

ESCUELA DE INGENIERIAS

Tema:

PLAN DE TRANSICIÓN DE IPV4 A IPV6 EN UNA RED LAN

**Proyecto de investigación previo a la obtención del título de Ingeniero en
Tecnologías de la Comunicación**

Línea de Investigación:

Tecnologías de la información y la comunicación

Autor:

Kevin Daniel Gallegos Osorio

Director:

Mg. Verónica Maribel Pailiacho Mena

Ambato – Ecuador

Febrero 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **Kevin Daniel Gallegos Osorio**, con cédula de ciudadanía **0503952194**, autor del trabajo de graduación intitulado: “PLAN DE TRANSICIÓN DE IPV4 A IPV6 EN UNA RED LAN”, previa a la obtención del título profesional de **INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN**, en la escuela de **INGENIERÍAS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, febrero 2024



Kevin Daniel Gallegos Osorio

CC. 0503952194

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**SEDE AMBATO****APROBACIÓN DEL TRIBUNAL DE GRADO****Tema:****PLAN DE TRANSICIÓN DE IPV4 A IPV6 EN UNA RED LAN****Línea de Investigación:**

Tecnologías de la información y la comunicación


Autor:

Kevin Daniel Gallegos Osorio

Verónica Maribel Pailiacho Mena, Ing. Mg.

f. **CALIFICADOR**

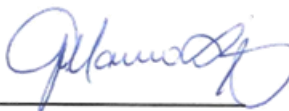
Liliana del Rocío Mena Hernández, Ing. Mg.

f. **CALIFICADOR**

Enrique Xavier Garcés Freire, Ing. Mg.

f. **CALIFICADOR**

Galo Mauricio López Sevilla, Ing. Mg.

f. **DIRECTOR ESCUELA DE SISTEMAS**

Diego Gonzalo Coca Chanaltal, Dr.

f. **SECRETARIO GENERAL PUCESA**f. 


Ambato – Ecuador

Febrero 2024

DEDICATORIA

Este trabajo se lo dedico en especial a mi madre por apoyarme en todo el camino, por los momentos buenos y malos de mi vida, ella es quien me dio las fuerzas para poder seguir adelante y nunca rendirme en especial este año que para mí fue realmente el más difícil, ella supo ayudarme a encarar todas adversidades que da la vida, estoy tan agradecido con Dios por tenerla a mi lado y quiero seguirla teniendo mucho más, todos los problemas pasan y estoy feliz de que ella siempre creyó en mí y lo seguirá haciendo, te quiero y no existen palabras para poder agradecerle todo el sacrificio tan enorme que haces por mí.

A mi hermana Jessica, tú sabes el esfuerzo que tuve que hacer para poder estar ahora, estoy tan orgulloso de ti porque eres realmente una persona increíble, en cada momento me resaltabas que agradezca a Dios por lo bueno y lo malo y a la vez me recordabas este versículo *“Escucha lo que te mando: Esfuérzate y sé valiente. No temas ni desmayes, que yo soy el Señor tu Dios, y estaré contigo por dondequiera que vayas.”* Josué 1:9, todo el apoyo que tú me das está dando frutos y este es un pequeño paso de mi vida, Gracias.

A mi hermano Miguel, de igual manera el tenerte presente en mi vida y saber que puedo contar con tu apoyo y el que tu creas en mí es una suficiente razón para poder agradecerte, y que sigamos adelante enfocados en que ningún problema es tan grande que no lo sepamos derribar.

De igual forma a mis dos sobrinos Sebastián y Nicolás que vienen siendo un pilar tan fundamental en la vida de cada uno de nosotros.

AGRADECIMIENTO

A Dios, por haberme permitido llegar a esta etapa de mi vida que algún día siempre la tuve presente y por fin lo alcancé.

A mi estimada tutora de tesis, la Ingeniera Verónica Pailiacho, la profe Verito, quiero expresar mi profundo agradecimiento por ser no solo una docente excepcional, sino también una guía en mi aprendizaje del fascinante y complejo mundo de las redes y la comunicación. A lo largo de este proceso, no solo he adquirido conocimientos académicos, sino que también he tenido el privilegio de contar con una mentora excepcional. La manera en que, en cada clase, dedicaba un momento para preguntarme cómo estaba, cómo me sentía y para compartir valiosos consejos de aporte muy significativos en mi vida. Su apoyo y paciencia incondicional, especialmente en los momentos más desafiantes, han sido fundamentales para culminar este proyecto. Valoraré siempre su dedicación y compromiso, que para mí representan el mejor ejemplo de lo que significa ser un docente excepcional. Gracias, profe, por ser más que una guía académica; por ser un ser humano excepcional. Me siento afortunado de haber tenido a la mejor tutora que podía desear.

A cada uno de mis viejos y nuevos amigos, quiero expresar mi profundo agradecimiento por el apoyo incondicional que me brindaron a lo largo de este año. Sus amistades han sido fundamentales en esta etapa de mi vida, y me siento muy contento por haberles llegado a conocer. Cada gesto de apoyo, cada risa compartida y cada momento han dejado una huella en mi vida. Estoy verdaderamente agradecido por tener amigos tan increíbles a mi lado.

A mi familia en general que siempre estuvieron presentes, y el apoyo de cada uno de ustedes para mí es y seguirá siendo muy esencial.

A todos los profesores de la escuela de ingenierías que llegaron a formar parte de este conocimiento académico que ahora tengo, Teresita, Lili, Santiago, Marcelo, Galito, Kike, Darío, Gracias.

RESUMEN

Actualmente, la creciente demanda de internet ha agotado las direcciones de IP versión 4 (IPv4), lo que impulsó que aparezca IPv6, más estable y versátil en la gestión de redes. A pesar de sus ventajas, no todas las empresas en Ecuador han adoptado IPv6, por lo que el Ministerio de Telecomunicaciones y Sociedad de la Información busca implementarlo debido a la necesidad de direcciones IP y el aumento de dispositivos.

En este contexto, surge la necesidad que las empresas necesiten un plan que les permita realizar la transición de IPv4 a IPv6, por lo que el objetivo de este trabajo es diseñar un plan de transición para una LAN tomando como caso práctico a la empresa TEIMSA (Textiles Industriales Ambateños S.A.), de la ciudad de Ambato. El proceso para la transición de IPv4 a IPv6, se lleva a cabo en tres fases las mismas que complementadas con Kanban, gestionan y procesan el trabajo de una manera ágil y con un límite de tiempo.

Como tareas fundamentales de la transición están: evaluar la infraestructura existente, abordando aspectos físicos y lógicos de la red. Selección de un mecanismo de transición, asignación del direccionamiento IPv6 y ajustes en dispositivos de red. Como resultado, se presenta el Plan de Transición de IPv4 a IPv6, que es sometido a validación por expertos, en donde se garantiza la calidad y comprensión del plan, estableciendo una base sólida para futuras implementaciones exitosas.

Palabras clave: LAN, IPv4, IPv6, IP.

ABSTRACT

Currently, the growing demand for Internet has exhausted IP version 4 (IPv4) addresses, which prompted the emergence of IPv6, a more stable and versatile one in network management. Despite its advantages, not all companies in Ecuador have adopted IPv6, so the Ministry of Telecommunications and Information Society seeks to implement it, due to the need for IP addresses and the increase of devices as well.

In this context, the necessity that companies need a plan which allows them to make the transition from IPv4 to IPv6 arises, so the objective of this work is to design a transition plan for a LAN, taking as a practical case, TEIMSA (Textiles Industrial Ambateños S.A.) company from the city of Ambato, as well. The process for the transition from IPv4 to IPv6 is carried out in three phases, which are complemented with Kanban in order to manage and process the work in an agile way, and, within a time limit.

Fundamental tasks of the transition as well are: evaluating the existing infrastructure, addressing physical and logical aspects of the network; selection of a transition mechanism, allocation of IPv6 addressing and adjustments to network devices. As a result, IPv4 to IPv6 Transition Plan is presented, which is submitted for validation by experts, where the quality and understanding of the plan is guaranteed, establishing a solid foundation for future successful implementations.

Keywords: LAN, IPv4, IPv6, IP.

ÍNDICE GENERAL DE CONTENIDOS

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD	ii
APROBACIÓN DEL TRIBUNAL DE GRADO	iii
DEDICATORIA	iv
AGRADECIMIENTO.....	v
RESUMEN	vi
ABSTRACT	vii
INTRODUCCIÓN	1
CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA.....	4
1.1 Protocolos IPv4 e IPV6	4
1.2 Mecanismos de transición de IPv4 a IPv6	9
1.3 Planes de transición de IPv4 a IPv6 aplicados	14
CAPÍTULO II. DISEÑO METODOLÓGICO	18
2.1 Caracterización de la Institución	18
2.2 Metodología de Investigación	18
2.3 Metodología de Desarrollo	20
CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN	49
3.1 Propuesta: Plan de transición de IPv4 a IPv6 en una red LAN	49
3.2 Validación de la propuesta	49
3.3. Análisis de los resultados de la validación por expertos	51
CONCLUSIONES	54
RECOMENDACIONES	56
BIBLIOGRAFÍA.....	57
ANEXOS	67

ÍNDICE DE GRÁFICOS

Figura 1. Reparto de espacios y direcciones IP	4
Figura 2. Clases y rango de direcciones IPv4	6
Figura 3. Tablero Kanban	21
Figura 4. Ubicación de TEIMSA	27
Figura 5. Topología física de la red TEIMSA	29
Figura 6. Topología lógica de la red TEIMSA	34

ÍNDICE DE TABLAS

Tabla 1. Tabla para definir la población	20
Tabla 2. Usuarios y dispositivos de la red TEIMSA edificio administrativo	28
Tabla 3. Usuarios y dispositivos de la red TEIMSA áreas operativas	28
Tabla 4. Equipamiento del cuarto de telecomunicaciones de TEIMSA	30
Tabla 5. Análisis de hardware de equipamiento de la red entorno a IPv6	32
Tabla 6. Descripción de VLAN's de la red TEIMSA.....	35
Tabla 7. Direccionamiento con IPv6 en TEIMSA	41
Tabla 8. Análisis de los resultados de la validación por expertos	52

ÍNDICE DE CUADROS

Cuadro 1. Estructura de una dirección IPv6	7
Cuadro 2. Análisis comparativo de los protocolos.....	8
Cuadro 3. Resumen de mecanismo de transición <i>Dual Stack</i> o doble pila.....	12
Cuadro 4. Resumen de mecanismos de transición en <i>Tunneling</i>	12
Cuadro 5. Resumen de mecanismos de transición en Traducción	14
Cuadro 6. Tablero de actividades Kanban	22
Cuadro 7. Actividades en Kanban Fase I	23
Cuadro 8. Descripción del software entorno IPv6	38
Cuadro 9. Actividades en Kanban Fase II	38
Cuadro 10. Actividades en Kanban Fase III	47
Cuadro 11. Experto N.1	50
Cuadro 12. Experto N.2	50
Cuadro 13. Experto N.3	50

INTRODUCCIÓN

En la sociedad moderna, las redes de computadoras juegan un papel fundamental, puesto que ayudan en el intercambio de información en todo el mundo. En estos complejos sistemas de conexiones digitales, el protocolo de internet, conocido como TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet) juega un papel fundamental. Según Comer (1996) “los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto” (p. 6). Actúan como cimientos invisibles, los mismos que proporcionan reglas y estándares que permiten que los datos se transmitan sin problemas entre todos los dispositivos conectados. Por algunos años el protocolo de internet versión 4 (IPv4) ha sido el pilar que sustenta la arquitectura de comunicación, pero por la creciente demanda de conectividad de este mundo impulsado por la tecnología, surgieron desafíos para este protocolo por la cantidad de direcciones limitadas que posee, debido a este agotamiento de direcciones por parte de este protocolo, nace el protocolo de versión 6 (IPv6) como una solución para abordar la escasez de direcciones IPv4 y así garantizar la conectividad en una escala global. Para comprender acerca del protocolo de versión 4 (IPv4) se menciona que “IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4,294,967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, multidifusión (multicast), etc” (Roman, 2017, p. 7). Esto conlleva a un crecimiento elevado de dispositivos conectados a internet a través de este protocolo y el mismo se está volviendo insuficiente.

En comparación con IPv4, IPv6 ofrece una gran cantidad de direcciones, según se explica en la investigación de Morales (2017), “IPv6 utiliza 128 bits, lo que es equivalente a 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 direcciones (3.4028237e+38 sextillones)” (p. 16). Ipv6 aborda el problema de escasez de direcciones de IPv4, la cifra de 3.4028237e+38 sextillones de direcciones disponibles a utilizarse es asombrosa, esto garantiza que cualquier dispositivo en la tierra pueda tener su propia dirección.

La acogida de este nuevo protocolo IPv6 en una red local (LAN) no conlleva solo una elección técnica, significa una evolución o un paso trascendental en el contexto actual que es la evolución de la comunicación digital global. A medida que el agotamiento de las direcciones IPv4 se está haciendo más evidente, nace una pregunta sobre cómo garantizar la conectividad y seguridad de todos los dispositivos y servicios que dependen de toda la infraestructura actual de internet, es por eso que surgen planes y guías para este proceso de transición de IPv4 a IPv6.

En este contexto, surge a nivel internacional la necesidad de adoptar este protocolo y es así que nacen procesos o guías que permiten desarrollar esta transición; por ejemplo el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia (MinTIC, 2021) , cuenta con un plan para esta transición en donde expone algunos de sus beneficios como son:

- Garantía contra el agotamiento de direcciones IP
- Mejoras en la seguridad
- Facilidad de conectividad de dispositivos
- Mejoras en el rendimiento o tiempos de respuesta
- Cumplimiento normativo

Por consiguiente, la situación problemática de esta investigación radica en la obsolescencia progresiva de IPv4 en una red LAN y la limitante capacidad de conectar nuevos dispositivos y servicios en la red local. Bajo ese contexto nace la pregunta de ¿Cómo puede una empresa implementar de manera efectiva un plan de transición de IPv4 a IPv6 en su red local?, es por eso que se desarrollaron tres preguntas esenciales en este trabajo que son:

- ¿Los estudios investigativos sobre el direccionamiento IPv4 e IPv6 consideran procesos de transición?
- ¿Cuál es el funcionamiento de una red LAN con direccionamiento IPV4?
- ¿Es posible diseñar un plan que facilite el proceso de transición de IPv4 a IPv6 en redes LAN?
- ¿Se puede aplicar algún análisis de la pertinencia técnica al proceso de transición de IPv4 a IPv6 para una red LAN?

De esta manera se trabajará con el siguiente objetivo general: Desarrollar un plan de transición de IPv4 a IPv6 para una red LAN, el mismo que se alcanzará a través de los siguientes objetivos específicos:

- Fundamentar teóricamente la transición del protocolo IPv4 a IPv6 en redes LAN.
- Diagnosticar el estado de la red LAN de una empresa mediana.
- Diseñar un plan de transición del protocolo IPv4 a IPv6 en redes LAN para una empresa mediana.
- Analizar la pertinencia técnica del plan de transición mediante el criterio de expertos.

TEIMSA (Textiles Industriales Ambateños S.A.) está ubicada en la ciudad de Ambato, es una empresa textil que se dedica a la fabricación de tejidos o telas pesadas e hilos a base de algodón de alta calidad, mantiene una infraestructura de red en IPv4 y los servicios con los que cuenta son de DHCP (Protocolo de configuración dinámica de host), DNS (Sistema de nombres de dominio) e impresión, la empresa necesita mejorar su infraestructura de red por lo que requiere determinar cuál es el proceso a seguir para implementar IPv6, pues necesita adquirir nuevas IP públicas para futuros proyectos, mejorar la conexión extremo a extremo y por ende el rendimiento de la misma.

Bajo todo lo expuesto la metodología utilizada es Kanban que desarrolla un método visual en donde se puede gestionar y procesar el trabajo de una manera ágil y por fases con un límite de tiempo lo que permite obtener como resultado un plan de transición de IPv4 a IPv6, cabe señalar que el plan se crea en base al análisis de todos los métodos existentes, tomando como base la infraestructura y necesidades de TEIMSA, como caso de estudio, lo que permite una transición fluida y eficaz de IPv4 a IPv6, asegurando que así la empresa estará preparada para el futuro en un entorno.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

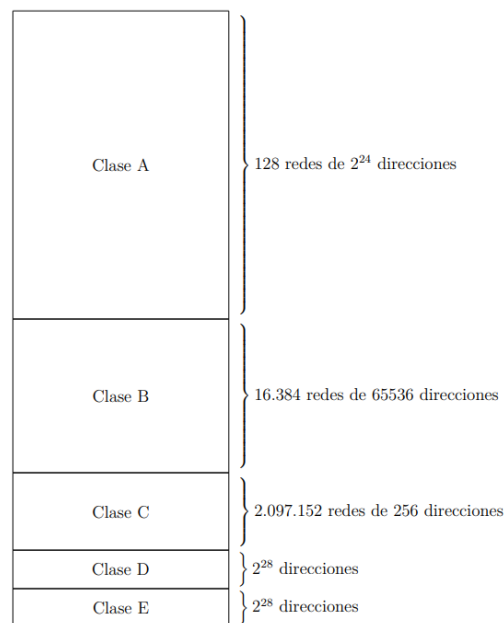
1.1 Protocolos IPv4 e IPV6

Características técnicas de IPv4

Las direcciones IPv4 tienen un formato de 32 *bits* y constituyen la columna de la comunicación en la red. Cada dispositivo dentro de una red se identifica de forma única por su dirección IP, esta se divide en cuatro segmentos llamados octetos o bytes separados por puntos, cada octeto puede tener un valor de entre 0 y 255. Es por eso que la estructura de la dirección IP permite una numeración única para cada dispositivo en la red, lo que facilita la ruta de los datos y la gestión de la conectividad.

Como se observa a continuación el reparto de dirección en IPv4:

Figura 1. Reparto de espacios y direcciones IP



Fuente: Lüke (2010)

En donde

Clase A: Rango: 1.0.0.0 a 126.0.0.0

Clase B: Rango: 128.0.0.0 a 191.255.0.0

Clase C: Rango: 192.0.0.0 a 223.255.255.0

Clase D: Rango: 224.0.0.0 a 239.255.255.255

Clase E: Rango: 240.0.0.0 a 255.255.255.255

Uno de los aspectos fundamentales en la asignación de direcciones IPv4 recae en el tipo de direcciones que mantiene, según Gonzales (2021), las clasifica en dos tipos públicas y privadas; publicas menciona que “Este tipo de direcciones son visibles desde todo Internet. Para conectarse a Internet se requiere tener una dirección IP Publica la cual es típicamente asignada por un ISP (Proveedor de servicios de Internet)” (p. 22); la afirmación que hace el autor es correcta, en el marco de direcciones IP públicas, los ISP desempeñan un rol fundamental en la asignación de estas direcciones.

Mientras tanto en las direcciones privadas se menciona que “Son direcciones IP usadas en ámbitos locales, son visibles únicamente por otros hosts dentro de la misma red de otras redes privadas interconectadas por dispositivos de capa 3. Este tipo de direcciones no tiene conectividad directa a Internet, para ello se requiere de un dispositivo intermedio (*Router, proxy*) que haga de *Gateway* mediante el protocolo NAT (*Network Address Traslation*) y permita conexión a Internet.” (p. 22), por lo tanto, estas direcciones privadas son de uso de redes locales la misma permiten una comunicación interna de dispositivos, esto mejora la seguridad en contra de amenazas externas.

Bajo el contexto de direcciones privadas se emplean rangos según su clase, como muestra la siguiente figura:

Figura 2. Clases y rango de direcciones IPv4

CLASE	RANGO
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Fuente: Gonzales (2021)

Características técnicas de IPv6

El protocolo de internet versión 6 IPv6 es la última versión de protocolos en la actualidad recae en su longitud de direcciones IP, amplía este espacio de direcciones en 128 bits, esto implica que crecimiento de cantidad de direcciones disponibles.

Según menciona Lüke (2019), “ La segunda diferencia importante es que ya no se emplean números decimales, sino que se pasan a utilizar conjuntos de cuatro dígitos hexadecimales separados por ”:”. Cada dirección al estar formada por 128 bits queda representada por 8 conjuntos de este tipo. A continuación un ejemplo de dirección IPv6: 2001:0DB8:0000:0000:0002:0000:5555:4777” (p. 26).

En el protocolo IPv6 se adopta una amplia variedad en tipos de direcciones, así, el autor Lüke (2019), las tipifican de la siguiente manera:

Direcciones de unidifusión global: Son direcciones que se asignan a hosts y que tienen validez a nivel global (Internet).

Direcciones únicas globales: Son direcciones que tienen validez únicamente dentro de un ámbito limitado como un sitio.

Direcciones de multidifusión: Son direcciones que permiten hacer envíos de multidifusión.

Direcciones de bucle local: Son direcciones que se emplean para depuración y se refieren al propio host. Sólo son válidas a nivel de host. Sustituyen a las direcciones del tipo 127.0.0.1 de IPv4 (p. 24)

Esto significa que estos tipos de direcciones IPv6 mantienen una característica fundamental que contribuyen así en su flexibilidad y adaptabilidad en la comunicación de la red. Esto incluye direcciones globales para conectividad en Internet, direcciones únicas globales para redes locales, direcciones de multidifusión para transmisión eficiente y direcciones de bucle local para propósitos de depuración. A continuación, se va a detallar la estructura de una dirección IPv6 en el siguiente cuadro, tomado como base de Fabero & Montero & Vozmediano (2016).

Cuadro 1. Estructura de una dirección IPv6

Dirección IPv6: 2001:0db8:2801:0000:0000:0000:0000/48		
2001:0db8:2801	:0000	:0000:0000:0000:0000
<p>Los primeros 48 bits 2001:0db8:2801, son llamados <i>Global Routing Prefix</i>, representa:</p> <p>200 Los 3 primeros sufijos son de asignación por la IANA.</p> <p>1:0d Los 3 siguientes son el registro que se le asigna a cada una de instituciones en nuestro caso a LACNIC.</p> <p>b8 Los dos siguientes se le asignan al proveedor de internet (ISP)</p> <p>2801: Llamados: <i>Site</i> aquí los (ISP) le dan un estilo de organización internamente, con una dirección a su sitio.</p>	<p>Los siguientes 16 bits 0000 están destinados a identificar la red o subredes.</p>	<p>Los últimos 64 bits 0000:0000:0000:0000 pertenecen a un único host o llamados <i>Interface ID</i></p>

Fuente modificada a partir de Fabero & Montero & mediano (2016)

Bajo en el contexto expuesto sobre las direcciones IPv6 Gonzales (2021), menciona la siguiente lista de características:

- Espacio de Direcciones

- Autoconfiguración
- Enrutamiento Eficiente
- Mejora QoS
- *Multi Homming*
- Movilidad
- Ampliación
- Fragmentación

El conjunto de estas características, fortalecen, mejoran seguridad, confiabilidad y la eficiencia de la infraestructura de red en IPv6.

Análisis comparativo de los protocolos

Estos protocolos son fundamentales en la infraestructura de Internet y la conectividad de redes a nivel mundial. A medida que IPv4 se encuentra en un estado de agotamiento de direcciones, IPv6 emerge como su sucesor, abordando desafíos como la escasez de direcciones y ofreciendo mejoras en términos de seguridad y eficiencia. En este cuadro que se muestra a continuación se comprenderán las diferencias clave entre estos dos protocolos.

Cuadro 2. Análisis comparativo de los protocolos

Aspecto	IPv4	IPv6
Longitud de Dirección	Direcciones de 32 bits	Direcciones de 128 bits
Notación de Direcciones	Separadas por puntos (decimal)	Separadas por dos puntos (hexadecimal)
Espacio de Direcciones	Limitado a alrededor de 4.3 mil millones	Prácticamente ilimitado (340 sextillones)
Seguridad	Requiere extensiones y soluciones adicionales	Incluye seguridad nativa (autenticación y cifrado)
Autoconfiguración de Direcciones	Requiere DHCP (<i>Dynamic Host Configuration Protocol</i>)	Admite autoconfiguración de direcciones es decir que cada dispositivo obtiene una dirección IPv6 de unidifusión global sin requerir de los servicios de un servidor DHCPv6 (SLAAC)
Soporte de Multicast	Soporte limitado	Soporte mejorado para multicast
Autenticación de Paquetes	Requiere soluciones de seguridad adicionales, como IPsec, para autenticar y proteger los paquetes de datos.	IPsec es una parte integral del protocolo IPv6 y proporciona autenticación y seguridad de los paquetes de datos a nivel de protocolo.

Encriptación de datos	Requiere implementaciones externas, como TLS/SSL, para proporcionar encriptación de datos en la capa de aplicación.	IPv6 tiene soporte nativo para encriptación y autenticación de datos a través de IPsec, lo que mejora la seguridad en la capa de red.
Protección contra ataques	Dispone de soluciones externas y configuraciones cuidadosas para protegerse contra ataques como escaneo de puertos y ataques de denegación de servicio (DDoS).	IPv6 incluye mejoras de seguridad, como la mitigación de ataques de inundación de multidifusión y la detección de vecinos falsificados, para protegerse contra ataques similares.

Fuente: Modificado a partir de Ariganello (2016); Barrientos (2016); Petersen (2011); Ruffi (2008); McDonald (2008); Dye (2008); Brady (2008); Gonzales(2021); Urueña (2005); Pérez (2010); Herrera (2010).

El análisis comparativo de los protocolos IPv4 e IPv6 revela diferencias significativas en aspectos clave que afectan la infraestructura de Internet y la conectividad de redes en todo el mundo. Mientras IPv4 se enfrenta a desafíos relacionados con el agotamiento de direcciones y la necesidad de soluciones adicionales de seguridad, IPv6 emerge como su sucesor, ofreciendo una solución integral que aborda estos problemas de manera efectiva. Con direcciones más abundantes, seguridad nativa, autoconfiguración mejorada y un enfoque simplificado en el enrutamiento, IPv6 se presenta como una opción esencial para el futuro de las comunicaciones digitales. A medida que la transición a IPv6 continúa su curso, es crucial que las organizaciones y proveedores de servicios aprovechen las ventajas de este protocolo para garantizar una conectividad eficiente y segura en un mundo cada vez más interconectado

1.2 Mecanismos de transición de IPv4 a IPv6

En el cambiante panorama de las comunicaciones globales, la transición de IPv4 a IPv6 emerge como un desafío ineludible y una oportunidad de vanguardia. A medida que los recursos de direcciones IPv4 se agotan y la demanda de conectividad continúa creciendo exponencialmente, es esencial adentrarse en los mecanismos que facilitan esta transición. En esta sección, se explorarán los ingeniosos mecanismos y estrategias diseñados para llevar a cabo una migración armoniosa de IPv4 a IPv6, allanando el camino hacia una infraestructura de red más robusta y escalable.

Según lo señalado por el Registro de Direcciones para América Latina y el Caribe (LACNIC). *Mecanismos de transición de IPv4 a IPv6*. Recuperado de <https://www.lacnic.net/5495/1/lacnic/mecanismos-de-transicion>, es que pudiera realizarse una transición hacia la nueva versión del protocolo IP sin que fuera necesario pasar de una versión a otra en forma abrupta. Con esta idea en mente, se diseñaron muchos mecanismos que pudieran ayudar a la convivencia entre ambas versiones.

Si bien en un comienzo se pensó que la adopción *gradual* de IPv6 crecería lo suficiente como para ir desplazando a IPv4 antes de su agotamiento, esto no sucedió así, razón por la cual estos mecanismos de transición tienen hoy en día una relevancia incluso mayor. Estos mecanismos de transición son cruciales para garantizar una migración suave hacia IPv6 y permitir que ambas versiones coexistan en la infraestructura de red. En América del sur, en donde LACNIC rige las políticas de asignación de direcciones IP, los mecanismos son especialmente relevantes, están diseñados específicamente para facilitar la transición en todo este continente.

Según Guarnizo (2015), los mecanismos de transición en el contexto de IPv4 a IPv6 se dividen en tres grupos principales: *Dual Stack* (doble pila), *Tunneling* (túneles) y Traducción.

- El método *Dual Stack* es considerado el más simple y económico, implica proporcionar a terminales y *routers* soporte completo para ambos protocolos, IPv4 e IPv6, permitiendo la interacción con nodos de ambas versiones sin necesidad de procesos de encapsulación o traducción costosos.

Dual Stack

- Los mecanismos de *Tunneling* implican encapsular información de un protocolo en paquetes de otro, facilitando la comunicación entre redes IPv6 aisladas sin modificar la estructura de enrutamiento. Estos pueden dividirse en túneles manuales, que requieren configuración manual, y túneles automáticos, que son dinámicos, a continuación, se enlistan cuales forman parte de este mecanismo:

Dual Stack Lite

MAP-E

MAP-T

464xlat

SIIT-DC

- Los mecanismos de Traducción permiten la comunicación transparente entre nodos que utilizan diferentes versiones del protocolo IP, realizando conversiones de direcciones y cabeceras. Un ejemplo de esto es NAT-PT (*Network Address Translation - Port Translation*), que realiza un mapeo de direcciones IPv6 a IPv4 mediante la modificación de la cabecera de los paquetes.

NAT64 DNS64

Estas categorías brindan una estructura útil para comprender y seleccionar las estrategias de transición más apropiadas según las necesidades de una organización o red.

A continuación, se presenta un cuadro resumido de algunos de los mecanismos de transición más comunes modificada según Pantoja (2016); Girón (2015); Milagros (2020), Adelaida (2010); Taffernaberry (2011); Carrasco (2015); Frere (2015); Vásquez (2017); Ianna (2023); Guarnizo (2015), junto con ejemplos de situaciones en las que pueden aplicarse. Esta información puede servir como una guía útil para tomar decisiones informadas sobre la implementación de IPv6 en una infraestructura de red:

Cuadro 3. Resumen de mecanismo de transición *Dual Stack* o doble pila

Mecanismo	Descripción	Ventajas	Desventajas	Ejemplo de Uso	Equipos
<i>Dual Stack</i>	Permite la coexistencia de IPv4 e IPv6 en una red, lo que significa que los dispositivos y la infraestructura admiten ambos protocolos.	<ul style="list-style-type: none"> - Facilita una transición gradual y controlada. -Garantiza la compatibilidad con sistemas heredados al admitir ambos protocolos simultáneamente 	<ul style="list-style-type: none"> - Aumenta la complejidad de la gestión de red al tener que lidiar con dos protocolos simultáneamente - Soporte en las aplicaciones y servidores sobre todo en (web, DNS, SMTP) 	Empresas que admiten IPv4 y desean habilitar IPv6	<ul style="list-style-type: none"> Enrutadores <i>Dual Stack</i>. Servidores <i>Dual Stack</i>. Dispositivos finales compatibles con <i>Dual Stack</i>. Personal de red capacitado en <i>Dual Stack</i>. Recursos de direcciones IPv4 e IPv6. Herramientas de monitoreo y diagnóstico compatible con <i>Dual Stack</i>.

Fuente modificado a partir de: Pantoja (2016); Girón (2015); Milagros (2020), Adelaida (2010); Taffernaberry (2011); Carrasco (2015); Frere (2015); Vásquez (2017); Ianna (2023); Guarnizo (2015).

Cuadro 4. Resumen de mecanismos de transición en *Tunneling*

Mecanismo	Descripción	Ventajas	Desventajas	Ejemplo de Uso	Equipos
<i>Dual Stack Lite</i>	Combina la coexistencia de IPv4 e IPv6 en los clientes finales y utiliza túneles IPv6 sobre IPv4 en la red de proveedores de servicios.	<ul style="list-style-type: none"> Reduce la necesidad de direcciones IPv4. -Para los proveedores de servicios de Internet (ISP), DS-Lite simplifica la gestión de direcciones IPv4 y facilita la migración a IPv6 al reducir la dependencia de IPv4 en la red. 	<ul style="list-style-type: none"> -Requiere implementación en proveedores de servicios. - DS-Lite puede no ser adecuado para organizaciones que necesitan mantener un alto nivel de soporte para IPv4, implica compartir direcciones IPv4 públicas entre múltiples usuarios. 	Proveedores de servicios que migran a IPv6 y minimizan el despliegue de IPv4.	<ul style="list-style-type: none"> Enrutadores DS-Lite. Servidores DS-Lite (incluyendo componentes como NAT64 y DNS64). <i>Firewalls</i> y dispositivos de seguridad configurados para <i>DS-Lite</i>. Servidores DNS IPv6 compatibles. Personal de red capacitado en <i>DS-Lite</i>. Herramientas de monitoreo y diagnóstico

					compatible con <i>DS-Lite</i> .
MAP-E	Los mecanismos de transición MAP (<i>Mapping of Address and Port</i>) se diseñan con la finalidad de permitir que los clientes que utilizan IPv4 puedan acceder a Internet a través de una red de transporte que opera exclusivamente en IPv6. Esto se logra mediante la aplicación de un esquema de asignación que relaciona direcciones IPv4 y puertos (TCP y UDP) con direcciones IPv6.	Permite una utilización eficiente de direcciones IPv4, múltiples clientes pueden compartir direcciones IPv4 públicas a través de la traducción y asignación de direcciones IPv6.	- Soporta el tráfico <i>Unicast</i> y no soporta y no soporta para <i>Multicast</i> - Implementar MAP puede requerir actualizaciones de hardware y software en la infraestructura de red existente, lo que puede generar costos adicionales para los proveedores de servicios.	Organizaciones con redes IPv4 que desean migrar a IPv6.	Enrutadores MAP compatibles. Servidores MAP (incluyendo componentes como NAT64 y DNS64 si es necesario). Equipos de red compatibles con IPv6. Herramientas de monitoreo y diagnóstico compatible con IPv6 y MAP. Personal de red capacitado en la configuración y el mantenimiento de MAP. Recursos de direcciones IPv4 e IPv6 disponibles. <i>Firewalls</i> y dispositivos de seguridad configurados para trabajar con MAP.
SIIT-DC	SIIT-DC (<i>Stateless IP/ICMP Translation for IPv6 Data Center</i>) es una técnica de traducción de direcciones que permite a las aplicaciones en un entorno IPv6 de un centro de datos comunicarse con recursos externos en Internet que utilizan IPv4. Lo hace traduciendo los paquetes IPv6 a IPv4 y viceversa, lo que permite que las aplicaciones continúen funcionando sin problemas en un entorno predominantemente IPv6	-Permite a las aplicaciones en un entorno IPv6 comunicarse con recursos externos IPv4, lo que facilita la adopción de IPv6 nativo en el centro de datos sin interrupciones en la conectividad hacia Internet.	-Se utiliza principalmente para permitir que las aplicaciones en un centro de datos accedan a recursos IPv4 en Internet. No es adecuado para todas las situaciones de transición IPv6, especialmente aquellas que involucran comunicación entre redes privadas.	Se utiliza en entornos de centros de datos para permitir que las aplicaciones y servicios operen en IPv6 mientras se conectan a recursos IPv4 en Internet	Enrutadores IPv6 compatibles. Servidores IPv6 configurados para operar en un entorno IPv6. Dispositivos de traducción de direcciones (para la implementación de SIIT-DC). Servidores DNS IPv6. Personal de red capacitado en la configuración y el mantenimiento de SIIT-DC. Herramientas de monitoreo y diagnóstico

					compatible con IPv6 y SIIT-DC. Recursos de direcciones IPv6 disponibles. Recursos de direcciones IPv4 (públicas) para la traducción de direcciones. <i>Firewalls</i> y dispositivos de seguridad configurados para trabajar con SIIT-DC.
--	--	--	--	--	--

Fuente modificado a partir de: Pantoja (2016); Girón (2015); Milagros (2020), Adelaida (2010); Taffernaberry (2011); Carrasco (2015); Frere (2015); Vásquez (2017); Ianna (2023); Guarnizo (2015).

Cuadro 5. Resumen de mecanismos de transición en Traducción

Mecanismo	Descripción	Ventajas	Desventajas	Ejemplo de Uso	Equipos
NAT64 DNS64	Traduce las direcciones IPv4 a IPv6 y proporciona acceso a servicios IPv4 desde redes IPv6.	-NAT Tradicional: Traduce direcciones entre conexiones de redes con direcciones IPv4 privadas. - Al permitir que dispositivos IPv6 accedan a servicios IPv4, NAT64 y DNS64 facilitan la adopción gradual de IPv6 sin interrupciones en la conectividad de Internet.	-Causa inestabilidad de las aplicaciones o fallos de seguridad por lo que este mecanismo está obsoleto.	Acceso a servicios IPv4 desde redes IPv6.	Enrutadores compatibles con NAT64 y DNS64. Servidores DNS configurados para realizar traducciones DNS64. Firewalls y dispositivos de seguridad compatibles con NAT64 y DNS64. Personal de red capacitado en NAT64 y DNS64. Herramientas de monitoreo y diagnóstico compatible con NAT64 y DNS64.

Fuente modificado a partir de: Pantoja (2016); Girón (2015); Milagros (2020), Adelaida (2010); Taffernaberry (2011); Carrasco (2015); Frere (2015); Vásquez (2017); Ianna (2023); Guarnizo

1.3 Planes de transición de IPv4 a IPv6 aplicados

La transición de IPv4 a IPv6 es un desafío global en constante evolución. Mientras que el agotamiento de las direcciones IPv4 es una realidad inminente, la adopción

de IPv6 se ha convertido en una necesidad imperante para garantizar la continuidad de las operaciones en redes de todo el mundo. En esta sección, se exploran planes de transición a diferentes escalas geográficas, desde estrategias aplicadas a nivel macro continental hasta implementaciones en América Latina y ajustes específicos en Ecuador. Estos planes ofrecen una visión detallada de cómo diferentes regiones enfrentan los desafíos y oportunidades de la transición hacia IPv6 en un contexto globalmente diverso.

Bajo todo lo expuesto se tomó en cuenta el Plan de transición de IPv4 a IPv6 para la Red de la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas en Colombia con los Autores (Potes & Gil, 2020), en donde presentan las siguientes fases:

En la Fase 1 de Análisis de Requerimientos, se lleva a cabo una evaluación que abarca desde la misión, visión y objetivos de la universidad hasta consideraciones presupuestarias e infraestructurales. En este proceso, se identifican metas técnicas y se analizan los pros y contras asociados con la adopción de IPv6, mientras se caracteriza la red existente y se propone un cambio en el direccionamiento para mejorar la seguridad y confidencialidad. En la Fase 2, conocida como Diseño Lógico de la Red, optan por la metodología de transición *Dual Stack* y se realiza una planificación de la configuración de direcciones IP, destacando la importancia de emplear direcciones IPv6 y la segmentación de la red mediante subredes. La Fase 3, enfocada en el Diseño de la Red Física, se concentra en la selección de tecnologías y dispositivos compatibles con IPv6, tales como *switches* de distribución, teléfonos, servidores web y servicios DHCPv6, destacando la necesidad de contar con equipos que sean plenamente compatibles con el nuevo enfoque.

Las conclusiones principales del plan resaltan la viabilidad de la transición de IPv4 a IPv6, respaldada por la elección de equipos de alto rendimiento, especialmente los *Switches* de Distribución. El diseño mejorado de la red, que incorpora la implementación de VLAN's, contribuye significativamente a mejorar la seguridad y la administración. Se reconoce la importancia de una transición gradual que permita

la coexistencia de IPv4 e IPv6 para una actualización progresiva de equipos y servicios. Además, se subrayan las ventajas sustanciales de IPv6 en términos de escalabilidad, seguridad, configuración y administración. Se emiten recomendaciones prácticas, como adquirir equipos certificados como IPv6 *ready*, capacitar al personal, mantener sistemas operativos actualizados y realizar auditorías de seguridad y por última instancia, se destaca la eficacia de la metodología *Dual Stack* para permitir la coexistencia eficiente de dispositivos IPv4 e IPv6 en el entorno de la red.

En tanto, en Ecuador se toma como referencia a una Propuesta de Transición de Servicios de IPv4 a IPv6 para la Red de Datos Cableada del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, con la autora Mera (2016), en donde se detallan las siguientes fases:

En la Fase 1 de Planificación, se concentra en preparar la entidad para la transición a IPv6. Esto implica la selección de personal clave, su capacitación en IPv6 y la elaboración de un cronograma para asegurar una transición eficiente. En la Fase 2 de Diseño, se realiza un análisis de la infraestructura de red existente, evaluando la topología física y lógica, la compatibilidad del hardware y software con IPv6, y seleccionan servicios y aplicaciones para su migración. Se destaca la elección del mecanismo de transición *Dual Stack*, junto con la implementación del protocolo de seguridad IPsec para salvaguardar la red. La Fase 3, Implementación y análisis de pruebas, se enfoca en la aplicación práctica de IPv6. Aquí, se planifica el direccionamiento IPv6, se actualiza el *hardware* y *software*, se configuran los equipos con IPv6 y se realizan pruebas para garantizar la accesibilidad de usuarios tanto IPv4 como IPv6. Se subraya la importancia del monitoreo continuo del tráfico de ambas versiones y se presenta un plan de contingencia para abordar posibles riesgos.

Las conclusiones de este proyecto resaltan la importancia de llevar a cabo una transición ordenada y eficaz de IPv4 a IPv6. Se destacan las ventajas de IPv6, como la autoconfiguración de dispositivos, la mejora en la calidad de servicio y la capacidad de soportar el Internet de las cosas (IoT). A pesar de los costos iniciales,

se subraya que los beneficios a largo plazo, tanto tecnológicos como sociales, justifican la inversión.

Otro caso de referencia en Ecuador es el Plan de Implementación para la migración a IPv6 en la Red de la Facultad de Ciencias Administrativas de la Universidad de Guayaquil, con el autor Guarnizo (2015), en donde menciona que:

El proceso de transición de IPv4 a IPv6 implica una serie de pasos fundamentales. En primer lugar, resaltan prepararse sin agobiarse, evaluando el impacto de la implantación del nuevo protocolo y adaptando los equipos a IPv6. La siguiente fase consiste en revisar a fondo la red, identificando servicios o aplicaciones que requieran actualizaciones para funcionar con IPv6. Posteriormente, se destaca la importancia de diseñar un calendario y ajustarse a él al establecer un cronograma para la transición. La estrategia consiste en evitar intentar solucionar todo simultáneamente, optando por identificar soluciones puntuales de doble protocolo y diseñar la red para satisfacer las necesidades a corto, medio y largo plazo. Además, se enfatiza la conciencia de las soluciones intermedias para una gestión eficiente del tráfico IPv6.

El proyecto continúa con el levantamiento de información de la red la facultad, donde se investigan los departamentos y la estructura de red, presenta un detallado mapa y un diagrama lógico de la red, subrayando componentes como *routers*, *switches*, *firewall* y estaciones de trabajo. La división de departamentos por bloques, la descripción de los equipos en los bloques detalla dispositivos como *switches*, *racks*, *patch panels* y terminales.

El análisis de resultados revela la ejecución de un análisis de tráfico en la red con IPv4 mediante *Wireshark*, destacando el problema del *broadcast*. La presentación en un simulador de la red donde exhibe la configuración en *routers* y la distribución de direcciones IPv6 por bloques. En las conclusiones, se destaca la viabilidad de la transición en la facultad, respaldada por la revisión adecuada, y se ofrecen mejoras en arquitectura y seguridad de la red. Además, se proporcionan recomendaciones prácticas, consideraciones de costos y riesgos para guiar la migración hacia IPv6.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1 Caracterización de la Institución

Textiles Industriales Ambateños S.A.-TEIMSA fue fundada en 1992 en Ambato, Ecuador, es una empresa que se dedica al proceso de fabricación, tinturado, acabado y comercialización de hilos *Open End* y tela en 100% de algodón, adicionalmente la empresa elabora suelas de zapatos.

La empresa cuenta con un total de 147 empleados, los mismos se encuentran distribuidos en diferentes áreas dentro de la empresa para asegurar que todo funcione de manera eficiente y sin problemas. Algunos forman parte del equipo administrativo, encargado de la dirección estratégica de la compañía. En conjunto con las diferentes áreas como son: Hilatura, Acabados, Inyección, Tisaje y Bodegas.

Bajo lo expuesto se hace énfasis en el departamento de Tecnologías de la Información (TI), compuesto por el Jefe del Departamento y un asistente. Opera desde un equipado *data center*, el departamento ofrece servicios como DHCP, DNS e impresión, desempeña un papel vital en el funcionamiento diario de TEIMSA. La empresa se destaca por su enfoque proactivo hacia la mejora constante de sus servicios y configuraciones de red. Como parte de esta mejora es necesario un plan de transición de IPv4 a IPv6, lo que refleja el compromiso de la empresa con la modernización y la adopción de tecnologías de vanguardia para garantizar un futuro sólido y eficiente en el mundo empresarial.

2.2 Metodología de Investigación

Enfoque de Investigación

Como parte de la investigación de este proyecto, se establece un enfoque de investigación cualitativo. Según menciona Castaño & Quecedo (2002), "En sentido amplio, puede definirse la metodología cualitativa como la investigación que produce

datos descriptivos: las propias palabras de las personas, habladas o escritas, y la conducta observable” (p. 7). En términos amplios este enfoque se centra en la recopilación de datos descriptivos o a su vez captura las experiencias individuales por parte de las personas y la observación de su comportamiento.

La investigación cualitativa es de utilidad, se puede manejar a través de aportes que brindan diversas investigaciones o planes proyectados e implementados, además toma las experiencias de los fallos que llegaron a tener, y cómo se pudieron solucionar hasta llegar a alcanzar los resultados deseados.

La investigación cualitativa es una herramienta para comprender a profundidad fenómenos sociales y humanos, pero es importante reconocer sus limitaciones en cuanto a la generalización y la necesidad de tiempo y recursos para el análisis.

Tipo de investigación

El tipo de investigación utilizado es una combinación entre la investigación de campo y la investigación bibliográfica, dado que la investigación de campo implica la recopilación directa de datos a través de entrevistas, observaciones y encuestas en el entorno de TI. La investigación de campo es aquella en la que los datos se recolectan o provienen directamente de los sujetos investigados o de la realidad en la que ocurren los hechos o datos primarios (Arias, 2012).

Entonces esta metodología permite explorar y comprender los eventos, situaciones o fenómenos en su contexto real, particularmente en operaciones y procesos de producción en el marco del caso de estudio de la empresa.

Por otro lado, la investigación bibliográfica se centra en revisar y analizar literatura académica y profesional relacionada así con la transición de protocolos de IPv4 a IPv6 y sus antecedentes. La investigación bibliográfica o documental implica examinar la literatura y documentos previamente publicados relacionados con el tema de estudio este proceso es fundamental en cualquier investigación y requiere la selección cuidadosa de fuentes de información esta investigación engloba una

serie de etapas que comprenden la observación, la búsqueda, la interpretación, la reflexión y el análisis (Matos, s.f). Este proceso permite comprender la perspectiva histórica y teórica que ayuda de mejor manera a sintetizar el contexto de estudio.

Población y muestra

La población de estudio se ha definido específicamente teniendo en cuenta al jefe del departamento de TI y a su asistente en la empresa TEIMSA. La elección de estos dos roles se basa en su papel como gestores de la infraestructura y en la toma de decisiones estratégicas relacionadas con el departamento de TI en la empresa. El jefe del departamento desempeña el rol como la formulación de políticas y la toma de decisiones de alto nivel, mientras que su asistente aporta apoyo directo en la implementación de las estrategias.

Tabla 1. Tabla para definir la población

Población	Frecuencia	Total
Jefe del departamento de TI	1	1
Asistente de TI	1	1
Total		2

Fuente: elaboración propia

Técnicas e instrumentos de recolección

Para el desarrollo de este proyecto se utilizó la técnica de la entrevista de tal manera que se pueda obtener información detallada según lo define los siguientes autores Díaz, L. Torruco, G. Martínez, M. Varela, M (2013), “Se argumenta que la entrevista es más eficaz que el cuestionario porque obtiene información más completa y profunda, además presenta la posibilidad de aclarar dudas durante el proceso, asegurando respuestas más útiles” (p. 163). Se resalta la adopción de esta técnica en una investigación, las mismas son ideales cuando se busca la comprensión detallada.

2.3 Metodología de Desarrollo

En el presente trabajo la metodología que se utilizó es Kanban. Kanban es un método visual que utiliza tarjetas para supervisar y avanzar en los procesos de un

proyecto, su objetivo es identificar y etiquetar tareas en tarjetas que se mueven a través de un tablero con columnas que representan las fases del proyecto, según las tareas avanzan, las tarjetas se desplazan de una columna a otra, que pueden ser "por hacer", "haciendo" o "terminada", es una herramienta flexible y adaptable a las necesidades específicas de cada proyecto (Garcés & Pailiacho, 2023).

Kanban se ha diseñado para adaptarse a las especificidades de la investigación, con fases o columnas que representan las etapas esenciales, las mismas son visualizadas en un tablero a través de tarjetas que consideran tareas o actividades y el estado en el que se encuentra cada una de ellas, como se muestra a continuación en un ejemplo de un tablero Kanban:

Figura 3. Tablero Kanban



Fuente: elaboración propia

Dentro de esta figura se visualizan 3 columnas principales que son: por hacer o las propuestas, se hace o en proceso y hechas o las terminadas. Es aquí donde se reflejan todas las actividades y el avance en el que se encuentran.

A continuación, se presentan los procesos desarrollados para la creación de este plan que facilite la transición de IPv4 a IPv6 en una red LAN, siguiendo la metodología previamente descrita, el mismo consta de una serie de actividades que proporciona los pasos concretos y una guía en el proceso de migración de direcciones IPv4 en una red local.

Planificación de actividades

Se describen las tareas o actividades involucradas en la creación de este plan, es importante recalcar que para la documentación del mismo utilizando Kanban, estas actividades se organizan en conjuntos que reflejan la actividad o fase específico de nuestro proyecto y está estrechamente vinculado con el progreso general del plan.

Además, para determinar las Fases que contempla la propuesta del plan de transición se definen fases y actividades a partir de las experiencias de investigación de Mera (2016) y Guarnizo (2015), quienes tienen propuestas que conjugadas permiten solventar las necesidades de la presente investigación.

Cuadro 6. Tablero de actividades Kanban

Por hacer	En proceso	Hechas
Fase I Análisis de la situación actual: Recopilación de información técnica con el personal responsable. Análisis de la infraestructura de la red LAN existente. Análisis de los servicios de red.		
Fase II Diseño de la Solución: Selección del método de transición. Cambios de la infraestructura. Plan de Direccionamiento IPv6. Cambios en los servicios de red. Levantamiento de la infraestructura general de la red.		
Fase III Implementación y Pruebas: Dejar los lineamientos establecidos para que las empresas realicen sus pruebas e implementación.		
Validación por expertos del plan de transición: Selección de expertos. Definición de una rúbrica. Análisis de resultados.		

Fuente: elaboración propia

A continuación, se proporciona la información detallada de cada una de las actividades que comprende este plan:

Fase 1: Análisis de la situación actual.

Cuadro 7. Actividades en Kanban Fase I

Por hacer	En proceso	Hechas
	Fase I Análisis de la situación actual	
Fase II Diseño de la Solución		
Fase III Implementación y Pruebas		
Validación por expertos del plan de transición		

Fuente: elaboración propia

En la fase 1, que se centra en el Análisis de la situación actual, se inició recopilando información técnica en colaboración con el equipo encargado del departamento de Tecnologías de la Información (TI) en TEIMSA. Esta recopilación se llevará a cabo a través de una entrevista diseñada para abordar una serie de preguntas clave con el objetivo de comprender a fondo el estado actual de la red. Posteriormente, se procedió a analizar detalladamente las respuestas de los dos entrevistados y la información recopilada para mejorar la comprensión de la situación actual.

Pregunta 1:

- ¿Puede describir brevemente la infraestructura de red actual en TEIMSA?

Análisis:

La infraestructura de red actual en TEIMSA se basa en el protocolo IPv4. En cuanto a dispositivos de red, la organización utiliza *routers*, *switches*, *firewall* y puntos de acceso. Además, la infraestructura incluye servidores que ofrecen servicios como almacenamiento de datos, aplicaciones empresariales, correo electrónico y bases de datos. La seguridad de la red se refuerza mediante un *firewall*, y se utilizan VLAN's para la gestión.

Pregunta 2:

- ¿Cuántos usuarios y dispositivos trabajan en la empresa incluyendo la cantidad de dispositivos y la topología general?

Análisis:

Actualmente, TEIMSA cuenta con una distribución de 80 puntos de red en todas sus plantas, lo que sugiere que se atiende a un número significativo de usuarios que dependen de la infraestructura de red. Además, de 10 dispositivos inalámbricos

para brindar conectividad a dispositivos móviles y portátiles, y sigue una topología de red en estrella.

Pregunta 3:

- ¿Cuáles son los servicios de red con los que trabaja actualmente la empresa?

Análisis:

Principalmente el servicio de acceso a internet, adicional a eso la empresa actualmente utiliza servicios de impresión, *Active Directory* (que funciona como servidor DNS) y mantiene el servicio de DHCP para la asignación de direcciones IP en su red.

Pregunta 4:

- ¿Cuáles son los motivos principales detrás de la decisión de TEIMSA de llevar a cabo la transición de IPv4 a IPv6?

Análisis:

TEIMSA ha tomado la decisión de realizar la transición de IPv4 a IPv6 debido a su compromiso con la vanguardia tecnológica y la preparación para el futuro. Esta elección se basa en el reconocimiento de que las direcciones IPv4 están agotándose y que IPv6 ofrece numerosas ventajas, especialmente en términos de seguridad y escalabilidad. Al optar por IPv6, TEIMSA se asegura de estar preparada para abordar los desafíos y demandas tecnológicas emergentes en un entorno de red en constante evolución.

Pregunta 5:

- ¿Cuáles son los objetivos clave que se esperan alcanzar con la transición a IPv6?

Análisis:

Los objetivos clave que se buscan alcanzar con la transición a IPv6 en TEIMSA incluyen la expansión de la capacidad de direcciones IP para respaldar el crecimiento futuro, mejorar la seguridad de la red mediante protocolos más robustos, facilitar la implementación de servicios avanzados, como el Internet de

las cosas (IoT), y garantizar la continuidad operativa y la compatibilidad con estándares tecnológicos globales.

Pregunta 6:

¿Qué recursos se asignarán al proceso de transición, incluyendo personal, hardware y software?

Análisis:

El proceso de transición a IPv6 en TEIMSA implicará la asignación de recursos clave. En cuanto al personal, se contempla la colaboración de expertos externos especializados en redes, además del compromiso del personal interno del departamento de TI de la empresa. En lo que respecta al hardware, se utilizarán los equipos existentes en la infraestructura de la red, y se considerará la adquisición de hardware adicional según las necesidades específicas de la transición. Asimismo, se evaluará la incorporación de software complementario si es requerido para facilitar el proceso de transición. La combinación de estos recursos busca garantizar una implementación exitosa y eficiente de IPv6.

Pregunta 7:

¿Cuáles son las proyecciones de costos e inversión en equipos basados en IPv6?

Análisis:

Las proyecciones de costos e inversión en equipos para la implementación de IPv6 en TEIMSA se encuentran sujetas a la aprobación de la gerencia. Aunque se busca optimizar los gastos, se reconoce que la empresa no escatimará en los recursos necesarios, los equipos actuales son compatibles con IPv6. Sin embargo, se espera que los servicios profesionales de personal externo para asistir en la transición generen costos adicionales. Estas proyecciones financieras se mantienen flexibles y se ajustarán de acuerdo a las necesidades y decisiones gerenciales.

Pregunta 8:

- ¿Cuáles son las características actuales de los equipos utilizados en la infraestructura de red para admitir IPv6?

Análisis:

La empresa cuenta principalmente con equipos que son compatibles con IPv6 en su infraestructura de red. Sin embargo, se reconoce que existen algunas máquinas que carecen de esta compatibilidad. Por lo tanto, es esencial elegir un método adecuado para garantizar que todos los dispositivos en la red puedan operar sin problemas durante la transición a IPv6.

Pregunta 9:

- ¿Cuáles son los plazos de tiempo previstos para la implementación del plan de transición a IPv6 en TEIMSA?

Análisis:

La empresa TEIMSA está interesada en que se proporcionen plazos de tiempo en el desarrollo y entrega del plan de transición a IPv6. Sin embargo, se destaca la importancia de que esta transición sea fluida y segura, priorizando la calidad sobre la prisa.

Análisis de la infraestructura de la red LAN existente.

Caracterización de la red existente en TEIMSA

Textiles Industriales Ambateños S.A.-TEIMSA, está ubicado en la ciudad de Ambato parroquia de Santa Rosa, sector parque industrial, calle Bernardino Echeverría. En la siguiente figura se indica gráficamente la ubicación de la empresa.

Figura 4. Ubicación de TEIMSA



Fuente: google maps.

Análisis de la infraestructura física de la red de datos

TEIMSA cuenta con una sólida infraestructura física que comprende diversos bloques o áreas fundamentales para sus operaciones.

Edificio Administrativo

El Edificio Administrativo no solo alberga el principal centro de telecomunicaciones de TEIMSA (*Data Center*), sino que también incluye el espacio destinado al Área Administrativa General. Este conjunto es esencial para la gestión centralizada y coordinación de las actividades empresariales, así como para las funciones administrativas que respaldan todas las áreas operativas. Se divide en varios departamentos, tales como Gerencia General, Contabilidad, Recursos Humanos, Ventas y Tecnologías de la Información (TI). Cabe recalcar que en el edificio administrativo también funciona la dependencia del área de sublimado y el departamento médico. Estos espacios proporcionan lugares especializados para la toma de decisiones clave, la gestión financiera, la administración de recursos humanos, el impulso de las estrategias de ventas y el soporte tecnológico, consolidando así un centro administrativo integral para TEIMSA. A continuación, se

detallan los usuarios (representa a las personas que interactúan con la tecnología) y dispositivos (son las herramientas físicas utilizadas por los usuarios en sus tareas diarias como impresoras y computadoras) estimados para el edificio administrativo:

Tabla 2. Usuarios y dispositivos de la red TEIMSA edificio administrativo

Usuarios	18
Dispositivos	26

Fuente: elaboración propia

Áreas Operativas

TEIMSA se estructura en diversas áreas operativas, cada una desempeñando un papel fundamental en el proceso productivo. Estas áreas, que comprenden Acabados, Inyección, Tisaje, Hilatura, y Bodegas. Cada área operativa cuenta con su propio espacio administrativo para coordinar y supervisar actividades específicas, garantizando una gestión eficiente y especializada en cada departamento. A continuación, se detallan los usuarios y dispositivos estimados para cada área, proporcionando una visión más precisa de la infraestructura y las necesidades tecnológicas en cada departamento.

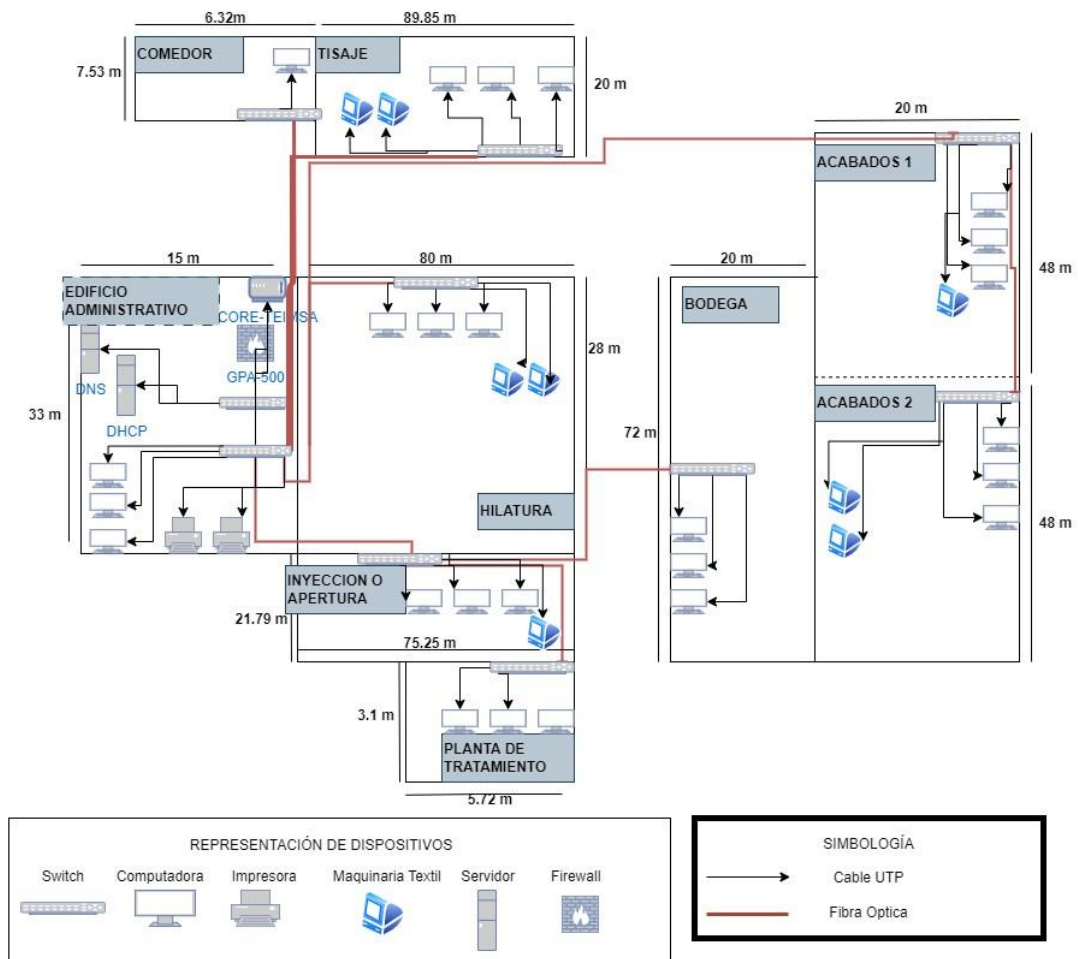
Tabla 3. Usuarios y dispositivos de la red TEIMSA áreas operativas

Áreas	Usuarios	Dispositivos
Acabados	15	15
Inyección	13	13
Tisaje	21	21
Bodega	3	4
Hilatura	12	12

Fuente: elaboración propia

A continuación, en la siguiente figura se muestra como está distribuida la red de datos para poder comprender de mejor manera la distribución de las áreas:

Figura 5. Topología física de la red TEIMSA



Fuente: Departamento de Tecnología y Sistemas TEIMSA (2023)

Data Center

Este centro de procesamiento de datos pertenece a la empresa TEIMSA y se encuentra en el departamento de Tecnologías de la Información. Ha sido diseñado y construido siguiendo estándares de seguridad como el diseño eléctrico, ambiental y protección de riesgos físicos, la misma se utiliza para interconectar todos los equipos de la red de datos que a continuación se presentan los más generales.

- La red local se basa en tecnología Ethernet.
- La topología a utilizarse es tipo estrella.
- Configuración de VLAN's (red virtual de área local).
- El cableado vertical en esta red es fibra óptica multimodo.
- El cableado horizontal de esta red es UTP categoría 6.

En la Figura 5, se evidencia la conexión del Switch Core principal con los de distribución, de igual manera la conexión de los servidores físicos. Es fundamental aclarar que, en el marco de este proyecto, se prioriza y enfoca principalmente en conexiones cableadas para la red local de datos. La decisión de centrarse en esta modalidad se justifica dado que la gran mayoría de las conexiones en TEIMSA se establecen a través de redes cableadas. Es importante señalar que las conexiones inalámbricas son limitadas, siendo utilizada por un número reducido de usuarios dentro de la infraestructura.

A continuación, se detallan los equipos con los que cuenta la empresa en cuanto a comunicación de red:

Tabla 4. Equipamiento del cuarto de telecomunicaciones de TEIMSA

Cantidad	Equipos	Marca/Modelo
1	Switch de Core Cisco Catalyst Capa 3 3560X, 24 Puertos 10/100/1000 IP Base	WS-C3560X-24TS-S
2	Switch de Distribución Cisco Catalyst 2960-X 48 GigE/4 * 1G SFP LAN Base	WS-C2960X-48TS-L
8	Switch de Distribución Cisco Catalyst 2960-X 24 GigE 4 * 1G SFP LAN Base	WS-C2960X-24TS-L
1	<i>Firewall gate protect</i>	GP500
1	Controladora CISCO WLC (<i>Wireless LAN Controller</i>) 2504	Cisco
9	<i>Access Point</i> Cisco AIR-CAP1602i-A-K9	Cisco
4	<i>Access Point</i> Cisco AIR-CAP2602i-A-K9	Cisco
2	Servidores físicos	HP

Fuente: Departamento de Tecnología y Sistemas TEIMSA (2023)

Cableado Horizontal y Vertical

En cuanto al cableado horizontal, en TEIMSA se emplea el estándar UTP categoría 6, proporcionando una sólida base para la interconexión del *backbone* (IDF) con las diversas áreas de trabajo en la empresa. Este tipo de cable se caracteriza por su capacidad para transmitir datos a altas velocidades y con baja interferencia electromagnética. En la infraestructura final, se han instalado cajas superpuestas que incluyen tapas de protección, diseñadas específicamente para resguardar las conexiones RJ-45 destinadas a la transmisión de datos. Este enfoque no solo asegura una conectividad eficiente y confiable en toda la red, sino que también facilita futuras expansiones y actualizaciones del sistema, cumpliendo con los

estándares de calidad necesarios para el óptimo funcionamiento de los sistemas de comunicación de TEIMSA.

El sistema de Cableado Vertical y *Backbone* juega un papel esencial al establecer conexiones entre el cableado de distribución de cada área de la empresa mediante el uso de fibra óptica, facilitando así la comunicación efectiva con los equipos ubicados en el *Data Center* (MDF). En el contexto específico de TEIMSA, el *backbone* se enlaza a través de fibra óptica con diversas áreas designadas como áreas de distribución (IDF), ubicadas en espacios clave como el comedor, tisaje, hilatura, inyección, planta de tratamiento, bodega, y acabados 1 y 2, es importante destacar, que la fibra óptica utilizada para estas conexiones es de tipo multimodo, asegurando una transmisión eficiente de datos entre el *Data Center* y las distintas áreas distribuidas estratégicamente dentro de la empresa. Este enfoque garantiza una conectividad robusta y de alto rendimiento en toda la infraestructura de TEIMSA.

Áreas de trabajo

En las áreas de trabajo, los dispositivos finales, como computadoras e impresoras, utilizan *patch cords* de categoría 6e con conectores RJ-45. Estos cables, esenciales para la conexión y transmisión de datos, llegan a través de canaletas, proporcionando una organización estructurada y segura para el cableado en el entorno laboral. De este modo, se garantiza una conexión confiable y de alta velocidad entre los equipos terminales y el sistema de red, contribuyendo a un rendimiento óptimo en la comunicación de datos.

Análisis de hardware de equipamiento de la red

A continuación, se llevó a cabo un análisis del inventario de hardware suministrado por el Departamento de Tecnologías y Sistemas de la empresa. Este inventario abarca tanto los equipos de comunicaciones de red como los dispositivos finales, incluyendo computadoras portátiles e impresoras. El objetivo primordial de este análisis es evaluar el estado actual de cada uno de estos componentes y determinar

su capacidad para admitir el protocolo IPv6. Se examinó las características individuales de cada dispositivo, desde sus capacidades de conectividad hasta sus especificaciones técnicas, con el fin de obtener una comprensión integral de la infraestructura de red existente y garantizar su preparación para la implementación y gestión efectiva de IPv6. Este proceso permitirá identificar posibles actualizaciones necesarias y asegurar un rendimiento óptimo en el entorno de red.

Tabla 5. Análisis de hardware de equipamiento de la red entorno a IPv6

Equipo	Cantidad	Marca	Modelo	Tiempo de uso	Soporte IPv6
<i>Firewall</i>	1	<i>Gateprotect</i>	GPA 500	2 años	Si
<i>Switch Core Catalyst</i> capa 3	1	Cisco	WS-C3560X-24TS-S	3 años	Si
<i>Switch</i> de Distribución Cisco <i>Catalyst X 48</i>	2	Cisco	WS-C2960X-48TS-L	3 años	Si
<i>Switch</i> de Distribución Cisco <i>Catalyst X 24</i>	8	Cisco	WS-C2960X-24TS-L	3 años	Si
Controladora Wlc	1	Cisco	(<i>Wireless Lan Controller</i>) 2504	3 años	Si
<i>Access Point</i> Cisco	9	Cisco	AIR-CAP1602i-A-K9	3 años	Si
<i>Access Point</i> Cisco	4	Cisco	AIR-CAP2602i-A-K9	3 años	Si
Servidor 1	1	HP Windows 19	Proliant	2 años	Si
Servidor 2	1	HP Windows 19	Proliant	2 años	Si
Computadores	60	Windows	-	3 años	Si
Impresoras	3	Kyocera	-	2 años	Si
Maquinaria de Diseño	4	Cixing	STL-72inch-8G	4 años	No
Maquinaria Telar	15	Toyota	710-280T	9 años	No
Maquinaria para suelas	6	Lesmak	-	6 años	No
Maquinaria para tinturado	5	Miditec	-	7 años	No

Fuente: Departamento de Tecnología y Sistemas TEIMSA (2023)

El análisis del *hardware* del equipamiento de red en relación con IPv6 revela un panorama general positivo en términos de compatibilidad. El *firewall* principal, un *Gateprotect* GPA 500, así como todos los switches de la red, incluyendo el *Switch Core Catalyst* capa 3 y los *Switches* de Distribución, cuentan con soporte para IPv6. En cuanto a los servidores físicos, tanto los dos servidores HP *Proliant*, tienen la capacidad de soportar IPv6, lo que es esencial para asegurar una integración

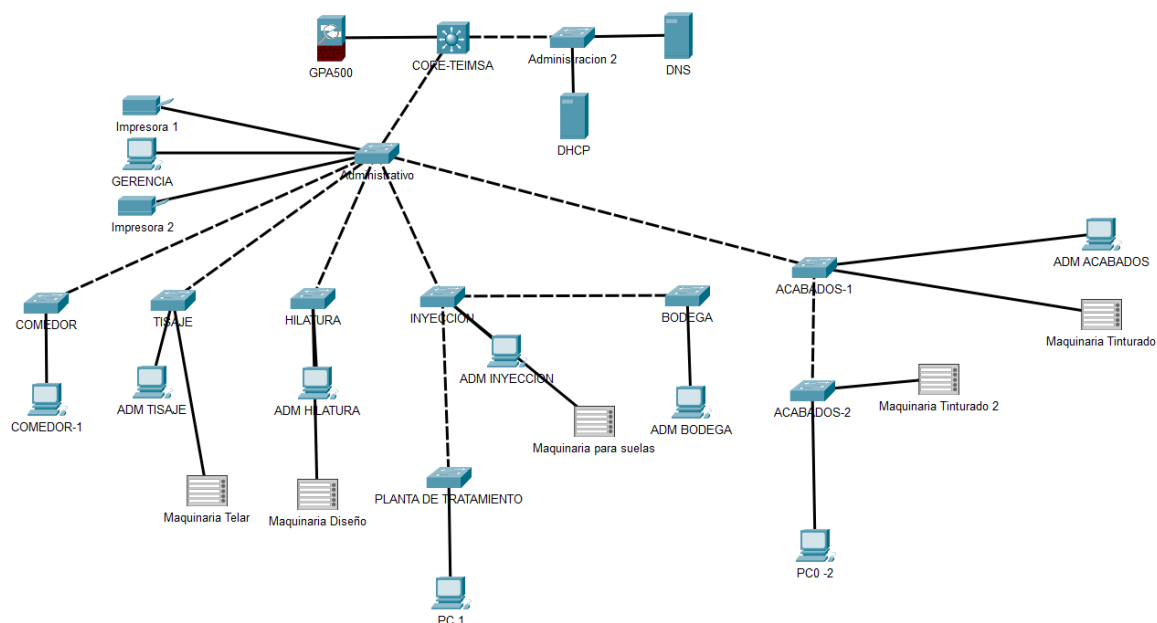
adecuada con la red. Además, la totalidad de los computadores, compuestos por sistemas operativos Windows, y las 3 impresoras Kyocera, también admiten IPv6. En cuanto al análisis de la maquinaria actual de la empresa, presenta un enfoque negativo, la misma trabaja mediante el protocolo IPv4, careciendo de compatibilidad con IPv6, estas máquinas de diseño, telar, suelas y tinturado necesitan de conectividad a la red, utilizan un software utilizado por el operador y necesitan operar en red.

Es relevante destacar que, aunque el análisis se basó en un muestreo de 60 computadoras, que incluye tanto computadoras de escritorio como portátiles, todos los sistemas examinados presentaron capacidad para soportar IPv6. Este resultado sugiere que la infraestructura de red y los dispositivos finales están en una posición sólida para hacer frente a los requisitos de la próxima generación de protocolos de Internet. Sin embargo, se recomienda realizar una evaluación continua y actualizaciones según sea necesario para mantener la compatibilidad a medida que evolucionan los estándares tecnológicos.

Análisis de la infraestructura lógica de la red de datos

Es esencial profundizar en la caracterización lógica de la red para un análisis. Por esta razón, se presenta en la figura 6 la representación detallada de la distribución lógica de la red, ofreciendo una visión clara y estructurada de cómo se organiza y opera digitalmente:

Figura 6. Topología lógica de la red TEIMSA



Fuente: Departamento de Tecnología y Sistemas TEIMSA (2023)

Es importante resaltar que, en la figura presentada, se ha simplificado la representación visual de los dispositivos finales en cada área utilizando solo una PC como ejemplo, de igual manera la maquinaria para área. La realidad es que cada área cuenta con múltiples dispositivos, como computadoras, impresoras e maquinaria industrial.

La red LAN de Textiles Industriales Ambateños S.A. se configura con un direccionamiento IPv4 de clase C (192.168.X.X) y una máscara de red de 255.255.255.0. Para optimizar la administración de la red, TEIMSA ha implementado la segmentación de la red en VLAN's (Redes Locales Virtuales). Esta estrategia permite organizar de manera eficiente los recursos de red y mejorar la seguridad y el rendimiento. La distribución de las VLAN's y sus respectivos direccionamientos IPv4 se presenta detalladamente en la Tabla 6. Este enfoque no solo facilita la gestión de la red, sino que también proporciona flexibilidad para asignar recursos según los requisitos específicos de cada grupo de usuarios o dispositivos.

Tabla 6. Descripción de VLAN's de la red TEIMSA

Nombre VLAN	Descripción	ID VLAN	ID RED	USUARIOS
Servidores	Segmentación de red dedicada para servidores en la red.	12	192.168.X.X	254
Troncal	Segmentación de la red dedicada a maquinaria en el área de Inyección y Acabados.	13	192.168.X.X	254
Datos-Tactiles Prod Impresoras	Segmentación de la red dedicada al área de administración.	14	192.168.X.X	254
Maquinaria Telares Toyota	Segmentación de la red dedicada a maquinarias en el área de Hilatura y Tiraje.	15	192.168.X.X	128
Wlc – Ap's	Segmentación de la red dedicada a la administración de la red inalámbrica.	16	192.168.X.X	254
WIFI - TEIMSA	Segmentación de la red dedicada a dispositivos inalámbricos personal Gerencia.	17	192.168.X.X	254
WIFI TEIMSA - Invitados	Segmentación de la red dedicada a dispositivos inalámbricos invitados.	18	192.168.X.X	254
Enlace - <i>Firewall</i>	Segmentación de la red desinada a gestión de seguridad.	30	192.168.X.X	30

Fuente: Departamento de Tecnología y Sistemas TEIMSA

Análisis de los servicios de red

DNS

En el análisis actual de DNS, se destaca la presencia de un solo servidor, generando preocupaciones sobre la redundancia y la continuidad operativa. Esta configuración puede resultar en un riesgo en caso de un posible fallo del servidor único, afectando la resolución de nombres y el acceso a los recursos en la red. Es necesario realizar una evaluación más detallada del rendimiento del servidor, centrándose en la velocidad de resolución de nombres y considerando posibles medidas para mejorar la eficiencia.

En relación con *Active Directory*, se observa la eficacia en la organización y replicación de datos entre controladores de dominio. No obstante, se plantea la recomendación de una revisión minuciosa de las políticas de seguridad

implementadas para garantizar su alineación con las mejores prácticas de seguridad.

En la empresa se está utilizando como nombre de dominio teimsa.int, el mismo se utiliza en los registros de DNS y en la configuración de *Active Directory*.

Servicio de Internet

En relación al servicio de Internet en TEIMSA, se reconoce su papel esencial para la conectividad externa y el acceso a recursos en línea. Actualmente, la empresa cuenta con un proveedor de servicios que suministra un ancho de banda adecuado.

DHCP

En la evaluación del servicio DHCP en la infraestructura de red, se destaca su función esencial al facilitar la asignación dinámica de direcciones IP de manera eficiente y automática a los dispositivos conectados. La agilidad en la incorporación de nuevos dispositivos y la eliminación de configuraciones manuales son puntos fuertes. Sin embargo, se señala la necesidad de una gestión cuidadosa del rango de direcciones IP disponible para prevenir conflictos y agotamiento. En términos de seguridad, se resalta la importancia de medidas preventivas contra asignaciones no autorizadas y ataques potenciales. La revisión constante de registros y la detección proactiva de posibles problemas aseguran la integridad y la disponibilidad continua del servicio DHCP en la red empresarial.

Cabe destacar que, actualmente, para los puntos de red en la VLAN 14, se dispone de 252 direcciones IP disponibles. De estas, las primeras 200 direcciones son asignadas estáticamente las mismas se destinan exclusivamente a dispositivos internos de la empresa, como computadoras e impresoras, mientras que las 52 direcciones restantes son distribuidas mediante DHCP, estas direcciones están destinadas a las necesidades temporales de invitados o clientes que puedan tener a la empresa. Lo expuesto se impone a requerimientos antepuestos de gerencia.

Impresión por red

El servicio de impresión por red en la infraestructura empresarial desempeña un papel fundamental al facilitar la impresión compartida entre diversos dispositivos, mejorando la eficiencia y colaboración. Actualmente, en el edificio administrativo, cuenta con 3 impresoras de la marca Kyocera, distribuidas estratégicamente en las áreas de contabilidad, gerencia y secretaría gerencial. Estas impresoras están exclusivamente destinadas al personal administrativo y se configuran individualmente bajo el dominio de cada usuario. Cabe señalar que es importante destacar que las direcciones IP de estas impresoras ingresan estáticamente en la VLAN 14 y el controlador de impresión reside en un servidor, en otras palabras, el servidor facilita la impresión a través de la red, al gestionar y dirigir las operaciones de las impresoras conectadas, asegurando una gestión eficiente de la red y un acceso controlado a estos recursos compartidos. Cabe resaltar que las impresoras no son compartidas entre áreas; por ejemplo, el personal de contabilidad solo tiene acceso a la impresora de contabilidad y no puede imprimir en la impresora de gerencia. Este enfoque permite una administración personalizada de las impresoras, manteniendo la seguridad y eficacia del servicio en el entorno empresarial.

Software

Como una parte principal en operaciones de la empresa en ámbito administrativo utilizan un software especializado que agiliza procesos en áreas muy específicas como son contabilidad, gerencia y ventas, adicional la maquinaria cuenta de igual forma con un software, como se ve a mayor detalle en el cuadro 8. Descripción del software entorno IPv6. Sin embargo, su profundización se ve limitada debido a las recomendaciones y directrices del departamento de Tecnologías de la Información (TI), que prioriza el análisis de servicios como DNS, DCHP y el servicio de impresión. Es importante señalar que los softwares que manejan en la actualidad, no es de desarrollo interno y, en caso de requerir actualizaciones o modificaciones, es preciso recurrir al personal propio del software para llevar a cabo cualquier ajuste necesario.

Cuadro 8. Descripción del software entorno IPv6

Software	Descripción	Soporte a IPv6
Adempiere	Es una aplicación integral que ayuda a gestionar y coordinar procesos de datos en diversas áreas como contabilidad, gerencia ventas, y en bodegas.	SI
Software Cixing	El software ayuda en las operaciones y diseño en telas, como modificación y control de diseños textiles.	NO
Software Lexmark	El software permite a esta maquinaria diseñar patrones detallados y personalizados para modelos en suelas de calzado.	NO
Software Miditec	El software de esta maquinaria permite establecer colores para la tintura y el acabado mediante temperaturas y especificaciones de color.	NO
Software Toyota	El software de esta maquinaria establece configuración y abordaje de ciertos tipos de tejido, como la tensión del hilo, el tipo de puntada entre otros.	No

Fuente: Departamento de Tecnología y Sistemas TEIMSA

Fase 2: Diseño de la solución

Después de obtener un conocimiento acerca del estado actual de la red, se procede con la Fase II: Diseño de la solución, en donde ingresa en especial énfasis la selección del método de transición. A continuación, se presenta el tablero Kanban con las actividades de la siguiente fase II:

Cuadro 9. Actividades en Kanban Fase II

Por hacer	En proceso	Hechas
		Fase I Análisis de la situación actual
	Fase II Diseño de la Solución	
Fase III Implementación y Pruebas		
Validación por expertos del plan de transición		

Fuente: elaboración propia

Selección del método de transición

En el contexto de la transición de IPv4 a IPv6 para TEIMSA, es esencial subrayar la importancia de realizar este proceso de manera gradual y manteniendo la interoperabilidad entre ambas versiones del protocolo. La elección de un mecanismo de transición adecuado es crucial para preservar las inversiones en infraestructuras IPv4 y garantizar una coexistencia eficiente. La migración en una organización como TEIMSA puede presentar desafíos, pero estrategias como el mecanismo *Dual Stack* o Doble pila, que combina la coexistencia de IPv4 e IPv6, ofrecen ventajas significativas. En base al análisis del capítulo 1, cuadro 3 en donde se presenta una comparativa detallada de diversos mecanismos de transición, y en base al análisis de la situación actual de la red, se opta por el mecanismo de doble pila o *Dual Stack* para la empresa. Esta elección permite la coexistencia de IPv4 e IPv6 sobre la infraestructura IPv4 existente. La adopción de *Dual Stack* se fundamenta en la importancia de tomar en cuenta a la maquinaria que no es compatible con IPv6, las mismas son el desarrollo económico mayoritario de la empresa, es por ello que se justifica la elección técnica de elegir este método el más apropiado para la empresa y se asegura que los servicios y dispositivos compatibles con IPv6 operen con dualidad y manejar la coexistencia de ambos protocolos minimizando cualquier impacto negativo en la productividad y eficiencia de la empresa.

Cambios de la infraestructura

El análisis realizado en el Capítulo 1 en cuanto al análisis de la situación actual de la empresa ha revelado que la infraestructura actual de TEIMSA posee una configuración tecnológica actualizada y eficiente en su gran mayoría. Tanto los equipos de comunicación Cisco, que presentan una dualidad para la adopción de IPv4 e IPv6, como los servidores, computadoras e impresoras, están alineados con las demandas tecnológicas actuales. No obstante, la maquinaria que actualmente posee la empresa no mantiene la compatibilidad con el protocolo IPv6, pero al ser estas un fundamental activo de la empresa trabajarán con IPv4. En virtud de estos hallazgos, se establece que, en este momento, no se justifica la implementación de

modificaciones en la infraestructura, los recursos y dispositivos actuales cumplen satisfactoriamente con los requisitos operativos y de conectividad. La infraestructura quedaría como se presenta en la figura 5 en la Topología física de la red.

Plan de Direccionamiento IPV6.

Para la elaboración del plan de direccionamiento IPv6, se ha seleccionado la siguiente dirección IP versión 6 como caso de estudio:

2001:acad:db8:0000:0000:0000:0000, con una máscara de red de /48. En su notación simplificada, esta dirección se presenta como 2001:acad:db8::/48, cabe señalar que dirección IPv6 presentada corresponde a una IP de documentación presentada por la LACNIC, y al momento de su implementación se cambiarían los tres primeros hextetos, los mismos como se presentó en la estructura IPv6 en el capítulo 1, cuadro 1 son asignados por el proveedor.

Para llevar a cabo el *subnetting* con los bits restantes en la dirección IPv6 2001:acad:db8:0000:0000:0000:0000, se procedió a determinar la cantidad de las VLAN's, manteniendo la misma cantidad de VLAN's que en IPv4 (8 en este caso). Para ello, la LACNIC propone que al diseñar un plan de direccionamiento esta sea ordenada y siguiendo mejores prácticas, proponiendo un /64.

2001:acad:db8:0001::/64

2001:acad:db8:0002::/64

2001:acad:db8:0003::/64

2001:acad:db8:0004::/64

2001:acad:db8:0005::/64

2001:acad:db8:0006::/64

2001:acad:db8:0007::/64

2001:acad:db8:0008::/64

En la tabla, se presenta el subneteo de VLAN's en IPv6:

Tabla 7. Direccionamiento con IPv6 en TEIMSA

Nombre VLAN	ID VLAN	RED IPv6	Gateway
Servidores	12	2001:acad:db8:0001::/64	2001:acad:db8:0001::1/64
Troncal	13	2001:acad:db8:0002::/64	2001:acad:db8:0002::1/64
Datos-Tactiles Prod Impresoras	14	2001:acad:db8:0003::/64	2001:acad:db8:0003::1/64
Maquinaria Telares Toyota	15	2001:acad:db8:0004::/64	2001:acad:db8:0004::1/64
Wlc – Ap's	16	2001:acad:db8:0005::/64	2001:acad:db8:0005::1/64
TEIMSA	17	2001:acad:db8:0006::/64	2001:acad:db8:0006::1/64
TEIMSA - Invitados	18	2001:acad:db8:0007::/64	2001:acad:db8:0007::1/64
Enlace - Firewall	30	2001:acad:db8: 0008::/64	2001:acad:db8: 0008::1/64

Fuente: elaboración propia

Cambios en los servicios de red

Cambios en los servicios de DNS y Active Directory

La transición hacia IPv6 en los servicios de DNS (Sistema de Nombres de Dominio) y *Active Directory* se basa en la dualidad adoptada por un servidor de TEIMSA. Este servidor ha sido analizado para admitir tanto IPv4 como IPv6, lo que significa que puede resolver nombres de dominio y gestionar servicios en ambas versiones del protocolo IP. En este contexto, es necesario implementar ajustes específicos para garantizar la compatibilidad con IPv6 en los registros DNS.

Configurar registros AAAA, se asocian nombres de dominio con direcciones IPv6, permitiendo que el servidor de DNS resuelva solicitudes en ambas versiones de IP. De manera similar, en el servicio de *Active Directory*, los registros DNS para los controladores de dominio reflejan esta dualidad, incorporando tanto direcciones IPv4 como IPv6.

El primer paso para la configuración establecer y habilitar en su tarjeta de red la dirección IPv6 para el servidor DNS, según el direccionamiento presentado servidores se encuentra en la VLAN 12 por lo tanto la dirección 2001:acad:db8:0001::2/64 se agregará a este servidor.

El sistema operativo de este servidor es Windows server 2019, se utiliza el asistente para poder llevar a cabo los siguientes pasos:

Paso 2: Cabe señalar que para este paso las configuraciones de zonas en el servidor, previamente ya fue instalado DNS por IPv4.

Zona directa: La zona directa se utiliza para traducir nombres de dominio a direcciones IP, aquí se agrega una nueva zona con el nombre que se tiene previamente creada en IPv4: Teimsa y agregamos la dirección IPv6 2001:acad:db8:0001::2

Zona de búsqueda inversa: La zona de búsqueda inversa se utiliza para traducir direcciones IP a nombres de host, la configuración de esta zona es crear una nueva, una nueva zona de búsqueda inversa para IPv6 aquí solicita Prefijo de la dirección IPv6 con la dirección y su prefijo será: 2001:acad:db8:0001::/64. El asistente una vez que se haya ingresado con la dirección de prefijo solicitará un nombre de archivo y será: Teimsa.int, se detallara lo que se está creando y se pulsara finalizar. Ahora se tendrá que agregar Registros nuevos en el tipo será Puntero (PTR), el mismo es el registro de un recurso del dominio, define direcciones IP en todos los sistemas en notación invertida, En este caso se busca en examinar el nombre del host que será Teimsa y queda de la siguiente manera Teimsa.Teimsa.int y creamos el Registro.

Cambios en los servicios de DHCP

La transición a IPv6 implica adaptar el Protocolo de Configuración Dinámica de Host (DHCP) para ofrecer soporte a la asignación dinámica de direcciones IPv6. En este contexto, se implementa el DHCPv6, que permite la asignación automática de direcciones IPv6 a dispositivos en la red de TEIMSA.

De manera similar con el servidor de DNS, el primer paso o cambio radica en habilitar y asignar una dirección IPv6 en la tarjeta de red por lo tanto la dirección 2001:acad:db8:0001::3/64 se agrega a este servidor.

Procediendo con el siguiente paso con la ayuda del asistente de configuración en DHCP, se crea un ámbito nuevo para IPv6 el mismo con un nombre de ServerDhcpv6 y en su descripción Red_local, una vez creado el nombre y descripción, a continuación solicita ingresar la dirección IPv6, se necesita que distribuya la siguiente dirección 2001:acad:db8:0003::, esta IP corresponde a la VLAN 14 en donde están ubicados las IP's para usuarios finales es decir computadoras e impresoras, a continuación se escribe el intervalo de direcciones IPv6 en inicio y el final:

```
2001:acad:db8:0003::500/64 // Dirección inicial del rango
```

```
2001:0db8:2801:0003::800/64 // Dirección final del rango
```

Se agregó las direcciones de inicio y final, ahora es importante configurar el ámbito en cuanto a lista de direcciones IPv6 de servidores DNS y se agrega la dirección de DNS 2001:acad:db8:0001::2, valida y agrega el servidor DNS.

Cambios en el servicio de impresión

En el proceso de adaptación al protocolo IPv6 en el servicio de impresión, se llevaría a cabo una actualización de la configuración para incorporar direcciones IPv6 a las impresoras existentes. Este cambio implica asignar a cada impresora una dirección IPv6 dentro de la red empresarial. Una impresora que actualmente posee la dirección IPv4 "192.168.X.X" como las impresoras mantienen una dualidad se le asigna una dirección IPv6 como "2001:0db8:2801:0003::801/64".

Una vez que se ha asignado la dualidad a estas impresoras mediante una única dirección IPv6, el procedimiento para actualizar la configuración recae en la administración del servidor. En las herramientas administrativas del servidor, se ubica la impresora específica que se pretende configurar para IPv6. En las propiedades de la impresora, se procede a agregar un nuevo puerto utilizando el asistente correspondiente. En este proceso, se selecciona la opción de dirección IPv6 y se proporciona la dirección específica, en este caso, 2001:0db8:2801:0003::801. Posteriormente, se finaliza el asistente y se aplica los

cambios para asegurar que la impresora esté ahora correctamente configurada para operar a través de IPv6.

Una vez completa la configuración en el servidor, la configuración de la impresora en cada computadora implica dirigirse a la sección de impresoras en la configuración del sistema. Se localiza la impresora que está vinculada al servidor y que ha sido recientemente configurada con IPv6. Si la impresora ya cuenta con una dirección IPv6 asignada, tiene que ser detectada automáticamente en la red.

Cambios en el servicio de internet

En el servicio de Internet, el cambio clave reside en la adopción de conectividad IPv6 con el proveedor de servicios de Internet (ISP). Esto implica configurar la infraestructura de red de la empresa para que pueda comunicarse y recibir tráfico IPv6 a través de su conexión a Internet. Para ello por parte de la red LAN se manejará los siguientes comandos:

Se ingresa a la interfaz gig0/0/0 para asignar una dirección de *Gateway* a la red LAN.

```
Switch-Core (config) #int gig0/0/0
Switch-Core (config-if) #ipv6 add 2001:acad:db8:0001::1/64
Switch-Core (config-if) #no shut
Switch-Core (config-if) #exit
```

En esta interfaz se establece la IP del giga es decir esto hacia un proveedor (ISP), para ello se utiliza un conector SX *transceiver* para fibra óptica el mismo es un adaptador que tiene como entrada fibra y la trasforma a giga.

```
Switch-Core (config) #int gig0/1/0
```

Esta dirección es proporcionada por el ISP

```
Switch-Core (config-if) #ipv6 add <Dirección_IPv6> / <Longitud_del_prefijo>
```

```
Switch-Core (config-if) #exit
```

Configuración de una ruta estática de igual manera estas direcciones son proporcionadas por el ISP

```
Switch-Core (config) #ipv6 route <Dirección_IPv6> / <Longitud_del_prefijo>
<Dirección_IPv6>
```

```
Switch-Core (config) #exit
```

```
Switch-Core (config) #ipv6 unicast-routing
```

```
Switch-Core (config) #
```

Levantamiento de la infraestructura general de la red.

En el *Switch Core Catalyst* capa 3 como caso de estudio se implementaría el siguiente cambio:

Se habilita IPv6

```
Switch-Core(config)# ipv6 unicast-routing
```

Se crea subinterfaces es decir, son interfaces lógicas creadas dentro de una interfaz física del *router* por cada VLAN en este caso se crea la subinterfaz 2 que es de servidores:

```
Switch-Core(config)# interface GigabitEthernet0/1.1
```

```
Switch-Core(config-if)# encapsulation dot1Q 2
```

```
Switch-Core(config-if)# ipv6 address 2001:0db8:2801:0001::1/64
```

```
Switch-Core(config-if)# no shutdown
```

A Continuación, se habilita la petición mediante DHCP

interface VLAN 4 // Es la interfaz de la VLAN en este caso 12

Se ingresa el siguiente comando indicando que se necesita asistencia en solicitudes de DHCP al servidor de DHCP

```
ip helper-address 2001:acad:db8:0001::3
```

En los Switchs Core Catalyst de distribución como caso de estudio se implementará el siguiente cambio:

Ingresando al rango de puertos destinados

```
Switch(config)# int range fa0/1 - 24
```

Establece el modo de puerto a acceso

```
Switch(config-if-range)# switchport mode access
```

Asigna el puerto a la VLAN 4

```
Switch(config-if-range)# switchport access VLAN 12
```

```
Switch(config-if-range)# exit
```

Dispositivos finales

Para implementar la transición a IPv6 en los dispositivos finales, como computadoras e impresoras, será necesario realizar los siguientes cambios:

Asignación y habilitación de Direcciones IPv6:

En el contexto de la transición a IPv6 en la infraestructura de red de TEIMSA, se llevó a cabo una evaluación de los dispositivos finales, como se detalla en la tabla 5. Se observó que las computadoras son compatibles con IPv6, lo que permite avanzar con la asignación de direcciones únicas a cada dispositivo. En cuanto en las computadoras del edificio de administración VLAN 14, cada dispositivo final

recibe una dirección única, permitiendo su identificación y comunicación en la red IPv6 de TEIMSA.

Fase III Implementación y pruebas.

Continuando con el desarrollo del trabajo de investigación, a continuación, se muestra el tablero Kanban:

Cuadro 10. Actividades en Kanban Fase III

Por hacer	En proceso	Hechas
		Fase I Análisis de la situación actual
		Fase II Diseño de la Solución
	Fase III Implementación y Pruebas	
Validación por expertos del plan de transición		

Fuente elaboración propia

Dejar los lineamientos establecidos para que las empresas realicen sus pruebas e implementación implica consolidar los procesos y directrices clave que guiarán a las organizaciones a través de la transición de IPv4 a IPv6, como la ejecución de cambios en la infraestructura de red, la implementación de nuevas configuraciones en dispositivos y servicios, y la realización de pruebas para asegurar la correcta funcionalidad del entorno IPv6.

✓ Simulación en el entorno

La creación de laboratorios de prueba que simulen el entorno de red es fundamental para la transición a IPv6. La elección de GNS3 como herramienta de simulación recae en sus múltiples ventajas como en su capacidad para generar escenarios altamente realistas. El proceso implica levantar la infraestructura de la red mediante la simulación, configurando tanto IPv4 como IPv6 en los *routers*, *switches*, dispositivos finales y servidores. Esta simulación ayuda a una representación del entorno antes de la implementación real, permitiendo ajustes y validaciones.

✓ Pruebas

Una vez que se simula el entorno, se procederá a realizar pruebas que abarcan la verificación de la conectividad, compatibilidad y comunicación. Estas pruebas pueden identificar posibles errores que permitirá solucionarlos de manera oportuna, y a la vez contribuye a modificarlos antes de implementarlas en el entorno de real. La detección y solución temprana de problemas garantiza una transición más fluida y minimiza posibles interrupciones o fallos en la red.

✓ Capacitación al personal

Asegurarse de que el personal esté familiarizado con herramientas y procedimientos específicos de IPv6.

✓ Aplicar al entorno real

En la aplicación al entorno de real, se espera una transición gradual es decir paso a paso y de manera coordinada. El proceso tiene que priorizar la estabilidad operativa y minimizando el impacto en las operaciones diarias. La experiencia adquirida en la simulación ayudará en una implementación eficiente y sin contratiempos.

Monitoreo Continuo es preciso mantener sistemas de gestión de red que ayude a evaluar el rendimiento de la red después de la implementación.

Validación por expertos del plan de transición

En esta sección de Validación por expertos del plan de transición, se llevan a cabo tres generalidades: la selección de expertos, la definición de una rúbrica y, finalmente, el análisis de los resultados obtenidos. La elección de expertos con experiencia asegura una revisión especializada del plan de transición. La rúbrica proporciona un marco detallado para evaluar cada aspecto del plan, garantizando así una evaluación objetiva y completa. Este proceso de validación, se abordara en el Capítulo 3 de la investigación.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1 Propuesta: Plan de transición de IPv4 a IPv6 en una red LAN

En vista que el estudio se enfocó en el caso práctico de la infraestructura de TEIMSA. Se procede a generalizar la propuesta, diseñando un plan que proporciona una guía hacia la migración de IPv4 a IPv6 en una red de área local, la misma se encuentra disponible en el Anexo 3. Este documento ofrece una guía clara en donde se abarcan diversas etapas del proceso y además se incluyen los entregables asociados a cada fase. Su estructura proporciona una visión muy sistemática que asegura la transición ordenada, minimizando posibles inconvenientes.

3.2 Validación de la propuesta

De acuerdo a los elementos establecidos en la planificación de la investigación, la validación de la propuesta se realizó mediante la técnica de validación por expertos, la misma que permite recopilar la apreciación de profesionales con experiencia en áreas afines a la temática, respecto a la estructura, contenidos, aspectos técnicos, entre otros, del plan de transición desarrollado. A continuación, se documenta el proceso de validación:

Selección de expertos

En la Selección de expertos, se plantea un perfil profesional con el propósito de validar de manera efectiva el plan de transición propuesto. Este perfil está elaborado, para contar con la participación de personal con experiencia y conocimientos especializados en áreas relevantes para la transición. La selección de expertos se basa en criterios que aseguren la representatividad de diversas perspectivas y la capacidad de evaluar críticamente los componentes clave del plan, como se detalla a continuación en los siguientes cuadros:

Cuadro 11. Experto N.1

Nombre:	Ing. Marcelo Balseca
Título:	Ingeniero en sistemas
Cargo Actual:	Docente Universitario PUCE sede Ambato
Especialización:	Magister en Gerencia Informática mención en Desarrollo de Software y Redes
Años de experiencia:	21 años de experiencia

Fuente elaboración propia

Cuadro 12. Experto N.2

Nombre:	Ing. Wiliam Atiencia
Título:	Ingeniero en sistemas
Cargo Actual:	Jefe de sistemas y tecnologías empresa TEIMSA
Especialización:	Magister en gerencia informática
Años de experiencia:	32 años de experiencia

Fuente elaboración propia

Cuadro 13. Experto N.3

Nombre:	Ing. Dennis Chicaiza
Título:	Ingeniero en sistemas
Cargo Actual:	Docente Universitario de la Universidad Técnica de Ambato
Especialización:	Magister en Gerencia Informática mención en Desarrollo de Software y Redes
Años de experiencia:	20 años de experiencia

Fuente elaboración propia

Matriz de validación por expertos

Definir una matriz para el proceso de validación por expertos, es un paso fundamental después de la presentación del plan de transición final ante dichos expertos. Esta matriz se introduce como una herramienta estructurada y sistemática que permite a los expertos evaluar de manera objetiva y detallada cada componente del plan.

Al presentar esta matriz, se busca proporcionar un marco claro y específico que guíe su evaluación, asegurando que cada aspecto del plan sea revisado. Para la elaboración del instrumento, al no estar establecidas o no existir rúbricas específicas para validar planes de transición, se analizaron diversos trabajos en donde los siguientes autores: Valverde, García, Hernández & Morales (2017); Maldonado & Conde (2009), Cordero, García y Maraón (2011) y López (2023), proponen distintos criterios de calidad respecto a la estructura y redacción de documentos técnicos así como recomendaciones y propuestas de rúbricas aplicadas para la evaluación de manuales o guías. Los autores detallan buenas

prácticas para evaluar este tipo de trabajos en base al establecimiento de criterios relacionados al contenido, redacción, estructura, entre otros. De lo expuesto y a partir del análisis de las referencias mencionadas, se establecen los siguientes criterios:

- Claridad y comprensión en donde el criterio que evalúa es que el plan presenta documentación de manera transparente, utilizando un lenguaje claro asegurando que la información sea útil para la audiencia involucrada en la transición de IPv4 a IPv6.
- Estructura y Organización este criterio busca asegurar que las fases de la transición estén claramente definidas en el plan, proporcionando una guía lógica para la implementación.
- Detalles Técnicos evalúa la presencia de detalles técnicos y comprensibles en cada fase del plan de transición. Se verifica que los procedimientos y mecanismos técnicos estén descritos de manera clara y adecuada para el personal en el área de tecnologías de la información.
- Actualización y Relevancia en donde el criterio que evalúa es que el plan está basado en información actualizada, estructurado de manera coherente y que la metodología propuesta sea relevante para la transición IPv4 a IPv6.
- Recursos considerados este criterio evalúa la suficiencia de la información técnica tomada en consideración para la elaboración del plan.
- Facilidad de uso y disponibilidad este criterio garantiza que el plan sea flexible y compatible como para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones específicas.

Estos criterios buscan que el plan presentado sea una herramienta informativa, una guía práctica y ejecutable que tenga como objetivo una transición en una red LAN, la misma se encuentra disponible en el anexo 4.

3.3. Análisis de los resultados de la validación por expertos

Después de la validación del plan de transición por parte de los expertos como se puede evidenciar en los anexos 5, 6 y 7, se procede al análisis de los resultados

obtenidos utilizando para ello una tabla en donde se centraliza cada valoración asignada en relación a cada criterio.

Tabla 8. Análisis de los resultados de la validación por expertos

CRITERIO	EXPERTO 1	EXPERTO 2	EXPERTO 3	RESULTADO DE LA VALIDACIÓN
Claridad y comprensión	100%	100%	100%	100%
Estructura y Organización	100%	100%	100%	100%
Detalles Técnicos	100%	100%	100%	100%
Actualización y Relevancia	100%	100%	100%	100%
Recursos considerados	100%	100%	100%	100%
Facilidad de uso y disponibilidad	100%	100%	100%	100%
VALIDACIÓN DEL PRODUCTO TOTAL				100%

Fuente elaboración propia

Criterio Claridad y comprensión: los 3 expertos lo evalúan con un 100%, lo que asegura que el documento se presenta de una manera transparente en donde se utiliza un lenguaje claro, la información que presenta es útil para la audiencia involucrada en la transición de IPv4 a IPv6.

Criterio Estructura y Organización: los 3 expertos determinan un 100% de la validación, lo cual evidencia que las fases de la transición están claramente definidas, proporcionando una guía lógica para su implementación.

Criterio Detalles Técnicos: los 3 expertos lo puntúan con 100% de la validación que corrobora que el documento contiene detalles técnicos y comprensibles, los procedimientos y mecanismos están descritos de una manera clara y adecuada para el personal de tecnologías de la información.

Criterio Actualización y Relevancia: los 3 expertos lo califican con 100% lo cual afirma que la información está estructurada de manera coherente, la metodología propuesta es relevante para la transición de IPv4 a IPv6.

Criterio Recursos considerados: los 3 expertos al considerar un 100% de la validación en este criterio, aseguran la suficiente información técnica tomada para la elaboración del plan.

Criterio Facilidad de uso y disponibilidad: los 3 expertos lo califican con el 100% lo que demuestra que se cuenta con un plan flexible y compatible para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones.

En conjunto, los resultados de validación del producto final respaldan la calidad integral del documento, obteniendo un valor del 100% por la evaluación de los expertos.

CONCLUSIONES

- A partir de la fundamentación teórica se definen características técnicas del protocolo IPv4 e IPv6; en donde se evidencia que IPv4 utiliza direcciones de 32 bits clasificadas en A, B, C, D, y E, las que tienen un tamaño específico, diferenciándose entre direcciones públicas y privadas; por otra parte, IPv6 utiliza direcciones de 128 bits representadas en formato hexadecimal, clasificadas con direcciones unidifusión global, unicast globales, direcciones multicast y de bucle local; en donde además se exploran las ventajas de IPv6, como su espacio de direcciones prácticamente ilimitado así como diversas características que mejoran la seguridad. Se detallan también mecanismos de transición de IPv4 a IPv6 como *Dual Stack* permitiendo la coexistencia de IPv4 e IPv6 en la misma red y dispositivos. *Tunneling* encapsulando paquetes IPv6 dentro de paquetes IPv4 para que puedan viajar a través de redes IPv4 que no admiten IPv6. Traducción facilitando la comunicación entre dispositivos IPv4 e IPv6 al convertir direcciones y protocolos entre ambos tipos de direcciones. Estos mecanismos presentan sus ventajas, desventajas y posibles casos de uso.
- La evaluación del estado actual de la red LAN del caso de estudio, permitió comprender su infraestructura, el diseño de la topología física de la red que permite visualizar cómo está distribuida la empresa a nivel administrativo y operativo, adicional se detalla y comprende la organización del cableado horizontal con cable UTP categoría 6 y vertical con fibra óptica multimodo; en esta etapa se detalla el inventario de hardware, identificando que la mayoría de los equipos de comunicación si soportan IPv6, mientras que los dispositivos finales como la maquinaria no soportan dicho protocolo. También se realizó el diseño de un diagrama lógico de la red, que muestra la organización y operación digital de la misma, observándose que mantiene un direccionamiento IPv4 de clase C y una segmentación por VLAN's; adicional los servicios de red que la empresa maneja como DNS, DHCP y servicio de impresión, con el software de operación correspondiente que se determina que sí soporta IPv6 a excepción del que utiliza la maquinaria.

- El plan desarrollado para la transición del protocolo IPv4 a IPv6 en la red LAN se basa en un enfoque práctico, toma como base el entorno de una empresa mediana como caso de estudio, y se desarrolló en tres fases: Fase I, Análisis de la situación actual, cuyo objetivo es la recopilación detallada de información, incluyendo la topología física y lógica, inventario de hardware, y análisis de servicios de red; Fase II, Diseño de la Solución, se enfoca en decisiones estratégicas, como la elección del mecanismo de transición, modificaciones en dispositivos finales, diseño del plan de direccionamiento IPv6, y configuración de la infraestructura general de red; y finalmente, la Fase III, Implementación y Pruebas, en donde se presentan lineamientos o acciones, como la simulación del entorno y pruebas hasta la aplicación gradual en el entorno real.
- Para la evaluación de la estructura, contenido y pertinencia técnica del plan de transición de IPv4 a IPv6, se establece una rúbrica con diversos criterios de calidad, aplicada por tres expertos en las áreas de redes y gerencia informática; se destaca que el 100% de los criterios evaluados confirman que el plan propuesto mantiene una sólida pertinencia técnica. Los expertos expresan, además, su aprobación al considerar que el plan es factible y cumple con los criterios establecidos. Esta alta aprobación sostiene la calidad y la adecuación técnica del plan, destacando su capacidad para abordarlo en una empresa de tamaño mediano.

RECOMENDACIONES

- Llevar a cabo la transición de IPv4 a IPv6 de forma gradual, es decir es importante priorizar áreas identificadas durante el diagnóstico que sea de mayor y menor impacto en operaciones.
- Seleccionar el mecanismo de transición en base a la infraestructura de la empresa en donde se evaluará detalladamente las necesidades y características particulares.
- Ejecutar programas de capacitación continua para el personal encargado de la gestión y mantenimiento de la red. Esto asegurará que estén actualizados con las nuevas tecnologías IPv6 y preparados para abordar cualquier desafío durante y después de la transición.

BIBLIOGRAFÍA

Acuña, M. (2023). *SISTEMA DE PROCESAMIENTO DE IMÁGENES CORPORALES MEDIANTE*. Pontificia Universidad Católica del Ecuador sede Ambato. Obtenido de <https://repositorio.pucesa.edu.ec/bitstream/123456789/4163/1/79329.pdf>

Adelaida, M. (2010). *MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6*. UNIVERSIDAD LIBRE. Obtenido de <https://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICION%20DE%20IPV4%20A%20IPV6.pdf?sequence=1&isAllowed=y>

Alan, D., & Cortez, L. (2017). *Procesos y Fundamentos de la Investigación Científica*. UTMACH.

Anderson, D., & Carmichael, A. (s.f.). *KANBAN ESENCIAL CONDENSADO*. Lean Kanban University. Obtenido de <https://www.tigalia.com/wp-content/uploads/2020/12/Essential-Kanban-Condensed-Spanish.pdf>

Anderson, T. (2016). *SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Center Environments*. RFC EDITOR.

Arias, F. (2012). *El Proyecto de Investigación*. Caracas: EPISTEME, C.A.

- Ariganello, E., & Barrientos, E. (2010). *REDES CISCO CCNP A Fondo*. Alfaomega .
- Avila, O. (2011). *Migración del protocolo IPv4 a IPv6*. Universidad Autónoma de Madrid. Obtenido de <http://www2.izt.uam.mx/newpage/contactos/anterior/n79ne/ipv6.pdf>
- Barba, H. (2022). *EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6*. Pontificia Universidad Católica del Ecuador sede Ambato. Obtenido de <https://repositorio.pucesa.edu.ec/bitstream/123456789/3702/1/77987.pdf>
- Bolivar, L., Guerrero, F., & Polanco, O. (2012). Diseño e implementación de una red IPv6 para transición eficiente desde IPv4. *Scielo*, 179 - 189. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0123-30332012000200017&lng=en&nrm=iso&tlng=es
- Carofilis, U. (2017). *ESTUDIO PARA LA MIGRACION DEL PROTOCOLO IPV4 AL PROTOCOLO IPV6. CASO DE ESTUDIO PLENARIO DE LA ASAMBLEA NACIONAL*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR. Obtenido de <http://repositorio.puce.edu.ec/bitstream/handle/22000/14002/Tesis%20Uilises%20Carofilis%20capt%201-2-3-4%20UV.pdf?sequence=1&isAllowed=y>
- Carrasco, P., & Frere, F. (2015). *DISEÑO DE PLAN DE MIGRACIÓN Y SEGURIDAD DE IPV4 A IPV6 PARA REDES DE EMPRESAS MEDIANAS Y PEQUEÑAS A BAJO COSTO ORIENTADO A LA EMPRESA CHIFLES S.A*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL. Obtenido de

<https://www.dspace.espol.edu.ec/retrieve/7bf81c79-9f75-4d03-98bb-b65eced0dd2d/D-103081.pdf>

CARRASCO, P., & FRERE, F. (2015). *DISEÑO DE PLAN DE MIGRACIÓN Y SEGURIDAD DE IPV4 A IPV6 PARA REDES DE EMPRESAS MEDIANAS Y PEQUEÑAS A BAJO COSTO ORIENTADO A LA EMPRESA CHIFLES S.A. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL*. Obtenido de <https://www.dspace.espol.edu.ec/retrieve/7bf81c79-9f75-4d03-98bb-b65eced0dd2d/D-103081.pdf>

CIMAT. (2022). *Plan de Transición al Protocolo de Internet versión 6 (IPv6)*. CIMAT. Obtenido de <https://www.cimat.mx/wp-content/uploads/2023/03/Plan-de-transicion-IPv6.pdf>

Cordero, C., García, M., & Marañón, J. (2011). *Plan Estratégico del Tercer Sector de acción social*. Obtenido de <https://www.plataformaong.org/ARCHIVO/documentos/biblioteca/3.pdf>

Coria, C. (24 de Enero de 2024). *8 MEDIDAS DE CIBERSEGURIDAD QUE SE DEBEN IMPLEMENTAR PARA ASEGURAR LAS REDES IPV6*. Obtenido de Noticias de seguridad informática: <https://noticiasseguridad.com/tutoriales/8-medidas-de-ciberseguridad-que-se-deben-implementar-para-asegurar-las-redes-ipv6/>

CUJILAN, A. (2017). *DISEÑO DE PLAN DE MIGRACIÓN Y SEGURIDAD DE IPV4 A IPV6 PARA UNA RED EDUCATIVA*. UNIVERSIDAD DE GUAYAQUIL. Obtenido de <https://repositorio.ug.edu.ec/bitstream/redug/27420/1/TESIS%20CUJILAN%20ROJAS%20ANTHONY%20ANDR%C3%89S.pdf>

Díaz, L., Torruco, U., Martínez, M., & Varela, M. (2013). *La entrevista, recurso flexible y dinámico*. Universidad Nacional Autónoma de México. Obtenido de <https://www.redalyc.org/pdf/3497/349733228009.pdf>

Dye, M., McDonald, R., Tony, R., & Brady, G. (2008). *Aspectos básicos de networking Guía de estudio de CCNA Exploration*. Pearson educacion S.A.

Garcés , E., & Pailiacho, V. (2023). Kanban como Herramienta de Gestión para Actividades en Grupos de Investigación Informáticos. *Centro de Publicaciones PUCE*, 733-739.

Girón, S. (2015). *PROPUESTA DE TÚNELES COMO TÉCNICA DE TRANSICIÓN DE IPV4 A IPV6 EN REDES DE PROVEEDORES DE SERVICIO*. Universidad de San Carlos de Guatemala. Obtenido de <https://core.ac.uk/download/pdf/35293533.pdf>

Gonzales, D. (2021). *Redes y Seguridad en IPv6*. Universidad de Almería. Obtenido de http://www.adminso.es/recursos/Proyectos/PFM/2014_15/PFM_Diego_IPV6/PFM_IPV6-Redes-Seguridad.pdf

GUARNIZO, J. (2015). *PLAN DE IMPLEMENTACIÓN PARA LA MIGRACIÓN A IPV6 EN LA RED DE LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL*. UNIVERSIDAD DE GUAYAQUIL. Obtenido de <https://repositorio.ug.edu.ec/server/api/core/bitstreams/b8c55085-fe30-4cb3-aec6-d8085a2f2ff0/content>

Landy, D. (2013). *Propuesta de un Plan de Implementación para la migración a IPV6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca*. UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/5332/1/UPS-CT002767.pdf>

López, J. (2023). *RÚBRICAS, EVALUACIÓN MÁS ALLÁ DE LA CALIFICACIÓN*. edukafé. Obtenido de <https://eduteka.icesi.edu.co/articulos/MatrizValoracion>

Lüke, J. (2019). *Guía sobre direccionamiento IP, subredes y enrutamiento*. Creative Commons. Obtenido de https://riull.ull.es/xmlui/bitstream/handle/915/14702/Guia_sobre_direccionamiento_IP__subredes_y_enrutamiento.pdf?sequence=1&isAllowed=y

Maldonado, P., & Conde, S. (2009). *Guía Técnica para la elaboración de manuales de procedimientos*. Gobierno de México. Obtenido de <https://sre.gob.mx/images/stories/docnormateca/dgpop/guias/guia01.pdf>

Matos, A. (s.f.). *Investigación Bibliográfica*.

Mera, G. (2016). *PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA*. UNIVERSIDAD TÉCNICA DEL NORTE.

Milagros, C. (2020). *MECANISMOS DE TRANSICIÓN PARA LA MIGRACIÓN DE IPV4 - IPV6*. Universidad Señor de Sipán. Obtenido de

[https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6568/Chingue
l%20Rodriguez%20Milagros%20Maribel.pdf?sequence=1&isAllowed=y](https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6568/Chingue%20Rodriguez%20Milagros%20Maribel.pdf?sequence=1&isAllowed=y)

Moreira, J., Minaya, C., & Cornejo, F. (2016). *Rendimiento de calidad de servicio(QoS) de IPV6 sobre tráfico RTP mediante emulación*. COMPAS.

Moreno, R., Montero, R., & Fabero, J. (S.F.). *Protocolo IPv6: Direccionamiento*. Universidad Complutense de Madrid. Obtenido de [https://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-
%20Protocolo%20IPv6.pdf](https://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-%20Protocolo%20IPv6.pdf)

Olivares, O. (2023). *Implementación de IPv6: El caso del Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California*. CICESE. Obtenido de [http://repositorio.cudi.edu.mx/jspui/bitstream/11305/2454/18/IPv6_Impleme
ntacion_CICESE.pdf](http://repositorio.cudi.edu.mx/jspui/bitstream/11305/2454/18/IPv6_Implementacion_CICESE.pdf)

PANTOJA, D. (s.f.). *“PLANIFICACIÓN DE PROCESOS PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 PARA LA CONTINUIDAD DEL SERVICIO EN LOS ISP’s*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR. Obtenido de [http://repositorio.puce.edu.ec/bitstream/handle/22000/11312/PLANIFICACI
%C3%93N%20DE%20PROCESOS%20PARA%20LA%20MIGRACI%C3%
93N%20DEL%20PROTOCOLO%20IPV4%20A%20IPV6%20PARA%20LA
%20CONTINUIDAD%20DEL%20SER.pdf?sequence=1&isAllowed=y](http://repositorio.puce.edu.ec/bitstream/handle/22000/11312/PLANIFICACION%20DE%20PROCESOS%20PARA%20LA%20MIGRACION%20DEL%20PROTOCOLO%20IPV4%20A%20IPV6%20PARA%20LA%20CONTINUIDAD%20DEL%20SER.pdf?sequence=1&isAllowed=y)

Pérez, J., & Herrera, E. (2010). *TECNOLOGÍAS Y MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6*. UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Obtenido de

<http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2807/Tesis.pdf?sequence=1>

Pérez, Y., & Puentes, A. (2018). TRANSICIÓN DE IPv4 A IPv6: REVISION. *Revista Colombiana de Tecnologías de Avanzada*, 19-23.
doi:<https://doi.org/10.24054/16927257.v32.n32.2018.3022>

Petersen, R. (2010). *Linux Manual de referencia*. Mexico: Corporativo Punta Santa.

Pineda, S. (2016). *Transición IPv4 a IPv6: Aspectos relacionados con Seguridad Informática*. Universidad Autónoma de Bucaramanga. Obtenido de https://repository.unab.edu.co/bitstream/handle/20.500.12749/16923/Generaci%C3%B3n_creativa_2016-265-266.pdf?sequence=1&isAllowed=y

POTES, J., & GIL, J. (2020). *PLAN DE TRANSICIÓN DE IPV4 A IPV6 PARA LA RED DE LA FACULTAD TECNOLÓGICA DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS*. UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Obtenido de <https://repository.udistrital.edu.co/bitstream/handle/11349/29836/GilBola%C3%B1osJuanSebastian2020.pdf?sequence=1&isAllowed=y>

Quecedo, R., & Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. *Revista de Psicodidáctica*, 5-39.

Ramírez, D., Guzmán, J., & Beltrán, J. (2015). *DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA AGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR CON BASE EN CONSIDERACIONES DE*

SEGURIDAD EN IMPLEMENTACIÓN DE IPV6. UNIVERSIDAD CATOLICA DE COLOMBIA. Obtenido de <https://repository.ucatolica.edu.co/server/api/core/bitstreams/013d3fd4-6bf2-4acf-a84f-c14a11071a6c/content>

Redes, D. d. (2022). *Plan de Transición Local a IPv6 del Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California*. CICESE. Obtenido de <https://telematica.cicese.mx/wp-content/uploads/2022/06/Plan-de-Transicion-Local-a-IPv6.pdf>

S.A. (2021). *LA GUÍA OFICIAL DEL MÉTODO KANBAN* . Seattle, WA : Mauvius Group Inc.

S.A. (s.f.). *LACNIC*. Obtenido de <https://www.lacnic.net/innovaportal/file/5495/1/map-e-y-map-t.pdf>

Sánchez, B. (2022). *PROTOTIPOS IOT DE MONITOREO Y CONTROL DE FUGAS DE GLP EN DOMICILIOS*. Pontificia Universidad Católica del Ecuador Sede Ambato. Obtenido de <https://repositorio.pucesa.edu.ec/bitstream/123456789/3620/1/77910.pdf>

Taffernaberry, J. (2011). *Mecanismos de Transición hacia redes IPv6*. Universidad Nacional de la Plata. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/4193/Documento_completo.pdf?sequence=1&isAllowed=y

Urueña, E. (2005). *Direccionamiento IPv4*. Obtenido de <http://isa.uniovi.es/docencia/SIGC/pdf/direccionamiento-ip.pdf>

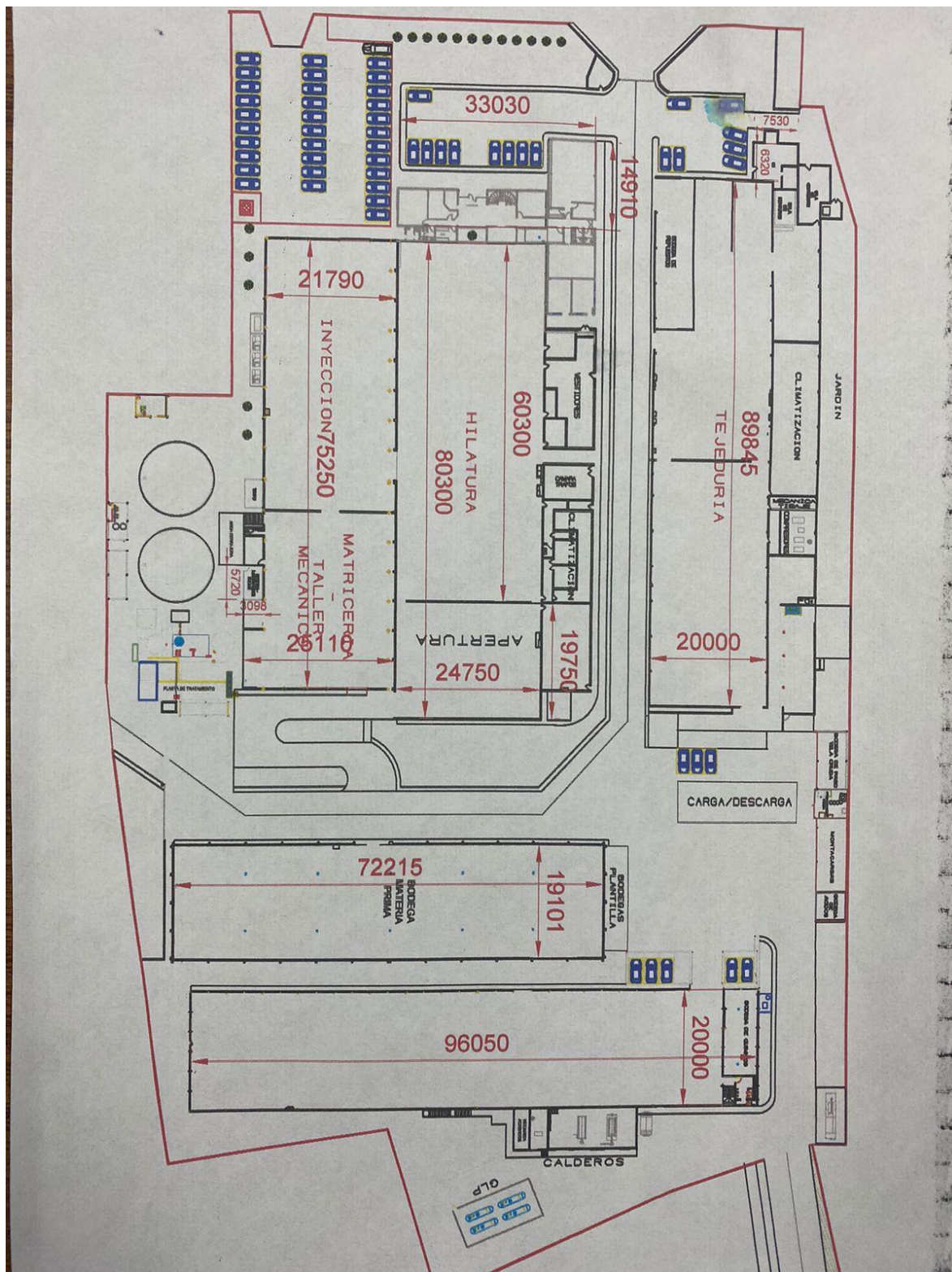
- Valverde, J., García, A., Hernández, A., & Morales, E. (2017). *Elaboración y validación de una rúbrica para la evaluación de los Trabajos de Fin de Máster (TFM) pertenecientes al Máster “Las TIC en educación. Análisis y diseño de procesos, recursos y prácticas formativas*. Universidad DSalamanga. Obtenido de https://www.researchgate.net/publication/320757144_Elaboracion_y_validacion_de_una_rubrica_para_la_evaluacion_de_los_Trabajos_de_Fin_de_Master_TFM_pertenecientes_al_Master_Las_TIC_en_educacion_Analisis_y_diseño_de_procesos_recursos_y_practicas_formati
- Vásquez, C., & Hidrobo, A. (2017). *TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE*. Universidad Técnica del Norte. Obtenido de <http://repositorio.utn.edu.ec/bitstream/123456789/7185/2/04%20RED%2093%20ARTICULO.pdf>
- VILLEGAS, W. (2014). *ESTUDIO PARA LA ELABORACIÓN DEL PLAN DE MIGRACIÓN A IPV6 Y LA COEXISTENCIA CON IPV4 EN LA RED DE LA UNIVERSIDAD INTERNACIONAL DEL ECUADOR*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/11940/Tesis_William%20Villegas.pdf?sequence=4&isAllowed=y
- Vives, A. (2010). *Despliegue de IPV6*. CONSULNET. Obtenido de http://www.6deploy.eu/workshops/20101018_sao_paulo_brasil/Consulintel_IPv6_ES_LACNIC-XIV.pdf
- Vozmediano, R., Montero, R., & Fabero, J. (S.F.). . *Protocolo IPv6: Direccionamiento*. Universidad Complutense de Madrid. Obtenido de

<https://www.fdi.ucm.es/profesor/rubensm/asor/Trasparencias/Tema%201-%20Protocolo%20IPv6.pdf>


Yépez, E., & Armijos, K. (2020). *APLICACIÓN DE LA METODOLOGÍA KANBAN EN EL DESARROLLO DEL SOFTWARE PARA GENERACIÓN, VALIDACIÓN Y ACTUALIZACIÓN DE REACTIVOS, INTEGRADO AL SISTEMA INFORMÁTICO DE CONTROL ACADÉMICO UNACH*. UNIVERSIDAD NACIONAL DE CHIMBORAZO. Obtenido de <http://dspace.unach.edu.ec/bitstream/51000/6457/1/APLICACI%C3%93N%20DE%20LA%20METODOLOG%C3%8DA%20KANBAN%20EN%20EL%20DESARROLLO%20DEL%20SOFTWARE%20PARA%20GENERACI%C3%93N.pdf>

ANEXOS

Anexo 1. Diagrama físico de la empresa TEIMSA



Anexo 2. Formato de entrevista

 Pontificia Universidad Católica del Ecuador Sede Ambato	
Modelo de entrevista para diagnosticar el estado de red en la empresa Textiles Industriales Ambateños S.A.	
Objetivo	Evaluar y comprender el estado actual de la red en Textiles Industriales Ambateños S.A. con el fin de identificar mejoras y desafíos potenciales para optimizar su rendimiento y seguridad en el marco del plan de transición de Ipv4 a Ipv6.
Entrevistados	Jefe de departamento de TI Asistente del departamento
Consideraciones Generales Se solicita se responda de manera objetiva. Los resultados de la presente entrevista poseen fines de investigación.	
Desarrollo <ul style="list-style-type: none"> • ¿Puede describir brevemente la infraestructura de red actual en TEIMSA? • ¿Cuántos usuarios y dispositivos trabajan en la empresa incluyendo la cantidad de dispositivos y la topología general? • ¿Cuáles son los servicios de red con los que trabaja actuante la empresa? • ¿Cuáles son los motivos principales detrás de la decisión de TEIMSA de llevar a cabo la transición de IPv4 a IPv6? • ¿Cuáles son los objetivos clave que se esperan alcanzar con la transición a IPv6? 	

- ¿Qué recursos se asignarán al proceso de transición, incluyendo personal, hardware y software?


¿Cuáles son las proyecciones de costos e inversión en equipos basados en IPv6?

- ¿Cuáles son las características actuales de los equipos utilizados en la infraestructura de red para admitir IPv6?

- ¿Cuáles son los plazos de tiempo previstos para la implementación del plan de transición a IPv6 en TEIMSA?

Anexo 3. Plan final de transición de IPv4 a IPv6

CONTENIDO

A decorative graphic on the left side of the page consists of a network of interconnected nodes and lines. The nodes are represented by small grey circles of varying sizes, and the lines are thin grey lines connecting these nodes in a complex, web-like structure. The overall appearance is that of a digital or social network diagram.

Introducción.....	3
Objetivo.....	4
Desarrollo.....	5
Fase I Análisis de la situación actual.....	5
Fase II Diseño de la solución.....	7
Fase III Implementación y pruebas.....	10
Riesgos a considerar.....	11
Glosario.....	11

INTRODUCCIÓN

En la era actual de expansión tecnológica, la adopción de IPv6 emerge como una necesidad imperativa debido al agotamiento de direcciones IPv4. Ante este escenario, las organizaciones se enfrentan al desafío de migrar sus redes locales (LAN) hacia IPv6 para garantizar la continuidad de sus operaciones y habilitar el crecimiento sostenible de sus infraestructuras.

Este plan de transición se concibe como una estrategia integral que aborda los diversos aspectos de la migración, desde la planificación y evaluación de la infraestructura existente hasta la gestión efectiva de IPv6. El plan busca minimizar la interrupción en los servicios mientras se asegura la conectividad futura.

Este documento presenta un enfoque paso a paso, desde la evaluación inicial de la red hasta la implementación progresiva de IPv6. El objetivo es guiar a la organización hacia una red LAN moderna y preparada para el futuro, respaldada por las capacidades y ventajas que IPv6 ofrece en términos de escalabilidad, y soporte para el crecimiento continuo de la infraestructura.





OBJETIVO

Facilitar la transición de una infraestructura de red basada en IPv4 a IPv6 de manera eficiente y ordenada, orientada a la continuidad de las operaciones, a la interoperabilidad con sistemas existentes y al crecimiento futuro de la red en cuanto a dispositivos y servicios.





DESARROLLO

El presente plan de transición de Ipv4 a Ipv6, ha sido diseñado mediante un análisis metodológico, utilizando como caso práctico a una empresa de tamaño mediana. Este enfoque ha facilitado la identificación y abordaje de los aspectos clave en el proceso de transición, estructurándolo en tres fases principales:

- Fase I: Análisis de la situación actual.
- Fase II: Diseño de la Solución.
- Fase III: Implementación.

Cada una detallada con un enfoque global que abarca actividades y entregables correspondientes, a continuación, se describen cada una de estas fases:

Fase I Análisis de la situación actual

Constituye el punto de partida en el proceso de transición de IPv4 a IPv6 en la red LAN de la empresa. En esta etapa, se realiza una recopilación de información con el objetivo de obtener una comprensión detallada de la red actual. Esta fase implica la identificación de activos de red, diseño de topología física y lógica, y el direccionamiento actual que mantiene como también el detalle de los servicios de red con los que trabaja.

A continuación, se presenta las actividades en la fase I:

Actividad: Análisis de Infraestructura de la red LAN existente.

Descripción: La tarea consiste en realizar un análisis integral de la infraestructura física de la red de datos de la empresa. En donde se divide en varias acciones que complementan este análisis.

·Tarea: Diseño de la topología lógica de la red.

Identificar la estructura global de la organización evaluando si existe división en bloques y áreas operativas. Posteriormente, se procederá al diseño de la topología física de la red, con el objetivo de visualizar y comprender la distribución de la infraestructura en toda la empresa. Este diseño incluirá la especificación del cableado horizontal y vertical, detallando como se conectan con las diversas áreas de trabajo.

·Tarea: Realizar un inventario de hardware de equipos, identificando soporte para IPv6.

Se lleva a cabo un inventario enfocado en identificar la cantidad, modelos y marcas de los equipos presentes en la infraestructura de red, proporcionando un adicional la capacidad de soportar IPv6, el objetivo principal de este inventario es evaluar el estado de los equipos de comunicaciones de red, incluyendo dispositivos finales, y su capacidad con soporte al protocolo IPv6. Esto contempla una visión clara y detallada de los recursos tecnológicos disponibles en la organización.

A continuación, se presenta un formato para realizar el inventario de equipos de hardware con capacidad de soportar IPv6:

EQUIPO	CANTIDAD	MACA	MODELO	TIEMPO DE USO	SOporta IPV6
Switch de Distribución Cisco Catalyst X 48	4	CISCO	WS-C3560X-24 TS-S	1 AÑO	SI



Tarea: Identificar usuarios y dispositivos asociados a cada área.

Detallar la información sobre la demanda de red en diferentes secciones de la empresa, implica obtener detalles sobre la cantidad y dispositivos. En otras palabras, incluye identificar a los usuarios que representan al personal que interactúa con la red, así como los dispositivos que constituyen las herramientas utilizadas por estos usuarios. Esto permitirá la obtención de requerimientos en las diferentes secciones de la empresa.

Actividad: Análisis de la infraestructura lógica de la red de datos

Descripción: En esta actividad de análisis de la infraestructura lógica de la red de datos, busca realizar la topología lógica, direccionamiento y segmentación de VLANs

Tarea: Diagrama de la topología lógica.

La tarea consiste en el diseño de un diagrama detallado de la topología lógica, mediante la utilización de herramientas de simulación de redes. Este diseño tiene como objetivo proporcionar una visión estructurada de la organización y operación digital de la red.

Tarea: Direccionamiento actual en IPv4 de la red de datos.

La tarea consiste en detallar el direccionamiento propuesto en IPv4. Con el objetivo de brindar información precisa y actual sobre la asignación de direcciones IP en la red.

Tarea: Segmentación y organización de VLANs.

La tarea consiste en proporcionar información acerca de la presencia y organización de las VLANs, asegurando un análisis detallado de la segmentación lógica de la infraestructura.

Actividad: Análisis de los servicios de red

Descripción: Se lleva a cabo en analizar los diversos servicios proporcionados por la infraestructura de red, incluyendo aspectos de software.

Tarea: Identificar y analizar servicios esenciales.

La tarea consiste en detallar servicios con conectividad a Internet, DNS, DHCP entre otros, para ello se requiere elaborar un formato en donde se detalle el análisis de servicios presentes en la empresa describiendo las funciones de cada uno de igual manera abordar aspectos de software en donde es relevante mencionar la utilidad de las aplicaciones y si mantiene compatibilidad si es el caso con IPv6. Como se evidencia a continuación formatos para el caso de análisis de servicios y de software:

SERVICIO DE RED	FUNCIÓN DEL SERVICIO EN LA EMPRESA
Correo electrónico	El servicio de correo electrónico cumple la función de facilitar la comunicación entre los empleados a través de una cuenta de usuario perteneciente a la organización

SOFTWARE	DESCRIPCIÓN	SOPORTE A IPV6
SAP- ERP	SAP ERP es un software de planificación de recursos empresariales que facilita la integración y gestión de diversas funciones empresariales en un solo sistema.	SI



Resumen de entregables

Una vez que se detalló las actividades y tareas correspondientes en la fase I, se presenta la siguiente lista a modo de checklist, la misma es una herramienta que se utiliza para listar tareas que deben ser completadas o revisadas en donde se debe agregar un check en cada entregable para cada actividad o tarea que esta culminada.

ENTREGABLES DE LA FASE I	CHECK ✓
Diagrama de la topología física de la red.	<input type="checkbox"/>
Disposición del cableado horizontal y vertical.	<input type="checkbox"/>
Inventario de hardware con detalles técnicos y capacidad para IPv6.	<input type="checkbox"/>
Registro de listado actualizado de usuarios y dispositivos que mantiene cada área de la empresa.	<input type="checkbox"/>
Diseñar un diagrama detallado de topología lógica que ilustre las relaciones entre dispositivos,	<input type="checkbox"/>
Direccionamiento actual en IPv4.	<input type="checkbox"/>
Organización de VLANs en la red.	<input type="checkbox"/>
Elaborar un análisis de servicios de red, adicional se detallará el software y su descripción.	<input type="checkbox"/>

Fase II Diseño de la solución

Durante esta fase, además de la elección del mecanismo de transición, se aborda la configuración del direccionamiento IPv6 y la adaptación de equipos y servicios.

A continuación, se presentan las actividades en la fase II:

Actividad: Elección del mecanismo de transición.

Descripción: Se lleva a cabo un análisis para seleccionar un mecanismo de transición adecuado, en donde se debe justificar esa elección en base a la infraestructura que mantiene empresa.

A continuación se muestra un análisis a detalle, donde se clasifican en tres mecanismos principales que son:

- Dual Stack
- Tunneling
- Traducción

Dual Stack o doble pila, este método es considerado el más simple y económico, ya que implica proporcionar a terminales y routers soporte completo para ambos protocolos. Como se evidencia en la siguiente tabla diversos aspectos claves de este mecanismo:

MECANISMO	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS	CASO PRACTICO
Dual Stack	Permite la coexistencia de IPv4 e IPv6 en una red, lo que significa que los dispositivos y la infraestructura admiten ambos protocolos.	Facilita una transición gradual y controlada. Garantiza la compatibilidad con sistemas heredados al admitir ambos protocolos simultáneamente.	Aumenta la complejidad de la gestión de red al tener que lidiar con dos protocolos simultáneamente. Soporte en las aplicaciones y servidores sobre todo en (web, DNS, SMTP).	Empresas que admiten IPv4 y desean habilitar IPv6, destacado así su dualidad es decir para la elección de este mecanismo no basta considerar que es el más simple más bien es considerar que dispositivos o servicios de red no admiten IPv6, los mismos trabajarán con IPv4 y no afectarán a actividades de la empresa.

Mecanismos de Tunneling encapsulan información de un protocolo en paquetes de otro, facilitando la comunicación entre redes IPv6 aisladas sin modificar la estructura de enrutamiento. Como se evidencia en la siguiente tabla algunos de estos mecanismos detallando aspectos importantes:



MECANISMO	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS	CASO PRACTICO
SIIT-DC	SIIT-DC (Stateless IP/ICMP Translation for IPv6 Data Center) es una técnica de traducción de direcciones que permite a las aplicaciones en un entorno IPv6 de un centro de datos comunicarse con recursos externos en Internet que utilizan IPv4. Lo hace traduciendo los paquetes IPv6 a IPv4 y viceversa, lo que permite que las aplicaciones continúen funcionando sin problemas en un entorno predominantemente IPv6	Permite a las aplicaciones en un entorno IPv6 comunicarse con recursos externos IPv4, lo que facilita la adopción de IPv6 nativo en el centro de datos sin interrupciones en la conectividad hacia Internet..	Se utiliza principalmente para permitir que las aplicaciones en un centro de datos accedan a recursos IPv4 en Internet. No es adecuado para todas las situaciones de transición IPv6, especialmente aquellas que involucran comunicación entre redes privadas.	Se utiliza en entornos de centros de datos para permitir que las aplicaciones y servicios operen en IPv6 mientras se conectan a recursos IPv4 en Internet, para ello es necesario: Enrutadores IPv6 compatibles. Servidores IPv6 configurados para operar en un entorno IPv6. Dispositivos de traducción de direcciones (para la implementación de SIIT-DC).
Dual Stack Lite	Combina la coexistencia de IPv4 e IPv6 en los clientes finales y utiliza túneles IPv6 sobre IPv4 en la red de proveedores de servicios.	Reduce la necesidad de direcciones IPv4. Para los proveedores de servicios de Internet (ISP), DS-Lite simplifica la gestión de direcciones IPv4 y facilita la migración a IPv6 al reducir la dependencia de IPv4 en la red.	Requiere implementación en proveedores de servicios. DS-Lite puede no ser adecuado para organizaciones que necesitan mantener un alto nivel de soporte para IPv4, ya que implica compartir direcciones IPv4 públicas entre múltiples usuarios.	Proveedores de servicios que migran a IPv6 y minimizan el despliegue de IPv4. Para ello son necesarios Enrutadores DS-Lite. Firewalls y dispositivos de seguridad configurados para DS-Lite
MAP-E	Los mecanismos de transición MAP (Mapping of Address and Port) se diseñan con la finalidad de permitir que los clientes que utilizan IPv4 puedan acceder a Internet a través de una red de transporte que opera exclusivamente en IPv6. Esto se logra mediante la aplicación de un esquema de asignación que relaciona direcciones IPv4 y puertos (TCP y UDP) con direcciones IPv6.	Permite una utilización eficiente de direcciones IPv4 ya que múltiples clientes pueden compartir direcciones IPv4 públicas a través de la traducción y asignación de direcciones IPv6.	Soporta el tráfico Unicast y no soporta para Multicast. Implementar MAP puede requerir actualizaciones de hardware y software en la infraestructura de red existente, lo que puede generar costos adicionales para los proveedores de servicios.	Un proveedor de servicios, con una infraestructura basada en IPv6, implementa MAP-E para brindar conectividad a clientes que aún utilizan IPv4. MAP-E encapsula el tráfico IPv6 de los clientes en paquetes IPv4, para ello es necesario Enrutadores MAP compatibles. Servidores MAP. Equipos de red compatibles con IPv6. Herramientas de monitoreo y diagnóstico compatible con IPv6 y MAP

Los mecanismos de Traducción permiten la comunicación transparente entre dispositivo que utilizan diferentes versiones del protocolo IP, realizando conversiones de direcciones y cabeceras. Como se evidencia en la siguiente tabla diversos aspectos claves de este mecanismo:

MECANISMO	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS	CASO PRACTICO
NAT64 DNS64	Traduce las direcciones de IPv4 a IPv6 y proporciona acceso a servicios IPv4 desde redes IPv6.	NAT Tradicional: Traduce direcciones entre conexiones de redes con direcciones IPv4 privadas. Al permitir que dispositivos IPv6 accedan a servicios	Se utiliza principalmente para permitir que las aplicaciones en un centro de datos accedan a recursos IPv4 en Internet. No es adecuado para todas las situaciones de transición IPv6, especialmente aquellas que involucran comunicación entre redes privadas.	Acceso a servicios IPv4 desde redes IPv6. Con Enrutadores compatibles con NAT64 y DNS64.



Actividad: Cambios en dispositivos finales de red

Descripción: Se implementan modificaciones necesarias en la infraestructura existente para facilitar la transición de IPv4 a IPv6. Se basa en los resultados del análisis previo de la red, donde se identifican los dispositivos que carecen de la capacidad requerida para Ipv6, esto significa que si una computadora no es compatible con Ipv6 la misma requiere de una actualización o cambio en su tarjeta de red. El objetivo de esta actividad se centra en detallar las modificaciones requeridas, en base a dispositivos que no admiten IPv6 y que necesitan ser cambiados o actualizados. Es muy importante mencionar que todos los cambios de la infraestructura están sujetos de acuerdo al mecanismo de transición que se elija.

Actividad: Plan de Direccionamiento IPV6.

Descripción: Diseñar un plan de direccionamiento Ipv6, en donde se describe la estructura de direccionamiento propuesto para la red, incluyendo la asignación de bloques a segmentos de red, subneteo, y directrices para la gestión de VLANs. El objetivo de esta actividad es detallar la estructura de direccionamiento IPv6 propuesto para la asignación de bloques IPv6 a segmentos de red, tomando en cuenta la estructura habilitada en IPv4. A continuación Se presenta la estructura de una dirección IPv6, es importante verificar los hextetos de red, adicional se presenta una tabla de direccionamiento en IPv6.

Estructura de una dirección IPv6

2001:0DB8:0001:0010:0000:0000:0000:0000		
2001:0DB8:0001	:0010	:0000:0000:0000:0000
Global Routing Prefix Son asignadas por la Ianna, Lacnic y un ISP	Subnet ID Destinados a identificar la red o subredes.	Interface ID Pertenece a un único host.

Guía de direccionamiento IPv6 - VLAN

NOMBRE VLAN /ID	DIRECCIÓN DE IPv6	RANGO DE HOST	GATEWAY	PREFIJO
CONTABILIDAD/ 10	2001:0DB8:0001:0001:- /64	2001:0DB8:0001:0001:1 2001:0DB8:0001:0001:ffff	2001:0DB8:0001:0001:-1 /64	/64

Actividad: Levantamiento de la infraestructura general de la red.

Descripción: Esto implica la habilitación de IPv6 a nivel de protocolos en los routers y switches, en donde se debe realizar configuraciones en estos equipos y en dispositivos finales, asegurando que la infraestructura pueda gestionar y enrutar tráfico IPv6 de manera eficiente. Además, se lleva a cabo la configuración de subredes y la asignación de direcciones IPv6 en los dispositivos finales.

Actividad: Cambios en los servicios de red.

Descripción: Se centra en la adaptación y su configuración de los servidores que ofrecen servicios de red diversos para integrar IPv6, con el fin de llevar una bitácora de los cambios de software y servicios de red en los servidores que incluyan ajustes realizados en cada uno, este proceso no solo debe centrarse en servidores, también debe incluir aspectos de configuración en software asociados que mantienen compatibilidad con Ipv6.



Resumen de entregables

Una vez que se detalló las actividades correspondientes en la fase II, se presenta el checklist pertinente a esta fase, en donde se enlista los entregables para cada actividad presentada

ENTREGABLES FASE II	CHECK ✓
Elección del mecanismo de transición seleccionado, justificando su elección.	<input type="checkbox"/>
Detallar de las modificaciones requeridas para la infraestructura, en base a dispositivos que no admiten IPv6 y que necesitan ser cambiados o actualizados.	<input type="checkbox"/>
Estructura de direccionamiento IPv6 propuesto como la asignación de bloques IPv6 a segmentos de red.	<input type="checkbox"/>
Bitácora de los cambios de software y red que incluyan ajustes realizados en cada uno.	<input type="checkbox"/>
Configuraciones realizadas en routers, switches y dispositivos finales.	<input type="checkbox"/>

Fase III Implementación y Pruebas

En la Fase III, Implementación y Pruebas, se traducen las decisiones estratégicas tomadas en las fases anteriores en acciones concretas. Esta fase implica la ejecución de cambios en la infraestructura de red, la implementación de nuevas configuraciones en dispositivos y servicios, y la realización de pruebas para asegurar la correcta funcionalidad del entorno IPv6.

Simulación en el entorno

La creación de laboratorios de prueba que simulen el entorno de red es fundamental para la transición a IPv6. La elección de GNS3 como herramienta de simulación recae en sus múltiples ventajas como en su capacidad para generar escenarios altamente realistas.

El proceso implica levantar la infraestructura de la red mediante la simulación, configurando tanto IPv4 como IPv6 en los routers, switches, dispositivos finales y servidores. Esta simulación ayuda a una representación del entorno antes de la implementación real, permitiendo ajustes y validaciones.

Pruebas

Una vez que se simula el entorno, se procederá a realizar pruebas que abarcan la verificación de la conectividad, compatibilidad y comunicación. Estas pruebas pueden identificar posibles errores que permitirá solucionarlos de manera oportuna, y a la vez contribuye a modificarlos antes de implementarlas en el entorno de real. La detección y solución temprana de problemas garantiza una transición más fluida y minimiza posibles interrupciones o fallos en la red.

Capacitación al personal

Asegurarse de que el personal esté familiarizado con herramientas y procedimientos específicos de IPv6.

Aplicar al entorno real

En la aplicación al entorno de real, se espera una transición gradual es decir paso a paso y de manera coordinada. El proceso debe priorizar la estabilidad operativa y minimizando el impacto en las operaciones diarias. La experiencia adquirida en la simulación ayudará en una implementación eficiente y sin contratiempos.



Monitoreo Continuo

Se debe mantener sistemas de gestión de red que ayude a evaluar el rendimiento de la red después de la implementación.

RIESGOS A CONSIDERAR

La transición de IPv4 a IPv6 implica ciertos riesgos y desafíos que deben ser gestionados cuidadosamente. Aquí hay algunos riesgos comunes asociados con el proceso de transición:

Errores en la Configuración de Dispositivos de Red:

Riesgo: Configuraciones incorrectas en routers, switches u otros dispositivos de red pueden afectar la conectividad y la seguridad.

Mitigación: Realizar copias de configuraciones y verificar las mismas antes de implementarlas en la red.

Desafíos en la Administración de Redes:

Riesgo: La administración de redes puede volverse más compleja con la coexistencia de IPv4 e IPv6.

Mitigación: Utilizar herramientas de gestión de red compatibles con IPv6 y proporcionar capacitación adecuada al personal de TI.

Problemas de Actualización de Software:

Riesgo: La falta de actualizaciones de software y para dispositivos de red podría afectar el rendimiento.

Mitigación: Mantener un plan de actualización regular y asegurarse de los dispositivos cuenten con versiones de software actualizadas Además la empresa debería contar con un plan de continuidad del negocio que garantice que los servicios que ofrece se mantengan estables.

Impacto en Usuarios Finales:

Riesgo: Cambios en la infraestructura y en la configuración de dispositivos pueden afectar la experiencia de los usuarios finales.

Mitigación: Proporcionar comunicación clara, capacitación y soporte técnico durante el proceso de transición para minimizar el impacto en los usuarios.

GLOSARIO

IPv6: (Protocolo de Internet versión 6): La versión más reciente del Protocolo de Internet que utiliza direcciones de 128 bits.

IPv4: (Protocolo de Internet versión 4): La versión anterior del Protocolo de Internet que utiliza direcciones de 32 bits

LAN (Red de Área Local): grupo de dispositivos conectados en un área pequeña y comparten conexión centralizada a internet.

Interoperabilidad: La capacidad de diferentes sistemas o dispositivos para trabajar juntos.

Cisco: Una empresa líder en tecnologías de redes y comunicaciones.

Topología Física: La disposición física o diseño de una red se visualmente de cómo están conectados físicamente los dispositivos.



Topología Lógica: La disposición lógica en que los datos viajan a través de la red de acuerdo con la dirección lógica de los dispositivos. Segmentación: La práctica de dividir una red en segmentos más pequeños.

VLANs (Redes de Área Local Virtuales): Segmentación de redes que agrupa dispositivos en la misma red lógica.

DNS (Sistema de Nombres de Dominio): Un sistema que traduce los nombres de dominio legibles en direcciones IP.

DHCP (Protocolo de Configuración Dinámica de Host): Un protocolo que asigna automáticamente direcciones IP.

SMTP (Protocolo Simple de Transferencia de Correo): Un protocolo estándar para el envío de correos electrónicos.

ISP (Proveedor de Servicios de Internet): Empresa que ofrece servicios de acceso a Internet.

TCP (Protocolo de Control de Transmisión): Un protocolo orientado a la comunicación que garantiza la entrega correcta de datos.

UDP (Protocolo de Datagramas de Usuario): Un protocolo que no está orientado a la comunicación no verifica la recepción de datos.

Enrutadores: Dispositivos de red que dirigen el tráfico entre redes.

Bitácora: Un registro detallado de eventos.

Router: Un dispositivo que dirige el tráfico entre redes.

Switch: Un dispositivo de red que opera en la capa de enlace de datos y conecta dispositivos en la misma red local.

GNS3: Un simulador de red que permite a los usuarios emular y configurar redes virtuales para propósitos de prueba y aprendizaje.

Anexo 4. Matriz de validación por expertos

MATRIZ DE VALIDACIÓN POR EXPERTOS

PLAN DE TRANSICIÓN DE IPV4 A IPV6 PARA UNA RED LAN

Objetivo:

- Este instrumento tiene como fin validar el Plan de transición de IPv4 a IPv6 para una red LAN construido como parte de un proyecto de investigación.

Experto: _____ Fecha: _____

Escala de validación: 5 (Muy Satisfactorio) – 4 (Satisfactorio) – 3 (Neutro) – 2 (Poco satisfactorio) – 1 (Nada satisfactorio)

CRITERIOS DE VALIDACIÓN

CRITERIO	DESCRIPCIÓN	Validación					RESULTADO
		5 (100%)	4 (80%)	3 (60%)	2 (40%)	1 (20%)	
Claridad y comprensión	El plan presenta documentación de manera transparente, utilizando un lenguaje claro asegurando que la información sea útil para la audiencia involucrada en la transición de IPv4 a IPv6.						
Estructura y Organización	Este criterio busca asegurar que las fases de la transición estén claramente definidas en el plan, proporcionando una guía lógica para la implementación.						
Detalles Técnicos	Evalúa la presencia de detalles técnicos y comprensibles en cada fase del plan de transición. Se verifica que los procedimientos y mecanismos técnicos estén descritos de manera clara y adecuada para						

	el personal en el área de tecnologías de la información.						
Actualización y Relevancia	El plan está basado en información actualizada, estructurado de manera coherente y que la metodología propuesta sea relevante para la transición IPv4 a IPv6.						
Recursos considerados	Este criterio evalúa la suficiencia de la información técnica tomada en consideración para la elaboración del plan.						
Facilidad de uso y disponibilidad	Este criterio garantiza que el plan sea flexible y compatible como para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones específicas.						

Firma Experto

Anexo 5. Validación por experto N 1



Pontificia Universidad
Católica del Ecuador

MATRIZ DE VALIDACIÓN POR EXPERTOS PLAN DE TRANSICIÓN DE IPV4 A IPV6 PARA UNA RED LAN

Objetivo:

- Este instrumento tiene como fin validar el Plan de transición de IPv4 a IPv6 para una red LAN construido como parte de un proyecto de investigación.

Experto: MARCO BALSECA

Fecha: 08/12/2023

Escala de validación: 5 (Muy Satisfactorio) – 4 (Satisfactorio) – 3 (Neutro) – 2 (Poco satisfactorio) – 1 (Nada satisfactorio)

CRITERIOS DE VALIDACIÓN

CRITERIO	DESCRIPCIÓN	Validación					RESULTADO
		5 (100%)	4 (80%)	3 (60%)	2 (40%)	1 (20%)	
Claridad y comprensión	El plan presenta documentación de manera transparente, utilizando un lenguaje claro asegurando que la información sea útil para la audiencia involucrada en la transición de IPv4 a IPv6.	X					100%
Estructura y Organización	Este criterio busca asegurar que las fases de la transición estén claramente definidas en el plan, proporcionando una guía lógica para la implementación.	X					100%
Detalles Técnicos	Evalúa la presencia de detalles técnicos y comprensibles en cada fase del plan de transición. Se verifica que los procedimientos y mecanismos técnicos estén descritos de	X					100%



Pontificia Universidad
Católica del Ecuador

	manera clara y adecuada para el personal en el área de tecnologías de la información.						
Actualización y Relevancia	El plan está basado en información actualizada, estructurado de manera coherente y que la metodología propuesta sea relevante para la transición IPv4 a IPv6.	X					100%
Recursos considerados	Este criterio evalúa la suficiencia de la información técnica tomada en consideración para la elaboración del plan.	X					100%
Facilidad de uso y disponibilidad	Este criterio garantiza que el plan sea flexible y compatible como para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones específicas.	X					100%

Firma Experto

Anexo 6. Validación por experto N 2



Pontificia Universidad
Católica del Ecuador

MATRIZ DE VALIDACIÓN POR EXPERTOS PLAN DE TRANSICIÓN DE IPV4 A IPV6 PARA UNA RED LAN

Objetivo:

- Este instrumento tiene como fin validar el Plan de transición de IPv4 a IPv6 para una red LAN construido como parte de un proyecto de investigación.

Experto: Wuorq Arriencia C. Fecha: 2023-12-07

Escala de validación: 5 (Muy Satisfactorio) – 4 (Satisfactorio) – 3 (Neutro) – 2 (Poco satisfactorio) – 1 (Nada satisfactorio)

CRITERIOS DE VALIDACIÓN

CRITERIO	DESCRIPCIÓN	Validación					RESULTADO
		5 (100%)	4 (80%)	3 (60%)	2 (40%)	1 (20%)	
Claridad y comprensión	El plan presenta documentación de manera transparente, utilizando un lenguaje claro asegurando que la información sea útil para la audiencia involucrada en la transición de IPv4 a IPv6.	X					100%
Estructura y Organización	Este criterio busca asegurar que las fases de la transición estén claramente definidas en el plan, proporcionando una guía lógica para la implementación.	X					100%
Detalles Técnicos	Evalúa la presencia de detalles técnicos y comprensibles en cada fase del plan de transición. Se verifica que los procedimientos y mecanismos técnicos estén descritos de	X					100%



Pontificia Universidad
Católica del Ecuador

	manera clara y adecuada para el personal en el área de tecnologías de la información.						
Actualización y Relevancia	El plan está basado en información actualizada, estructurado de manera coherente y que la metodología propuesta sea relevante para la transición IPv4 a IPv6.	X					100%
Recursos considerados	Este criterio evalúa la suficiencia de la información técnica tomada en consideración para la elaboración del plan.	X					100%
Facilidad de uso y disponibilidad	Este criterio garantiza que el plan sea flexible y compatible como para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones específicas.	X					100%


Firma Experto

Anexo 7. Validación por experto N 3



Pontificia Universidad
Católica del Ecuador

MATRIZ DE VALIDACIÓN POR EXPERTOS PLAN DE TRANSICIÓN DE IPV4 A IPV6 PARA UNA RED LAN

Objetivo:

- Este instrumento tiene como fin validar el Plan de transición de IPv4 a IPv6 para una red LAN construido como parte de un proyecto de investigación.

Experto: Ing. Dennis Clucayza Fecha: 8 de diciembre

Escala de validación: 5 (Muy Satisfactorio) – 4 (Satisfactorio) – 3 (Neutro) – 2 (Poco satisfactorio) – 1 (Nada satisfactorio)

CRITERIOS DE VALIDACIÓN

CRITERIO	DESCRIPCIÓN	Validación					RESULTADO
		5 (100%)	4 (80%)	3 (60%)	2 (40%)	1 (20%)	
Claridad y comprensión	El plan presenta documentación de manera transparente, utilizando un lenguaje claro asegurando que la información sea útil para la audiencia involucrada en la transición de IPv4 a IPv6.	X					
Estructura y Organización	Este criterio busca asegurar que las fases de la transición estén claramente definidas en el plan, proporcionando una guía lógica para la implementación.	X					
Detalles Técnicos	Evalúa la presencia de detalles técnicos y comprensibles en cada fase del plan de transición. Se verifica que los procedimientos y mecanismos técnicos estén descritos de	X					



Pontificia Universidad
Católica del Ecuador

	manera clara y adecuada para el personal en el área de tecnologías de la información.						
Actualización y Relevancia	El plan está basado en información actualizada, estructurado de manera coherente y que la metodología propuesta sea relevante para la transición IPv4 a IPv6.	X					
Recursos considerados	Este criterio evalúa la suficiencia de la información técnica tomada en consideración para la elaboración del plan.	X					
Facilidad de uso y disponibilidad	Este criterio garantiza que el plan sea flexible y compatible como para ser implementado en diversas organizaciones LAN, independientemente de sus configuraciones específicas.	X					

Firma Experto

José Blázquez