

Información Importante

La Universidad Santo Tomás, informa que el(los) autor(es) ha(n) autorizado a usuarios internos y externos de la institución a consultar el contenido de este documento a través del Catálogo en línea de la Biblioteca y el Repositorio Institucional en la página Web de la Biblioteca, así como en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

Se permite la consulta a los usuarios interesados en el contenido de este documento, para todos los usos que tengan **finalidad académica**, nunca para usos comerciales, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de grado y a su autor.

De conformidad con lo establecido en el Artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, la Universidad Santo Tomás informa que “los derechos morales sobre documento son propiedad de los autores, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.”

Centro de Recursos para el Aprendizaje y la Investigación, CRAI-Biblioteca

Universidad Santo Tomás, Bucaramanga

**Consultoría para la adopción del protocolo IPv6 en la red del Centro Industrial de
Mantenimiento Integral – SENA CIMI**

Edgardo Javier Rúa Rangel

Trabajo de grado para optar el título de Magister en Redes y Sistemas de Comunicación

Director

Tito Raúl Vargas Hernández

Codirector:

Diana Teresa Parra Sánchez

Magister en Telemática

Universidad Santo Tomas, Bucaramanga

División de Ingenierías y Arquitectura

Maestría en Redes y Sistemas de Comunicación

2019

Tabla de contenido

Introducción.....	3
1. Definición del Problema.....	5
1.1 Formulación del problema.....	6
2. Objetivos.....	6
2.1 Objetivo general	6
2.2 Objetivos específicos.....	6
3. Metodología.....	7
3.1 Fases del Proyecto	7
3.1.1 Fase I . Realizar un diagnóstico de la actualidad de la red y su infraestructura. ..	7
3.1.2 Fase II. Diseñar la políticas de la adopción del protocolo IPv6 en la red CIMI siguiendo las recomendaciones de MINTIC.	8
3.1.3 Tabla de actividades de la Fase II – Diseño de políticas de adopción de IPv6	9
3.1.4 Fase III. Proyectar plan de apropiación de funcionalidad de IPv6.	9
3.1.5 Fase IV– Pruebas de Funcionalidad de IPv6 y socialización de las políticas de adopción.	10
4. Resultados.....	11
4.1 Análisis actual del estado de la red CIMI y su infraestructura física	12

4.1.1 Análisis del estado actual de la red y los servicios y procesos que se implementan para la red IPv4 del SENA	13
4.1.2 Topología y conectividad del SENA con sus diferentes sedes.....	14
4.1.3 Topología y conectividad actual Red CIMI	19
4.1.4 Montaje experimental propuesta de implementación IPv6 en el CIMI.....	24
4.2 Diseño e implementación de las políticas de la adopción del protocolo IPv6 y seguridad basándose en las recomendaciones del MINTIC.....	39
4.2.1 Aspectos Regulatorios	40
4.2.2. Políticas definidas para el proceso de Adopción IPv6.	42
4.2.2 Modelo para el proceso de adopción IPv6.	45
4.2.3 Diseño de Políticas de seguridad y privacidad de la información.....	47
4.2.4 Modelo de seguridad y Privacidad de la Información (MSPI).....	48
4.2.5 Indicadores De Gestión	49
4.2.6 Dominio de seguridad de la red.....	51
4.3 Análisis de seguridad implementada en el SENA y recomendaciones de configuración para para equipos de acceso a la Red CIMI	52
4.3.1 Ataques y medidas preventivas a nivel de capa 2	53
4.4 Proyección del plan de apropiación para la adopción del protocolo IPv6 en la red CIMI.....	54
4.4 Socialización del análisis inicial de la red, el diseño de las políticas de adopción del protocolo IPv6 y el Plan de apropiación propuesto al personal directivo y técnico del SENA CIMI.	58

5. Conclusiones.....	61
5.1 Trabajo Futuro	62
Apéndices	63
Referencias	64

Lista de tablas

Tabla 1. Fase I Análisis de la Adopción del Protocolo IPv6 en el CIMI.	7
Tabla 2. Fase II implementación de IPv6.....	9
Tabla 3. Fase IV Implementación de IPv6.	11
Tabla 4. Equipos de Centro de Datos	16
Tabla 5. Centros adscritos a la regional Santander.	25
Tabla 6. Equipos utilizados para la simulación de la coexistencia.	31

Lista de figuras

Figura 1. Penetración de IPv6 en Latinoamérica.	4
Figura 2. Funcionamiento TIC del SENA.....	12
Figura 3. Mesa de Servicio.....	14
Figura 4. Capacidad operativa de ENLACE.	14
Figura 5. Topología integrada.	15
Figura 6. Conectividad WAN.	16
Figura 7. Infraestructura de Centro de Datos.	17
Figura 8. Infraestructura de Comunicaciones del Centro de Datos.....	17
Figura 9. Infraestructura de Comunicaciones con los servicios que presta.	18
Figura 10. Infraestructura computacional.	18
Figura 11. Grupos de Dominio.....	19
Figura 12. Ciclo de responsabilidades conectividad SENA.....	19
Figura 13. Modelo del Servicio SENA.	20
Figura 14. Conectividad sede central con Red CIMI.	21
Figura 15. Topología CIMI.	21
Figura 16. Direccionamiento actual en la red CIMI.	22
Figura 17. Direccionamiento actual en la red CIMI segunda parte.	22
Figura 18. Valores de distribución del ancho de banda en SENA CIMI.	23
Figura 19. División de regiones de sedes SENA por zona.	25
Figura 20. Distribución geográficas sedes SENA Santander.....	26

Figura 21. Distribución de IPv6 según las regionales.....	27
Figura 22. Subnetting de las sedes de Santander	28
Figura 23. Direccionamiento IPv4 e IPv6 Red CIMI.	29
Figura 24. Habilitación protocolo IPv6 en el Switch.	30
Figura 25. Activar protocolo IPv6 Router.....	30
Figura 26. Red jerárquica IPv6 CIMI.	31
Figura 27. Tabla de direccionamiento de la Red CIMI.....	32
Figura 28. Subinterfaces con IPv4 e IPv6.....	32
Figura 29. Subinterfaces activas del Router.....	32
Figura 30. Configuración DHCPv6 en el Router.	33
Figura 31. Habilitación server DHCPv6 en la Subinterfaz.	33
Figura 32. Pool DHCPv6.	33
Figura 33. Direcciones IPv4 e IPv6 por DHCP.	34
Figura 34. Captura de Wireshark entre la comunicación DHCP entre Router y Host.....	34
Figura 35. Captura del protocolo ICMPv6.....	35
Figura 36. Topología para Tunnel entre CIMI y CASA.	36
Figura 37. Tabla de direccionamiento conexión WAN entre CIMI y CASA.	36
Figura 38. Configuraciones interfaces seriales Router CIMI y CASA.	37
Figura 39. configuración del Tunnel.....	37
Figura 40. configuración OSPF para redes IPv4.....	38
Figura 41. configuración OSPF para redes IPv6.....	38
Figura 42. Direccionamiento IPv4 e IPv6 de host CASA.....	38
Figura 43. Modelo para el proceso de adopción IPv6 recurso humano.	46

Figura 44. Modelo para el proceso de adopción IPv6 recurso humano parte 2.	47
Figura 45. Niveles de madurez del MSPI.	50
Figura 46. TECNOLOGÍA FIREEYE.	52
Figura 47. Alcance para la implementación IPv6	55
Figura 48. Metodología PHVA.	56
Figura 49. Línea de tiempo de adopción.	56
Figura 50. Cronograma de actividades para el proceso de adopción.	57
Figura 51. Socialización y sensibilización del proyecto ante funcionarios SENA CIMI.	58

Lista de Apéndices

Apéndice A. Ante proyecto Consultoría para la adopción del protocolo IPv6 en la red del Centro Industrial de Mantenimiento Integral SENA-CIMI	63
Apéndice B. Artículo Coexistencia entre el protocolo IPv4 e IPv6 en la red convergente del Centro Industrial de Mantenimiento Integral – SENA CIMI.....	63
Apéndice C. Estado de la red y equipos activos.....	63
Apéndice D. Configuración LAN CIMI e implementación del protocolo ipv6 en los equipos activos.	63
Apéndice E. Recomendaciones de Seguridad en la red CIMI.	63
Apéndice F. Plan de apropiación para la adopción del protocolo IPv6 en la red CIMI.	63
Apéndice G. Documento presentado y aceptado por el MinTic del proyecto IPv6.	63
Apéndice H. Acta de socialización del modelo de adopción del proyecto.	63

Resumen

El presente trabajo tiene como objetivo realizar una propuesta de un método para la eficiente adopción del protocolo IPv6 (*Internet Protocol versión 6*). Se explica con detalle como ejecutar la adopción adecuada en la entidad pública del Servicio Nacional de Aprendizaje (SENA) en su sede ubicada en el municipio de Girón (Santander) conocido como Centro Industrial de Mantenimiento Integral (CIMI). Se tendrán en cuenta aspectos tecnológicos como el marco regulatorio vigente.

Con la realización de este trabajo investigativo y consultivo se pretende ayudar a promover la introducción de IPv6 en las entidades públicas de Colombia, a pesar de que este protocolo lleva ya años desde su creación ha sido poco implementado en el país, este documento pretende servir de guía de coexistencia y transición para toda entidad pública que requiera su implementación basándose en las condiciones regionales y nacionales.

Una de las razones de la necesidad de implementar IPv6 se debe al crecimiento exponencial de demanda de servicios y oportunidades en la red mundial de Internet; Con el aumento de las tecnologías de computación y comunicación, el proceso de innovación tecnológica se ha incrementado en varios dispositivos inalámbricos y por cable, como teléfonos celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento, entre otros, que comenzaron a aumentar la conectividad en muchas redes en el mundo y para esto han tenido que hacerlo con direcciones de Internet que permiten establecer conexiones para cada elemento conectado a la red.

Palabras claves: IPv6 , Pv4, TCP, Doble pila.

Abstract

This document aims to define the need to implement the IPv6 internet protocol in telecommunications networks that due to the exponential growth have been generating greater demand for services and opportunities in the global internet network; With the increase in computer and communication technologies, the process of technological innovation has increased in the various wired and wireless devices, such as cell phones, access points, tablets, servers, storage equipment, among others, which began to increase connectivity in many networks in the world and for this they have had to do it with internet addresses that allow connections to be established for each element connected to the network. Framed in the digital governance guidelines of the TIC Ministry, the Industrial Maintenance Industrial Center (SENA CIMI) as an entity of the state is adapted to the implementation of a design and subsequent execution of a native IPv6 network, expanding the coverage and security of the network. This is intended to offer a viable alternative without losing access to IPv4 services and without incurring the disadvantages implicit in other approaches in terms of administration, inherent in the operation of IPv4 and IPv6 simultaneous.

Keywords— Dual stack, IPv4 to IPv6 transition mechanisms, Tunnel type mechanisms.

Introducción

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 determinó 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 red que ha tenido un avance exponencial[1].

En Colombia la implementación del protocolo IPv6 no ha tenido un avance significativo ya que según estadísticas de asignaciones suministradas por LACNIC (The Latin American and Caribbean Internet Address Registry) en el transcurso del año 2018 solo se han asignado un bloque de direcciones IPv6 que solo abarca el 2,4% ubicado en un cuarto lugar detrás de Chile con 2,6% y Argentina con 9.4% y en un primer lugar se encuentra Brasil que tiene la utilización de este protocolo en un 72% como se muestra en la Fig. 1 esta estadística refleja el déficit de penetración del protocolo en Colombia y que Brasil lidera el proceso de adopción de IPv6 y tiene una gran ventaja con respecto a los demás países de Latinoamérica. En la figura 1 se puede observar las cifras estadísticas de implementación del protocolo en los países que pertenecen a la LACNIC[2].

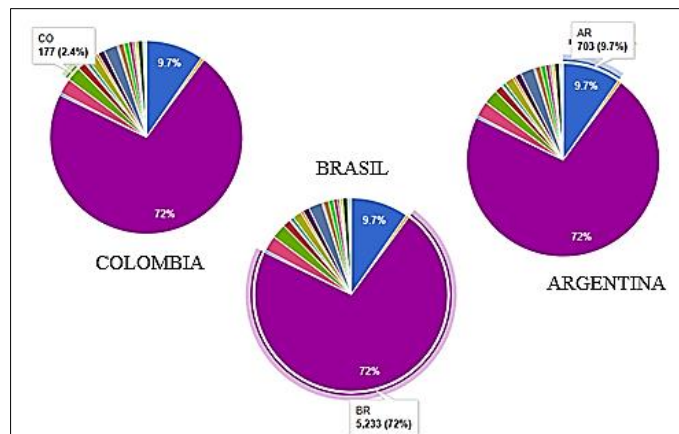


Figura 1. Penetración de IPv6 en Latinoamérica.
Adaptado de "LACNIC: 2018."

IPv4 ha funcionado desde su creación de manera correcta y con éxito porque se adaptado a las diferentes tecnologías gracias a su flexibilidad. IPv6 ha surgido como la necesidad de aprovechar las limitaciones y escasas de direcciones IPv4 agregando mejoras sobre todo en la seguridad e integridad de la información. El protocolo IPv6 fue creado por la IETF (*Internet Engineering Task Force*)[3]. Los inicios de este protocolo se remontan a comienzos de la década de los 90 y a partir del año 1995 se publicaron las primeras RFCs (*Request For Comments*), a partir de ahí se ha podido afianzar normas que le dan más solides al protocolo. En julio de 2004 fue anunciado por la ICANN (*Internet Corporation for Assigned Names and Numbers*) que los DNS (*Domain Name System*) deberían ser modificados para soportar IPv4 e IPv6[4]. IPv6 conserva muchas características de IPv4 sin embargo introduce cambios y simplifica más su cabecera, los cambios más significativos son la longitud de la dirección y su notación. IPv6 es cuatro veces mayor que IPv4 en su dirección, ya que usa 128 bits en comparación con 32 bits de IPv4, con esto se garantiza una fuente inagotable de direcciones para la población mundial y además mantiene el mecanismo CIDR (*Classless Inter-Domain Routing*) como una organización flexible y jerárquica[4].

1. Definición del Problema

A continuación, se describe de manera general el problema planteado. Para abordar el problema es necesario analizarlo desde tres aspectos diferentes como son el planteamiento del problema el cual explica el problema desde su causa y efecto, la formulación del problema que sintetiza el problema y la sistematización del problema mediante cuestionamientos que conducen a la solución de este mismo.

El crecimiento exponencial de las redes e Internet, y un país que está en proceso de desarrollo debe tener como premisa modernizar sus entidades gubernamentales para estar a la vanguardia de los nuevos desarrollos tecnológicos de la información, para así poder cumplir los requerimientos que exige el ciudadano como es un acceso ágil, seguro y confiable a la información.

El Servicio Nacional de Aprendizaje- (SENA) siguiendo la directriz del Ministerio de las Tecnologías de la Información – MINTIC a través de la Resolución 0002710 estipula que *“todas las entidades del estado entre sus planes de compras de equipos TIC (hardware y software), aplicaciones plataformas TIC y servicios se exija que estén implementados sobre el protocolo IPv6 con compatibilidad y soporte total IPv4 demostrable mediante los RFCs (Request For Comments) concretos del IEFT y demás normas que determinan esta comparabilidad”*[5]. Tenido en cuenta lo anterior la entidad requiere de un estudio del estado actual en toda su plataforma tecnológica y diseñar los mecanismos necesarios para ejecutar una adopción de IPv6 con las mejores prácticas a nivel de seguridad y poder cumplir con la normatividad impartida. Este proyecto se enfoca en aplicar los lineamientos del MinTic de buenas prácticas para la adopción de IPv6, debido a la carencia de este en el SENA-CIMI[6].

1.1 Formulación del problema.

¿Dado el crecimiento exponencial de usuarios y aprendices y la escases de direcciones IPv4 se plantea a través de una consultoría como adoptar el protocolo IPv6 en la red del Centro Industrial de Mantenimiento Integral (SENA CIMI) ?

2. Objetivos

2.1 Objetivo general

Realizar una consultoría al SENA para la adopción del protocolo IPv6 en la red del centro Industrial de Mantenimiento Integral (CIMI), mediante una propuesta basada en la normativa vigente, estándares y buenas prácticas.

2.2 Objetivos específicos

1. Analizar el estado de la red del CIMI y su infraestructura y configuración actual utilizando el manual de las buenas prácticas del Min TIC.
2. Diseñar las políticas de la adopción del protocolo IPv6 y seguridad basándose en las recomendaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y según el estado actual de la red IP del CIMI.
3. Proyectar el Plan de apropiación para la adopción del protocolo IPv6 en la red CIMI en un periodo de un año a través de estrategias que se basen en lineamientos del decreto 1078 de 2015.

4. Socializar el análisis inicial de la red, el diseño de las políticas de adopción del protocolo IPv6 y el Plan de apropiación propuesto al personal directivo y técnico del SENA CIMI.

3. Metodología

A continuación, se mencionan cada una de las etapas que se tuvieron en cuenta para el desarrollo de la consultoría propuesta. En el sector de la investigación, este proyecto se enfoca en implementar aplicaciones telemáticas avanzadas que permitan facilitar el acceso a los usuarios, fomentar que empresas estatales y privadas en redes nacionales o especializadas, participen y logren alcanzar posiciones avanzadas en redes de alto rendimiento y enlaces de alta capacidad.

La entidad deberá tener en cuenta las siguientes fases que le lleve desarrollar cada actividad:

3.1 Fases del Proyecto

3.1.1 Fase I . Realizar un diagnóstico de la actualidad de la red y su infraestructura.

En la tabla 1 se muestra la planeación de implementación IPv6 en CIMI. iniciando por el análisis y diagnóstico de la situación actual de la infraestructura de red.

Tabla 1. *Fase I Análisis de la Adopción del Protocolo IPv6 en el CIMI.*

Fase I	Actividades Generales
	Análisis de la topología de la infraestructura actual y su funcionamiento y construir un plan diagnóstico.
	Inventario de TI (Hardware, software)
	Validación de estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos y revisión de los RFC correspondientes.

Nota: *La tabla muestra la primera fase para la implementación de la adopción. Tomado de “MinTic, Transición de IPv4 a IPv6 para Colombia,” Bogota, 2015.

Análisis y Diagnóstico de la Situación Actual de la red CIMI.

Identificación de esquemas de seguridad de la información y seguridad de los sistemas de comunicaciones
Planeación de la adopción de los servicios tecnológicos de la entidad.

3.1.2 Fase II. Diseñar la políticas de la adopción del protocolo IPv6 en la red CIMI siguiendo las recomendaciones de MINTIC.

1. Diseñar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la primera Fase del proceso de adopción IPv6 y teniendo en cuenta el inventario de los activos de información del CIMI[7].
2. Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 en modalidad de 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 la Entidad[7].
3. 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[7].

Entregables de esta Fase

- 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.

3.1.3 Tabla de actividades de la Fase II – Diseño de políticas de adopción de IPv6

Las entidades deberán tener en cuenta las siguientes actividades para el diseño del plan de implementación de la apropiación y coexistencia del protocolo IPv6.

Tabla 2. *Fase II implementación de IPv6.*

Fase II	Actividades Generales
Diseño del Plan de implementación	Diseño de direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase. Definir configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, Aplicativos, Sistemas de Comunicaciones, Sistemas de Almacenamiento. Coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6 hacia el exterior.

Nota: *La tabla muestra la segunda fase para la implementación de la coexistencia. Tomado de “MinTic, Transición de IPv4 a IPv6 para Colombia,” Bogota, 2015.

3.1.4 Fase III. Proyectar plan de apropiación de funcionalidad de IPv6.

Las pruebas de funcionalidad de esta fase cubren las siguientes actividades:

1. 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, utilizando las buenas prácticas basadas en el decreto 1078 de 2015[7].
2. 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 II[7].
3. Elaborar un inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6[7].

Entregables de esta Fase III

- Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la Fase II de Implementación.
- Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.
- Se deberá cumplir el plazo de Diciembre de 2019 para la adopción según la resolución 0002710 del 3 de octubre de 2017.

3.1.5 Fase IV– Pruebas de Funcionalidad de IPv6 y socialización de las políticas de adopción.**Entregables de esta Fase**

- Validar la funcionalidad de los servicios que operen en la red del CIMI.
- Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea la entidad[7].
- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet para establecer la conectividad integral en IPv6 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 normalmente[7].
- Acta de socialización del análisis inicial de la red, el diseño de las políticas de adopción del protocolo IPv6 y el Plan de apropiación propuesto al personal directivo y técnico del SENA CIMI[7].

Las entidad tendrá en cuenta las siguiente las siguientes actividades en relación a la fase IV

Tabla 3. *Fase IV Implementación de IPv6.*

Fase IV	Actividades Generales
Pruebas de funcionalidad de IPv6	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.

Nota: *La tabla muestra la tercera fase para la implementación de la coexistencia. Adaptado de “MinTic, “Transición de IPv4 a IPv6 para Colombia,” MINTIC, 2015”.

4. Resultados

Para el desarrollo del proyecto de investigación y consultoría para la adopción de IPv6 en el SENA CIMI se tiene en cuenta las fases y actividades propuestas por el MinTIC, pero debido a que el desarrollo del mismo requiere la intervención de la organización en el proceso, este trabajo se presenta como una hoja de ruta para la correcta implementación de IPv6 en el SENA-CIMI por parte del personal encargado siguiendo los siguientes resultados: (1) Análisis del estado actual de la red SENA nacional y específicamente Red CIMI, (2) Diseño y configuraciones a realizar en la Red real del SENA-CIMI que se ejecutó en red piloto y simulada, (3) Políticas de adopción del protocolo IPv6 en el SENA-CIMI, (4) plan de apropiación según procesos internos de propuesta de proyectos tecnológicos de la institución incluyendo inversión económica y (5) entrega y socialización ante el personal directivo y técnico del SENA-CIMI sobre estas pautas de adopción de IPv6. De esta manera el SENA-CIMI con estos resultados podrá iniciar el proceso de adopción de IPv6 y ser referente para los demás centros SENA a nivel nacional.

A continuación, se presenta cada uno de los resultados del desarrollo del proyecto, es importante resaltar que el desarrollo y los procedimientos aplicados de cómo se llega a esos resultados esta explicado de forma amplia y detallada en cada uno de los anexos que sustentan este trabajo de maestría.

4.1 Análisis actual del estado de la red CIMI y su infraestructura física

El método para la adopción a IPv6 en el CIMI, siguiendo los pasos de las fases de la metodología para la implementación como requerimiento a seguir, se analizó la estructura y el funcionamiento de la red actual del CIMI y el funcionamiento operativo del SENA en la cual se pudo observar como el proveedor de servicios CLARO es el que se encarga de dar soporte y conectividad a nivel nacional a 214 sedes.

Otra función importante el cual se debe apoyar la adopción de IPv6 es el reporte y tiempos de respuesta con los incidentes que se puedan presentar y recuperar lo más rápido posible el servicio afectado, a la operación normal, minimizando el impacto adverso en la operación del SENA-CIMI y garantizando la disponibilidad de los servicios, enmarcados en los niveles de servicios establecidos. En la imagen a continuación se muestra un diagrama de procesos que se sigue en busca de Soporte y Cobertura.

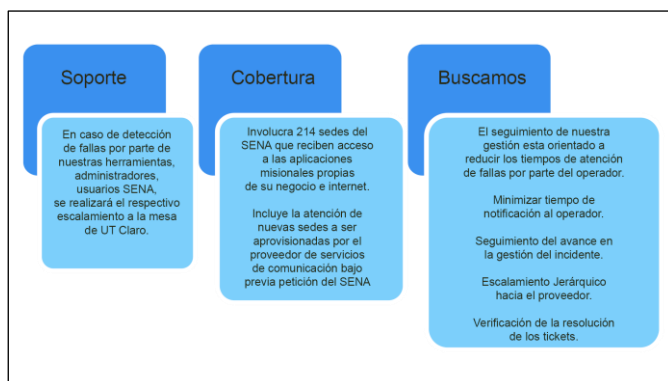


Figura 2. Funcionamiento TIC del SENA.

A continuación, se muestran los resultados de un análisis investigativo de la Red actual del SENA y el CIMI, y vale recalcar que esta sección está sustentada con mayor detalle en el anexo “ESTADO DE LA RED Y EQUIPOS ACTIVOS DEL CIMI”.

4.1.1 Análisis del estado actual de la red y los servicios y procesos que se implementan para la red IPv4 del SENA

Para el proceso de la adopción IPv6 en la LAN del SENA CIMI y dar salida hacia a internet e interconectarlo con las diferentes sedes, se debe coordinar el proceso actualmente con tres outsourcing que se encargan de gestionar y administrar la red SENA en todas sus sedes las cuales son:

1. **UT CLARO** que garantiza al SENA el acceso a Internet e intercambiar información entre sedes y cualquier otro interesado y prestar servicios en línea al ciudadano.
2. **SYNOPSIS** que Presta el servicio de Centro de Datos con flexibilidad, eficiencia, escalabilidad, innovación, redundancia y alta disponibilidad que ofrece la tecnología actual.
3. **ENLACE** es la UTSD (Unión Temporal SENA Digital) que es la unión de las compañías (INDRA - TELEFÓNICA) para prestar e integrar los servicios TIC del SENA. Posteriormente se registra la marca **enlace** que representa al proveedor de los servicios TIC, los cuales abarca los componentes del servicio que se muestran en la imagen a continuación.

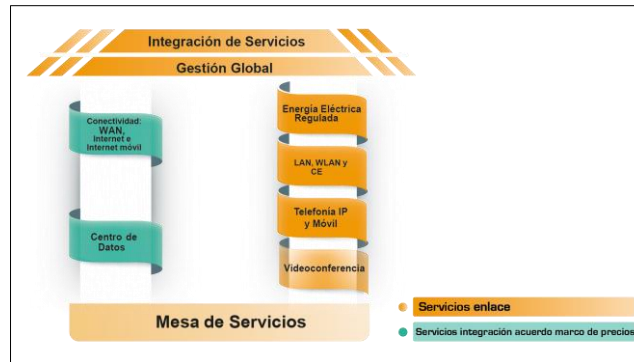


Figura 3. Mesa de Servicio del SENA CIMI.

Se hace particularmente énfasis en ENLACE ya que es el outsourcing que se encuentra en la sede como mesa de ayuda y respaldo para la LAN CIMI, y serán los principales protagonistas en llevar el proceso de adopción. Se muestra en la siguiente imagen la capacidad operativa de ENLACE en el SENA a nivel nacional.

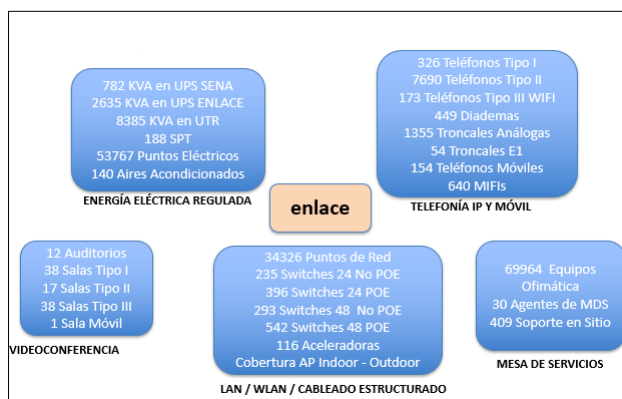


Figura 4. Capacidad operativa de ENLACE.

4.1.2 Topología y conectividad del SENA con sus diferentes sedes

En esta sección se describe el servicio de **Integración de Conectividad**, para el cumplimiento de los objetivos entorno a la gestión, monitoreo y seguimiento del servicio de Conectividad (**WAN e Internet**) adquirido por el SENA bajo el amparo del Acuerdo Marco de Precios.

A continuación, se muestra la WAN, DATACENTER y la Integración de Conectividad, en su labor de interoperabilidad con los demás servicios con las Tecnologías de la Información del SENA, y como interactúa con la Mesa de servicios, y los proveedores que se deberán tener en cuenta para la adopción del protocolo IPv6 a nivel nacional si así lo requiere.

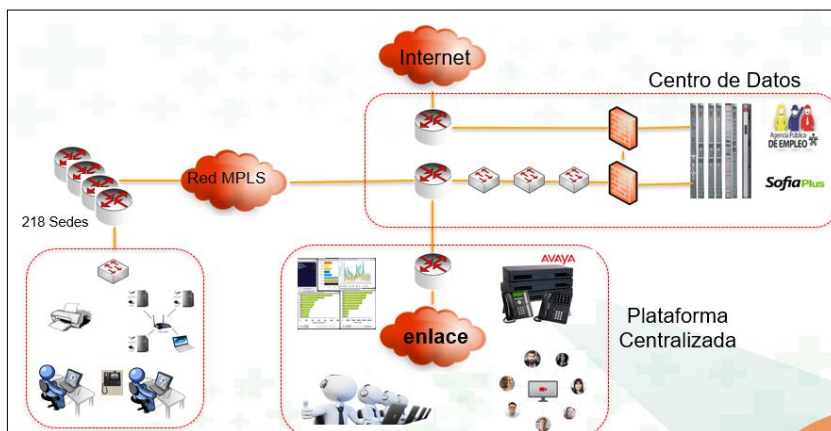


Figura 5. Topología integrada.

La conectividad del Centro de Datos con las sedes remotas actualmente usa una infraestructura “Multiprotocolo Label Switching” (MPLS), en la cual se utiliza un canal principal y otro de respaldo que es de Radio enlace. Si actualmente se pretendiera implementar IPv6 en el SENA a nivel nacional, tal cual como está la infraestructura no sería problema ya que IPv6 usaría la infraestructura MPLS existente, la alternativa seleccionada para solucionar la conexión con las oficinas remotas IPv6, la cual consiste en la implementación por parte del ISP del mecanismo 6PE sobre MPLS; este mecanismo consiste en activar el intercambio de rutas IPv6 entre los encaminadores de borde del proveedor. La ventaja de este mecanismo es que no requiere la realización de cambios en el núcleo MPLS ya que una vez el datagrama IPv6 llega a los equipos 6PE, es encapsulado dentro de MPLS y el encaminamiento se hace a nivel de etiquetas y no de IP, lo cual permite transportar paquetes IPv6 sobre una red MPLS IPv4 [8]. En la figura a continuación se muestra la topología de conectividad.

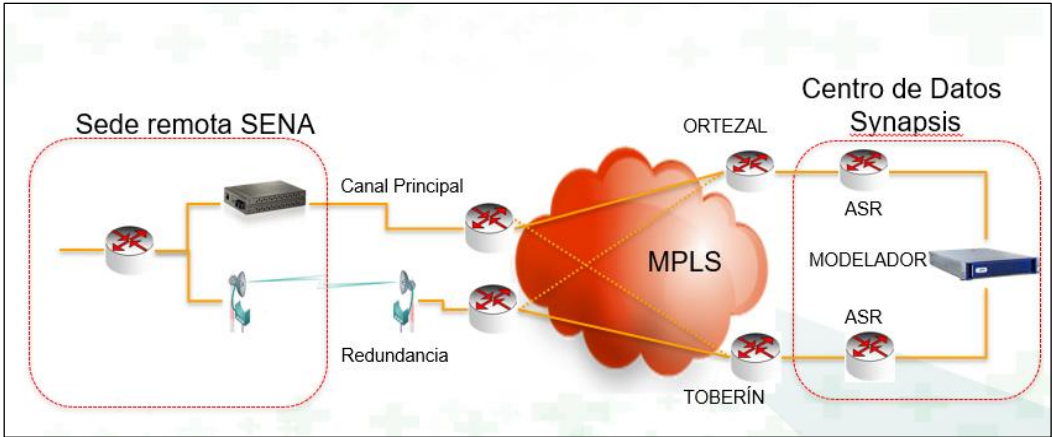


Figura 6. Conectividad WAN.

4.1.2.1 Centro de Datos (DATACENTER).

En el DATACENTER encontramos una serie de equipos y servicios que se proveen a las diferentes sedes remotas del SENA. En la siguiente tabla se encuentra los equipos del DATACENTER.

Tabla 4. Equipos de Centro de Datos

EQUIPOS Y SERVICIOS
Correo Electrónico
Base de Datos SQL
Base de Datos ORACLE
Servidores Solaris
Servidores Linux
Servidores Windows y DA
Respaldos y Almacenamiento
Virtualización

Nota: *La tabla muestra los servicios y equipos en el DATACENTER.

En la siguiente imagen se muestra la Infraestructura de comunicaciones del DATACENTER que interviene en los servicios de comunicaciones de SYNAPSIS:

EQUIPOS	REFERENCIA EQUIPO	RESPONSABLE
ASR WAN e Internet	Cisco ASR 1002	UT CLARO
Gateway de VPN	FortiGate 200D	UT CLARO
Modelador Allot	Allot NetEnforcer Sigma E6	UT CLARO
Aceleración	Interceptor - SteelHead Riverbed	UTSD
BlueCoat SSL Visibility	BlueCoat SV 3800	UTSD
FireEye NX	NX 10450	UTSD
Switch LAN	Cisco Catalyst 4500X	UTSD
Proxy	McAfee Web Gateway	UT SYNAPSIS
Firewall	FortiGate 3700D	UT SYNAPSIS
IPS	FortiGate	UT SYNAPSIS
Balaceador	Citrix NetScaler	UT SYNAPSIS
WAF	Citrix NetScaler	UT SYNAPSIS
Firewall DB	Imperva	UT SYNAPSIS

Comunicaciones

Centro de Datos

Figura 7. Infraestructura de Centro de Datos.

En la siguiente imagen se muestra la infraestructura de Comunicaciones del Centro de Datos en donde se muestra el tráfico SENA hacia internet

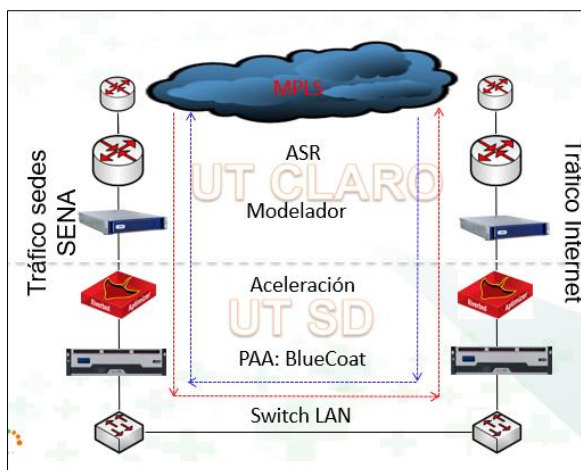


Figura 8. Infraestructura de Comunicaciones del Centro de Datos.

En la siguiente imagen se muestra la infraestructura de Comunicaciones del DATACENTER con aplicaciones que prestan información y servicios a la comunidad en general como es www.senasofiaplus.com.co y <https://agenciapublicadeempleo.sena.edu.co>.

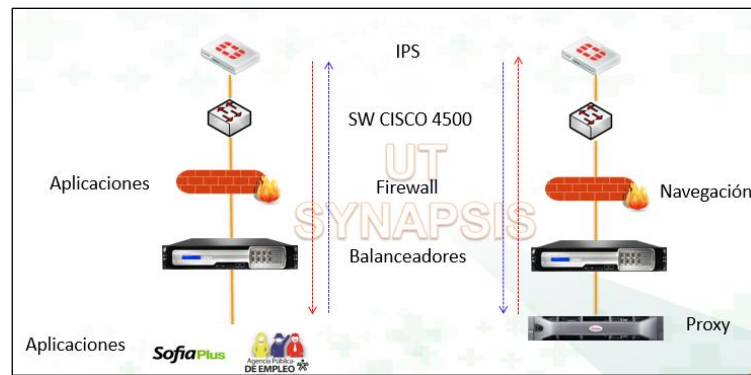


Figura 9. Infraestructura de Comunicaciones con los servicios que presta.

En la siguiente imagen se muestra como está distribuido la infraestructura computacional del DATACENTER.

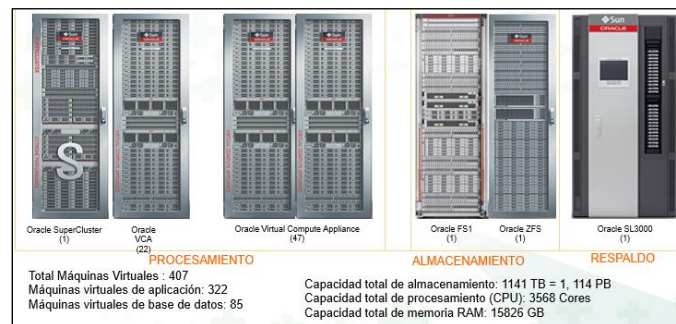


Figura 10. Infraestructura computacional.

Otro aspecto relevante son los perfiles, dominios y reglas que se crean tanto para usuarios inalámbricos como red cableada. En las siguientes imágenes se muestra los Perfiles PROXY y los grupos de dominio creados desde el DATACENTER para las diferentes sedes del SENA. El grupo global de dominios se utiliza para organizar los usuarios que comparten requisitos similares de acceso a redes, agrupar usuarios con funciones similares bajo un ámbito global y otorgar permisos para acceder a recurso como una impresora o carpetas y archivos compartidos, que están disponibles en un dominio local o en otro dominio del mismo bosque. Puede utilizar grupos globales para otorgar permisos para acceder a recursos de ubicados en cualquier dominio

de un único bosque ya que la pertenencia es restringida. Puede agregar cuentas de usuario y grupos globales sólo desde el dominio en el que se crea el grupo global. En la imagen siguiente se muestra los perfiles creados de usuarios o dependencias.

Nombre del Perfil	Usuarios o Dependencias involucradas
Directivo	Usuarios caracterizados como Directivos en Regionales
Sistemas	Oficina de Sistemas
Formación	Instructores - Aprendices (Dominio formación) en Regionales, Sedes y Subsedes
Comunicaciones	Oficina de Comunicaciones en Regionales, Sedes y Subsedes
Administrativo	✓ Dirección Administrativa y Financiera ✓ Dirección de Planeación y Direccionamiento Corporativo ✓ Dirección de Promoción y Relaciones Corporativas ✓ Dirección Empleo y Trabajo ✓ Dirección Formación Profesional ✓ Dirección Jurídica ✓ Oficina Control Interno de Gestión y Disciplinario ✓ Secretaría General Y aplica para sus equivalentes en las Direcciones Regionales y Centro de Formación
Aprendiz	Usuarios aprendices en Regionales, Sedes y Subsedes

Figura 11. Grupos de Dominio.

4.1.3 Topología y conectividad actual Red CIMI

Para la adopción de IPv6, primero se debe considerar una coexistencia de IPv4 e IPv6 y se deben considerar no solo aspectos técnicos si no de funcionalidad administrativa y logística para poder tener un perfecto engranaje entre todos los actores de la comunidad CIMI. Para esto se debe tener presente quienes y como están representados con sus diferentes responsabilidades a su cargo. En la siguiente imagen se muestra el ciclo de responsabilidad de la conectividad CIMI.

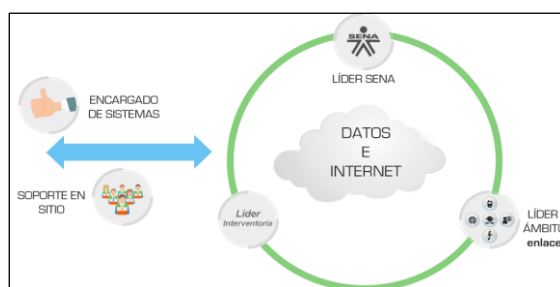


Figura 12. Ciclo de responsabilidades conectividad SENA.

En la sede CIMI se definen el modelo de servicio que servirá como ruta a seguir para definir las políticas de diseño para la implementación de la adopción y los ejes que interactúan sobre la red. El modelo de servicio TI del SENA tiene como principio:

- Identificar la Topología Integral de TI de SENA CIMI.
- Describir la Topología en las sede SENA CIMI.
- Identificar cada uno de los servicios que presta los proveedores de TI del SENA.

Se encuentran 4 ejes fundamentales que si se adopta el protocolo IPv6 se tendrá que trabajar de la mano para que el proceso de coexistencia entre IPv4 e IPv6 sea exitoso.

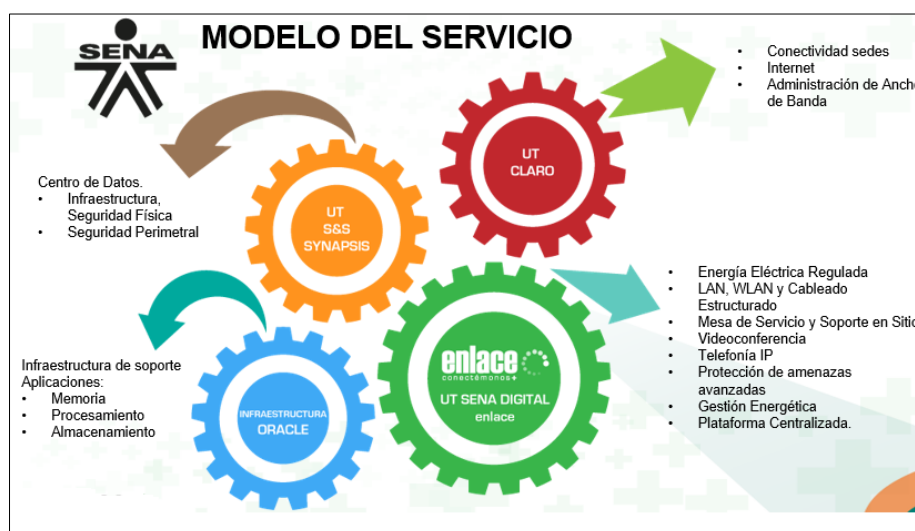


Figura 13. Modelo del Servicio SENA.

Como se mencionó anteriormente el outsourcing ENLACE es el que encuentra en cada una de las sedes y en este caso el CIMI y tiene como objetivo ofrecer y controlar el acceso a los sistemas de información del SENA CIMI y garantizar que los accesos otorgados se utilicen apropiadamente según los lineamientos de seguridad, etc.

En la siguiente imagen se muestra la conectividad con la sede central y la sede remota que en este caso es la Red CIMI y su topología intranet.

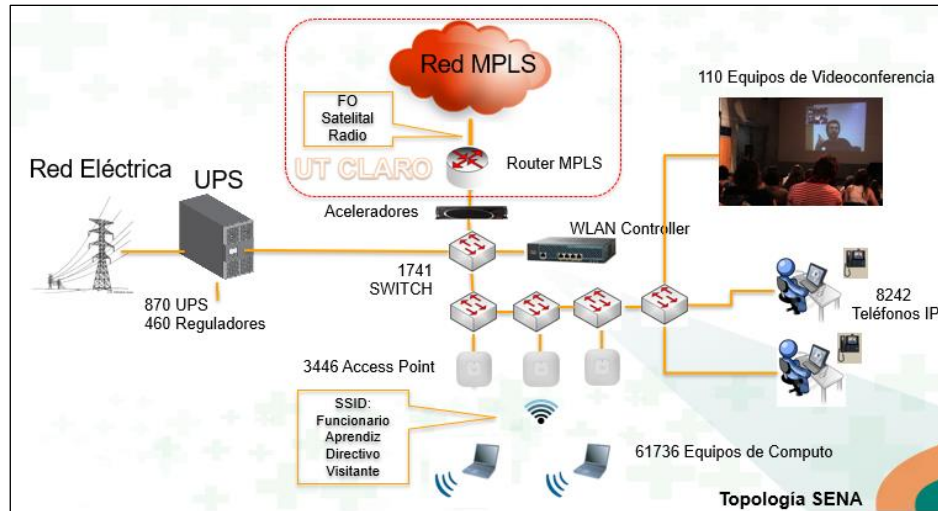


Figura 14. Conectividad sede central con Red CIMI.

Dentro de la Red Convergente del Centro Industrial de Mantenimiento Integral (CIMI) encontramos una topología de tipo estrella para su red de acceso como LAN y WLAN en el centro de la topología se encuentra un Switch Core interconectados a los Switch de acceso que son las diferentes subredes del CIMI.

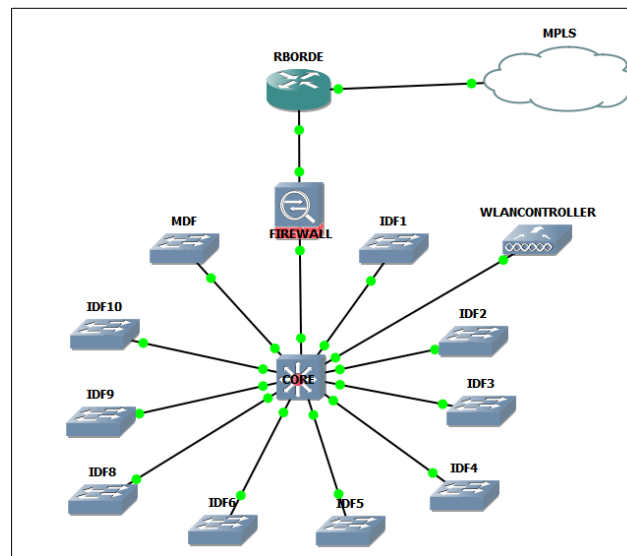


Figura 15. Topología CIMI.

En las siguientes figuras se muestra el direccionamiento lógico IPv4 que actualmente esta implementado en la Red CIMI con sus respectivas VLAN..

DIRECCIONAMIENTO IP		
DESCRIPCIÓN	VLAN ID	RANGO DE DIRECCIONAMIENTO
VLAN DATOS	201	10.72.0.0 /26 – 62 HOST
	202	10.72.0.64 /26 – 62 HOST
	203	10.72.0.128 /26 – 62 HOST
	204	10.72.0.192 /26 – 62 HOST
	205	10.72.1.0 /26 – 62 HOST
	206	10.72.1.64 /26 – 62 HOST
	207	10.72.1.128 /26 – 62 HOST
	208	10.72.1.192 /26 – 62 HOST
	209	10.72.2.0 /26 – 62 HOST
	210	10.72.2.64 /26 – 62 HOST
	211	10.72.2.128 /26 – 62 HOST
	212	10.72.2.192 /26 – 62 HOST
	213	10.72.3.0 /26 – 62 HOST
	215	10.72.13.0 /26 – 62 HOST
VLAN VOZ	264	10.72.8.0 /26 – 62 HOST
	265	10.72.8.64 /26 – 62 HOST
	266	10.72.8.128 /26 – 62 HOST
	267	10.72.8.192 /26 – 62 HOST
	268	10.72.9.0 /26 – 62 HOST

Figura 16. Direccionamiento actual en la red CIMI.

DIRECCIONAMIENTO IP		
DESCRIPCIÓN	VLAN ID	RANGO DE DIRECCIONAMIENTO
APRENDIZ	232	10.72.4.0 /26 – 62 HOST
	233	10.72.4.64 /26 – 62 HOST
	234	10.72.4.128 /26 – 62 HOST
	235	10.72.4.193 /26 – 62 HOST
FUNCIONARIO	240	10.72.6.0 /25 – 62 HOST
	241	10.72.6.128 /25 – 62 HOST
DIRECTIVO	248	10.72.7.0 /25 – 126 HOST
WLANVOZ	296	10.72.12.0 /25 – 126 HOST
DIRECCIONAMIENTO FIJO	586	10.72.60.64 /26 – 62 HOST

Figura 17. Direccionamiento actual en la red CIMI segunda parte.

Otro aspecto de gran relevancia y que se tendrá que parametrizar en la coexistencia y posterior migración al protocolo IPv6 es la distribución de ancho de Banda, que le siguiente imagen se muestra cómo se distribuidos entre servicios y perfiles creados en la red.

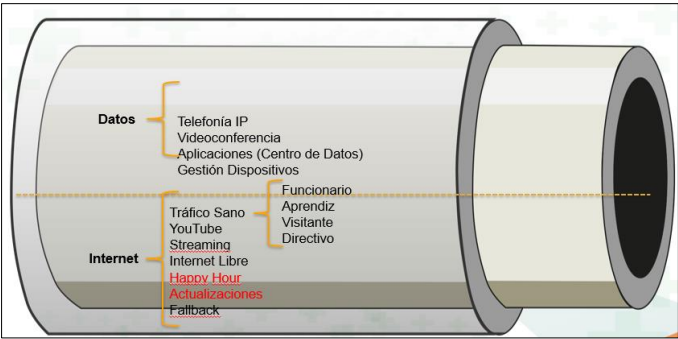


Figura 15. Distribución de ancho de Banda.

En la siguiente figura se muestra los valores de distribución del ancho de banda en SENA CIMI.

ID	NOMBRE			REGIONAL	CIUDAD	BW	WAN TOTAL		BW TOTAL - Datos		ToIP (Kbps)	VIDEO (Kbps)	APLICACIONES DG - (Kbps)		APLICACIONES DATA CENTER (Kbps)		MONITOREO (Kbps)
110	CENTRO INDUSTRIAL DE MANTENIMIENTO INTEGRAL			SANTANDER	GIRÓN	20	20.480		8.960		512	2.560	1.536		4.096		256

BW TOTAL - INTERNET	FUNCIONARIO (Kbps)	VISITANTE (Kbps)		APRENDIZ (Kbps)	DIRECTIVO (Kbps)	YOUTUBE (Kbps)		STREAMING (Kbps)		FALLBACK (Kbps)	INTERNET LIBRE (Kbps)		Happy Hour (Kbps)		ACTUALIZACIONES (Kbps)	
11.520	4.096	128	256	4.608	1.024	512	1.024	128	192	128	256	512	128	192	512	640

Figura 18. Valores de distribución del ancho de banda en SENA CIMI. Adaptado de Autor.

Como se mencionó anteriormente en el anexo “Estado de la red actual” se encuentra los diferentes dispositivos inventariados en el cuarto de Telecomunicaciones y los que están distribuidos por todo el CIMI.

Se concluye que la red CIMI es viable para la implementación del protocolo IPv6 según inventario de los equipos con que cuenta la red los Sistemas Operativos de la red y con respecto a los costos no hay que realizar una gran inversión ya que los equipos soportan dualidad de protocolos.

La siguiente sección tiene como finalidad mostrar los resultados que se obtuvieron de la implementación de simulaciones y pruebas pilotos con equipos reales de laboratorio, software GNS3 y el cálculo del direccionamiento IPv6, para la adopción en una Red del protocolo IPv6

es importante recalcar que el desarrollo de las practicas propuestas esta explicado de manera más amplia en el anexo “Apéndice D. Configuración actual en la red CIMI y recomendaciones de configuración del protocolo IPv6 en los equipos activos de la LAN”

4.1.4 Montaje experimental propuesta de implementación IPv6 en el CIMI

En esta sección se realiza un propuesta de implementación de una coexistencia entre el protocolo IPv4 e IPv6 en el CIMI teniendo en cuenta el inventario y características de los equipos de la red, siguiendo parámetros y lineamientos del MINTIC y como de LACNIC.

4.1.4.1 Asignación y cálculo del direccionamiento lógico IPv6 para el CIMI

Teniendo en cuenta la topología lógica de la red basado en el protocolo IPv4 se procede a diseñar un direccionamiento lógico IPv6 y ejecutar un prototipo de configuración , con base en las VLANs evidenciadas en el estado de la red actual. La asignación y utilización de la dirección IPv6 en la red CIMI se ha realizado en correspondencia con la estructura de la red IPv4 existente. Los cálculos se han realizado teniendo en cuenta las distintas sedes con que cuenta el SENA a nivel regional, de esta forma siguiendo las políticas para el uso de asignaciones y direcciones IPv6 sugeridas por LACNIC, como se explicó anteriormente en el anexo “Apéndice D. Configuración actual en la red CIMI y recomendaciones de configuración del protocolo IPv6 en los equipos activos de la LAN”, se explica con mayor detalle los resultados de la configuración para la simulación.

El SENA como entidad estatal nacional se encuentra presente con 33 regionales dividido en zonas las cuales son como se muestra en la figura.

Zonas	Regiones
Zona 1	Caribe
Zona 2	Andina
Zona 3	Pacífica
Zona 4	Amazónica
Zona 5	Orinoquía

Figura 19. División de regiones de sedes SENA por zona.

Adaptado de “<http://www.sena.edu.co/es-co/regionales/Paginas/default.aspx>”, por SENA, 2010.

La Regional Santander pertenece a la Zona Andina la cual tiene ocho sedes como se ve en la siguiente tabla.

Tabla 5. *Centros adscritos a la regional Santander.*

Regional	Centro
Regional Santander	Centro Industrial de Mantenimiento Integral (CIMI).
	Centro Agroempresarial y Turístico de los Andes (CATA).
	Centro Agroturístico (CA).
	Centro de Atención al Sector Agropecuario (CASA).
	Centro de Gestión Agroempresarial del Oriente (CGAO).
	Centro de Servicios Empresariales y Turísticos (CSET).
	Centro Industrial del Diseño y la Manufactura (CIDM).
	Centro Industrial y del Desarrollo Tecnológico (CIDT).

Nota: *La tabla diferentes centros de la Regional Santander. Tomado de “<http://www.sena.edu.co/es-co/regionales/Paginas/default.aspx>”, por SENA, 2010.

En la Figura 15 se muestra la distribuciones geográficas de los centros de formación en Santander. El objetivo de mostrar la distribuciones geográficas es por si en futuro se implemente Interconexión IPv6 con todas las sedes.

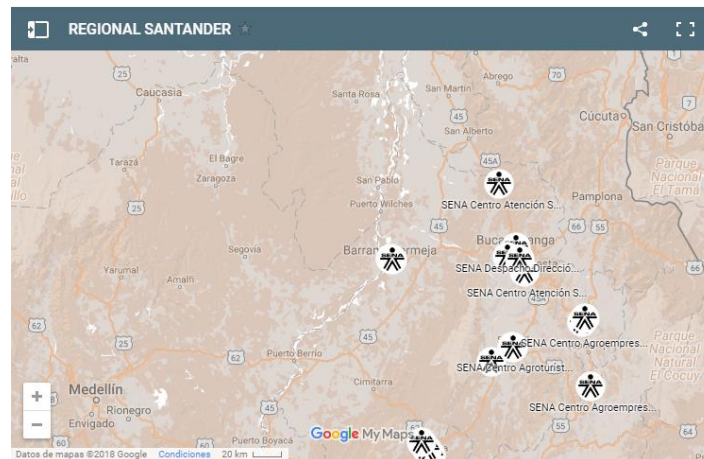


Figura 20. Distribución geográficas sedes SENA Santander.

Adaptado de "<http://www.sena.edu.co/es-co/regionales/Paginas/default.aspx>", por SENA, 2010.

A diferencia de IPv4, IPv6 es generalmente asignado a usuarios finales en cantidades fijas. La utilización real de direcciones dentro de cada asignación será bastante baja comparada con las asignaciones de IPv4. En IPv6, la "utilización" es medida en términos de prefijos asignados a usuarios finales, y no al tamaño de estos, ni al número de direcciones realmente utilizadas dentro de dichos prefijos, y así deberá entenderse a lo largo de este documento. LACNIC distribuirá un bloque de direcciones IPv6 a un LIR (Local Internet Registry) o ISP (Internet Services Provider) que cuente con distribuciones de direcciones IPv4 previamente realizadas por LACNIC.

La selección exacta del tamaño del prefijo a asignar es una decisión operacional del LIR/ISP, aunque se recomienda una infraestructura más simple y funcional con /48 para todos los extremos de la red[10].

Una práctica importante por motivos de seguridad es no asignar los bloques y las direcciones

de manera consecutiva, recordemos que el espacio de IPv6 es enorme y adicionalmente deseamos realizar la implementación lo menos vulnerable posible[10]. Las mejores prácticas nos indican que para segmentos LAN se asignan de la siguiente forma:

- **Tomar todo el 2001:db8:000E::/48**
- **2001:db8:000E:0: :/64 Segmento LAN #1**
- **2001:db8:000E:23::/64 Segmento LAN #2**
- **2001:db8:000E:286::/64 Segmento LAN #3**

Teniendo en cuenta las recomendaciones anteriormente se realiza el cálculo lógico experimental de direccionamiento IPv6 para el CIMI:

Para 33 Regionales necesitamos 6 bits, $2^6 = 64$ Regionales. Sólo nos interesa prefijos para 33 Regionales, las demás quedan para futuro crecimiento. Se realiza subntetting con los bits del cuarto hexteto 2001:db8:57:0000:0:0:0:0/48.

En la siguiente imagen se muestra el diagrama lógico de direcciones por la Zona Andina para sus diferentes regionales.

ZONA ANDINA			
Nº	Regional	IPv6	Longitud de Prefijo
1	Antioquia	2001:db8:57:0000:0:0:0:0	/56
2	Bogota	2001:db8:57:0100:0:0:0:0	/56
3	Boyaca	2001:db8:57:0200:0:0:0:0	/56
4	Caldas	2001:db8:57:0300:0:0:0:0	/56
5	Cundinamarca	2001:db8:57:0400:0:0:0:0	/56
6	Huila	2001:db8:57:0500:0:0:0:0	/56
7	Norte Santander	2001:db8:57:0600:0:0:0:0	/56
8	Quindío	2001:db8:57:0700:0:0:0:0	/56
9	Risaralda	2001:db8:57:0800:0:0:0:0	/56
10	Santander	2001:db8:57:0900:0:0:0:0	/56
11	Tolima	2001:db8:57:0A00:0:0:0:0	/56

Figura 21. Distribución de IPv6 según las regionales.

Teniendo en cuenta la anterior tabla se realiza el cálculo del Prefijo para las Sedes.

Se cuenta con 123 centros distribuidos por todo el país pertenecientes a las regionales. En nuestro caso específico nos basaremos en la Regional Santander y tomaremos como inicio de dirección 2001:db8:57:0900:0:0:0:0/56.

El prefijo para los centros será: /60 ($56+4=60$), como se evidencia en la siguiente tabla donde se muestra la distribución para los centros o sedes. El cambio está el tercer nibble del cuarto hexteto ver la figura.

REGIONAL SANTANDER			
Nº	Centro	Dirección IPv6	Longitud de Prefijo
1	CIDM	2001:db8:57:0900:0:0:0:0	/60
2	CATA	2001:db8:57:0910:0:0:0:0	/60
3	CA	2001:db8:57:0920:0:0:0:0	/60
4	CASA	2001:db8:57:0930:0:0:0:0	/60
5	CGAO	2001:db8:57:0940:0:0:0:0	/60
6	CSET	2001:db8:57:0950:0:0:0:0	/60
7	CIMI	2001:db8:57:0960:0:0:0:0	/60
8	CIDT	2001:db8:57:0970:0:0:0:0	/60

Figura 22. Subnetting de las sedes de Santander.

Tomando como referencia la tabla anterior se realiza el cálculo del prefijo para la red CIMI. Para este requerimiento no es necesario realizar ningún cálculo porque la recomendación es que cada subred debe tener una longitud mínima de /64 y lo tiene de /65.

28 Vlan, $2^5=32$

Se tomaría un nibble completo, y también el siguiente nibble cada VLAN tendrá un prefijo /68 ($60+8$).

64 Vlan o $2^8=64$

En la siguiente figura se muestra la distribución de direcciones IPv6 para cada departamento que estarán separados en VLAN. Se muestra el direccionamiento IPv6 a implementar según los cálculos realizados anteriormente, asociados a sus respectivos VLANs.

ID 141 - DIRECCIONAMIENTO IP		
DESCRIPCIÓN	VLAN ID	RANGO DE DIRECCIONAMIENTO
VLAN DATOS	201	2001:db8:57:0960:0000::/68
	202	2001:db8:57:0960:1000::/68
	203	2001:db8:57:0960:2000::/68
	204	2001:db8:57:0960:3000::/68
	205	2001:db8:57:0960:4000::/68
	206	2001:db8:57:0960:5000::/68
	207	2001:db8:57:0960:6000::/68
	208	2001:db8:57:0960:7000::/68
	209	2001:db8:57:0960:8000::/68
	210	2001:db8:57:0960:9000::/68
	211	2001:db8:57:0960:A000::/68
	212	2001:db8:57:0960:B000::/68
	213	2001:db8:57:0960:C000::/68
	215	2001:db8:57:0960:D000::/68
VLAN VOZ	264	2001:db8:57:0960:E000::/68
	265	2001:db8:57:0960:F000::/68
	266	2001:db8:57:0961:0000::/68
	267	2001:db8:57:0962:0000::/68
	268	2001:db8:57:0963:0000::/68
ID 141 - DIRECCIONAMIENTO IP		
DESCRIPCIÓN	VLAN ID	RANGO DE DIRECCIONAMIENTO
APRENDIZ	232	2001:db8:57:0964:0000::/68
	233	2001:db8:57:0965:0000::/68
	234	2001:db8:57:0966:0000::/68
	235	2001:db8:57:0967:0000::/68
FUNCIONARIO	240	2001:db8:57:0968:0000::/68
	241	2001:db8:57:0969:0000::/68
DIRECTIVO	248	2001:db8:57:096A:0000::/68
WLANVOZ	296	2001:db8:57:096B:0000::/68
DIRECCIONAMIENTO FIJO	586	2001:db8:57:096C:0000::/68

Figura 23. Direccionamiento IPv4 e IPv6 Red CIMI.

4.1.4.2 Habilitación del protocolo IPv6 de los equipos activos de la Red

En la siguiente sección se muestra la configuración y habilitación del protocolo IPv6 en los Switches como en el Router ya que no viene configurado de manera predeterminada en los Switches capa 2 de CISCO como si lo es el protocolo IPv4. El desarrollo con mayor detalle se encontrará en el anexo “Apéndice D. Configuración actual en la red CIMI y recomendaciones de configuración del protocolo IPv6 en los equipos activos de la LAN”.

Para nuestros propósito, podemos iniciar escribiendo el siguiente comando:

```
SwAcceso(config)#sdm prefer dual-ipv4-and-ipv6 default
```

Figura 24. Habilitación protocolo IPv6 en el Switch.

Para habilitar IPv6 en el Router se ejecuta “ipv6 unicast-Routing” Para nuestros propósito, podemos iniciar escribiendo el siguiente comando:

```
Router(config)ipv6 unicast-routing
```

Figura 25. Activar protocolo IPv6 Router.

4.1.4.3 Diseño, configuración y simulación de la convivencia IPv4 e IPv6 en el CIMI

En esta sección lo que se pretende es mostrar los resultados del diseño y configuración del protocolo IPv6 coexistiendo con IPv4, a través de un montaje experimental, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales, estas pruebas fueron realizadas sobre el método de Doble Pila.

Para efectos de simulación de la red CIMI y configuración del protocolo IPv6 se ha planteado una topología de distribución similar a la que existe implementada actualmente. A continuación, se muestra la topología con los equipos utilizados en la siguiente imagen.

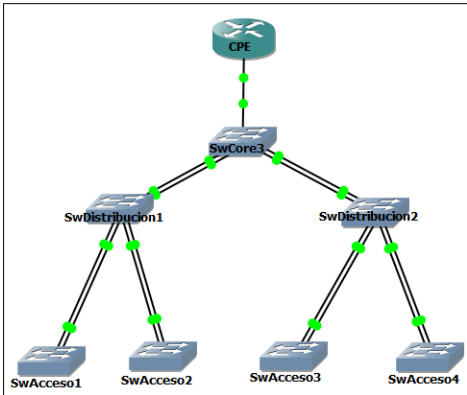


Figura 26. Red jerarquica IPv6 CIMI.

Tabla 6. Equipos utilizados para la simulación de la coexistencia.

CANTIDAD	MODELO	TIPO
4	WS-C2960X-TS-LL	Switch de Acceso
2	WS-C2960X-TS-LL	Switch de Distribución
1	Cisco Catalyst 3560 Series POE.	Switch Capa 3 (Core)
1	Router Gigabit Integrated Services Router Cisco 2901	Router (CPE)

Nota: *En esta tabla se muestra los equipos disponibles.

En la siguiente figura se muestra el direccionamiento IPv4 e IPv6 que se configuro en los equipos activos de la red para la simulación de la red CIMI coexistiendo entre ellos los protocolos a través de Dual Stack. Este prototipo de simulación lo que pretende es demostrar lo versátil y adaptable que se puede implementar el protocolo IPv6 en una red en los dispositivos de enrutamiento y conmutación.

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		
Router CPE CIMI	G0/0.100	192.168.100.1	255.255.255.224	N/A
		2001:DB8:58:968::1/64		N/A
	G0/0.201	10.72.0.1	255.255.255.224	N/A
		2001:db8:57:0960::1/68		N/A
	G0/0.264	10.72.8.0	255.255.255.224	N/A
		2001:db8:57:0960:E000::1/68		N/A
Link-local	FE80:: Link Local			N/A
SwCore	VLAN100	192.168.100.2	255.255.255.224	192.168.100.1
		2001:DB8:58:968::2/64		FE80:: Link Local
SwDistribución	VLAN100	192.168.100.3	255.255.255.224	192.168.100.1
		2001:DB8:58:968::3/64		FE80:: Link Local
SwAcceso	VLAN100	192.168.100.4	255.255.255.224	192.168.100.1
		2001:DB8:58:968::4/64		FE80:: Link Local

Figura 27. Tabla de direccionamiento de la Red CIMI.

Ahora, asumiendo que ha seguido las instrucciones iniciales de configuración en el ROUTER para crear las subinterfaces correspondientes a la VLAN 100. Puede asegurarse de que el dispositivo tiene un perfil de aplicación así:

```
interface GigabitEthernet1/0.100
 encapsulation dot1Q 100 native
 ip Address 192.168.100.1 255.255.255.224
 ipv6 Address 2001:DB8:58:968::1/64
```

Figura 28. Subinterfaces con IPv4 e IPv6.

Se observa el perfil de las dos subinterfaces activas, con el comando “show ipv6 interface brief”.

```
GigabitEthernet1/0.100 [up/up]
 FE80::C805:3DFF:FE54:1C
 2001:DB8:58:968::1
 GigabitEthernet1/0.201 [up/up]
 FE80::
 2001:DB8:57:960::1
```

Figura 29. Subinterfaces activas del Router.

Se configuro tanto DHCPv4 como DHCPv6 para el direccionamiento de los equipos finales y se puede hacer un chequeo inmediato para verificar que todo salió según lo planeado se observara tanto un pool de DHCP para IPv4 y otro para las direcciones IPv6, como se evidencia en la imagen siguiente se muestra el Pool IPv6 para datos. Ver la Fig.

```
ip dhcp pool Datos
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
!
ip dhcp pool Voz
  network 192.168.150.0 255.255.255.0
  default-router 192.168.150.1
  option 150 ip 192.168.150.1
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool Datos6
  prefix-delegation pool Datos6
  dns-server 2001:DB8:1:1::1234
  domain-name sena.gov.co
```

Figura 30. Configuración DHCPv6 en el Router.

Direccionamiento dinámico con IPv6 a diferencia con IPv4 que no hace falta. A continuación, se muestra el resultado.

```
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip Address 192.168.10.1 255.255.255.0
  ipv6 Address FE80:: link-local
  ipv6 Address 2001:DB8:57:968::1/64
  ipv6 enable
```

Figura 31. Habilidad server DHCPv6 en la Subinterfaz.

El resultado que se muestra a continuación es el rango de direccionamiento que Proporcionará y delegará prefijos a los enrutadores solicitantes o clientes DHCPv6, cadena de hasta 16 caracteres alfanuméricos.

```
ipv6 local pool Datos6 2001:DB8:57:960::/60 64
```

Figura 32. Pool DHCPv6.

Se verifica que haya conectividad con la Subinterfaz VLAN nativa tanto IPv6 como IPv4. Y se demuestra que el computador toma las respectivas direcciones tanto IPv4 como IPv6 asignadas por DHCPv6 y DHCPv4. Ver la Fig. 33.

```

C:\WINDOWS\system32\cmd.exe

Adaptador de Ethernet Ethernet:

  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : 2001:db8:57:968:502e:67e8:9307:67c6
  Dirección IPv6 temporal. . . . . : 2001:db8:57:968:9d58:4d51:f6dd:ab4c
  Vínculo: dirección IPv6 local. . . . . : fe80::502e:67e8:9307:67c6%3
  Dirección IPv4. . . . . : 192.168.10.2
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::%3
                                           192.168.10.1
  
```

Figura 33. Direcciones IPv6 e IPv6 por DHCP.

En la siguiente imagen se muestra las capturas de Wireshark cuando el host solicita direccionamiento al Router en donde se puede ver el mensaje RA (Router Advertisement). Ver la Fig. 34.

No.	Time	Source	Destination	Protocol	Length	Info
3693	660.821185	fe80::	fe80::502e:67e8:9307:67c6	ICMPv6	86	Neighbor Solicitation for fe80::502e:67e8:9307:67c6 from 78:ca:9b:16:18:50
3694	660.821315	fe80::502e:67e8:9307:67c6	fe80::	ICMPv6	86	Neighbor Advertisement fe80::502e:67e8:9307:67c6 (sol, ovr) is at d8:c4:97:2f:27:91
3813	688.695382	fe80::	ff02::1	ICMPv6	118	Router Advertisement from 78:ca:9b:16:18:50
3828	693.456535	fe80::502e:67e8:9307:67c6	fe80::	ICMPv6	86	Neighbor Solicitation for fe80:: from d8:c4:97:2f:27:91
3829	693.457356	fe80::	fe80::502e:67e8:9307:67c6	ICMPv6	70	Neighbor Advertisement fe80:: (rtr, sol)
3831	693.973287	fe80::	2001:db8:57:968:594:e8cd:e737:889d	ICMPv6	86	Neighbor Solicitation for 2001:db8:57:968:594:e8cd:e737:889d from 78:ca:9b:16:18:50
3832	693.973427	2001:db8:57:968:594:e8cd:e737:889d	fe80::	ICMPv6	86	Neighbor Advertisement 2001:db8:57:968:594:e8cd:e737:889d (sol, ovr) is at d8:c4:97:2f:27:91
3842	698.521367	fe80::	fe80::502e:67e8:9307:67c6	ICMPv6	86	Neighbor Solicitation for fe80::502e:67e8:9307:67c6 from 78:ca:9b:16:18:50
3843	698.521577	fe80::502e:67e8:9307:67c6	fe80::	ICMPv6	86	Neighbor Advertisement fe80::502e:67e8:9307:67c6 (sol, ovr) is at d8:c4:97:2f:27:91
3948	731.237557	fe80::	2001:db8:57:968:594:e8cd:e737:889d	ICMPv6	86	Neighbor Solicitation for 2001:db8:57:968:594:e8cd:e737:889d from 78:ca:9b:16:18:50
3949	731.237699	2001:db8:57:968:594:e8cd:e737:889d	fe80::	ICMPv6	86	Neighbor Advertisement 2001:db8:57:968:594:e8cd:e737:889d (sol, ovr) is at d8:c4:97:2f:27:91
3951	731.956389	fe80::502e:67e8:9307:67c6	fe80::	ICMPv6	86	Neighbor Solicitation for fe80:: from d8:c4:97:2f:27:91
3952	731.957641	fe80::	fe80::502e:67e8:9307:67c6	ICMPv6	70	Neighbor Advertisement fe80:: (rtr, sol)
3973	737.817658	fe80::	fe80::502e:67e8:9307:67c6	ICMPv6	86	Neighbor Solicitation for fe80::502e:67e8:9307:67c6 from 78:ca:9b:16:18:50
3974	737.817873	fe80::502e:67e8:9307:67c6	fe80::	ICMPv6	86	Neighbor Advertisement fe80::502e:67e8:9307:67c6 (sol, ovr) is at d8:c4:97:2f:27:91
4089	767.233687	fe80::	2001:db8:57:968:594:e8cd:e737:889d	ICMPv6	86	Neighbor Solicitation for 2001:db8:57:968:594:e8cd:e737:889d from 78:ca:9b:16:18:50

Frame 3831: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 Ethernet II, Src: Cisco_16:18:50 (78:ca:9b:16:18:50), Dst: QuantaCo_2f:27:91 (d8:c4:97:2f:27:91)
 Destination: QuantaCo_2f:27:91 (d8:c4:97:2f:27:91)
 Address: QuantaCo_2f:27:91 (d8:c4:97:2f:27:91)
0. = 1G bit: Globally unique address (factory default)
0. = 1G bit: Individual address (unicast)

Figura 34. Captura de Wireshark entre la comunicación DHCP entre Router y Host.

La figura siguiente muestra una captura ICMPv6 en la cual se comprueba conectividad en la red y se puede observar tráfico IPv6.

No.	Time	Source	Destination	Protocol	Length	Info
508	462.852286	2001::2	2001::1	ICMPv6	172	Destination Unreachable (Port...)
510	464.641229	2001::2	2001::db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x02e5...
511	464.688845	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x02e5, ...
512	464.695016	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x02e5...
513	464.710420	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x02e5, ...
514	464.716271	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x02e5...
515	464.731895	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x02e5, ...
516	464.737752	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x02e5...
517	464.753331	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x02e5, ...
518	464.759116	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x02e5...
519	464.775811	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x02e5, ...
523	467.535521	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x2588...
524	467.547163	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x2588, ...
525	467.557006	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x2588...
526	467.569683	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x2588, ...
527	467.578465	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x2588...
528	467.593009	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x2588, ...
529	467.600444	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x2588...
530	467.614159	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x2588, ...
531	467.621095	2001::2	2001:db8:57:968:205...	ICMPv6	124	Echo (ping) request id=0x2588...
532	467.635688	2001:db8:57:968:2050:79ff:fe66:6800	2001::2	ICMPv6	124	Echo (ping) reply id=0x2588, ...

Figura 35. Captura del protocolo ICMPv6.

4.1.4.4 Diseño, configuración y simulación del SENA CIMI con SENA CASA a través de Tunneling.

Aunque el alcance del proyecto solo contempla la emulación del protocolo IPv6 en la LAN del CIMI, el objetivo de sección es simular hipotéticamente una comunicación entre dos sedes del SENA y que configuraciones se deberían realizar si en futuro se requiera, en este caso se utiliza la técnica de Tunneling. El desarrollo con mayor detalles se muestra , en el anexo **“Apéndice D. Configuración actual en la red CIMI y recomendaciones de configuración del protocolo IPv6 en los equipos activos de la LAN”**. En la sección de simulación de conectividad con otra sede. En la siguiente imagen se muestra la topología de interconexión entre la sede CIMI y otra sede del SENA llamada CASA la cual se escogió para métodos didácticos.

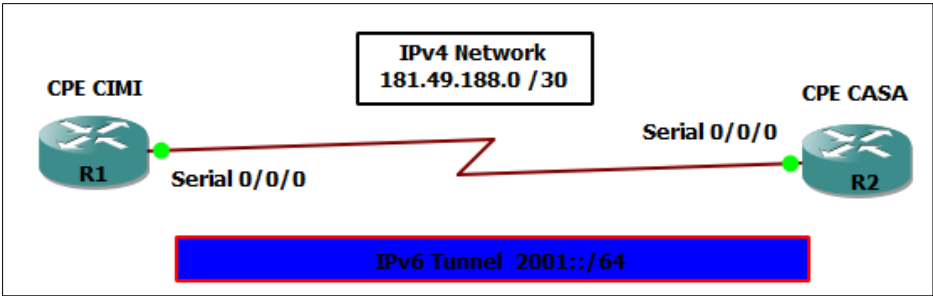


Figura 36. Topología para Tunnel entre CIMI y CASA.

Como se pudo observar anteriormente se aplicó la doble pila en la red corporativa CIMI, el paso siguiente es dar conectividad al exterior de esa red con otra sede, en este caso se ha simulado la conectividad entre las sedes CIMI y CASA, utilizando la técnica de Tunnel. En la siguiente imagen se muestra direccionamiento a utilizar para la simulación en los Router Borde de cada sede.

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gate way pre de terminado
		Dirección/Prefijo IPv6		
Router CPE CIMI	S 0/0/0	181.49.188.1	255.255.255.252	N/A
	Tunnel0	2001::1/64		N/A
Router CPE CASA	S 0/0/0	181.49.188.2	255.255.255.252	N/A
	Tunnel0	2001::2/64		N/A

Figura 37. Tabla de direccionamiento conexión WAN entre CIMI y CASA.

Se muestran los resultados de la configuración de las interfaces en cada uno de los Routers de la sede como la configuración del Tunnel. las interfaces seriales del extremo de la red CIMI y CASA, las cuales se les configura con una IPv4 publica 181.49.188. 0 /30.

```
interface Serial0/0/0
ip address 181.49.188.1 255.255.255.252
ipv6 enable
serial restart-delay 0
```

```
interface Serial0/0/0
ip address 181.49.188.2 255.255.255.252
ipv6 enable
clock rate 9600
```

Figura 38. Configuraciones interfaces seriales Router CIMI y CASA.

```
interface Tunnel0
no ip address
ipv6 address 2001::1/64
ipv6 ospf 1 area 0
tunnel source Serial5/0
tunnel destination 181.49.188.1
```

```
interface Tunnel0
no ip address
ipv6 address 2001::2/64
ipv6 ospf 1 area 0
tunnel source Serial5/0
tunnel destination 181.49.188.2
```

Figura 39. configuración del Tunnel.

Para conectar las subredes de las dos sedes se realiza la configuración del protocolo de enrutamiento dinámico OSPF para IPv4 y activar el protocolo OSPFv3 para las interfaces que tendrán habilitado IPv6. Hay que recordar que es una convivencia entre los dos protocolos por lo tanto es una red Dual Stack, conectado entre las distintas sedes a través de un Tunnel.

En la figura siguiente se muestra la configuración de OSPF tanto para IPv4 en la cual se debe configurar las redes que tiene el Router directamente conectadas como para IPv6.

```
router ospf 1
 log-adjacency-changes
 network 192.168.200.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
```

Figura 40. configuración OSPF para redes IPv4.

```
interface Serial0/0/0
 ip address 181.49.188.1 255.255.255.252
 ipv6 enable
 serial restart-delay 0
 ipv6 ospf 1 area 0
```

```
interface Serial0/0/0
 ip address 181.49.188.2 255.255.255.252
 ipv6 enable
 serial restart-delay 0
 ipv6 ospf 1 area 0
```

Figura 41. configuración OSPF para redes IPv6.

En el SENA-CASA, la cual si observamos la tabla de direccionamiento la red tendrá una IPv6 2001:db8:57:930::/64, y una IPv4 192.168.20.0/24. Ver la Fig. 32.

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2001:db8:57:930:9cae:8830:cb28:4132
Dirección IPv6 temporal. . . . . : 2001:db8:57:930:75c5:20ff:c7cc:5195
Vínculo: dirección IPv6 local. . . : fe80::9cae:8830:cb28:4132%11
Dirección IPv4. . . . . : 192.168.20.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::%11
                                           192.168.20.1
```

Figura 42. Direccionamiento IPv4 e IPv6 de host CASA.

En la siguiente sección se muestra las políticas normativas por las cuales se debe ejecutar la adopción del protocolo IPv6 en el SENA-CIMI el cual basado en un análisis de la red actual se

ha propuesto una simulación en donde configura el protocolo IPv6, teniendo estos insumos se plantean una política de implementación teniendo varios aspectos que se muestran a continuación.

4.2 Diseño e implementación de las políticas de la adopción del protocolo IPv6 y seguridad basándose en las recomendaciones del MINTIC

Partiendo del análisis del estado actual de la red convergente CIMI en esta sección se describe las políticas, buenas prácticas y normativas generadas por el MINTIC que se deben tener en cuenta en las entidades públicas en este caso el SENA-CIMI para la adopción del protocolo IPv6 en la infraestructura lógica de la red convergente.

Este Ministerio estructuró en el año 2011 un plan de acción que perseguía reunir los insumos para la construcción, promoción y divulgación de lineamientos de políticas para la adopción de IPv6 en Colombia, así mismo, proyectó una propuesta de Plan de promoción y divulgación de la adopción del IPv6 en Colombia y uno de sus logros fue la expedición de Circular No.0002 del 6 de julio de 2011 y el manual GEL V3.0, que incorporan iniciativas de políticas y planes para la adopción del IPv6, así mismo, en el 2012 realizó un el estudio llamado “Adopción de IPv6 en Colombia”, que identificó los desarrollos normativos técnicos necesarios para impulsar la adopción de IPv6 en Colombia.

Otro aspecto relevante que se debe tener en cuenta para la adopción de IPv6 es la que la Organización para la Cooperación y el Desarrollo Económico (OCDE), en la cual Colombia es miembro desde el 2017, ha establecido que la falta de implementación del protocolo IPv6, impactará el desarrollo de la economía sobre Internet en términos de reducción de innovación y de desarrollo de nuevos servicios.

Basados en las anteriores recomendaciones este documento tiene como fin diseñar y citar políticas establecidas por medio la Dirección de Estándares y Arquitectura de TI, publicó los documentos de referencia denominados “Guía de transición de IPv4 a IPv6 para Colombia” y “Guía para el aseguramiento del Protocolo IPv6”, con el fin de proporcionar lineamientos técnicos que permiten adoptar el protocolo IPv6 en el País.

4.2.1 Aspectos Regulatorios

A continuación, se dan conocer los aspectos regulatorios en la cual está basado este documento para llevar a cabo la adopción de IPv6 en la entidad pública, según Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015 y los Proveedores de Redes y Servicios de Telecomunicaciones para la adopción del protocolo IPv6 en Colombia. Se muestran los artículos en los cuales se sustenta esta documentación:

“ARTÍCULO 3. PLAZO DE ADOPCIÓN. *Las Entidades Estatales de carácter Nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso completo de transición a IPv6 en convivencia con IPv4 para el 31 de diciembre de 2019 y las Entidades del Orden Territorial que trata el artículo anterior, para el 31 de diciembre del año 2020.*

PARÁGRAFO: *Los Proveedores de Redes y Servicios de Telecomunicaciones, deberán haber realizado la transición completa de sus redes y servicios al protocolo IPv6 de forma tal que el servicio ofrecido, sea plenamente operativo.*

ARTÍCULO 4. NEUTRALIDAD TECNOLÓGICA. *El proceso de transición a IPv6 nativo debe ser compatible con los servicios y aplicaciones de IPv4, conforme a lo previsto en el numeral 6 del artículo 2 de la Ley 1341 de 2009.*

ARTÍCULO 5. TRANSICIÓN. *La transición de IPv4 a IPv6 deberá soportar los servicios de Internet en IPv6 nativo. Las versiones 4 y 6 del protocolo de Internet durante el período de transición deberán coexistir para mantener las infraestructuras de TI en operación.*

PARÁGRAFO: *Las entidades públicas de que trata el Artículo 2 de la presente Resolución, en el proceso de transición al protocolo IPv6 utilizarán como referencia los documentos denominados: “Guía de transición de IPv4 a IPv6 para Colombia” y “Guía para el aseguramiento del Protocolo IPv6”, expedidos por la Dirección de Estándares y Arquitectura de TI del Ministerio de Tecnologías de la Información y las Comunicaciones, los cuales forman parte como anexo 1 y anexo 2 respectivamente de la presente Resolución.*

ARTÍCULO 6. INDICADORES. *El Ministerio de Tecnologías de la Información y las Comunicaciones implementará dentro del SISTEMA DE INFORMACIÓN INTEGRAL DEL SECTOR DE TIC - COLOMBIA TIC, los indicadores de medición de los procesos de adopción, transición y tráfico de IPv6 en Colombia con el fin de recaudar la información adecuada que permita medir el nivel de penetración de IPv6 en Colombia.*

ARTÍCULO 7. CONTRATACIÓN TIC. *A partir de la publicación de la presente resolución, las entidades públicas deberán exigir soporte IPv6 nativo en la contratación de bienes y servicios relacionados con las TIC. Lo anterior aplica también a todos los procesos de selección de Colombia Compra Eficiente relacionados con la adquisición de equipos, redes, software, hardware, aplicaciones, comunicaciones, servicios de almacenamiento, servidores de correo electrónico, páginas web oficiales, plataformas de interacción con los usuarios, redes móviles y fijas y demás dispositivos y plataformas tecnológicas de comunicación basadas en IP; los cuales deberán desde los mismos pliegos de condiciones o lo que haga sus veces ser exigidos con soporte de IPv6 nativo en coexistencia con IPv4.*

ARTÍCULO 8. SANCIONES. *El incumplimiento de las disposiciones de la presente Resolución dará lugar a la aplicación de las sanciones respectivas de conformidad con lo establecido en las normas vigentes”.*

4.2.2. Políticas definidas para el proceso de Adopción IPv6.

Se enumeran aspectos importantes para la implementación de la adopción IPv6 en el CIMI:

A. Definición de actividades, objetivos y responsables

Es necesaria la determinación de tareas que ayuden en la realización de las actividades que a continuación se sugieren dentro del plan de adopción, además de la creación de objetivos concretos que permitan a los responsables mantener la línea de acción dentro de los alcances de cada actividad de los responsables de la red CIMI. Por ello se recomienda la creación de un cronograma de actividades que no sólo sea una guía, sino que permita el cumplimiento óptimo en el tiempo de las diferentes tareas[11].

B. Estimación de costos

Dentro del proceso de implementación según análisis previo se ve la necesidad de invertir económicamente no necesariamente en dispositivos, sino en personal capacitado para garantizar que la adopción se realice de manera correcta, por ello, una de las actividades primordiales al iniciar con el proceso de adopción es la estimación de costos, teniendo en cuenta el recurso humano[12].

C. Análisis del impacto en la red, descripción planes de contingencia y creación de protocolos de prueba por actividad.

El proceso de adopción a IPv6 trae consigo cambios que pueden generar gran impacto no sólo en la red convergente sino en el desarrollo cotidiano de las actividades a las que se dedica la entidad, por ello es importante analizar previamente los siguientes

riesgos que son algunos de muchos que se pueden correr y de esta manera buscar cómo evitarlos y/o determinar el modo de actuar cuando sucedan[12].

- Pérdida y/o fuga de información.
- Daños físicos en los equipos.
- Incompatibilidad de hardware.
- Inestabilidad de las aplicaciones.
- Problemas de funcionamiento en los sistemas operativos.
- Fallas de instalación y conexión de los equipos de red.

Es importante analizar qué pasaría si suceden los anteriores inconvenientes antes de |contingencia que se deben llevar a cabo en cada caso, realizar pruebas con una sección de la red y determinar que dichos planes den los resultados esperados.

D. Contacto con el ISP para informar acerca del proceso y acordar trabajo en conjunto.

Desde que inicia el proceso de adopción es conveniente contactar con el proveedor del servicio de Internet para empezar un trabajo en conjunto, de él no se necesita sólo la asignación del pool de direcciones, en muchas ocasiones se tienen dispositivos de la entidad en gestión del ISP o dispositivos de éste en alquiler a las entidades, lo que obliga directamente a crear en conjunto una comunicación que no impida el proceso de migración[12].

E. Solicitud pool de direcciones ante el ISP o entidad regional.

Se recomienda utilizar bloques IPv6 propios, solicitados al ISP o recibidos directamente del RIR (Regional Internet Registry); conviene revisar nuevamente las políticas del registro; por ejemplo, en el caso de un proveedor de banda ancha que está utilizando direcciones IPv4 privadas (RFC1918) para sus clientes y desea reemplazar ese direccionamiento privado por direcciones IPv6 públicas (denominadas IPv6 globales), podrá hacer un requerimiento al registro pidiendo las direcciones IPv6 necesarias para ese cambio. Dado que no todos los ISP o demás redes con las que tiene contacto la entidad disponen de IPv6, es necesario utilizar los denominados mecanismos de transición y coexistencia; básicamente, estos mecanismos permiten que IPv4 e IPv6 coexistan, e incluso que cuando IPv6 no está disponible de forma “nativa”, se pueda utilizar a través de la red IPv4, fundamentalmente mediante “túneles”.

Dado que se habla de mecanismos de transición automáticos, generalmente no se requiere configuración alguna y el sistema operativo se ocupará automáticamente de detectar si existe conectividad IPv6 en la red (por ejemplo, proporcionada por el ISP), y en caso contrario, de activar 6to4 o Teredo.

F. Actualización software en nodos y dispositivos finales para habilitar IPv6.

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; aun así, se debe definir la actualización de los sistemas operativos en equipos de comunicación y de los firmware en dispositivos de red y hacerlo con versiones originales del fabricante para evitar posibles huecos de seguridad. De

acuerdo con ello, se tendría la facilidad de habilitar Ipv6 en los dispositivos que lo soportan[12].

G. Establecer planes de direccionamiento y enrutamiento

Para definir los planes de direccionamiento y enrutamiento se deben revisar los existentes en IPv4 y coordinarlos para IPv6 lo más similares posibles a los ya configurados.

H. Monitoreo.

Normalmente las redes empresariales ponen al servicio de sus usuarios diversos sistemas de información sobre el tráfico que pasa por la red, pudiendo medirse características tales como los servicios utilizados, IP de origen y destino del tráfico e incluso sistemas autónomos entre los cuales se realiza mayor intercambio de información, a su vez, los administradores de la red necesitan tener control sobre los enlaces que forman la infraestructura de la red.

4.2.2 Modelo para el proceso de adopción IPv6.

En la figura “Modelo para el proceso de adopción IPv6 recurso humano” se proyecta para el CIMI, implementar el siguiente modelo de transición desde el punto de vista del recurso humano y recurso técnico, a seguir para todo el ciclo de IPv6.

		Diagnostico	Planeación	Implementación	Seguimiento	Lanzamiento
Recurso Humano	Gerencia de Proyecto	Revisión políticas y plan de trabajo Revisión manuales de procedimientos Requerimientos y necesidades	Determinación de alcance y tiempo, cronograma, obtención presupuesto y recursos Construcción plan de proyecto y planes específicos	Desarrollo del plan detallado de trabajo del proyecto. Desarrollo de planes específicos	Controles de riesgo. Informes de avance y gestión. Control de alcances, tiempo, costo y calidad. Mediciones de rendimiento, controles de cambios.	Acta de cierre de proyecto y aceptación. Cierre de contratos. Entrega documentación y recomendaciones generales.
	Talento Humano	Evaluación de recurso humano equipo de trabajo	Especificación de roles, perfiles y competencias	Desarrollo del equipo de trabajo	Indicadores de gestión y rendimiento. Gestión de equipo de trabajo.	Cierre de contratos
Recurso Tecnico	Infraestructura	Inventario de activos de información y servicios. Banco de configuraciones.	Especificación equipos, plan de integración. Protocolo de pruebas. Factores de éxito y aceptación	Ambiente de coexistencia y pruebas. Conexiones físicas. Gestión de calidad. Control de versiones. Validación de factores de éxito y aceptación	Controles de cambio, gestión de riesgos, gestión de calidad.	Entrega documentación y manuales de usuario. Entrega de configuraciones.

Figura 43. Modelo para el proceso de adopción IPv6 recurso humano. Adaptado de “Lineamientos para la adopción de IPv6”, por Ministerio de las Tecnologías de la Información y las Telecomunicaciones, 2017.

Recurso Técnico	Aplicaciones	Inventario de aplicaciones Evaluación estado de aplicación. Derechos de autor) Mapa de comunicaciones por cada aplicación	Especificación equipos, plan de integración. Protocolo de pruebas. Factores de éxito y aceptación	Ambiente de coexistencia y pruebas. Modificación librerías, APIs, código fuente, etc. Ejecución protocolo de pruebas	Controles de cambio, gestión de riesgos, gestión de calidad.	Puesta en producción. Entrega documentación y manuales de usuario.
	Seguridad	Revisión de políticas de seguridad. Revisión de inventario de activos	Plan de seguridad para la coexistencia de los dos protocolos. Protocolo de pruebas de aceptación.	Aseguramiento de servidores y de servicios. Ejecución de pruebas de seguridad.	Gestión de incidentes de seguridad. Gestión de riesgos de seguridad.	Ajustes a políticas de seguridad. Entrega documentación.

Figura 44. Modelo para el proceso de adopción IPv6 recurso humano parte 2. Adaptado de “Lineamientos para la adopción de IPv6”, por Ministerio de las Tecnologías de la Información y las Telecomunicaciones, 2017.

4.2.3 Diseño de Políticas de seguridad y privacidad de la información

Cuando se configura IPv6 en una red, se está habilitando el acceso a través de una nueva capa de red. Esto hace que las reglas de seguridad perimetral existentes para IPv4, ya no sean válidas para IPv6. Pero la seguridad no es solamente la configuración del cortafuegos u otro equipamiento, también son procesos y procedimientos que han sido elaborados a través de los

años que deben ser revisados y analizados. Lo importante es considerar que IP es la denominación del Protocolo Internet que involucra a los dos IPv4 e IPv6, lo que implica que esta distinción debe realizarse en los procedimientos correspondientes. El otro caso de interés es sobre el filtrado de multicast y en particular de multicast local al enlace. En IPv6 no existe dirección de difusión (o “broadcast”), y elementos como la autoconfiguración de direcciones, la detección de direcciones duplicadas y el descubrimiento de vecinos dependen del uso de multicast. El filtrado de multicast local al enlace por parte de un cortafuegos impide su funcionamiento en IPv6[12].

4.2.4 Modelo de seguridad y Privacidad de la Información (MSPI)

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación. Procedimientos de Seguridad de la Información.

En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

4.2.5 Indicadores De Gestión

El SENA CIMI deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir[13]:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

Se tiene un esquema que permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado[13].

El esquema de la imagen siguiente muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en una entidad del Estado[13].

NIVEL	DESCRIPCION
Inexistente	Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. No se reconoce la información como un activo importante para su misión y objetivos estratégicos. No se tiene conciencia de la importancia de la seguridad de la información en el CIMI
Inicial	Se han identificado las debilidades en la seguridad de la información. Los incidentes de seguridad de la información se tratan de forma reactiva. Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en el CIMI.
Repetible	Se identifican en forma general los activos de información. Se clasifican los activos de información. Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. La Entidad tiene procedimientos formales de seguridad de la Información La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. La Entidad ha realizado un inventario de activos de información aplicando una metodología. La Entidad trata riesgos de seguridad de la información a través de una metodología. Se implementa el plan de tratamiento de riesgos. La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	Se revisa y monitorea periódicamente los activos de información de la Entidad. Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. La entidad genera tráfico en IPv6.

Figura 45. Niveles de madurez del MSPI. Adaptado de “Lineamientos para la adopción de IPv6”, por Ministerio de las Tecnologías de la Información y las Telecomunicaciones, 2017.

4.2.6 Dominio de seguridad de la red

Es vital para los profesionales de la seguridad de la red del CIMI comprender los motivos de la seguridad de la red. También deben estar familiarizados con las organizaciones dedicadas a la seguridad de la red, así como con los 12 dominios de seguridad de la red que resume todo lo que se ha explicado anteriormente con respecto a las políticas de seguridad.

Hay 10 dominios de seguridad de red especificados por la Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC). Descrito por ISO / IEC 27002, estos 12 dominios sirven para organizar, a un alto nivel, el vasto reino de la información bajo el paraguas de la seguridad de la red.

Los 12 dominios están destinados a servir como una base común para desarrollar estándares de seguridad organizacionales y prácticas de administración de seguridad efectivas. También ayudan a facilitar la comunicación entre las organizaciones. Estos 12 dominios proporcionan una separación conveniente de los elementos de seguridad de la red[13]:

- Evaluación de Riesgos
- Políticas de seguridad
- Organización de Información de la seguridad
- Gestión de Activos
- Recursos Humanos de la Seguridad
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Adquisición, desarrollo y mantenimiento de sistemas de la información.
- Controles de acceso.
- Gestión de incidentes de seguridad y la información.

En la siguiente sección se realizan recomendaciones de seguridad que se deben implementar en la red SENA-CIMI, para el buen funcionamiento de la misma.

4.3 Análisis de seguridad implementada en el SENA y recomendaciones de configuración para para equipos de acceso a la Red CIMI

En esta sección tiene como fin mostrar un resume las recomendaciones de seguridad que se deben ejecutar en la Red SENA-CIMI al implementar el protocolo IPv6. Y se muestran que técnicas son utilizadas actualmente y se deben adaptar. Esto es el producto de un análisis y recopilación de los métodos de seguridad implementados en toda la Red del SENA. Vale destacar que en el anexo “Recomendaciones de Seguridad en la red CIMI”, se encuentra desarrollado con mayor detalle donde se realizan simulaciones y se muestran sus resultados.

El SENA como método de defensa y prevención utiliza la tecnología FIREEYE la cual provee visibilidad en todas las etapas del ciclo de vida del ataque y bloqueo en tiempo real de amenazas. En la siguiente imagen se muestra la características de esta Tecnología.

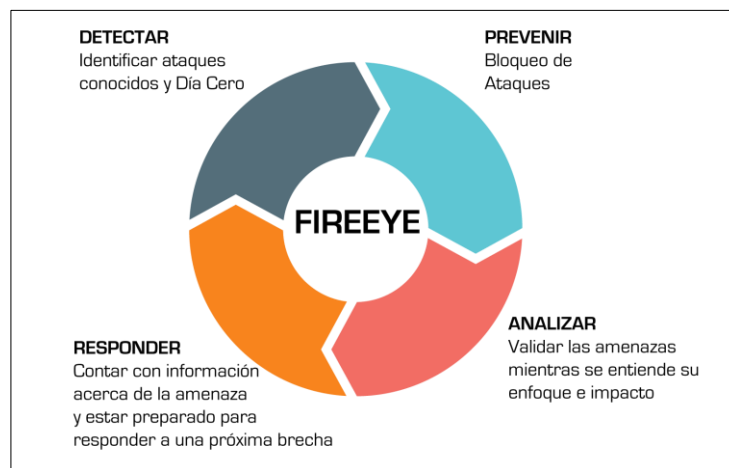


Figura 46. TECNOLOGÍA FIREEYE. Adaptado de “SENA-CIMI”, por SENA, 2019

4.3.1 Ataques y medidas preventivas a nivel de capa 2

En esta sección se muestran los diferentes ataques que se exponen a nivel de capa 2 si no se administra de manera correcta los equipos de acceso como son los Switches. Como se mencionó anteriormente en el anexo concerniente a este resultado, se esboza y se emulan las configuraciones para prevenir este tipo de suplantaciones y vulnerabilidades, Estos tipos de ataques son vulnerables tanto para IPv4 como para IPv6 ya que se realizan a nivel de capa de enlace y son:

- Mac Flooding Attack
- DHCP Spoofing
- ARP Spoofing

Otro ataque que si es propio de IPv6 es el Ataque empleando Fragmentación, El ataque típico de DoS es contra la memoria del sistema que implementa IPv6. Para cada nuevo fragmento, el sistema reserva algunas estructuras de memoria para el manejo de reensamblado, si un atacante envía una gran cantidad de fragmentos (pretendiendo ser de diferentes paquetes), el sistema puede agotar su memoria y otros fragmentos pueden ser rechazados.

Lo que se pretende demostrar en este resultado es demostrar los diferentes ataques que podrían vulnerar una red desde adentro de la LAN, tanto para el protocolo IPv6 como IPv4 si no se toman las medidas de configuración preventivas en los equipos activos de la red. En el anexo correspondiente a esta sección se enumeran y se hace una demostración de los más relevantes y que se recomiendan que se deben ejecutar en la Red CIMI.

En la siguiente sección se muestra un plan de apropiación de la adopción del protocolo IPv6 en el SENA-CIMI, donde se realiza una planeación basado en un cronograma y actividades propuestas.

4.4 Proyección del plan de apropiación para la adopción del protocolo IPv6 en la red CIMI

En esta sección se pretende aterrizar el proyecto a través de un cronograma, actividades a ejecutar y se ha formulado un proyecto productivo que se muestra como anexo “**Apéndice F. Plan de apropiación para la adopción del protocolo IPv6 en la red CIMI.**” Este proyecto tiene como fin dar mas insumos conceptuales y pedagógicos para poder ser integrado en un futuro a la comunidad estudiantil de las carreras tecnológicas afines al proyecto. Teniendo en cuenta esta realidad, el Ministerio de Tecnologías de la Información y las comunicaciones ha adelantado actividades con el fin de promover y divulgar la pronta adopción del protocolo IP versión 6 (IPv6) en Colombia, iniciando con la expedición del decreto 1078 de 2015, y la inclusión de las actividades pendientes a su implementación en la estrategia de **Gobierno en Línea** en la cual está enmarcado este trabajo de maestría.

Actualmente como se ha explicado a lo largo de este documento en el SENA CIMI utiliza el protocolo IPv4 en la configuración de todos sus dispositivos institucionales; la necesidad de adopción del nuevo IPv6 es, además de una necesidad, una obligación según los lineamientos de **Gobierno en Línea**. Las Tecnologías de la Información y las comunicaciones anunció que el 3 de febrero de 2011, la IANA (Agencia Internacional de Asignación de Números de Internet) entregó el último bloque de direcciones IP disponibles con formato IPv4, lo cual obliga a todos los países del mundo a hacer una transición al protocolo IPv6.

Aunque el Ministerio de Tecnologías de la Información y las Comunicaciones ha recomendado que la transición debió completarse para el año 2019, no ha sido posible cumplirlo.

Es importante entonces entender que "No se trata de una migración como erróneamente se

indica en muchas ocasiones, sino que ambos protocolos, IPV4 e IPV6, existirán durante algún tiempo, es decir se produce una coexistencia", en otras palabras, se debe producir una coexistencia delimitada de los dos protocolos que garantice el mantenimiento de los servicios, hasta que se utilice de manera definitiva IPv6. En la siguiente imagen se muestra el alcance que se pretende en el SENA CIMI vigencia 2020 se incluye la actividad TIC denominada "Implementar soluciones a través de plataforma tecnológica"

Actividad TIC	(¿Que se va a hacer? Qué comprende y qué NO, en qué cantidad, para cuántos usuarios, para cuántos sitios o sedes, con qué capacidad)	Productos/Entregables (Bienes y/o servicios cuantificados que se van a entregar)	Fecha de entrega estimada	Está en el plan de Gobierno en línea o Vive ¿Digital? (Si/No)
Implementar soluciones a través de plataforma tecnológica	Consultoria para la migración de IPv4 a IPv6 en el SENA CIMI.	Documento para la implementación de la Coexistencia entre IPv4 e IPv6	Marzo de 2020	Si

Figura 47. Alcance para la implementación IPv6.

Para hacer más efectivo el proceso de plan de apropiación de la adopción del protocolo en la entidad CIMI, es oportuno aplicar la metodología Planear, Hacer, Verificar y Actuar. Este proceso aplicaría una mayor eficiencia 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.

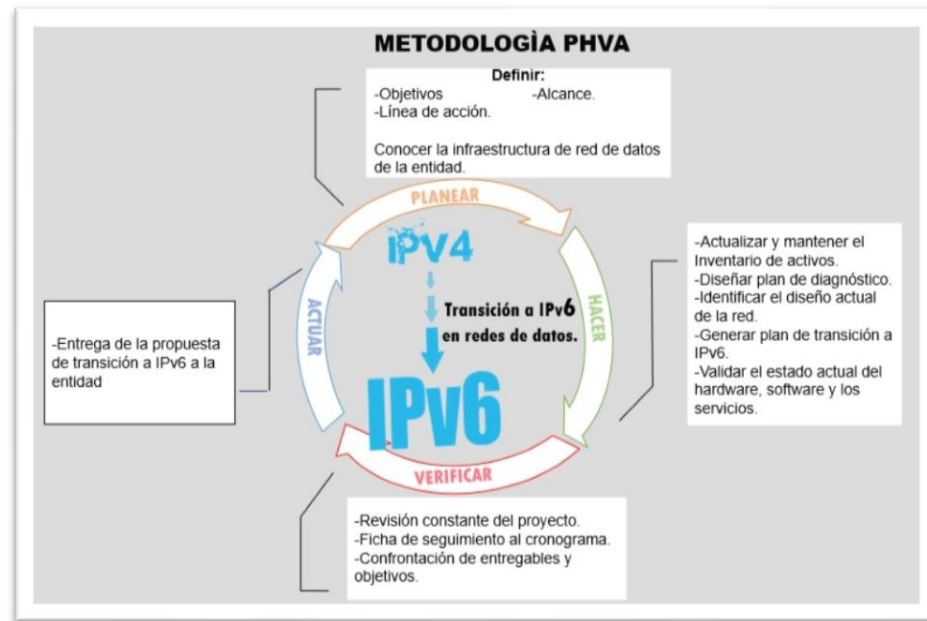


Figura 48. Metodología PHVA.

En la siguiente imagen muestra una línea de tiempo en el cual se ha proyectado este trabajo de grado y se tiene como meta implementar la adopción del protocolo IPv6 en el CIMI en el año 2020, como limite interpuesto por MINTIC.



Figura 49. Línea de tiempo de adopción.

Según las recomendaciones de las políticas de implementación que se esbozaron en este documento anteriormente se creó un cronograma con actividades alcanzables y medibles dentro de los plazos establecidos según lineamientos del MINTIC.

N°	ACTIVIDAD DEL PROYECTO	2018			2019							
		OCTUBRE	NOVIEMBRE	DICIEMBRE	ENERO	FEBRERO	MARZO	ABRIL				
1	Análisis y Diagnóstico de la Situación Actual de la red CIMI: Análisis de la topología de la infraestructura actual y su funcionamiento y construir un plan diagnóstico. Inventario de TI (Hardware, software). Validación de estado actual de los sistemas de											
2	Diseño del Plan de implementación: Diseño de direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase. Definir configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios											
3	Proyectar plan de apropiación de Funcionalidad de IPv6: 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 permit											
4	Pruebas de Funcionalidad de IPv6 y socialización de las políticas de adopción: Validar la funcionalidad de los servicios que operen en la red del CIMI. Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea la en											
5	Fase de Cierre: Acta de socialización del análisis inicial de la red, el diseño de las políticas de adopción del protocolo IPv6 y el Plan de apropiación propuesto al personal directivo y técnico del SENA CIMI.											

Figura 50. Cronograma de actividades para el proceso de adopción.

4.4 Socialización del análisis inicial de la red, el diseño de las políticas de adopción del protocolo IPv6 y el Plan de apropiación propuesto al personal directivo y técnico del SENA CIMI.

En esta sección se muestra los resultados y conclusiones que se obtuvieron después de realizar el plan de acción, promoción, sensibilización y divulgación que se realizó ante la Subdirectora del CIMI la Ingeniera Claudia Celina Marín Ariza, el Líder TI Oficina de Sistemas el Ingeniero Jesús Antonio Delgado Alba, el Coordinador Académico el Ingeniero Carlos Arturo Núñez Bohórquez, El líder de la Red de Telecomunicaciones el Ingeniero Jorge Ricardo Rozo Hernández y el Director de la Maestría de Redes y Sistemas de Comunicaciones de la USTA el Ingeniero Tito Raúl Vargas Hernández. En la siguiente imagen se evidencia la realización de la socialización.



Figura 51. Socialización y sensibilización del proyecto ante funcionarios SENA CIMI.

Para cumplir con los requerimientos de este objetivo se socializaron los resultados alcanzados de los objetivos propuestos en este proyecto como fueron:

1. Se recopila información documentada de la red actual del CIMI y cómo funciona la interconexión con el DATA CENTER y el proveedor de servicios.
2. Se presenta un diseño de un prototipo de simulación para la adopción de IPv6 en el CIMI y como se interconectaría con las diferentes sedes.
3. Se desarrolló políticas de adopción dentro de los marcos regulatorios para la adopción del protocolo IPv6.
4. Se genera un Proyecto formativo de modernización de ambientes el cual está alineado con las políticas de MinTic y el proyecto de adopción de IPv6.

En la reunión de sensibilización se realiza un acta donde se generaron unos compromisos como son:

1. Implementar la adopción del protocolo IPv6 como prueba piloto en los ambientes de formación de Telecomunicaciones y Gestión de Redes de Datos, a través de un proyecto de Actualización y Modernización Tecnológica de Centros de Formación 2019-SENNOVA.
2. Realizar recomendaciones de los pliegos con el nuevo proveedor de Servicios recomendando que los acuerdos y contratos generados se deberá exigir que la infraestructura de la red deberá soportar y estar preparada para la adopción del protocolo IPv6.

Se concluyeron aspectos importantes para la implementación del protocolo IPv6 como son:

- Topología actual de la red con sus diferentes equipos activo y software y que no hay necesidad de adquirir nuevo equipamiento según especificaciones del fabricante.
- Las fases y tiempos del proyecto de implementación de IPv6 de manera exitosa.
- La necesidad de personal calificado para capacitación y ejecución del proyecto.

- La Entidad no tendrán que preocuparse por el agotamiento de las direcciones IP (Internet Protocol) pues se garantizará que las infraestructuras de TI deben seguir conectadas con los dos protocolos coexistentes, ofreciendo a los usuarios múltiples oportunidades de seguir conectados y apuntar a los nuevos mercados y servicios que surgen alrededor de IPv6.
- El nuevo protocolo IPv6 permitirá a la entidad, introducir nuevas funciones que mejorarán aspectos tales como la seguridad informática, vista desde del escenario del funcionamiento del protocolo mismo, la facilidad para conectar una gran variedad de dispositivos de comunicaciones, de computación y de almacenamiento.

5. Conclusiones

1. Para lograr una ordenada coexistencia y transición a IPv6 en la red se debe seguir ciertos parámetros, se debe seguir una metodología de implementación , partiendo de que los equipos de la red que están operando sean funcionales para el protocolo IPv6.
2. Se debe tener en cuenta las regulaciones globales y existentes vale resaltar que este proyecto está enmarcado en los lineamientos del Min Tic en concordancia con el programa Gobierno en Línea (GEL), y el SENA a través de estas pruebas ya está preparado para la implementación de la coexistencia.
3. La transición en una red IPv6 debe ser un proceso gradual y que generalmente con los equipos actuales que actúan en las corporaciones no producirá gastos significativos a la hora de aplicar la transición.
4. Este nuevo protocolo permitirá implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos que demanda el SENA CIMI.
5. Si se quiere implementar IPv6 a nivel nacional SENA se deberá sincronizar con los tres proveedores que prestan los servicios de soporte interconectividad a la entidad.

5.1 Trabajo Futuro

1. Hacer pruebas de implementación con otras técnicas de transición de IPv6 para ver su rendimiento en la misma red SENA CIMI, implementar diferentes tecnologías de Routers y Switches, comprobar las ventajas y desventajas de aplicabilidad y throughput y realizar comparaciones de rendimiento con CISCO de esta manera se tendrá un espectro más amplio del protocolo IPv6 con respecto a su eficiencia no solo basado en CISCO.
2. El SENA CIMI es el comienzo de esta investigación y se pretende que se replique primero a nivel regional en todos los centros de formación y paulatinamente se implemente en todas las sedes del SENA a nivel nacional y se aplique los lineamientos estipulados por MinTIC con respecto a la transición del protocolo IPv6 aprovechando los beneficios.

6. Apéndices

En esta sección se referencian los anexos que ayudan a darle profundidad y sustento a cada uno de los resultados obtenidos y expuestos a lo largo de este trabajo de maestría. A continuación, se enumeran:

Apéndice A. Ante proyecto Consultoría para la adopción del protocolo IPv6 en la red del Centro Industrial de Mantenimiento Integral SENA-CIMI

(Ver archivo en medio digital)

Apéndice B. Artículo Coexistencia entre el protocolo IPv4 e IPv6 en la red convergente del Centro Industrial de Mantenimiento Integral – SENA CIMI.

(Ver archivo en medio digital)

Apéndice C. Estado de la red y equipos activos.

(Ver archivo en medio digital)

Apéndice D. Configuración LAN CIMI e implementación del protocolo ipv6 en los equipos activos.

(Ver archivo en medio digital)

Apéndice E. Recomendaciones de Seguridad en la red CIMI.

(Ver archivo en medio digital)

Apéndice F. Plan de apropiación para la adopción del protocolo IPv6 en la red CIMI.

(Ver archivo en medio digital)

Apéndice G. Documento presentado y aceptado por el MinTic del proyecto IPv6.

(Ver archivo en medio digital)

Apéndice H. Acta de socialización del modelo de adopción del proyecto.

(Ver archivo en medio digital)

7. Referencias

- [1] MinTIC, “Aseguramiento del Protocolo IPv6,” 2017.
- [2] LACNIC, “Portal IPv6 - LACNIC.” [Online]. Available: <http://portalipv6.lacnic.net/estadisticas-ipv6/>. [Accessed: 25-Aug-2018].
- [3] IETF, “IETF | World IPv6 Launch - 6th Anniversary.” [Online]. Available: <https://www.ietf.org/blog/world-ipv6-launch-6th-anniversary/>. [Accessed: 25-Aug-2018].
- [4] D. Ferney, R. Pulido, J. G. Pantoja, J. Alirio, and B. Diaz, “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.,” UNIVERSIDAD CATOLICA DE COLOMBIA, 2015.
- [5] Ministerio de las Tecnologías de la Información y las Telecomunicaciones., “Lineamientos para la adopción de IPv6,” Bogota, 2017.
- [6] MinTic, “Modelo de Seguridad y Privacidad de la Información,” Bogota, 2016.
- [7] MinTic, “Transición de IPv4 a IPv6 para Colombia,” Bogota, 2015.
- [8] J. Doyle, *Routing TCP / IP , Volume II.* .
- [9] SENA, “SENA.” [Online]. Available: <http://www.sena.edu.co/es-co/regionales/Paginas/default.aspx>. [Accessed: 08-May-2018].
- [10] LACNIC, “Políticas para la Distribución y Asignación de Direcciones IPv6.” [Online]. Available: <http://www.lacnic.net/547/1/lacnic/4-politicas-para-la-distribucion-y->

asignacion-de-direcciones-ipv6. [Accessed: 25-Aug-2018].

- [11] P. Minagricultura, “Plan Estratégico de Tecnologías de Información y Comunicación del,” 2020.
- [12] R. Realizadas, P. O. R. El, D. Catalina, F. Castro, and E. I. Electrónica, “PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS MIN TIC COLOMBIA PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS,” 2017.
- [13] MinTic, “Modelo de Seguridad y Privacidad de la Información,” BOGOTA, COLOMBIA.