en Windows 2000 e incluso en la primera versión de Windows XP, antes del lanzamiento del denominado Service Pack 1 (SP1). Cada vez es más frecuente que diversas plataformas o sistemas operativos, no solo incorporen IPv6, sino que además sea activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario.

Teóricamente, todos los equipos de cómputo en una entidad pueden soportar IPv6, pues Microsoft implementó este protocolo desde la versión Windows XP en adelante de igual manera en las diferentes distribuciones que ofrece Linux, sin embargo, no todas las versiones

traen activo este soporte, este tipo de protocolo generalmente viene en las versiones PROFESSIONAL; en la mayoría de equipos se debe realizar la activación y configuración de manera manual.

Adicionalmente, los equipos con sistema Operativo Windows XP y Windows Vista, requieren de una actualización o en su defecto un cambio, ya que la vida útil de dichos equipos ya estaría sobrevaluada; además que sus características técnicas, como memoria RAM y Disco Duro, los hacen equipos obsoletos.

Sugerencias para la transición a IPv6.

Si bien todos los equipos existentes pueden estar en el proceso de transición a IPv6, se sugiere realizar actualizaciones y/o cambios en los equipos cuyas versiones sean Windows XP o Windows Vista, pues son versiones desarrolladas hace una década o más y probablemente presenten problemas con algunas configuraciones necesarias, además, Microsoft ya no brinda ningún tipo de soporte para Windows XP, lo que eventualmente puede presentar un gran inconveniente en el proceso de transición a IPv6.

b) Equipos de impresión

A continuación se muestra un modelo para la recopilación de información de los diversos equipos de impresión.

Tabla N° 5. 2:

Tabla para levantamiento de información de los equipos de impresión

N°	Dependencia	Marca y Modelo	Tipo de Impresora y Tecnología Utilizada	Soporta IPv4	Soporta IPv6
-----------	--------------------	-----------------------	---	---------------------	---------------------

Fuente: Elaboración Propia

Verificar si las impresoras soportan el protocolo IPv6 consultando el datasheet del fabricante para verifica si se puede realizar actualizaciones para la activación del protocolo IPv6 en el Equipo, en caso no cuente con el soporte para el protocolo recomendar la adquisición de nuevos equipos para su adquisición.

c) Equipos de comunicación

La plantilla utilizada para el inventario de los equipos de comunicación es como se puede ver a continuación.

Tabla N° 5. 3:
Tabla para levantamiento de información de los equipos de información

N°	Equipo	Marca y Modelo	Ubicación	Puertos Ethernet	Soporte IPv6
----	--------	----------------	-----------	------------------	--------------

Fuente: Elaboración Propia

Sugerencias para la transición a IPv6.

Si bien la sección de la red de datos de la entidad que está funcionando con los Switches que no son compatibles con el protocolo versión 6 debe seguir funcionando de la manera en la que está, se sugiere empezar la transición con los dispositivos que sí poseen el soporte del nuevo protocolo; aun así, se indica que poco a poco se vayan adjuntando a la red nuevos dispositivos que faciliten el proceso de transición, algunas sugerencias se muestran a continuación.

d) Aplicativos

La plantilla utilizada para relacionar la información concerniente a los aplicativos de uso en la entidad se muestra a continuación.

Tabla N° 5. 4:
Tabla para levantamiento de información de los equipos de aplicativos

N°	Aplicativo	Tipo	Sistema Operativo	Dependencia	Responsable del Aplicativo	Propietario del Aplicativo	Soporte IPv6
----	------------	------	-------------------	-------------	----------------------------	----------------------------	--------------

Fuente: Elaboración Propia

Los Gobierno locales y regionales utilizan diversos aplicativos desarrollados por su personal de TI, terceros o por convenios con otras instituciones.

El claro ejemplo es del SIGA y SIAF del MEF, al ser software desarrollado por el MEF se debe de Consultar si estos aplicativos a futuro tendrán compatibilidad con IPv6 al ser de vital funcionamiento en una entidad pública; en caso la respuesta sea negativa se tendrá que realizar un acta de aceptación de riesgos, puesto que la entidad no tiene permisos

para la modificación y/o adaptación del aplicativo para que soporte el protocolo IPv6.

5.2.4. Implementación del protocolo IPv6

La fase de implementación debe cubrir las siguientes actividades:

- Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Fase de diagnóstico del proceso de transición de IPv4 a IPv6, teniendo en cuenta el inventario de los activos de información de cada una de las infraestructuras de TI de las Entidades del Estado y teniendo en cuenta el diseño de la red bajo IPv6.
- Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs creadas, con un número especial de usuarios que aprovechen la homogeneidad de la red, con servicios de filtrado, críticos a fin de evitar traumatismos en el normal funcionamiento de la red.
- Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en Doble Pila; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.
- Aplicar el modelo de transición de IPv6 definido por la Entidad, permitiendo la coexistencia de los aplicaciones, infraestructuras y servicios bajo los protocolos tanto de IPv4 como de IPv6, en modalidad de transición en doble pila.
- Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 bajo doble pila; esta técnica permite que tanto los servicios de IPv4 como los servicios de IPv6

deben estar funcionando de manera independiente pero coexistente dentro de las Entidades.

- Validar la funcionalidad en IPv6 de los siguientes servicios y aplicaciones de las Entidades sobre IPv6: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servicios Voz sobre IP, Servidores de Monitoreo, Servicios con sistema IPTV, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicios que soporten canales TDT, Servicio de Respaldo, Servicio de Comunicaciones Unificadas, Servicios VPN, Integración entre Sistemas de Información, Sistemas de Almacenamiento, Servicios de Administración de Red, Sistemas en la Nube y Sistema Ininterrumpido de Potencia.
- Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad, por ejemplo, servidores AAA, firewalls, NAC, y equipos perimetrales de conformidad, zonas desmilitarizadas, con los RFC de seguridad en IPv6; al respecto, se recomienda revisar los RFC de seguridad en IPv6 asociados.
- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral, desde el interior de las redes LAN, hacia el exterior de las redes WAN a fin de garantizar que las entidades puedan generar tráfico de IPv6 nativo ante la comunidad de Internet.

a) CRONOGRAMA

Las entidades deberán tener en cuenta un cronograma y diligenciar el tiempo en meses que le lleve desarrollar cada actividad:

Tabla N° 5. 5:
Modelo de cronograma para la implementación del protocolo IPv6

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

Fuente: Elaboración Propia

b) RESPONSABLES

Indicar los Responsables del Área de TI que estarán a cargo de Realizar las acciones en esta etapa.

c) ENTREGABLES

- Preparación y presentación del Informe del plan detallado de implementación del nuevo protocolo.
- Documento con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta

fase, incluye las configuraciones a realizar sobre el canal (canales) de comunicaciones con acceso a internet.

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

5.2.5. Pruebas

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

- Realizar las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la Entidad en un ambiente que permita empezar a generar tráfico de IPv6 de la entidad hacia Internet y viceversa.
- Realizar las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones y presentar el Informe de las pruebas realizadas.
- Al momento de las pruebas de funcionalidad se debe realizar el afinamiento de las configuraciones de hardware, software y servicios de las Entidades, con base en la información resultante de la fase anterior, se recomienda realizar las siguientes pruebas:

➤ Verificación de conectividad física

Documentando la implementación que se hizo en la transición, se observa según los esquemas de distribución e infraestructura, las conexiones físicas que deben estar presentes en los router's, switch'e's, host y demás dispositivos que se encuentren en la red. Además, confirmar las conexiones a la red WAN mediante el proveedor de servicio encargado de entregar el pull de direcciones IPV6.

➤ **Generación de Ping**

Asegurando las conexiones físicas, se hacen pruebas por el método de Ping a los distintos dispositivos que están en la red; Aquí se puede verificar los tiempos de respuesta del dispositivo destino y que estén conectados acorde con la distribución ofrecida a la organización. Este método se debe aplicar para las direcciones IPv4 e IPv6 ya que como se ha visto en esta metodología los dos protocolos tienen que convivir en la misma red de acuerdo a la técnica dual Stack. Es conveniente revisar los pines con el servicio DNS que existen en los servidores de la red, garantizando el servicio de conectividad con las aplicaciones que no están soportadas con IPv6

➤ **Analizador de Trafico**

Haciendo pruebas enviando paquetes de datos, se instala en el sistema del administrador un analizador de tráfico como WireShark, que permita observar las direcciones origen y destino de los paquetes de datos; con ello se puede confirmar que se estén utilizando los dos protocolos dependiendo del tráfico que se está enviando por IPv4 o IPv6. Otra forma de utilizar el analizador de tráfico es observar los protocolos adyacentes con los que se está ejecutando la metodología de dual Stack. Además de analizar los protocolos y las direcciones origen destino se puede observar la calidad del servicio dependiendo del ancho de banda que se adquiera con el prestador de servicio.

- Elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

a) CRONOGRAMA

Tabla N° 5. 6:
Modelo de cronograma para la fase de pruebas en la transición al protocolo IPv6

	Actividades generales	Tiempo en meses de la actividad
Prueba de Funcionalidad	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad. Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI. Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.	

Fuente: Elaboración Propia

b) RESPONSABLES

Indicar los Responsables del Área de TI que estarán a cargo de Realizar las acciones en esta etapa.

c) ENTREGABLES

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

5.2.6. Capacitación y sensibilización

La capacitación y sensibilización es un tema muy importante puesto que se tiene que informar a los usuarios que se está llevando a cabo la transición de protocolos y quizá afecte en sus labores diarias, así como también la sensibilización a los diversos funcionarios de la alta gerencia,

gerentes de línea, sub gerentes y jefes de área para que brinden el apoyo en la elaboración y desarrollo del plan de transición, y así generar directivas, normativas y demás documentos normativos que contemplen la transición y adaptación al nuevo protocolo por parte de la entidad.

- Reunión con los gerentes, sub gerentes, jefes de área para la sensibilización sobre la adopción del nuevo protocolo en el Gobierno Regional de Ancash.
- Capacitación y sensibilización a los diferentes empleados del gobierno regional de Ancash, indicando las acciones que se van a tomar; previniendo de posibles fallas y cortes del servicio informáticos.
- Coordinación con las oficinas competentes la generación de documentos, directivas y/o normas que sustenten y apoyen la adopción del protocolo ipv6 en el Gobierno Regional de Ancash; tales como la compra de nuevos equipos con soporte en IPv6, contratación del servicio de internet y demás normativas que se crean conveniente.

a. CRONOGRAMA

Tabla N° 5. 7:

Modelo de cronograma para la capacitación y sensibilización del protocolo IPv6

Actividades generales	Tiempo en meses de la actividad
Capacitación y sensibilización Reunión con los Directores de línea y jefes de área para informar sobre el plan de transición de protocolos.	
Capacitación y sensibilización a los diferentes empleados del Gobierno Regional de Ancash.	
Coordinación Con los jefes de las diferentes áreas para la generación de normativas, resoluciones ejecutivas, resoluciones gerenciales que involucren al nuevo protocolo ipv6.	

Fuente: Elaboración Propia

b. RESPONSABLES

Indicar los Responsables del Área de TI que estarán a cargo de Realizar las acciones en esta etapa.

c. ENTREGABLES

- Documentos tales como normativas, resoluciones ejecutivas, resoluciones gerenciales y ordenanzas que contemplen acciones que permitan hacer un buen uso respecto al protocolo IPv6 en la sede central del GRA.

5.2.7. Presupuesto

En este punto debe de indicarse todos los costos que implica la transición del protocolo IPv4 al protocolo IPv6 indicando los costos en los siguientes ítems:

- Personal
- Equipos computacionales
- Equipos de Comunicación
- Servicios de adaptación de software
- Y demás costos que implica la transición de protocolos.

5.2.8. Anexos

Anexar documentos en los cuales se base el diseño del plan de transición de protocolos, tales como directivas de adquisición de nuevos equipos, normativas de acceso al nuevo protocolo, etc.

5.3. Diseño de la funcionalidad de la solución

- Utilizar la metodología de transición de IPv4 a IPv6 en Doble Pila (Dual Stack), consistente en permitir la coexistencia de los dos protocolos simultáneamente con el fin de continuar con los servicios y aplicaciones tanto en el ambiente de IPv4 como en el ambiente de IPv6.
- Elaborar el nuevo plan de direccionamiento en IPv6 totalmente segmentado bajo los tipos de direccionamiento en anycast, multicast y unicast.
- El esquema de enrutamiento debe contener la definición del propio bloque o segmento de direcciones IPv6 asignado para la Entidad, en este sentido se recomienda que cada Entidad solicite previamente su propio bloque o

segmento ante LACNIC5, para mayor detalle de este procedimiento favor consultar el siguiente enlace: <http://www.lacnic.net/web/lacnic/IPv6-end-user>.

- Revisar el pool de direccionamiento IPv4 de cada Entidad y hacer la equivalencia técnica de direccionamiento, servicios y aplicaciones para IPv6.
- El nuevo bloque de direccionamiento IPv6, que se recomienda solicitarlo ante LACNIC, debe funcionar de manera transparente para los usuarios finales e independientemente del proveedor del servicio de internet – ISP que se tenga en la Entidad. En caso de que la organización llegue a la fase de implementación de IPv6 sin todavía haber solicitado el bloque de IPv6 ante LACNIC, este deberá solicitarse de manera temporal a su actual proveedor del servicio, advirtiéndole que este bloque seguirá perteneciendo siempre al proveedor del servicio y no a la entidad. La segmentación del bloque de direcciones IPv6 debe establecerse por zonas lógicas de seguridad acorde a las necesidades de la red de la organización, contemplando zona de comunicaciones, zona de administración de servidores, zona de aplicaciones, zona de bases de datos, zona de ambiente de pruebas, zona de respaldos y monitoreo, zona Wifi y zona de publicaciones Web.
- Para cada zona lógica debe ser configurada en el firewall y deben contener las políticas de seguridad de acuerdo a la gestión y uso de los servicios prestados en las Entidades.
- Coordinar con los Proveedores de Servicio de Internet - ISP (Internet Services Provider) de cada Entidad, las acciones técnicas necesarias para que estos apoyen la implementación de los nuevos enrutamientos de IPv6, que sean necesarios hacer en las aplicaciones y/o servicios de red con el fin de garantizar la generación de tráfico IPv6 por medio de estos canales; así mismo como se mencionó antes, para esta instancia es recomendable tener el nuevo bloque de direcciones IPv6 (prefijo), previamente solicitado ante LACNIC.
- Se requiere la definición de un cronograma general para cada una de las fases del proceso de transición a IPv6, a fin de establecer con tiempo, las ventanas

de mantenimiento e indisponibilidad cuando se requieran a fin de evitar traumatismos en la continuidad de los servicios.

- Definir un plan de marcha atrás (Plan de Contingencias) en caso de presentarse inconvenientes de indisponibilidad de las aplicaciones y servicios de la Entidad dentro de la fase de Implementación de IPv6,
- Para la fase implementación de IPv6 es importante generar previamente un ambiente de pruebas que simule completamente la topología de red propuesta para IPv6.
- Evaluar el soporte de IPv6 para los servicios de Directorio Activo, Servicio de DNS, Servicios de Voz sobre IP, Servicios con Sistemas IPTV, Servicio de Correo Electrónico, Servicio de DHCP, Servicios de aplicaciones, Servicios Web, Servicios de Gestión y Servicios en la Nube, Servicios que soporten canales de acceso a internet y otros servicios.
- Revisar las políticas y/o reglas de seguridad de los siguientes componentes que cada organización tenga como son: Enrutadores, Equipos de Seguridad (Firewalls), Servidores, Equipos de Conmutación (Switches), Controladoras, Puntos de Acceso (APs), Servidores, Equipos de Almacenamiento de Datos (SAN), Terminales Inteligentes, Controladoras Inalámbricas (WiFi), Controladoras de Gestión de Redes, Centro de Datos (Data Center), Centros de Cableado, Centrales Telefónicas, Sistemas Ininterrumpidos de Potencia (UPS), Sistemas de Aire Acondicionado, Sistemas de Detección y Prevención contra Incendio y Servicios de Impresoras, dispositivos móviles al servicio de la Entidad, entre otros.
- Realizar la evaluación y selección de protocolos de enrutamiento internos y externos para implementar la solución IPv6 requerida, como es el caso de protocolos IGRP, EIGRP, BGP, IGP, EGP, entre otros.
- Se requiere trabajar en el proceso de transición a IPv6 para las aplicaciones; en coordinación con los proveedores de las aplicaciones a fin de revisar el cumplimiento de las aplicaciones en IPv6; para esta labor es indispensable contar con el acompañamiento de Terceros (si es desarrollo externo) que sean los responsables de las aplicaciones, revisar los contratos de soporte y

mantenimiento con ellos y realizar la evaluación final sobre que aplicaciones que pueden migrar directamente a IPv6 y cuáles requieren cambios para cumplir con el funcionamiento de los aplicativos sobre el nuevo protocolo.

- De acuerdo al inventario de las aplicaciones y servicios existentes dentro de la Entidad, se requiere clasificar las aplicaciones de acuerdo al tipo e identificación de proveedor que la ha desarrollado, esto permite identificar por cada una de ellas las bases de datos de compatibilidad. Para este punto es importante revisarlos distintos RFC que indican las recomendaciones a seguir para la adopción de IPv6 en las aplicaciones.⁶
- Definir las acciones necesarias para permitir la correcta operación de las aplicaciones que soporten IPv6 en compatibilidad con IPv4, de acuerdo a un protocolo de pruebas y validaciones establecido por la Entidad y que deberá ser ejecutado por cada uno de los proveedores de las aplicaciones y servicios.
- Realizar la actualización de las versiones de software que requieran aplicarse para los elementos activos de la red, aplicativos, sistemas operativos y demás que se ajusten a los requerimientos funcionales para la implementación IPv6. Lo anterior estará sujeto a los contratos de soporte con el fabricante de los equipos. Cada Entidad deberá suministrar el software y el proveedor deberá encargarse de ejecutar la actualización sobre los equipos a que haya lugar de este proceso.
- Coordinar con el Proveedor de Servicios de Internet de cada Entidad, todas las acciones técnicas necesarias para permitir que los servicios y aplicativos puedan desplegarse con el protocolo IPv6, desde el interior hacia el exterior con el fin de poder generar tráfico de IPv6 nativo desde y hacia sus canales de comunicación.
- Los proveedores de servicio de internet, deberán estar provistos de un sistema de Backbone⁷ en IPv6 Nativo, que permitan ofrecer y garantizar el enrutamiento de tráfico de IPv6 nativo que demanden las entidades corporativas del país.

CAPITULO VI:

CONSTRUCCION DE LA SOLUCION

En este capítulo se describen los patrones de desarrollo planteados en el proyecto, así como las tecnologías utilizadas y cómo éstas serán empleadas para facilitar el desarrollo del plan de transición de protocolos del IPv4 al IPv6 con el empleo de las mejores técnicas y prácticas.

6.1. Construcción

El plan de transición al protocolo IPv6 para el Gobierno Regional de Ancash que se elaboró siguiendo los pasos y lineamientos antes mencionados en el capítulo V, es el siguiente:

Gráfico N° 6. 1: Carátula del plan de transición al protocolo IPv6



GOBIERNO REGIONAL DE ANCASH

**GERENCIA REGIONAL DE
PLANEAMIENTO, PRESUPUESTO Y
ACONDICIONAMIENTO TERRITORIAL**

**SUB GERENCIA DE DESARROLLO
INSTITUCIONAL Y TECNOLOGIA DE LA
INFORMACIÓN**

UNIDAD DE TECNOLOGIA DE LA INFORMACIÓN

**PLAN DE TRANSICIÓN AL PROTOCOLO
IPv6 – GRA.**

2018

Fuente: Plan de transición al protocolo IPv6 – GRA.

Gráfico N° 6. 2:
Contenido del plan de transición al protocolo IPv6

Contenido

1.	BASE LEGAL.....	
2.	OBJETIVOS	
2.1.	Objetivo General	
2.2.	Objetivos Específicos	
3.	ALCANCE.....	
4.	DIAGNOSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA.....	
4.1.	Diagnóstico de Hardware	
4.2.	Diagnóstico de Servicios	
4.3.	Diagnóstico de Aplicativos	
4.4.	Diagnóstico de Políticas	
5.	IMPLEMENTACIÓN DEL PROTOCOLO IP V6	
5.1.	Cronograma y Responsables	
5.2.	Entregables	
6.	PRUEBAS	
6.1.	Cronograma y Responsables	
6.2.	Entregables	
7.	CAPACITACIÓN Y SENSIBILIZACIÓN.....	
7.1.	Cronograma y Responsables	
7.2.	Entregables	
8.	PRESUPUESTO	
8.1.	Equipo de Trabajo.....	
8.2.	Tiempo de Ejecución del Proyecto	
9.	ANEXOS	
9.1.	Cronograma Fase Implementación.....	
9.2.	Cronograma Fase Pruebas	
9.3.	Cronograma Fase Capacitación y Sensibilización	
9.4.	Declaración en Demora de inicio de la Implementación del Plan ..	

Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.1. Base legal

- **Decreto Supremo N° 081 – 2017 – PCM**, decreto supremo que aprueba la formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública.
- **Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado**, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un estado moderno, descentralizado y con mayor participación del ciudadano.
- **La Ley N° 29158 – Ley Orgánica del Poder Ejecutivo**. Tiene por objeto establecer los principios y las normas básicas de organización, competencias y funciones del Poder Ejecutivo.
- Decreto Legislativo N° 604, **Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática**. Crea el Sistema Nacional de Informática, el cual tiene por finalidad asegurar que sus actividades se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión.
- Decreto Legislativo N° 604.
- Decreto Supremo N° 022-2017-PCM. Artículo 47 del reglamento de organización y funciones de la PCM. La **Secretaría de Gobierno Digital** es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y promover políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y Gobierno electrónico; asimismo, es el órgano rector del Sistema Nacional de Informática y brinda asistencia técnica en la implementación de los procesos de innovación tecnológica para la modernización del estado.
- Decreto Supremo N° 081-2013-PCM. **Política Nacional de Gobierno Electrónico**. Prevé determinados lineamientos estratégicos

para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la infraestructura, el mismo que busca contar con una red informática que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, bases de datos, entre otros.

- Decreto supremo N° 066-2011-PCM. **Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0.** Establece en su **objetivo 1**, “**Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la Sociedad de la Información y del Conocimiento**”, disponiendo a su vez, en su **Estrategia 7**, “**Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el Protocolo de Internet v6 (IP V6)**”
- Decreto Supremo N°006-2017-JUS - Decreto supremo que aprueba el texto único ordenado de la **Ley N° 27444**, **Ley del Procedimiento Administrativo General.**
- Resolución Ministerial N° **246-2007- PCM**, que aprueba el uso obligatorio de la Norma Técnica Peruana “**NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición**”, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° **004-2016- PCM**, que aprueba el uso obligatorio de la Norma Técnica Peruana “**NTP-ISO/IEC 27001:2014 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos 2ª. Edición**”, en todas las entidades integrantes del Sistema Nacional de Informática.

6.1.2. Objetivos

6.1.2.1. Objetivo General

- Diseñar el Plan de Transición del Protocolo IPv4 a IPv6 sobre los componentes de comunicación y redes en la sede central del Gobierno Regional de Ancash y replicarlo en cada una de las sedes que son parte del Gobierno Regional de Ancash, y acorde a los lineamientos indicado en el **DS N° 081-2017-PCM** y bajo la realidad tecnológica en cada una de las sedes del GRA.

6.1.2.2. Objetivos Específicos

- Elaborar y validar el inventario de activos de información en la sede central del Gobierno Regional de Ancash.
- Analizar y llevar a cabo el plan de diagnóstico en la sede central del Gobierno Regional de Ancash.
- Generar el plan de trabajo para la adopción del IPv6 en la sede central del Gobierno Regional de Ancash.
- Comunicar a cada una de las sedes que son parte del Gobierno Regional de Ancash el presente plan para que repliquen cada una de las actividades presentadas.

6.1.3. Alcance

- El presente documento busca **proponer de acuerdo al estado actual de la infraestructura de redes y comunicaciones de cada una de las sedes que son parte del Gobierno Regional de Ancash un “Plan de Transición del Protocolo IPv4 a IPv6”**, bajo lo indicado en el **DS N° 081-2017-PCM** que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública señala: Las entidades de la AP señaladas en el alcance del artículo 2 del presente Decreto Supremo **deben elaborar un Plan de Transición al Protocolo IPv6, el cual será aprobado por el Titular de cada entidad.**

- Bajo lo indicado en el **DS N° 081-2017-PCM**, se deben planear actividades concretas para obtener un plan de diagnóstico que incluya el inventario de activos de información, un informe de la infraestructura de red de comunicaciones y sugerencias con respecto a los dispositivos que no soportan el nuevo protocolo, además de una propuesta con el plan del proceso de transición. Todo esto con base en la información y necesidades presentes en la infraestructura de redes y comunicaciones del Gobierno Regional de Ancash.
- Además, debe quedar claro que el **Protocolo de Internet IPv4**, es un sistema de identificación que se utiliza en internet para enviar información entre dispositivos, la cuarta es la versión más utilizada del protocolo. Este asigna una serie de cuatro números, cada uno de ellos comprendido entre 0 y 255, por lo tanto, cada dirección es de 32 bits y sólo permite aproximadamente 4.000 millones de direcciones únicas, **las cuales entraron en proceso de agotamiento desde hace varios años.**
- Ahora bien, el **Protocolo de Internet IPv6**, es un protocolo de internet de última generación, diseñado en los años 90 por el IETF para sustituir a IPv4. A diferencia de la anterior versión, en esta las direcciones se componen de 128 bits, lo que permite la existencia de aproximadamente 340 billones de direcciones IP únicas.

6.1.4. Diagnóstico de la infraestructura tecnológica

- El presente punto tiene por objetivo **reunir información de los principales actores del ecosistema para que cada una de las sedes que son parte del Gobierno Regional de Ancash**, puedan identificar posibles acciones encaminadas a fomentar la adopción del IPv6 de conformidad con las tendencias y recomendaciones internacionales, así se podrá identificar las posibles acciones:
 - Detectar retos y oportunidades para impulsar la adopción de IPv6.
 - Conocer principales preocupaciones y obstáculos de los involucrados.

- Identificar factores que retrasen e inhiben la adopción del IPv6.

Gráfico N° 6. 3:
Evolución de las capacidades de comunicación



Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.4.1. Diagnóstico de Hardware

- El diagnóstico presentado está relacionado a la **Sede Central del GRA**, de **igual forma debe ser realizado por cada sede o unidad ejecutora del GRA**, en coordinación directa con la Unidad de Tecnología de la Información del GRA.

Tabla N° 6. 1:
Inventario de los servidores en el GRA

Descripción de los Servidores	Características
Servidor de Datos SIAF-SP	Marca: HP
	Modelo: PROLIANT DL 380 G7
	Procesador: INTEL XEON X5690
	Memoria: 36 GB
	Disco Duro: 1200 GB
	Soporte en IPV6: si

Servidor de Datos SIGA-MEF	Marca: HP
	Modelo: PROLIANT DL 380 G7
	Procesador: INTEL XEON X5690
	Memoria: 36 GB
	Disco Duro: 1000 GB
	Sistema Operativo: WINDOWS SERVER 2008
	Soporte en IPV6: si
Servidor de Datos SISGEDO V.2.0	Marca: HP
	Modelo: PROLIANT DL 380 G7
	Procesador: INTEL XEON X5690
	Memoria: 36 GB
	Disco Duro: 1000 GB
	Sistema Operativo: WINDOWS SERVER 2008
	Soporte en IPV6: si
Servidor Firewall - Proxy	Marca: HP
	Modelo: PROLIANT DL 360 GEN 9
	Procesador: INTEL XEON E5-2450
	Memoria: 32 GB
	Disco Duro: 500 GB
	Sistema Operativo: PfSENSE
	Soporte en IPV6: si
Servidor WEB	Marca: HP
	Modelo: PROLIANT DL 360 GEN 9
	Procesador: INTEL XEON E5-2450
	Memoria: 32 GB
	Disco Duro: 1000 GB
	Sistema Operativo: Windows server 2012
	Soporte en IPV6: si

Fuente: Unidad de Tecnología de la Información del Gobierno Regional de Ancash

- Así también se identificó **los equipos tipo Switchs** distribuidos en las dependencias ubicadas en la Sede Central del GRA, los cuales ya tienen un tiempo prudente de uso y en algunos casos ya empezaron a presentar inconvenientes

para poder transmitir datos, generando incomodidades a los usuarios de las oficinas de la sede central del GRA.

Tabla N° 6. 2:
Cuadro de resumen de los equipos de comunicación del GRA

Modelo	Tipo de Capa	Soporte de IPv6
<i>at-9000/24</i>	capa 2	Si
<i>at-9424ts/xp</i>	capa 2	Si
<i>hp-2530 (j9773a)</i>	capa 2	Si
<i>AT-GS950</i>	capa 2	Si
<i>HPE-1920S(25fpb)</i>	capa 3	Si

Fuente: Plan Estratégico de Tecnología de la información del Gobierno Regional de Ancash

- Así también se identificó los equipos de cómputo distribuidos en las dependencias ubicadas en la sede central del GRA.

Gráfico N° 6. 4:
Cuadro de resumen de equipos informáticos del GRA

Nº	AREA	EQUIPOS DE CÓMPUTO SEGÚN PROCESADOR - SEDE CENTRAL											TOTAL X AREAS	
		P. DUAL	P. II	P.III	P.IV	XEON	CELERO N	CORE DUO	CORE 2 DUO	CORE QUAD	CORE I3	CORE I5		CORE I7
1	AGENCIA REGIONAL DE COOPERACIÓN TÉCNICA INTERNACIONAL	0	0	0	1	0	0	0	1	0	0	1	1	4
2	ALMACEN	0	0	0	0	0	0	0	0	1	0	0	2	3
3	ARCHIVO REGIONAL	0	0	0	1	0	0	0	0	2	2			5
4	CONSEJO REGIONAL	0	0	0	0	0	0	0	1	0	4	1	4	10
5	DIRECCION REGIONAL DE VIVIENDA, SANEAMIENTO Y CONSTRUCCIÓN	0	0	0	0	0	0	0	0	0	0	2	3	5
6	GERENCIA DE DESARROLLO ECONÓMICO	0	0	0	0	0	0	0	1	0	1	1	1	4
7	GERENCIA DE DESARROLLO ECONÓMICO - DIRECCIÓN REGIONAL DE COMERCIO EXTERIOR Y TURISMO	0	1	0	0	0	0	0	1	0	0	12	1	15
8	GERENCIA DE DESARROLLO ECONÓMICO - DIRECCIÓN REGIONAL DE ENERGIA Y MINAS	1	0	0	0	0	0	0	5	2	0	5	7	20
9	GERENCIA DE DESARROLLO SOCIAL	0	0	0	0	0	0	0	2	0	0	6	4	12
10	GERENCIA DE PLANEAMIENTO, PRESUPUESTO Y ACONDICIONAMIENTO TERRITORIAL	0	0	1	0	3	0	2	4	0	0	6	30	46
11	GERENCIA DE RECURSOS NATURALES	0	0	0	0	0	0	0	1	0	0	5	1	7
12	GERENCIA GENERAL REGIONAL	0	0	0	0	0	0	0	0	0	2	1	3	6
13	GERENCIA REGIONAL DE ADMINISTRACION	1	0	0	0	0	1	0	8	1	5	10	26	52
14	GERENCIA REGIONAL DE ASESORIA JURÍDICA	1	0	0	0	0	0	0	1	0	1	6	6	15
15	GERENCIA REGIONAL DE INFRAESTRUCTURA	0	0	2	2	0	0	0	0	7	0	10	30	51
16	GERENCIA REGIONAL DE INFRAESTRUCTURA - UNIDAD FORMULADORA	0	0	0	0	0	0	0	0	0	0	3	2	5
17	GOBERNACION REGIONAL	0	0	0	0	0	0	0	0	0	1	0	5	6
18	OF.SEGURIDAD	0	0	0	0	0	0	0	0	0	1	0	0	1
19	OFICINA DE CONTROL INTERNO	0	0	0	0	0	0	0	3	0	0	10	2	15
20	PROCURADURIA REGIONAL	0	0	0	0	0	0	1	1	0	2	3	3	10
21	SECRETARIA GENERAL	0	0	0	0	0	0	0	4	1	1	1	6	13
22	SUB GERENCIA DE DEFENSA CIVIL	0	0	0	0	0	0	0	0	1	1	7	4	13
23	SUB GERENCIA DE RECURSOS HUMANOS	1	0	0	0	0	0	0	1	0	0	2	4	8
24	VICEGOBERNACION REGIONAL	0	0	0	0	0	0	0	0	0	2	0	0	2
AL X PRO CE_S		4	1	3	4	3	1	3	34	15	21	94	145	328
Total Requerimientos														

Fuente: Plan Estratégico de Tecnología de la información del Gobierno Regional de Ancash

- Así también se identificó los equipos de impresión distribuidos en las dependencias ubicadas en la sede central del GRA.

Tabla N° 6. 3:
Cuadro de resumen de equipos de impresión del GRA

Equipo Multifuncional / Impresora	Soporta	
	IPv4	IPv6
Bizhub 184	No	No
Bizhub 211	Si	No
Bizhub 350	Si	No
Bizhub 363	Si	Si
Bizhub 367	Si	Si
Bizhub 421	Si	Si
Bizhub C300	Si	No
Color LaserJet CP4525	Si	Si
Designjet 500	Si	No
Designjet T610	Si	No
DFX 9000	No	No
Ecosis FS1035	Si	Si
FS-1020D	No	No
IR 2525	Si	Si
IR 2535	Si	Si
Laserjet 1010	No	No
Laserjet 1020	No	No
Laserjet 1320	No	No
Laserjet 1536dmf	Si	Si
Laserjet Color 5550dn	Si	No
Laserjet CP3525dn	Si	Si
Laserjet P1005	No	No
Laserjet P1006	No	No
Laserjet P1006w	No	No
Laserjet P1102w <i>(Inalámbrico)</i>	Si	No
Laserjet P1106	No	No
Laserjet P1160	No	No
Laserjet P1505	No	No
Laserjet P2015	No	No
Laserjet p2055dn	Si	No
Laserjet P3015	No	No
Laserjet P3015dn	Si	Si
Laserjet Pro 400	Si	No
Praser 3140	No	No

Fuente: Plan Estratégico de Tecnología de la información del Gobierno Regional de Ancash.

- ✓ Por lo tanto, **podemos concluir luego de haber revisado el inventario de equipos de cómputo, así como de los componentes de comunicaciones y redes, se verifica que todos los equipos son compatibles para poder realizar la transición con el protocolo ipv6, así que no se tendría inconvenientes durante la actividad de transición en cuanto al parque informático y de los componentes de comunicaciones y redes.**
- ✓ Así también podemos observar que se presente un inconveniente en la parte de equipos multifuncionales y/o de impresión puesto que, según el cuadro de compatibilidad, se visualiza que la mayor parte de equipos no están preparados para soportar el protocolo IPv6 e inclusive algunos equipos solo poseen la conexión USB para conectar directamente en las computadoras, de esta manera se **hará llegar la recomendación necesaria para la adquisición de equipos multifuncionales y/o de impresión con soporte a IPv6 a la Sub Gerencia de Abastecimiento y Servicios Generales de la Gerencia Regional de Administración del Gobierno Regional de Ancash, de manera que tengan en cuenta la recomendación para llevar a cabo las futuras compras de los equipos cuando sean requeridos por las distintas oficinas de las dependencias de la sede central del GRA.**
- ✓ Y finalmente también encontramos un punto crítico debido a la existencia de equipos de cómputo personales (**Laptop**) con algunas limitaciones en potencia de procesamiento, memoria interna y de almacenamiento; si bien estos equipos son compatibles con el protocolo IPv6, es necesario realizar la recomendación a la Sub Gerencia de Abastecimiento y Servicios Generales de la Gerencia Regional de Administración del Gobierno Regional de Ancash, sobre la adquisición de nuevos equipos de tipo Laptop para poder sustituirlos.

6.1.4.2. Diagnóstico de Servicios

➤ Servicio del Trámite de Gestión Documentario (SISGEDO v2.0)

- El Sistema de Trámite de Gestión Documentario – SISGEDO V2.0, es un servicio para el seguimiento del trámite documentario el cual se utiliza en la sede central del Gobierno Regional de Ancash, así como en las Ejecutoras dependientes del GRA.
- Este sistema fue desarrollado por el Gobierno Regional de Lambayeque y en convenio entre ambas entidades se llegó a facilitar al Gobierno Regional de Ancash llevándose a cabo su implementación.
- El SISGEDO al ser un sistema del cual su administración e implementación no depende directamente del Gobierno Regional de Ancash se tiene que realizar las coordinaciones con el Gobierno Regional de Lambayeque para ver si se llevara a cabo una posible actualización a la nueva versión y ver el aplicativo para que tenga soporte al IPv6, en caso la institución no de soporte con este protocolo se sugiere elaborar un acta de aceptación de riesgos por parte de la UTI.

➤ Servicio de Firewall - Internet (Intranet)

- El servicio de Firewall que se utiliza en la sede central del Gobierno Regional de Ancash es mediante el **software Pfsense V.2.3.4**, el mismo que se utiliza para las restricciones en el acceso a la navegación en las páginas de internet. El software tiene soporte en IPv6 así que es compatible para la transición.

➤ **Servicio de Internet (Movistar)**

- El servicio de Internet que es brindado a la sede central del Gobierno Regional de Ancash es a través de la Empresa de Telecomunicaciones Movistar el Cual, el cual viene brindado el servicio de internet a través de **dos circuitos digitales cada uno con SubNet /28 (16 host)** y un **equipo Fortinet** el cual es administrado directamente por Movistar.
- De esta forma también surge la siguiente recomendación: solicitar a Movistar que nos ceda la administración de dicho equipo para el servicio de internet, pero con direcciones IP con base en el protocolo IPv6.
- Caso contrario se debería hacer las coordinaciones para buscar un proveedor que nos permita tener el servicio para el protocolo IPv6.

6.1.4.3. Diagnóstico de Aplicativos

➤ **SIGA**

- Es un aplicativo informático que ayuda al ordenamiento y simplificación de los procesos administrativos. Tiene por objetivo, mejorar la gestión de las Finanzas Públicas, permitiendo la integración de los procesos de ejecución presupuestaria, financiera y contable (**página web del MEF**), y cada unidad ejecutora perteneciente al GRA tiene independencia sobre su uso.
- Es un aplicativo informático desarrollado por el MEF, por lo cual es necesario realizar la consulta, sobre si este aplicativo tendrá soporte para el IPv6 caso que no sea así se tiene que realizar un acta de aceptación de riesgo por parte de la UTI.

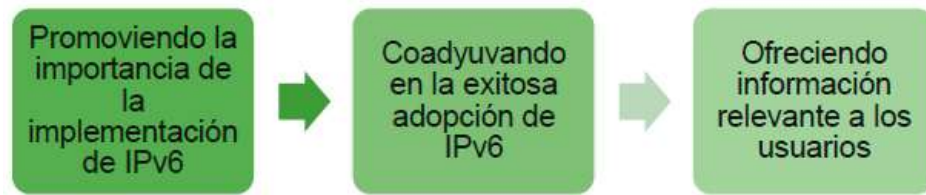
➤ **SIAF**

- EL SIAF es un aplicativo informático de Ejecución, este aplicativo ha sido diseñado como una herramienta muy ligada a la Gestión Financiera del Tesoro Público en su relación con las denominadas Unidades Ejecutoras (**página web del MEF**), y cada unidad ejecutora perteneciente al GRA tiene independencia sobre su uso.
- Al ser un aplicativo informático desarrollado por el MEF, por lo cual es necesario realizar la consulta, sobre si este aplicativo tendrá soporte para el IPv6 caso que no sea así se tiene que realizar un acta de aceptación de riesgo por parte de la UTI.

6.1.4.4. Diagnóstico de Políticas

- Se revisó la documentación correspondiente a las normativas, resoluciones ejecutivas, resoluciones gerenciales y no se encontró política, norma, u otro documento de gestión que indique algo sobre IPv6.
- Por lo cual se concluye realizar una reunión con los Gerentes de línea del Gobierno Regional de Ancash, para recomendar se genere normativas que indiquen aspectos como la adquisición de equipos con soporte del protocolo ipv6, contratación de servicios compatibles con el protocolo, y demás normativas que involucren la transición del protocolo y la correcta funcionalidad del mismo dentro de las oficinas de la sede central del GRA.

Gráfico N° 6. 5:
Flujograma de sensibilización al personal del GRA



Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.5. Implementación del protocolo IPv6

La presente fase de implementación debe cubrir las siguientes actividades:

- Capacitación al personal de la Unidad de Tecnología de la información – UTI de la Sub Gerencia de Desarrollo Institucional y Tecnología de la información, en la configuración para equipos y servicios sobre el protocolo IPV6.
- Habilitar el direccionamiento IPv6 para cada uno de los componentes de Hardware y Software de acuerdo al plan de diagnóstico del proceso de transición de IPv4 a IPv6.
- Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs creadas, con un número especial de usuarios que aprovechen la homogeneidad de la red, con servicios de filtrado, críticos a fin de evitar traumatismos en el normal funcionamiento de la red (**validar el impacto sobre aplicaciones cruciales en la institución como el SIGA, SIAF, etc.**).
- Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en **Doble Pila (dual stack)**; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.

- Aplicar el modelo de transición de IPv6 definido por el GRA, permitiendo la coexistencia de las aplicaciones, infraestructuras y servicios bajo los protocolos tanto de IPv4 como de IPv6, en modalidad de transición en doble pila.
- Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 bajo doble pila; esta técnica permite que tanto los servicios de IPv4 como los servicios de IPv6 deben estar funcionando de manera independiente pero coexistente dentro del Gobierno Regional de Ancash.
- Validar la funcionalidad en IPv6 de los siguientes servicios y aplicaciones de las Entidades sobre IPv6: **Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios tipo WEB y Servidores de Monitoreo.**
- Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad del GRA, por ejemplo: **Servidores AAA, Firewalls, NAC, y equipos perimetrales de conformidad, zonas desmilitarizadas, con los RFC de seguridad en IPv6;** al respecto, se recomienda revisar los RFC de seguridad en IPv6 asociados.
- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral, desde el interior de las redes LAN, hacia el exterior de las redes WAN a fin de garantizar que las entidades puedan generar tráfico de IPv6 nativo ante la comunidad de Internet.

6.1.5.1. Cronograma y Responsables

- A continuación, se muestra en un único cuadro adjunto el cronograma y los responsables por cada actividad que se desarrollara en la Sede Central del GRA (**Ver anexo 9.1**)

- De igual forma debe ser planificado para ser realizado en cada sede o unidad ejecutora del GRA, en coordinación directa con la Unidad de Tecnología de la Información del GRA.

Tabla N° 6. 4:
Cronograma de transición al protocolo IPv6

	ACTIVIDADES GENERALES	TIEMPO DE DURACIÓN	RESPONSABLE(S)
DESARROLLO DEL PLAN DE IMPLEMENTACIÓN	Coordinar capacitaciones en configuración y despliegue de IPv6 para el Personal de TI del Gobierno Regional de Ancash	03/09/2018 Al 28/09/2018	SGDITI - UTI
	Construcción del Plan de Diagnóstico	01/10/2018 Al 19/10/2018	Director UTI
	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.	22/10/2018 Al 12/11/2018	Ingeniero de Redes - UTI
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	13/11/2018 Al 03/12/2018	Ingeniero de Redes - UTI
	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.	04/12/2018 Al 26/12/2018	Ingeniero de Redes - UTI
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	27/12/2018 Al 11/01/2019	Director UTI Ingeniero de Redes - UTI
	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	14/01/2019 Al 18/01/2019	Director UTI realizara las coordinación con el proveedor del servicio de internet

Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.5.2. Entregables

- Informe del Plan detallado de implementación del nuevo protocolo.
- Documento que contendrá todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta fase, incluye las configuraciones a realizar sobre el canal (canales) de comunicaciones con acceso a internet.
- Informe de configuración de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

6.1.6. Pruebas

En esta fase se realizarán las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios del Gobierno Regional de Ancash.

Por lo tanto, dichas pruebas de funcionalidad del IPv6 esta fase deben cubrir las siguientes actividades:

- Realizar las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la Entidad en un ambiente que permita empezar a **generar tráfico de IPv6 de la entidad hacia Internet y viceversa.**
- Realizar las **pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral**, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones y presentar el Informe de las pruebas realizadas.
- Al momento de las pruebas de funcionalidad se debe **realizar el afinamiento de las configuraciones de hardware, software y servicios** dentro del Gobierno Regional de Ancash.

- **Elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones** bajo el nuevo esquema de funcionamiento de IPv6.

6.1.6.1. Cronograma y Responsables

- A continuación, se muestra en un único cuadro adjunto el cronograma y los responsables por cada actividad que se desarrollara en la Sede Central del GRA (Ver anexo 9.2)
- De igual forma debe ser planificado para ser realizado en cada sede o unidad ejecutora del GRA, en coordinación directa con la Unidad de Tecnología de la Información del GRA.

Tabla N° 6. 5:
Cronograma de Pruebas

	ACTIVIDADES	TIEMPO DE DURACIÓN	RESPONSABLE(S)
PRUEBAS DE FUNCIONALIDAD DE IPV6	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la sede central del GRA.	21/01/2019 Al 01/02/2019	Ingeniero de Redes - UTI
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI en la sede central del GRA.	04/02/2019 Al 15/02/2019	Ingeniero de Redes – UTI
	Afinamiento de las configuraciones de hardware, software y servicios en la sede central del GRA.	18/02/2019 Al 01/03/2019	Ingeniero de Redes - UTI

Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.6.2. Entregables

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

6.1.7. Capacitación y sensibilización

En esta fase se debe de cubrir las siguientes actividades:

- Reunión con los gerentes regionales, sub gerentes, jefes de área para la sensibilización sobre la adopción del nuevo protocolo en el Gobierno Regional de Ancash.
- Capacitación y sensibilización a los diferentes empleados del gobierno regional de Ancash, indicando las acciones que se van a tomar; previniendo de posibles fallas y cortes del servicio informáticos.
- Coordinación con las oficinas competentes la generación de documentos, directivas y/o normas que sustenten y apoyen la adopción del protocolo IPv6 en el Gobierno Regional de Ancash; tales como la compra de nuevos equipos con soporte en IPv6, contratación del servicio de internet y demás normativas que se crean conveniente.

6.1.7.1. Cronograma y Responsables

- A continuación, se muestra en un único cuadro adjunto el cronograma y los responsables por cada actividad que se desarrollara en la Sede Central del GRA (**Ver anexo 9.3**).
- De igual forma debe ser planificado para ser realizado en cada sede o unidad ejecutora del GRA, en coordinación

directa con la Unidad de Tecnología de la Información del GRA.

Tabla N° 6. 6:
Cronograma de capacitación y sensibilización

	ACTIVIDADES	TIEMPO DE DURACIÓN	RESPONSABLE(S)
CAPACITACION Y SENSIBILIZACION	Reunión con los Directores de línea y jefes de área para informar sobre el plan de transición de protocolos.	22/10/2018 Al 26/10/2018	Director UTI y Gerentes Regionales del GRA
	Coordinación Con los jefes de las diferentes áreas para la generación de normativas, resoluciones ejecutivas, resoluciones gerenciales que involucren al nuevo protocolo IPv6.	29/10/2018 Al 10/12/2018	Director UTI y Jefes de Oficinas del GRA
	Capacitación y sensibilización a los diferentes empleados del Gobierno Regional de Ancash.	04/03/2019 Al 08/03/2019	Equipo UTI
	Feedback con los diferentes empleados del Gobierno Regional de Ancash	11/03/2019 Al 15/03/2019	Equipo UTI

Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.7.2. Entregables

- Documentos tales como normativas, resoluciones ejecutivas, resoluciones gerenciales y ordenanzas que contemplen acciones que permitan hacer un buen uso respecto al protocolo IPv6 en la sede central del GRA.
- Resumen del Feedback realizado a los empleados del Gobierno Regional de Ancash.

6.1.8. Presupuesto

- Para la elaboración de este Plan (**entiéndase como proyecto**) se ha tenido en cuenta factores de dedicación de mano de obra especializada, el cual estará comprendido por un equipo de trabajo con una dedicación de tiempo completo y un salario fijo mensual durante la ejecución de las diferentes fases del proyecto.

- También se tendrá en cuenta suministro de materiales puesto que son necesarios para desarrollar cada una de las actividades propuestas en el presente documento, y que serán usados al momento de realizar las actividades de la transición, lo cual se sumara a los servicios profesionales de la mano de obra especialidad a contratar.

6.1.8.1. Equipo de Trabajo

➤ Jefe del Proyecto (Director Unidad de Tecnología de la Información)

- Administrar la estructura organizacional del proyecto.
- Establecer objetivos y pautas de desarrollo del proyecto.
- Manejar las técnicas operativas para el análisis y toma de decisiones necesarias en el cumplimiento de los objetivos del proyecto.
- Asignar los diferentes tipos de recursos para el desarrollo del proyecto.
- Manejar el riesgo del proyecto.

➤ Ingeniero de Redes (2 Especialistas)

- Transición de servidores a IPv6.
- Transición de la plataforma de virtualización.
- Realización de ventanas de mantenimientos necesarias para la transición.
- Dar soporte en sitio a los servidores.
- Elaboración de la documentación de las actividades de transición correspondientes a Datacenter.
- Transición de a IPv6 de la capa e Switching.
- Realización de ventanas de mantenimientos necesarias para la transición.
- Activación del protocolo IPv6 sobre la capa 3 de todas la Vlan.
- Elaboración de la documentación de las actividades de transición correspondientes a Routing and Switching

- Configuración de firewall de la entidad para la transición a IPv6.
 - Creación de políticas de seguridad para IPv6.
 - Pruebas de funcionamiento de las políticas de seguridad.
 - Elaboración de la documentación de las actividades de transición correspondientes a seguridad.
- **Equipo UTI (2 Colaboradores de la Unidad de Tecnología de la Información)**
- Colaboración en actividades de la transición de servidores a IPv6.
 - Colaboración en las pruebas de funcionamiento de las políticas de seguridad.
 - Colaboración en la elaboración de la documentación de las actividades de transición correspondientes a Routing and Switching
 - Colaboración en la elaboración de la documentación de las actividades de transición correspondientes a seguridad.
 - Colaboración en la elaboración de la documentación de las actividades de transición correspondientes a Datacenter.

6.1.8.2. Tiempo de Ejecución del Proyecto

- El desarrollo del presente proyecto (**implementar la transición al IPv6**) tendrá un **tiempo de 6 meses para la sede central del GRA**. Cada una de las sedes que pertenecen al GRA deben preparar y presentar su presupuesto bajo las premisas expuestas en el presente documento.
- Se muestra el siguiente cuadro con los costos asociados según lo planificado para la sede central GRA, donde el jefe de proyecto y el equipo UTI por ser personal del GRA no incurrirá en costo alguno:

Tabla N° 6. 7:
Cuadro de Costeo de la implementación

Personal / Otros	Cantidad	Salario Básico	Costo Total Empleado por Mes	Tiempo en Meses	Sub Total
Jefe de Proyecto	1	-	S/ 1,000	6	S/ 6,000
Ingeniero de Redes	2	S/ 5,000	S/ 6,500	4	S/ 52,000
Equipo UTI	2	-	S/ 1,000	6	S/ 6,000
Total Parcial					S/ 64,000
Gastos Administrativos	-	-	S/ 2,000	6	S/ 12,000
TOTAL					s/ 76,000

Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.9. Anexos

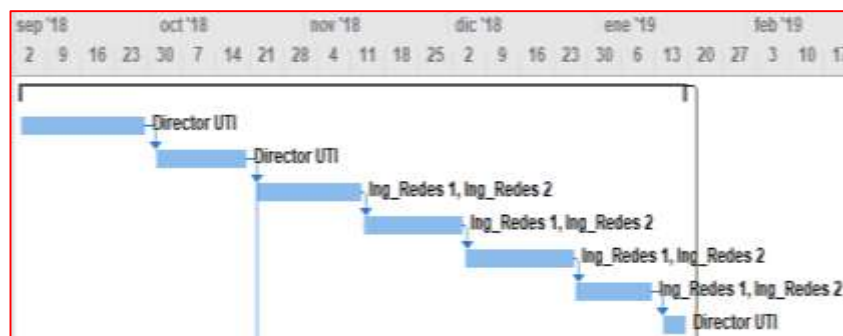
6.1.9.1. Cronograma Fase Implementación

Equipo que trabaja en la presente fase:

- **Director UTI** (Jefe de Proyecto).
- **Ingeniero de Redes 1** (Ing_Redex 1).
- **Ingeniero de Redes 2** (Ing_Redex 2).

Gráfico N° 6. 6:
Cronograma de la Fase de Implementación

Nombre de tarea	Comienzo	Fin
IMPLEMENTACIÓN	lun 3/09/18	vie 18/01/19
Capacitación al personal UTI-GRA	lun 3/09/18	vie 28/09/18
Construcción del Plan de Diagnostico	lun 1/10/18	vie 19/10/18
Habilitar direccionamiento IPv6	lun 22/10/18	lun 12/11/18
Configurar Servicios GRA	mar 13/11/18	lun 3/12/18
Configurar Protocolo IPv6	mar 4/12/18	mié 26/12/18
Activar políticas se seguridad IPv6	jue 27/12/18	vie 11/01/19
Coordinar con los proveedores de servicios	lun 14/01/19	vie 18/01/19



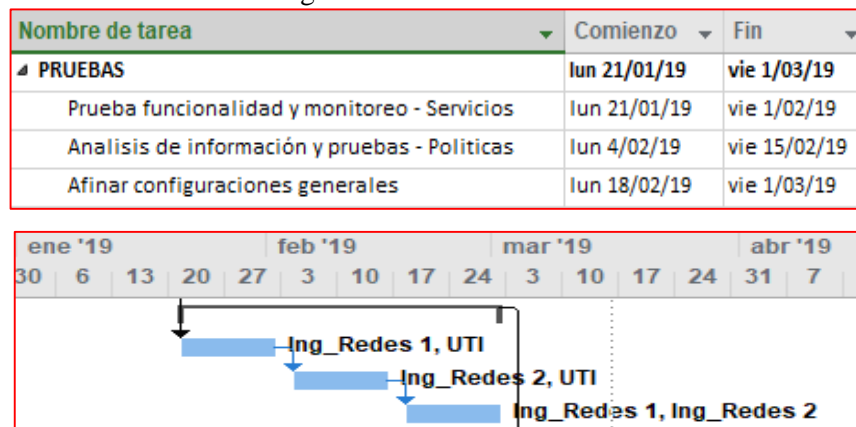
Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.9.2. Cronograma Fase Pruebas

Equipo que trabaja en la presente fase:

- **UTI** (Equipo UTI).
- **Ingeniero de Redes 1** (Ing_Redex 1).
- **Ingeniero de Redes 2** (Ing_Redex 2).

Gráfico N° 6. 7:
Cronograma de Fase de Pruebas



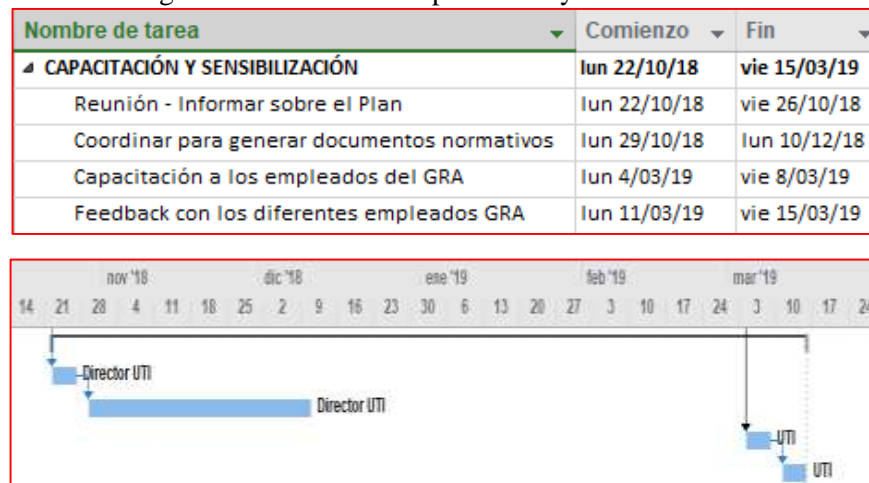
Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.9.3. Cronograma Fase Capacitación y Sensibilización

Equipo que trabaja en la presente fase:

- **Director UTI** (Jefe de Proyecto).
- **UTI** (Equipo UTI).

Gráfico N° 6. 8:
Cronograma de la Fase de Capacitación y Sensibilización



Fuente: Plan de transición al protocolo IPv6 – GRA.

6.1.9.4. Declaración en Demora de inicio de la Implementación del Plan

- El presente documento debe ser **aprobado por el titular del Gobierno Regional de Ancash** para poder dar inicio a las actividades planificadas. Esto se encuentra indicado en el **Artículo 3°.- Plan de Transición al Protocolo IPv6 del D.S. 081 – 2018 –PCM.**
- Por lo tanto, las actividades del Plan **serán iniciadas en la sede central al día siguiente de haberse aprobado el presente documento.** Así mismo cada una de las sedes debe iniciar con la planificación de sus actividades, las cuales deben ser coordinadas de manera directa con la Unidad de Tecnología de la Información del GRA.
- Así queda declarado que, si el presente documento no es aprobado hasta el 31 de agosto del presente año, lo planificado en los puntos 5, 6 y 7, deberán sufrir una actualización en cuanto a las fechas presentadas, llevando a tener una 2da versión sobre lo planificado, de esta manera recién será puesta en práctica cada una de las actividades.
- **El presupuesto propuesto en el punto 8, no debe sufrir variación alguna, pero debe estar disponible en cada una de las fases.**

CAPITULO VII: IMPLEMENTACION

7.1. Monitoreo y evaluación de la solución

7.1.1. Elementos del monitoreo y evaluación

Las acciones de monitoreo se realizarán más eficientemente cuando las actividades, recursos y activos relacionados se gestionen como un proceso, para ello se debe tener identificado la interacción entre los mismos. Además se deberá tener en cuenta las medidas preventivas a tomar y llevar un registro de los mismos. Para llevar un control de todo esto, se propone realizarlo a través del ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, =planificar-hacer-verificar-actuar).

Es una estrategia de mejora continua de la calidad en cuatro pasos, que tienen por función:

- a) Toma de datos y registro en las tablas respectivas
- b) Contrastación de los datos contra el nivel esperado de cumplimiento
- c) Decisión respecto de las acciones correctivas o de retroalimentación necesarias de acuerdo a la información obtenida
- d) Implementación de las acciones correctivas o de retroalimentación

7.1.2. Plan de monitoreo y evaluación

El Plan de monitoreo y evaluación debe necesariamente dar respuesta al menos a las siguientes interrogantes: ¿Cómo se va a recoger la información?, ¿Quién va a recogerla?, ¿Cuándo se va a obtener?, ¿Cómo se va a analizar la información recogida?, ¿Quién la va a analizar?, ¿Cuándo se va a hacer el análisis?, ¿Quién va a recibir los resultados?, ¿En qué formato se van a distribuir?

7.2. Bitácora y puesta a punto

Para el registro de las observaciones, ideas, datos, avances y obstáculos en el desarrollo de las actividades que se llevan a cabo durante el proyecto, se empleó

el siguiente cuadro para consolidar las condiciones bajo las cuales se desarrolló el proyecto.

Tabla N° 7. 1:
Bitácora de proyecto

Fecha	Etapas	Actividad	Observación
Del 05/02/2018 Al 28/03/2018	Evaluación preliminar	Presentación del proyecto al Gobierno Regional de Ancash.	Se observó el interés y la necesidad de contar con un sistema de gestión para la elaboración del plan de transición.
		Entrevista a Usuarios	Se contó con la participación del personal involucrado para el proyecto.
		Recolección de datos generales	Se recopiló información acerca de los lineamientos a los cuales se tiene que ceñir el desarrollo del plan de transición.
Del 29/03/2018 Al 15/04/2018	Análisis	Análisis de los procesos identificados en la entrevista	Se nos brindó información de los requerimientos básicos para el desarrollo del plan de transición.
		Análisis de los resultados de la entrevista.	Se registró y analizó los resultados de la entrevista.
		Obtención de Requerimientos	Se identificó los requerimientos globales.
		Análisis de gestión de riesgos	Se identifican problemas que puede ocurrir durante el desarrollo del proyecto y tener un plan de contingencia.
		Análisis de Requerimientos	Se hizo el análisis de requerimientos.
Del 16/04/2018 Al 28/06/2018	Diseño	BASE LEGAL	Se determinó las bases legales a tener en cuenta para la elaboración del plan
		ALCANCE	Se determinó los lineamientos que debe de tener el alcance del plan de transición.
		DIAGNOSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA	Se elaboró pautas y cuadros referenciales para el levantamiento de la información.

		IMPLEMENTACIÓN DEL PROTOCOLO IPV6	Se elaboró pautas y secuencias para la implementación de del protocolo IPV6.
		PRUEBAS	Se elaboró las pruebas necesarias para validar la correcta transición al protocolo IPV6.
		CAPACITACIÓN Y SENSIBILIZACIÓN	Se elaboró un cronograma y los aspectos para realizar la capacitación y sensibilización del plan desarrollado.
		PRESUPUESTO	Se elaboró las pautas para la construcción del presupuesto aproximado que será necesario para realizar la transición al protocolo IPV6.
		ANEXOS	Se elaboró las pautas sobre los anexos que se tienen que añadir al plan.
Del 29/06/2018 Al 09/07/2018	Implementación	Capacitación y difusión	Se capacito al personal del área de UTI del Gobierno regional de Ancash, acerca del sistema de gestión para la elaboración del plan de transición de protocolos
		Generación del Plan de transición al protocolo IPV6 para el Gobierno Regional de Ancash	Los errores detectados fueron reportados para su corrección.

Fuente: Elaboración Propia

CAPITULO VIII: RESULTADOS

8.1. Resultados de acuerdo a los objetivos planteados

8.1.1. Evaluar el decreto supremo N° 081-2017-PCM

En cumplimiento con el objetivo específico 1, se analizó el decreto supremo N° 081-2017-PCM, del cual se identificó la estructura básica a tener en cuenta para la elaboración del plan de transición de protocolos.

8.1.2. Identificar las acciones para hacer la implementación de Ipv6 en base a lineamientos, recomendaciones y buenas prácticas a nivel de seguridad.

En cumplimiento con el objetivo 4, se identificó los procesos claves para la implementación del plan de transición de protocolo, siendo el pilar fundamental el levantamiento de información en los equipos de cómputo (hardware y software), servicios prestados en la institución, aplicativos informáticos y demás que se vean afectados por la transición al protocolo IPv6, puesto que las siguientes fases varían según la información identificada en el levantamiento de información; continuando con la fase de transición, en el cual se identifican los pasos a seguir para la implementación del plan de transición y finalmente las pruebas necesarias a realizar para corregir cualquier inconveniente y así llevar una transición al protocolo IPv6 transparente.

8.1.3. Identificar las pruebas que se deben realizar después de la implementación del protocolo IPv6.

En cumplimiento al objetivo 4, las pruebas que se generan en este sistema de gestión para la transición de protocolos son mecanismos muy prácticos de implementar, los pasos a seguir en esta parte de la metodología son creados sin llevar ningún parámetro descrito o referencia. Este desarrollo se genera a partir de conocimientos previos.

8.1.4. Validar y medir el nivel de satisfacción del personal encargado de elaborar el plan de transición del protocolo IPv4 a IPv6.

En cumplimiento con el objetivo 5, se realizó la validación del sistema de gestión con los encargados de su desarrollo e implementación (personal que labora en el área de Unidad de Tecnologías de la información del Gobierno Regional de Ancash), identificando los puntos a tener en cuenta para la inclusión de estos en el presente proyecto.

8.2. Resultados cuantitativos

8.2.1. Diagnostico e interpretación de resultados

Para la evaluación del sistema de gestión para la elaboración del plan de transición se realizó una encuesta donde se pudiera medir el grado de satisfacción de la misma, teniendo en cuenta aspectos de calidad, aplicabilidad, normatividad y toda la parte relacionada con la infraestructura de la entidad.

De acuerdo a lo anterior se tomó una muestra representativa con personas del Gobierno Regional de Ancash involucradas con el desarrollo del plan de transición de IPv4 a IPv6, ellos son el jefe de la unidad de Tecnologías de la Información, el coordinador del área infraestructura y el encargado de la seguridad informática, adicional a esto cuentan con el conocimiento y la experiencia para realizar el proceso de evaluación.

Para la tabulación de datos se utilizó un cuadro para cada pregunta y una gráfica de la misma, para su cuantificación se manejó la siguiente formula:

$$\% = \frac{X \cdot 100}{N}$$

%=Es el porcentaje que se encuentra en el total de estudio

X=Cantidad de veces que se repite el dato

100=Constante de la muestra

N=Total de datos

A continuación, se presentados los resultados obtenidos en el proceso de evaluación de algunas de las preguntas realizadas.

✓ **Pregunta 1**

¿Considera usted que el sistema de gestión está alineado al establecido en el Decreto Supremo N° 081-2017-PCM?

Tabla N° 8. 1:
Tabulación de la pregunta 1

Respuesta	Cantidad	Porcentaje
Se superaron mis expectativas	1	33%
Se cumplieron mis expectativas	2	67%
Se cumplieron parcialmente mis expectativas	0	0%
No se cumplieron mis expectativas	0	0%
TOTAL	3	100%

Fuente: Elaboración propia

Gráfico N° 8. 1:
Resultados de la pregunta 1



Fuente: Elaboración propia

Interpretación

En la gráfica se evidencia que el 67% de las personas encuestadas respondieron que se superaron las expectativas, el 33% manifiesta que se cumplieron con las expectativas.

✓ **Pregunta 2**

¿Considera usted que las acciones establecidas en el sistema de gestión son un instrumento de ayuda para la implementación de IPv6 en su institución?

Tabla N° 8. 2:
Tabulación de la pregunta 2

Respuesta	Cantidad	Porcentaje
Se superaron mis expectativas	2	67%
Se cumplieron mis expectativas	1	33%
Se cumplieron parcialmente mis expectativas	0	0%
No se cumplieron mis expectativas	0	0%
TOTAL	3	100%

Fuente: Elaboración propia

Gráfico N° 8. 2:
Resultados de la pregunta 2



Fuente: Elaboración propia

Interpretación

En el gráfico anterior se evidencia que el 67% de las personas encuestadas informan que superan las expectativas y el 33% restante se cumplen con las expectativas.

✓ **Pregunta 3**

¿Las pruebas indicadas en el sistema de gestión son apropiadas para la validación de la implementación del protocolo IPv6?

Tabla N° 8. 3:
Tabulación de la pregunta 3

Respuesta	Cantidad	Porcentaje
Se superaron mis expectativas	2	67%
Se cumplieron mis expectativas	1	33%
Se cumplieron parcialmente mis expectativas	0	0%
No se cumplieron mis expectativas	0	0%
TOTAL	3	100%

Fuente: Elaboración propia

Gráfico N° 8. 3:
Resultados de la pregunta 3



Fuente: Elaboración propia

Interpretación

En el anterior gráfico se evidencia que el 67% de las personas encuestadas superaron las expectativas y el 33% cumple con las expectativas de acuerdo con la relación de la guía con la entidad.

✓ **Pregunta 4**

¿El sistema de gestión para la transición del protocolo IPv4 a IPv6 sirve como aporte para el fortalecimiento estratégico en la elaboración del plan para la transición a IPv6?

Tabla N° 8. 4:
Tabulación de la pregunta 4

Respuesta	Cantidad	Porcentaje
Se superaron mis expectativas	0	0%
Se cumplieron mis expectativas	2	67%
Se cumplieron parcialmente mis expectativas	1	33%
No se cumplieron mis expectativas	0	0%
TOTAL	3	100%

Fuente: Elaboración propia

Gráfico N° 8. 4:
Resultados de la pregunta 4



Fuente: Elaboración propia

Interpretación

En el gráfico se observa que el 67% de las personas encuestadas manifiestan que el documento sirve para el fortalecimiento estratégico y el 33% afirman que la guía cumple de manera parcial.

CAPITULO IX:

DISCUSION DE RESULTADOS

9.1. En base a los antecedentes mencionados en la investigación se presentan las siguientes discusiones:

9.1.1. Análisis comparativo con los antecedentes internacionales

- Tesis de Grado: Diseño, desarrollo e implementación del plan de transición del protocolo IPv4 a IPv6 de la entidad FENIX (Bogotá 2016); con respecto a esta tesis se coincide en los siguientes puntos:
 - En ambas investigaciones se determina que el método más efectivo y con menor impacto en el cambio de equipos informáticos para la transición al protocolo IPv6 es el de Dual Stack o doble pila; el cual permite la convivencia de los protocolos IPv4 e IPv6 para que la transición sea de manera adecuada y progresiva hacia una red totalmente en IPv6.
- Tesis de Grado: Propuesta de diseño para la transición del protocolo de internet versión 4 (IPv4) al protocolo de internet versión 6 (IPv6) en la empresa MARKET MIX S.A.S; con respecto a esta tesis se coincide en los siguientes puntos:
 - En ambas investigaciones se determina que un punto importante para el desarrollo del plan de transición es el levantamiento de información para planear y preparar la red informática con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de desempeñar las especificaciones del nuevo protocolo, sin descartar completamente las aplicaciones admitidas en IPv4.
 - Además en ambas investigaciones se concluye que la etapa de transición debe de ser sectorizada por áreas.

- Tesis de Grado: Transición de Protocolos IPv4 a IPv6, para una empresa del estado, con aplicación en una ciudad intermedia (Pereira, 2016); con respecto a esta tesis se coincide en los siguientes puntos:
 - En ambas investigaciones se determina que la transición entre el protocolo IPv4 a IPv6, puede llevarse a cabo de manera efectiva, si se sigue el marco de un modelo o sistema de gestión, como el enunciado en este proyecto, de una manera amigable, en donde incluso se buscará una transición gradual, y asentando las bases para una transición definitiva.
 - En ambas investigaciones se concluye, que El protocolo IPv6 nace, en respuesta a las necesidades subyacentes del contexto actual, en donde la expansión del internet es un proceso que crece de manera acelerada y que da surgimiento a nuevas tecnologías, aplicaciones y servicios, como por ejemplo el internet de las cosas.

9.1.2. Análisis comparativo con el antecedente nacional

- Tesis de maestría: Modelo de referencia de transición de IPv4 a IPv6 para el sector gobierno de Perú); con respecto a esta tesis se coincide en los siguientes puntos:
 - En ambas investigaciones se determina que 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 dónde empezar (Modelo de Referencia o sistema de gestión) y capacitación de su recurso humano.
 - En ambas tesis se concluye que el sistema de gestión y los documentos técnicos elaborados en ambas tesis permitirá a las instituciones públicas establecer un punto de partida para iniciar sus planes de transición hacia el nuevo protocolo IPv6; con la

inclusión en la presente tesis de los lineamientos incluidos en el decreto supremo N°081-2017-PCM.

9.2. Sobre el impacto del sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Áncash

- **Análisis:** ¿Considera usted que el sistema de gestión está alineado al establecido en el decreto supremo N° 081-2017-PCM?

Se demuestra que la mayoría de personas encuestadas supera las expectativas con un 67 % que esperaban que el sistema de gestión este alineado en lo establecido al decreto supremo N° 081-2017-PCM.

- **Análisis:** ¿Considera usted que las acciones establecidas en el sistema de gestión son un instrumento de ayuda para la implementación de IPv6 en su institución?

Se demuestra que la mayoría de personas encuestadas 67% indican que superaron sus expectativas en las acciones definidas en el sistema de gestión para la transición del protocolo IPv4 a IPv6.

- **Análisis:** ¿Las pruebas indicadas en el sistema de gestión son apropiadas para la validación de la implementación del protocolo IPv6?

Se demuestra que la mayoría de personas encuestadas 67% indican que las pruebas que se describen en el presente documento son útiles y fáciles de aplicar.

- **Análisis:** ¿El sistema de gestión para la transición del protocolo IPv4 a IPv6 sirve como aporte para el fortalecimiento estratégico en la elaboración del plan para la transición a IPv6?

Teniendo en cuenta que la muestra es mínima se puede evidenciar que el sistema de gestión cumple con su objetivo que es la orientación en el diseño del plan de transición a IPv6, ya que se tuvo en cuenta las necesidades de la entidad, los comentarios y sugerencias del personal de la unidad de tecnologías de la información del Gobierno Regional de Áncash.

CONCLUSIONES

- Después de Analizar el decreto supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”, identificándose la estructura que tiene que contener el plan, los cuales se tiene en cuenta para la elaboración del sistema de gestión para la transición de protocolos
- Los requerimientos técnicos y acciones requeridas para implementar en 2 escenarios como en redes que pasan de IPv4 a IPv6 o en aquellas que se generan desde su comienzo con IPv6, tienen distintas técnicas según la red a la cual se piensa aplicar la transición; por una parte, se tiene la red WAN, que utiliza técnicas de tunelización y aplicaciones las cuales pretenden hacer el cambio de protocolo sobre servicios que son exclusivamente de IPv4. En una red LAN se distribuye las operaciones necesarias en el Core, la distribución y el acceso, con el fin de dar la convivencia de los dos protocolos, teniendo en cuenta que los sistemas operativos y las aplicaciones necesitan de la configuración necesaria para que reciban las direcciones en las dos pilas.
- Después de verificar la posibilidad de aplicar Dual Stack en la solución, se pudo determinar que en muchos casos se hace necesario la integración de otras métodos, es así como el método de Dual Stack se debe aplicar pero a nivel de la LAN, sin embargo en la red en el borde, en la comunicación con el ISP para tener un encaminamiento de la información seguro y eficaz entre IPv4 e IPv6 se debe en algunos casos contar con los otro método, y tunelización estos se podrían aplicar en la red Interna, sin embargo el método más recomendado es el de Dual Stack por su facilidad de implementación, lo que lo ha llevado a ser el más económico por la masificación.
- Las secuencias de acciones para realizar la implementación de IPv6 se definió de manera clara y precisa, indicando los aspectos fundamentales a

tener en cuenta en cada una de las etapas, puesto que cada etapa es importante para el normal desarrollo de la etapa siguiente.

- Las pruebas que se generan en este documento son mecanismos muy prácticos de implementar, los pasos a seguir en este documento son creados sin llevar ningún parámetro descrito o referencia. Este desarrollo se genera a partir de conocimientos previos.
- Se realizó la validación del sistema de gestión para la transición al protocolo IPv6, recopilando las necesidades en la elaboración del plan de transición y realizar las correcciones correspondientes en el sistema de gestión.
- Este documento es en general para cualquier persona u organización que quiera informarse sobre una metodología para hacer una transición, según los requerimientos y el decreto supremo N°081-2017-PCM emitido por la Presidencia del Consejo de Ministros. Es una acción social que ayuda a mitigar el impacto de la poca adopción de la transición de IPv4 a IPv6; influyendo directamente el desarrollo del país y la evolución de sus redes; y mientras que se hagan estos procesos antes de que sea mandatorio el país podrá estar a la par con las tecnologías convergentes que se están implementando en el resto del mundo.

RECOMENDACIONES

- 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 la presente tesis.
- Elaborar un gestor de monitoreo que permita realizar el control y seguimiento del proceso de implementación de IPv6 a nivel de las Instituciones Públicas.
- Incluir en la estructura curricular de los estudios 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.
- Esta tesis es en general para cualquier persona u organización que quiera informarse sobre una metodología para hacer una transición, según los requerimientos del decreto supremo N°081-2017 PCM. Es una acción social que ayuda a mitigar el impacto de la poca adopción de la transición de IPv4 a IPv6; influyendo directamente el desarrollo del país y la evolución de sus redes.

REFERENCIAS BIBLIOGRÁFICAS

- Hernandez, R, Fernández, C, & Baptista, P. (2010). *Metodología de la Investigación. 5º ed.* Madrid: McGraw – HILL/ INTERAMERICANA EDITORES S.A.
- Landy Rivera, D.X. (2013). *Propuesta de un plan de implementación para la migración a ipv6 en la red de la universidad politécnica salestina sede-cuenca* (Tesis de grado). Ecuador: Cuenca.
- Melo Moreno, L.J. (2015). *Propuesta de diseño para la transición del protocolo de internet versión 4 (ipv4) al protocolo de internet versión 6 (ipv6) en la empresa market mix s.a.s* (Tesis de grado). Colombia: Bogotá.
- Ramírez Pulido, D.F, Guzmán Pantoja, J, & Beltrán Díaz, J.A. (2015). *Diseño de la transición del protocolo ipv4 hacia ipv6 en la agencia colombiana para la reintegración-acr con base en consideraciones de seguridad en implementación de ipv6* (Trabajo de grado). Colombia: Bogotá.
- Stallings, W. (2.004). *Comunicaciones y redes de computadores.* España: Pearson Educación.
- Suarez, M.M. & Rovina, M.A. (2016). *Diseño, desarrollo e implementación del plan de transición del protocolo ipv4 a ipv6 de la entidad fénix* (Tesis de Grado). Colombia: Bogotá.
- Tomasi, W. (2.003). *Sistemas de comunicaciones electrónicas.* México: Pearson Educación.
- Tomy Baltazar, M.A. (2017). *Modelo de referencia de transición de ipv4 a ipv6 para el sector gobierno de Perú* (Tesis de grado). Perú: Lima.

Direcciones electrónicas

COBIT. (s.f.). ISACA. Obtenido el 10 de febrero del 2018, desde:

<http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>

IPv6Mx. (s.f.). Obtenido el 9 de febrero del 2018, desde:

<http://www.ipv6.mx/index.php/informacion/rfcs>

Gobierno Regional de Ancash. Obtenido el 14 de Febrero del 2018, desde:

<http://www.regionancash.gob.pe/>

ANEXOS

Anexo N° 1: Matriz de consistencia	105
Anexo N° 2: Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”	106
Anexo N° 3: Guía de entrevista	111
Anexo N° 4: Encuesta	112
Anexo N° 5: Manual de configuración de una red para la transición hacia el protocolo IPv6	113

Anexo N° 1:
Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES Y DIMENSIONES	METODOLOGIA
<p>PROBLEMA GENERAL ¿Cómo influye el tener un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash?</p> <p>PROBLEMA ESPECÍFICO 1 ¿El decreto supremo N° 081-2017-PCM, contempla requerimientos para la elaboración del plan de transición?</p> <p>PROBLEMA ESPECÍFICO 2 ¿Cuáles son las acciones para hacer la implementación de IPv6 en base a lineamientos, recomendaciones y buenas prácticas a nivel de seguridad?</p> <p>PROBLEMA ESPECÍFICO 3 ¿Cómo determinar cuáles son las pruebas que se deben de realizar después de la implementación del protocolo IPv6?</p> <p>PROBLEMA ESPECÍFICO 4 ¿La guía cumple con las expectativas de los encargados del desarrollo del plan de transición de protocolos?</p>	<p>OBJETIVO GENERAL Proponer un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash.</p> <p>OBJETIVO ESPECÍFICO 1 Evaluar el decreto supremo N° 081-2017-PCM, para identificar requerimientos para la elaboración del plan de transición al protocolo IPv6.</p> <p>OBJETIVO ESPECÍFICO 2 Identificar las acciones a seguir para hacer la implementación de IPv6 en base a lineamientos, recomendaciones y buenas prácticas a nivel de seguridad.</p> <p>OBJETIVO ESPECÍFICO 3 Identificar las pruebas que se deben realizar después de la implementación del protocolo IPv6.</p> <p>OBJETIVO ESPECÍFICO 5 Validar y medir el nivel de satisfacción del personal encargado de elaborar el plan de transición del protocolo IPv4 a IPv6.</p>	<p>HIPOTESIS GENERAL La elaboración de un Sistema de gestión para la transición de IPv4 a IPv6 en el Gobierno Regional de Ancash.</p> <p>HIPÓTESIS ESPECIFICA 1 * el decreto supremo N° 081-2017-PCM, nos brinda lineamientos para la elaboración del plan de transición de protocolos.</p> <p>HIPÓTESIS ESPECIFICA 2 *las acciones de implementación de IPv6 se basan en lineamientos, recomendaciones y buenas practicas a nivel de seguridad.</p> <p>HIPOTESIS ESPECIFICA 3 *las pruebas designadas para la validación del protocolo cumplen con la mejora continua a la transición de protocolos</p> <p>HIPOTESIS ESPECIFICA 4 La guía cumple con las expectativas de los encargados de TI ara la elaboración del plan de transición de protocolos</p>	<p>VARIABLE INDEPENDIENTE X= Sistema de gestión para la transición de IPv4 a IPv6</p> <p>DIMENSIONES</p> <ul style="list-style-type: none"> Desarrollo de etapas para la transición de protocolos <p>VARIABLE DEPENDIENTE Y= Plan de transición del protocolo IPv4 al protocolo IPv6.</p> <p>DIMENSIONES</p> <ul style="list-style-type: none"> Adecuación de los equipos para el soporte del nuevo protocolo. 	<p>TIPO DE INVESTIGACIÓN</p> <p>De acuerdo a la orientación: Investigación aplicada, por qué parte de un marco teórico nacional e internacional que es la guía fundamental de éste trabajo para formular teorías en base a nuestra realidad local. Estas fuentes serán ejes principales para lograr elaborar un modelo de referencia.</p> <p>DE ACUERDO A LA TÉCNICA DE CONTRASTACIÓN Investigación descriptiva, tomada de la realidad del país y de la localidad con respecto a entidades que realizaron planes de transición de protocolos de comunicación.</p> <p>DISEÑO DE INVESTIGACIÓN No experimental, transaccional o transversal.</p> <p>PROBLACION Y MUESTRA</p> <p>POBLACIÓN DE ESTUDIO *La población de estudio está conformado por los responsables de TI de las diferentes unidades ejecutoras dependientes del Gobierno Regional de Ancash a nivel de pliego.</p> <p>MUESTRA DE ESTUDIO *Personal del Área de TI del Gobierno Regional de Ancash (Sede Central) – 3 personas – Jefe de UTI, personal encargado de la seguridad de la información y coordinador de la infraestructura de la red de datos</p>

Fuente: Elaboración propia

Anexo N° 2:
Decreto Supremo N° 081-2017-PCM “Decreto Supremo que Aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública”



ES COPIA FIEL DEL ORIGINAL

Cesar Rangel Silva

CESAR RANGEL SILVA
FEDATARIO
Presidencia del Consejo de Ministros

Decreto Supremo

DECRETO SUPREMO QUE APRUEBA LA FORMULACIÓN DE UN PLAN DE TRANSICIÓN AL PROTOCOLO IPV6 EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

N° 081-2017-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, la Ley N° 27558 - Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; por lo que deviene en necesario mejorar la gestión pública a través del uso de nuevas tecnologías que permitan brindar mejores servicios a los ciudadanos;

Que, el Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, crea el Sistema Nacional de Informática, el cual tiene por finalidad asegurar que sus actividades se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión; teniendo como competencia la instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del Estado, entre otros;

Que, de acuerdo a lo establecido en el artículo 47 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, la Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnica normativa a nivel nacional, responsable de formular y promover políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico; asimismo, es el órgano rector del Sistema Nacional de Informática y brinda asistencia técnica en la implementación de los procesos de innovación tecnológica para la modernización del Estado;

Que, la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Infraestructura, el mismo que busca contar con una red informática que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, bases de datos, entre otros;

Que, el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0, aprobada mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo 1, "Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y



rurales a la Sociedad de la Información y del Conocimiento", disponiendo a su vez, en su Estrategia 7, "Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el Protocolo de Internet v6 (IPv6)";

Que, el Protocolo IP (Internet Protocol) es utilizado para el intercambio de información entre redes o dispositivos conectados a la Internet, existiendo a la fecha dos versiones de este protocolo, la versión 4 (IPv4) y la versión 6 (IPv6);

Que, una dirección IP identifica a un dispositivo dentro de una red IP, siendo su uso imprescindible para la comunicación entre dispositivos, acceso a servicios a través de Internet u otros, y conforme a lo manifestado por el Registro de Direcciones de Internet para América Latina y el Caribe- (LACNIC por sus siglas en inglés) sobre el agotamiento de la cantidad de direcciones de IPv4, emerge el uso de las direcciones basadas en el protocolo IPv6, como mecanismo para asegurar la provisión y acceso a servicios digitales basados en IPv6;

Que, para que las computadoras, servidores de datos, laptops, tabletas, teléfonos móviles multimedia (smartphones) y otros dispositivos se conecten a través del Internet, requieren de una dirección IP – Internet Protocol, provista por un Proveedor de Servicio de Internet;

Que, mediante la Resolución N° 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (UIT), detallada en el documento "Actas Finales de la Conferencia de Plenipotenciarios, Guadalajara, 2010", se invita a los Estados Miembros a elaborar políticas nacionales para fomentar la actualización tecnológica de los sistemas, a fin de asegurar que los servicios públicos ofrecidos a través del Protocolo de Internet (IP), la infraestructura de comunicaciones y las aplicaciones correspondientes, sean compatibles con IPv6;

Que, en la mencionada Resolución, también se invita a los Estados Miembros, a garantizar que, en las acciones que lleven a cabo en relación con los equipos de comunicaciones e informáticos, se tomen las medidas necesarias para que los equipos cuenten con capacidad de IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6;

Que, el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC por sus siglas en inglés) es la organización responsable de la asignación y administración de los recursos de numeración de Internet conocidos como IPv4 e IPv6, entre otros, en la región;

Que, LACNIC señala que el agotamiento de las direcciones IPv4 en América Latina y el Caribe se encuentra en su tercera y última fase, debiendo los gobiernos priorizar el despliegue del protocolo IPv6, quienes deben asegurar que las acciones que se lleven a cabo garanticen que los nuevos recursos TIC cuenten con capacidad IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6, ello conforme con lo dispuesto en la Resolución N° 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones;

Que, se hace necesario que el Perú propicie un entorno que garantice la adopción del protocolo IPv6 por parte de las entidades de la Administración Pública ante el inminente agotamiento de las direcciones IPv4, de tal manera que se asegure la comunicación y accesibilidad a dispositivos o servicios que utilizan el sistema de direccionamiento IPv6;

De conformidad con lo establecido en la Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado; la Ley N° 29158 - Ley Orgánica del Poder Ejecutivo; el Decreto Legislativo N° 604; y, el Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros;

ES COPIA FIEL DEL ORIGINAL


CESAR RANGEL SILVA
FEDATARIO
Presidencia del Consejo de Ministros





ES COPIA FIEL DEL ORIGINAL

CESAR RANGEL SILVA
FEDATARIO
Presidencia del Consejo de Ministros

Decreto Supremo

DECRETA:

Artículo 1°.- Objeto

Disponer la formulación de un Plan de Transición al Protocolo IPv6, a implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública.

Artículo 2°.- Alcance

El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el [Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General](#), aprobado con [Decreto Supremo N° 006-2017-JUS](#), con excepción de las personas jurídicas señaladas en el [numeral 8 del citado artículo](#).

Artículo 3°.- Plan de Transición al Protocolo IPv6

Las entidades de la Administración Pública señaladas en el alcance del artículo 2 del presente Decreto Supremo deben elaborar un Plan de Transición al Protocolo IPv6, el cual será aprobado por el Titular de cada entidad.

Artículo 4°.- Contenido mínimo del Plan de Transición al Protocolo IPv6

El Plan de Transición al Protocolo IPv6, debe contener como mínimo, lo siguiente:

1. Título
2. Introducción
3. Base Legal
4. Objetivos del Plan de Transición
5. Alcance del Plan de Transición
6. Diagnóstico de la Infraestructura Tecnológica, el cual debe incluir un cronograma con actividades, plazos y responsables para elaborar un inventario de software, hardware, infraestructura tecnológica, aplicaciones y servicios que no soportan IPv6 y evaluación de riesgo; para su posterior análisis.
7. Implementación del protocolo IPv6, el cual debe incluir un cronograma con actividades (configuración de servicios, configuración del protocolo IPv6, formulación de política de seguridad, entre otros), plazos, responsables y entregables para la implementación del IPv6 en la entidad. Debe ser coordinado con el Oficial de Seguridad de la Información.
8. Realización de Pruebas, el cual debe incluir un cronograma con actividades (pruebas de funcionalidad, calidad del servicio, compatibilidad de los equipos y monitoreo del IPv6, pruebas frente a las políticas de seguridad, afinamiento de las configuraciones realizadas, entre otros), plazos, responsables y entregables para el desarrollo de pruebas en la entidad.
9. Capacitación y sensibilización, el cual debe incluir un cronograma con actividades, plazos, y responsables para la capacitación a especialistas en Tecnologías de Información (TI) y sensibilización a funcionarios en el protocolo IPv6.



ES COPIA FIEL DEL ORIGINAL

- 10. Presupuesto estimado
- 11. Anexos


CESAR RANGEL SILVA
FEDATARIO
Presidencia del Consejo de Ministros

Artículo 5°.- Plazo

Las entidades de la Administración Pública cuentan con un plazo máximo de un (01) año, contado a partir de la vigencia del presente Decreto Supremo, para la elaboración y aprobación de sus respectivos Planes de Transición al que se refiere el Artículo 3° del presente Decreto Supremo, el mismo que una vez aprobado deberá ser comunicado a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros.

El referido Plan debe implementarse progresivamente en un plazo máximo de cuatro (04) años luego de su aprobación.

En el caso de los Gobiernos Locales, los plazos son los siguientes:

- a. Gobiernos Locales de ciudades principales tipo A (según Anexo A):
 - Plan de Transición: dieciocho (18) meses.
 - Implementación progresiva del Plan de Transición: cinco (05) años.
- b. Gobiernos Locales de ciudades principales tipo B (según Anexo B)
 - Plan de Transición: dos (02) años.
 - Implementación progresiva del Plan de Transición: cinco (05) años.

Artículo 6°.- Adquisición de Hardware y Software en las entidades públicas

Las entidades de la Administración Pública que adquieran hardware o software que reciba, transmita o procese información por medio del protocolo IP, a partir de la fecha de la entrada en vigencia del presente Decreto Supremo, deben asegurar que estos soporten el Protocolo IPv6 con compatibilidad o soporte al protocolo IPv4.

Cualquier excepción a la adopción del Protocolo IPv6 requerirá la autorización expresa y justificada del responsable del área informática o quien haga sus veces en la entidad.

Artículo 7°.- Asistencia Técnica

La Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, brindará asistencia técnica y capacitaciones a las entidades de la Administración Pública que lo requieran, y monitorea el efectivo cumplimiento del presente Decreto Supremo.

Artículo 8°.- Publicación

El presente Decreto Supremo es publicado en el Diario Oficial "El Peruano", en el Portal del Estado Peruano (www.pesu.gob.pe), y en Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe), el mismo día de su publicación.

Artículo 9°.- Vigencia

El presente Decreto Supremo entra en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano".

Artículo 10°.- Refrendo

El presente Decreto Supremo es refrendado por el Presidente del Consejo de Ministros.





ES COPIA FIEL DEL ORIGINAL

Cesar Rangel Silva
CESAR RANGEL SILVA
FEDATARIO
Presidencia del Consejo de Ministros

Decreto Supremo

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Estrategia para la implementación del protocolo IPv6 del Estado Peruano

La Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros en coordinación con los actores pertinentes desarrollará las acciones necesarias (lineamientos, guías, proyectos, capacitaciones, otros) para la adecuada implementación del protocolo IPv6.

Segunda.- Implementación del protocolo IPv6 en los Gobiernos Locales

Los Gobiernos Locales fuera del alcance del presente Decreto Supremo, que en función de sus capacidades técnicas, infraestructura tecnológica, acceso al servicio de Internet podrán elaborar su Plan de Transición al Protocolo IPv6, en base a lo estipulado en el presente Decreto Supremo, y atendiendo a la Estrategia para la implementación del protocolo IPv6 en el Estado Peruano, indicada en la Primera Disposición Complementaria Final.

DISPOSICIÓN COMPLEMENTARIA TRANSITORIA

Única.- Procesos de adquisición en trámite

El presente Decreto Supremo no será aplicable a los procesos de adquisición que hayan sido iniciados con anterioridad a la entrada en vigencia de esta norma.

Dado en la Casa de Gobierno, en Lima, a los ^{ocho} días del mes de agosto del año dos mil dieciséis.



Pedro Pablo Kuczynski Godard
PEDRO PABLO KUCZYNSKI GODARD
Presidente de la República

Fernando Zavala Lombardi
FERNANDO ZAVALA LOMBARDI
Presidente del Consejo de Ministros

Anexo N° 3:
Guía de entrevista
GUIA DE ENTREVISTA

Buenos días estimados personal de UTI, la siguiente entrevista busca establecer un marco referencial del Proyecto de Sistema de Gestión para la transición al protocolo IPv6 que se viene ejecutando en estas instalaciones para realizar un análisis de los procesos que lo conforman de manera que se pueda contribuir con un aporte a este proyecto:

1. **Pregunta 1:** ¿Considera importante la etapa de modernización del Estado peruano? ¿Por qué?
2. **Pregunta 2:** ¿Cuál es su opinión acerca del decreto supremo N°081-2017-PCM?
3. **Pregunta 3:** ¿Cuáles cree que sean indicadores para la elaboración del plan de transición al protocolo IPv6?
4. **Pregunta 4:** ¿Qué pruebas usted consideraría importantes para validar la transición de protocolos?
5. **Pregunta 5:** ¿Considera Ud. que existe un buen ambiente laboral en la institución y más aún en el Proyecto?
6. **Pregunta 6:** ¿Considera importante la capacitación constante al personal con respecto al proyecto de transición al protocolo IPv6?

Gracias por su tiempo.

Anexo N° 4:
Encuesta
ENCUESTA

Estimado personal de la Unidad de Tecnologías de la Información del Gobierno Regional de Ancash, la siguiente encuesta fue elaborada con el fin de validar el sistema de gestión para la elaboración del plan de transición de protocolos, le pedimos veracidad en sus respuestas ya que ayudara a establecer correctamente las estrategias a tener en cuenta para la mejora de procesos en el proyecto, Gracias.

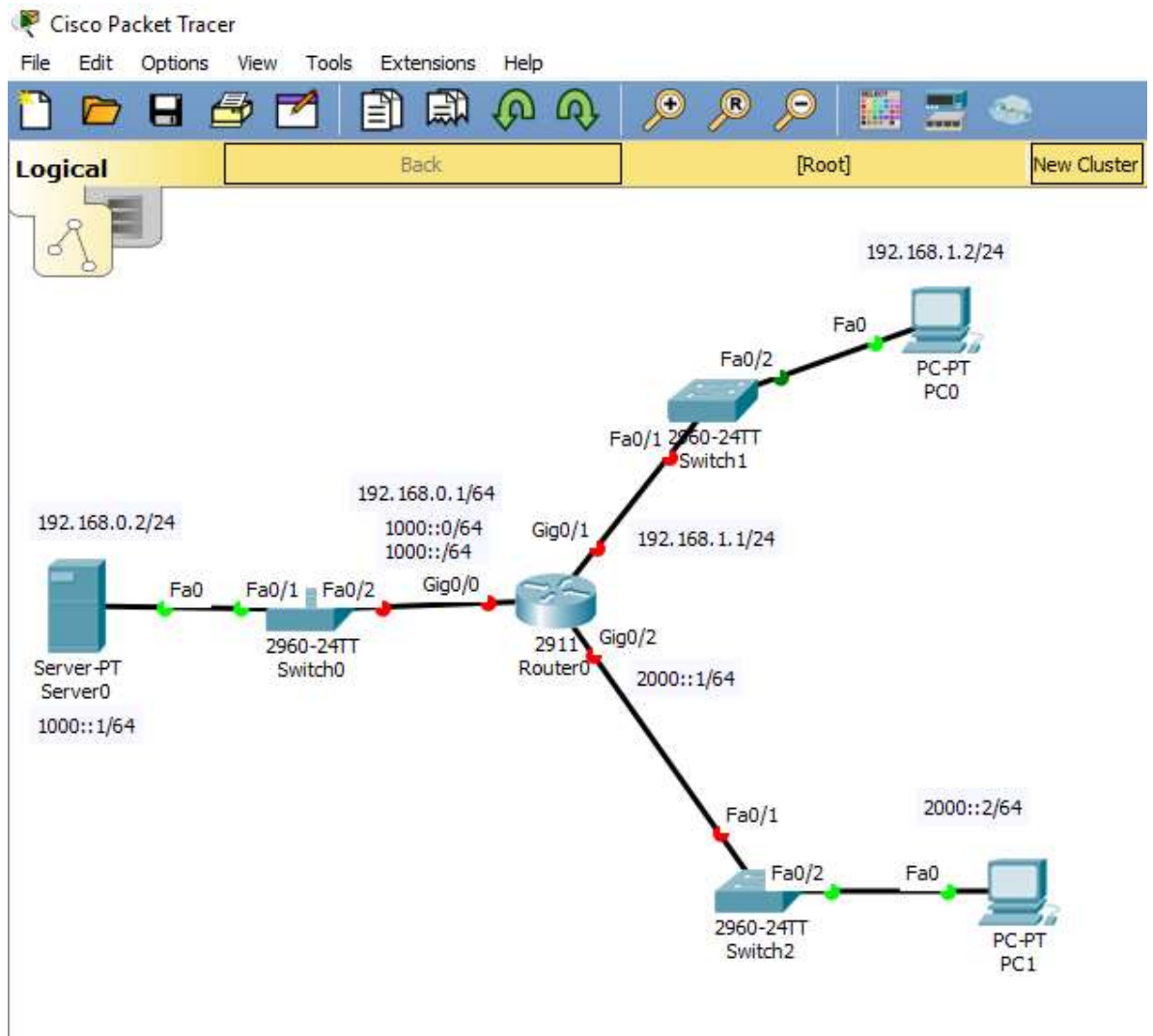
- 1. Pregunta 1: ¿Considera usted que el sistema de gestión está alineado al establecido en el decreto supremo N° 081-2017-PCM?**
 - a) Se superaron mis expectativas
 - b) Se cumplieron mis expectativas
 - c) Se cumplieron parcialmente mis expectativas
 - d) No se cumplieron mis expectativas
- 2. Pregunta 2: ¿Considera usted que las acciones establecidas en el sistema de gestión son un instrumento de ayuda para la implementación de IPv6 en su institución?**
 - a) Se superaron mis expectativas
 - b) Se cumplieron mis expectativas
 - c) Se cumplieron parcialmente mis expectativas
 - d) No se cumplieron mis expectativas
- 3. Pregunta 3: ¿Las pruebas indicadas en el sistema de gestión son apropiadas para la validación de la implementación del protocolo IPv6?**
 - a) Se superaron mis expectativas
 - b) Se cumplieron mis expectativas
 - c) Se cumplieron parcialmente mis expectativas
 - d) No se cumplieron mis expectativas
- 4. Pregunta 4: ¿El sistema de gestión para la transición del protocolo IPv4 a IPv6 sirve como aporte para el fortalecimiento estratégico en la elaboración del plan para la transición a IPv6?**
 - a) Se superaron mis expectativas
 - b) Se cumplieron mis expectativas
 - c) Se cumplieron parcialmente mis expectativas
 - d) No se cumplieron mis expectativas

Anexo N° 5:

Manual de configuración de una red para la transición hacia el protocolo IPv6

Manual de configuración de una red para la transición hacia el protocolo ipv6 utilizando el método Dualstack

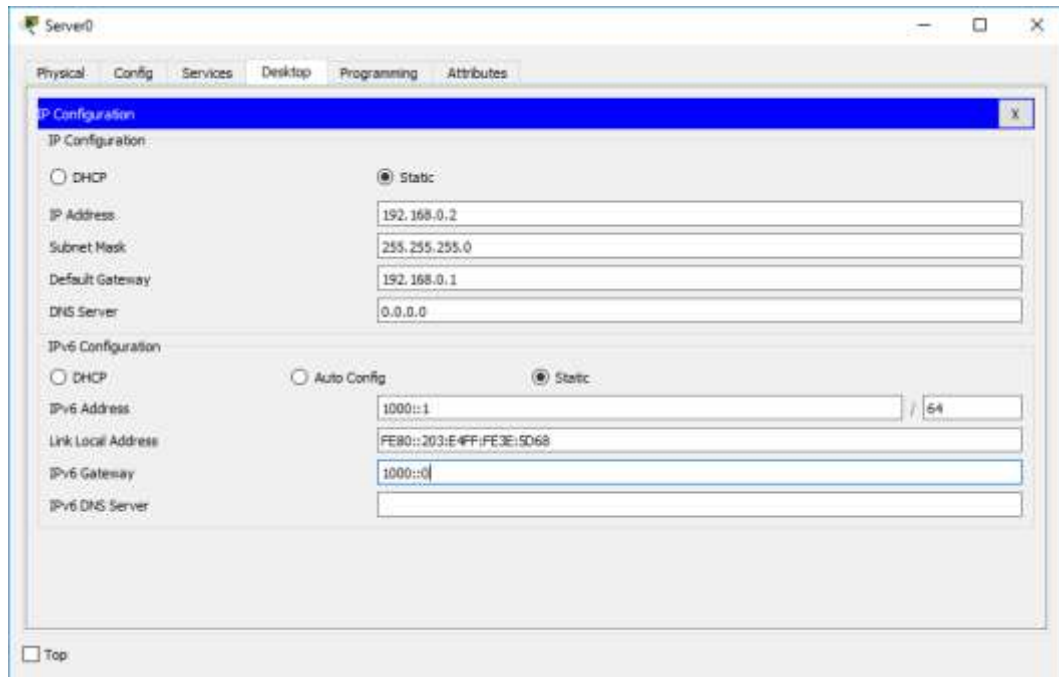
Para la simulación de esta red se utilizó el software cisco packet tracer 7.1.1



El ejemplo muestra una red común que se encuentra en cualquier institución pública, ha esta red se le aplica la técnica de transición dual Stack; en el cual se aprecia un servidor web que trabaja en ambos protocolos, una pc que trabaja bajo el protocolo IPv6 y otra pc que trabaja bajo el protocolo IPv4, 3 switch de capa 2 que son indiferentes al tipo de la versión del protocolo con el cual se genera el tráfico y finalmente un router quien va a ser la parte principal de esta red pues va a ser el encargado de la comunicación de los servidores con los equipos en sus respectivos protocolos.

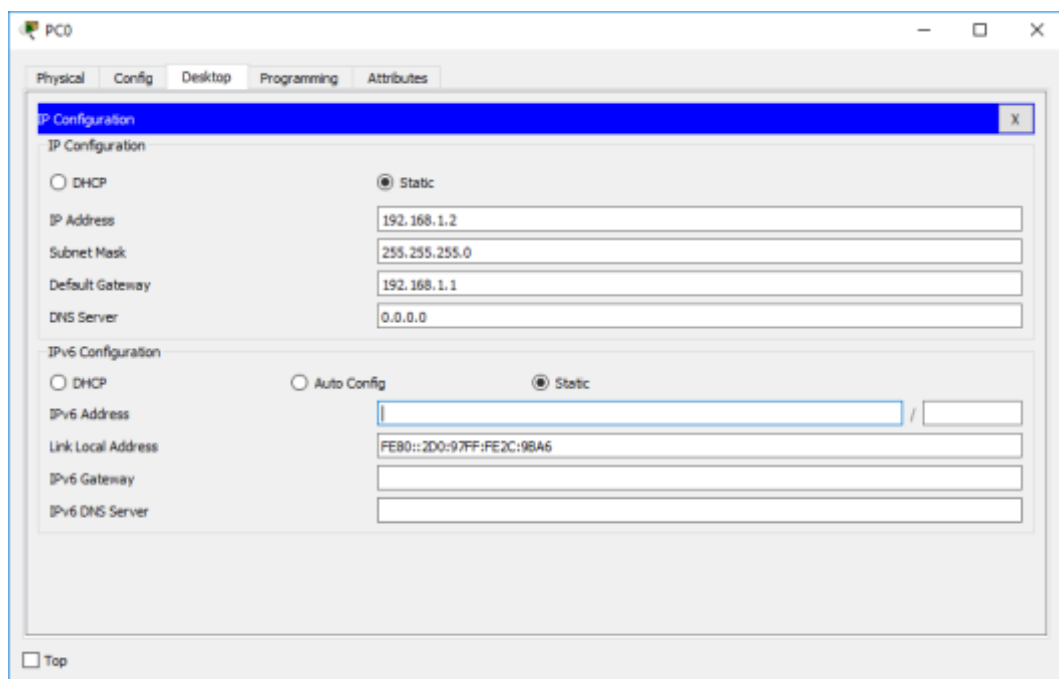
En la red podemos encontrar los siguientes componentes con sus configuraciones:

- Servidor(Server0) trabajando con las 2 versiones del protocolo ip (ipv4:192.168.0.2/24 e ipv6-1000::1/64)



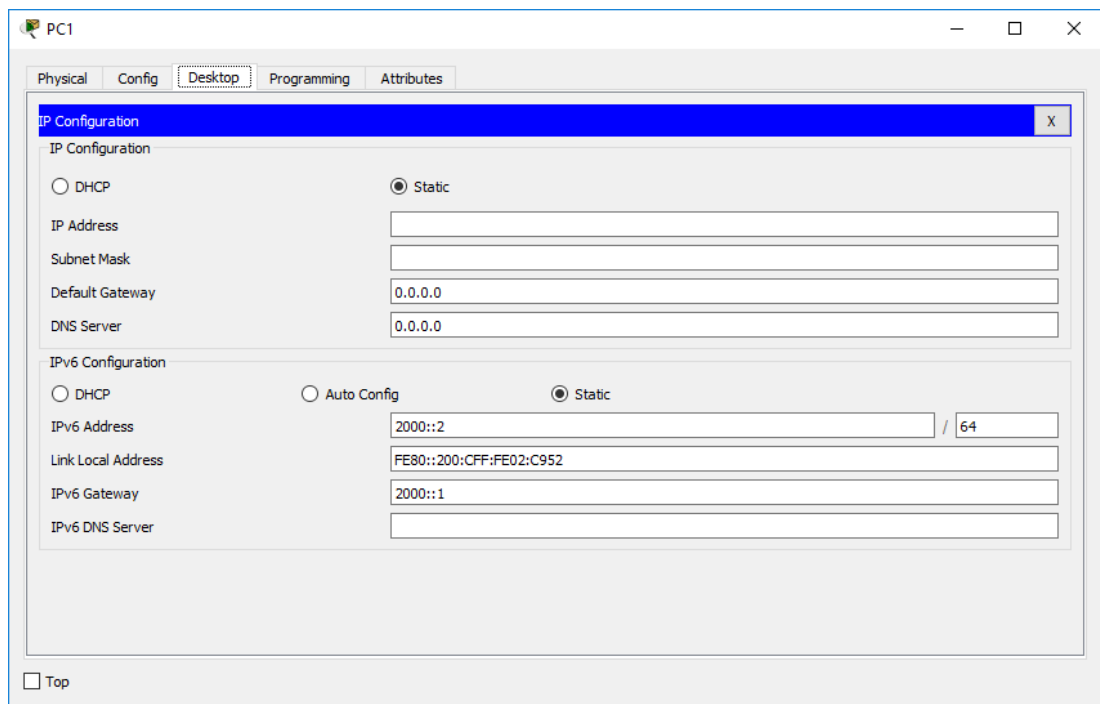
Configuración de ipv4 e ipv6 en el servidor

- Pc0 con la versión del protocolo ipv4 (192.168.1.2/24)



Configuración del protocolo ipv4 en la pc0

- Pc1 con la versión del protocolo ipv6 (2000::2/64)



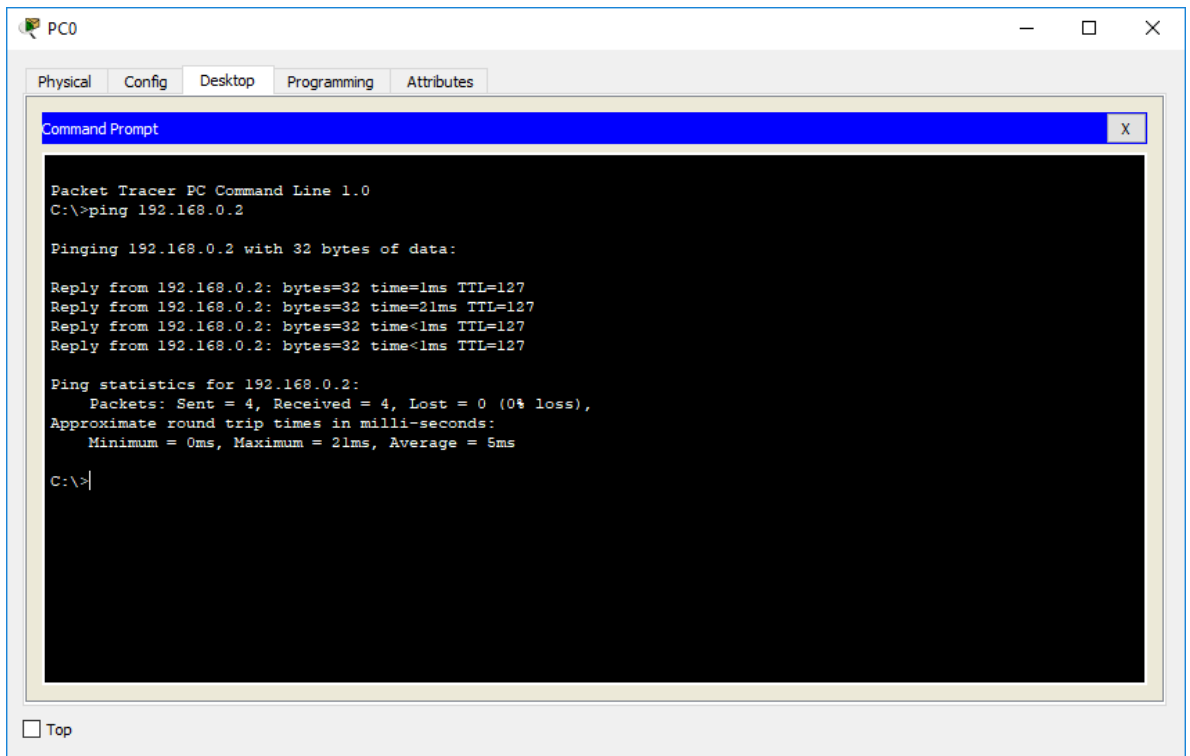
Configuración de ipv6 en pc1

- 3 switch (swicth0, swicth1, swicth2) el cual al ser de capa 2 le es indiferente el tipo de la versión de protocolo ip el cual le cause trafico
- Un router0 el cual posee 3 interfaces:
 - La interfaz gig0/0: por el cual se conecta a la red del servidor y trabajara con ambos protocolos de ip, su configuración de ipv4 e ipv6 es: 192.168.0.1/64 e 1000::/64
 - La interfaz gig0/1: por el cual se conecta la red con ipv4 su ip vendrá a ser 192.168.1.1/24
 - La interfaz gig0/2: por el cual se conecta la red con ipv6 su ip vendrá a ser 2000::1/64

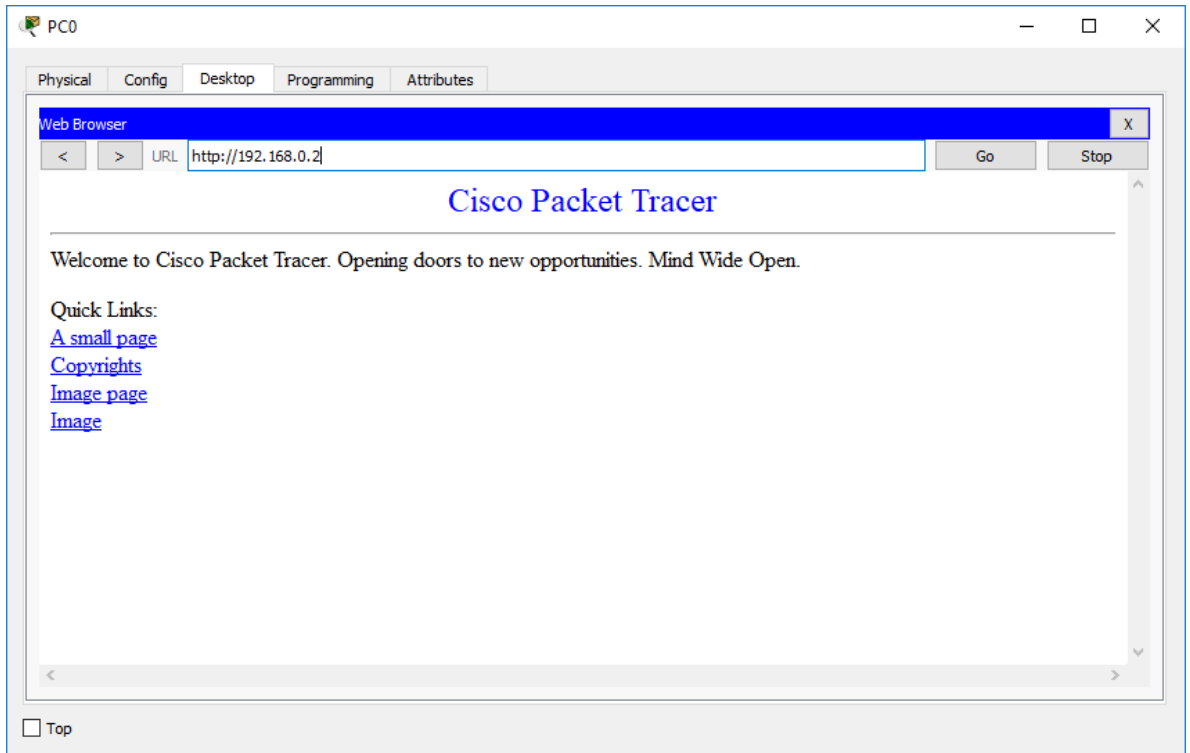
A continuación, se muestra los comandos para la configuración del router con las ips y en los puertos ya mencionados.


```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gi 0/0
Router(config-if)#no shut
Router(config-if)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#ipv6 add 1000::0/64
Router(config-if)#exit
Router(config)#int gi 0/1
Router(config-if)#no shut
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#int gi 0/2
Router(config-if)#no shut
Router(config-if)#ipv6 add 2000::1/64
Router(config-if)#exit
Router(config)#ipv6 un
Router(config)#ipv6 unicast-routing
Router(config)#exit
Router#wr
Router#wr men
```

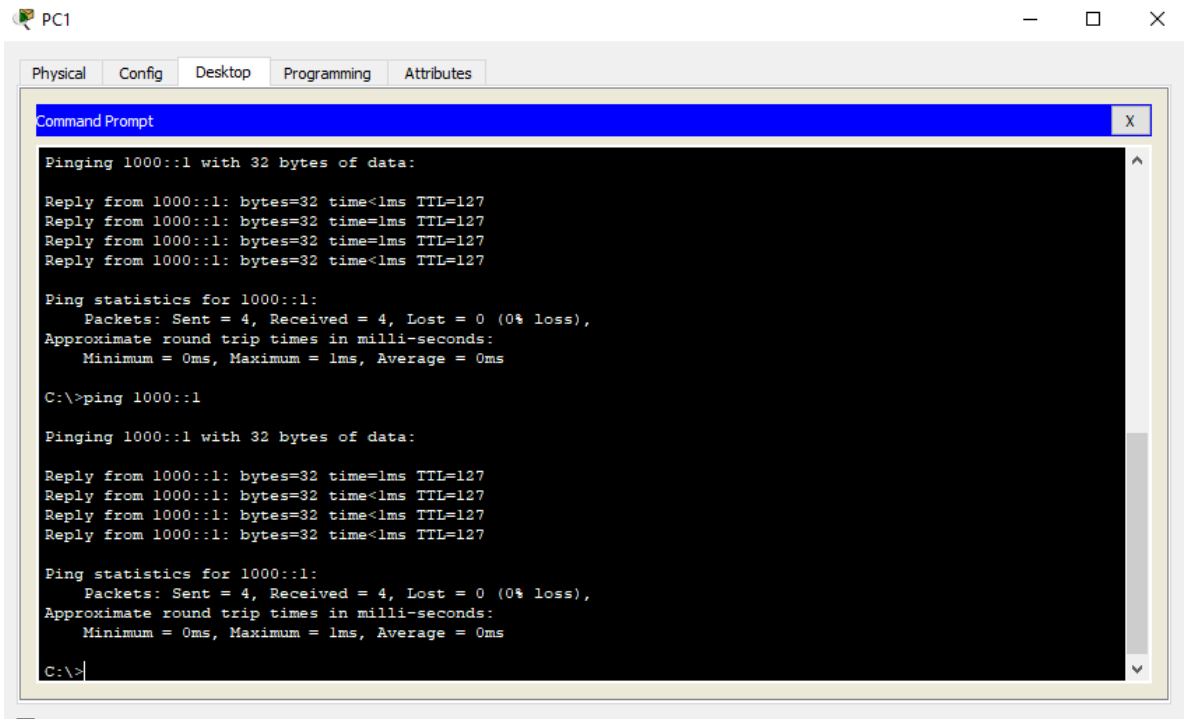
Para realizarse las pruebas correspondientes vemos la conectividad desde la pc1 al servidor con el comando ping



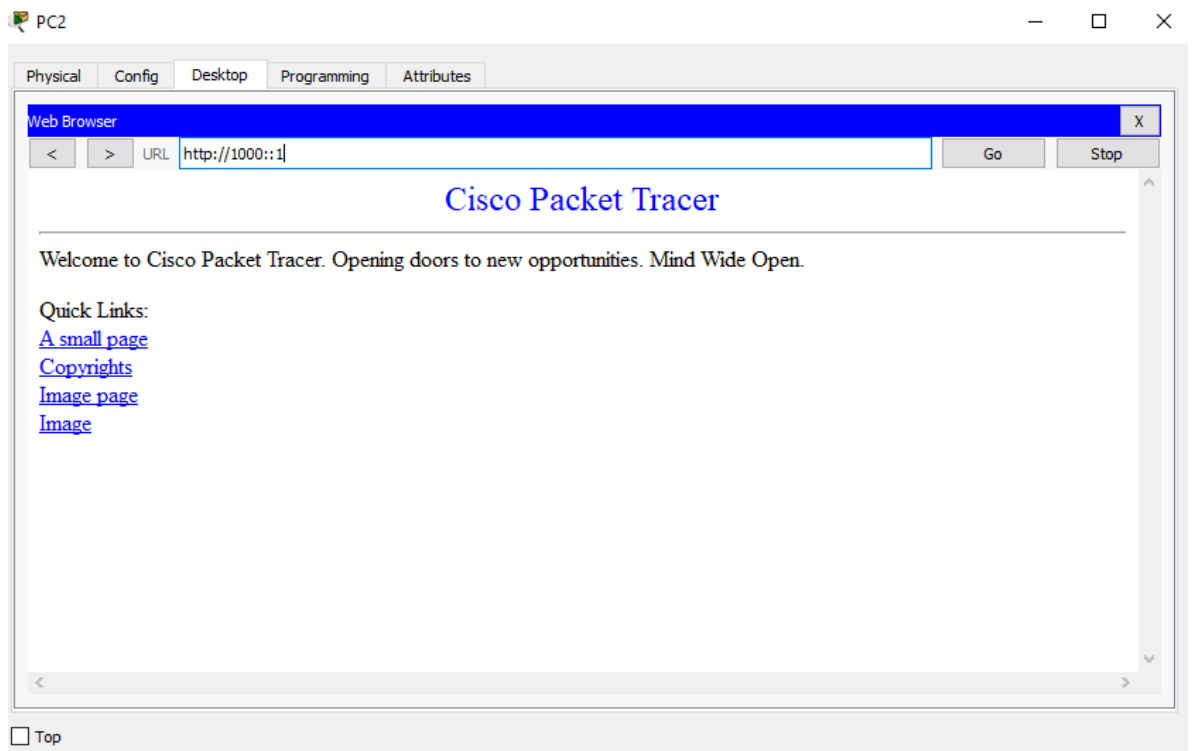
Y también vemos que puede acceder a la página de prueba del servidor



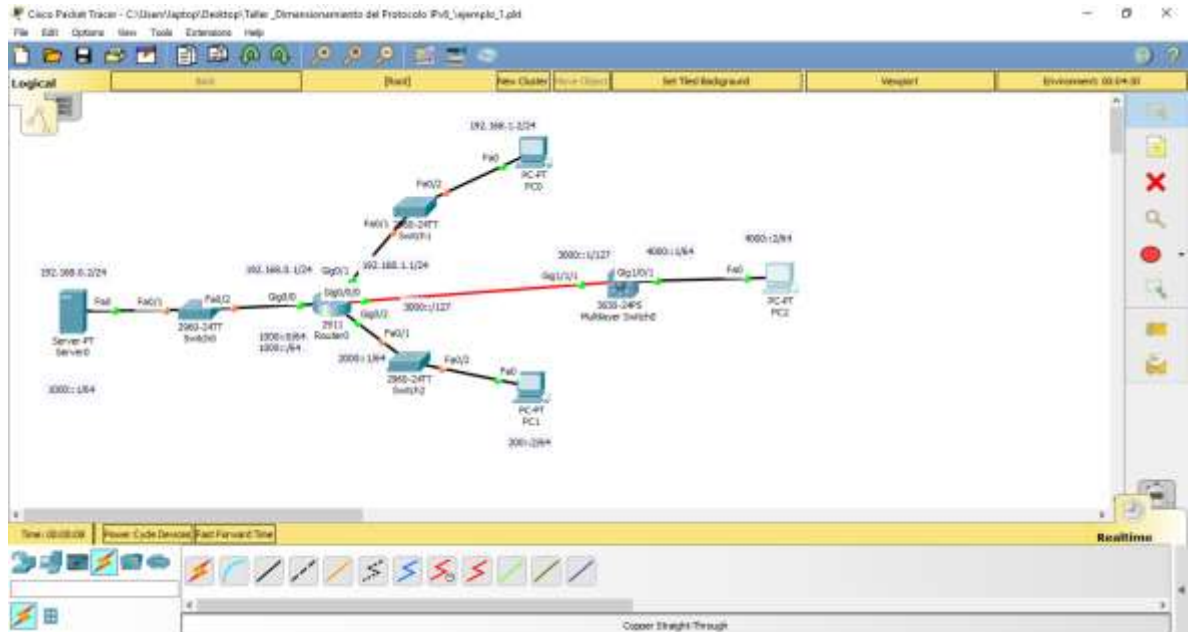
A continuación, vemos la conectividad desde la PC1 hacia el servidor



Y también vemos que puede acceder a la página de prueba del servidor



Ahora ampliaremos la red, añadiendo un switch tipo capa 3; realizaremos las configuraciones necesarias para su adaptación a la red



Las configuraciones que añadiremos son las siguientes:

- Para la PC2: con ipv6 4000::2/64

PC2

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

DHCP Static

IP Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address 4000::2 / 64

Link Local Address FE80::201:64FF:FE4B:9306

IPv6 Gateway 4000::1

IPv6 DNS Server

Top

- Para el router se le agrega un puerto de fibra óptica y se realiza las siguientes configuraciones al puerto gig0/0/0

```
Router>en
Router#conf t
Router(config)#int gi 0/0/0
Router(config-if)#no shut
Router(config-if)#ipv6 add 3000::/127
Router(config-if)#exit
Router(config)#ipv6 route ::/0 3000::1
Router#wr
Router#wr mem
```

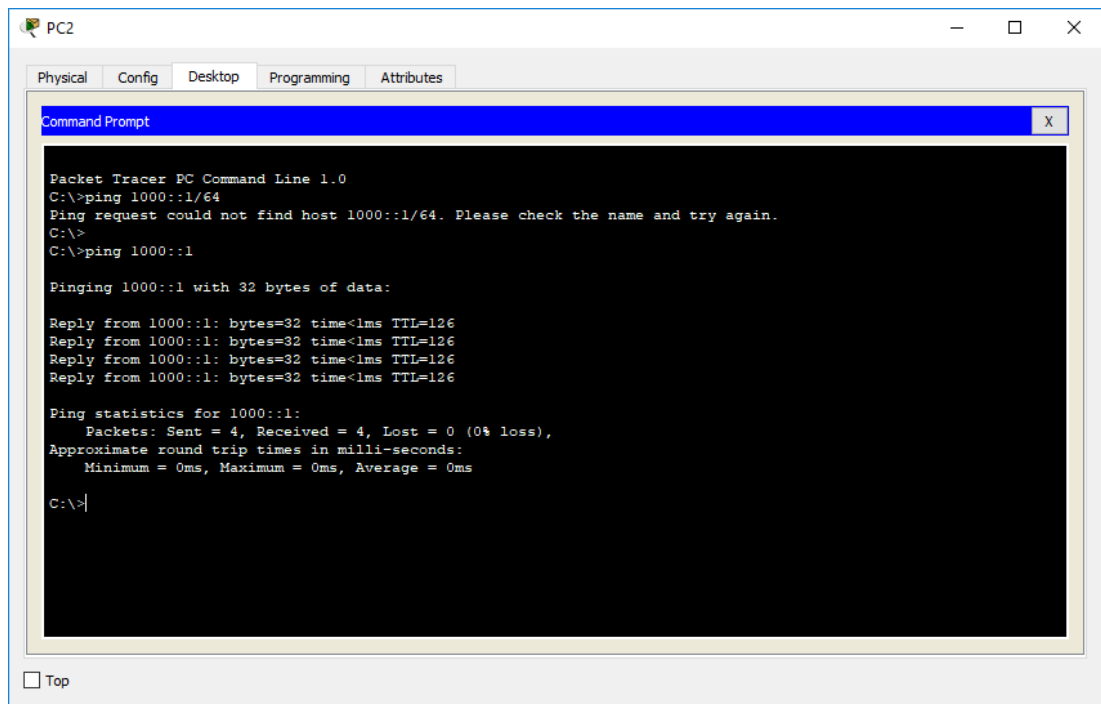
Con esto se asigna la ip al nuevo puerto de fibra óptica añadido al router y se realiza el ruteo por defecto de asignar las salidas que no reconozca de cualquier red hacia el switch tipo capa 3.

- Para el switch de capa se realiza las siguientes configuraciones

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gi 1/0/1
Switch(config-if)#no sw
Switch(config-if)#ipv6 add 4000::1/64
Switch(config-if)#exit
Switch(config)#int gi 1/1/1
Switch(config-if)#no sw
Switch(config-if)#ipv6 add 3000::1/127
Switch(config-if)#exit
Switch(config)#ip routing
Switch(config)#ipv6 un
Switch(config)#ipv6 unicast-routing
Switch(config)#ipv6 route ::/0 3000::
```

Después realizamos las pruebas correspondientes en la PC2

Verificamos haciendo ping al servidor



Y luego validamos ingresar al servidor por medio del navegador

