Análisis del nivel de implementación en Seguridad de la Información del protocolo IPv6 en una Entidad Distrital

Analysis of the level of implementation in Information Security of the IPv6 protocol in a Government Entity

Juan Carlos Piñeros García[1]
Jimmy Alejandro Ortiz Peláez[2]
Yenny Isabel Serrato Rodríguez[3]

Resumen

El objetivo principal de este documento es analizar cuál es el estado en la implementación del protocolo IPv6 en una entidad pública de orden distrital. El estudio abordó la metodología de investigación cualitativa que permite recopilar información en textos y evidencia descriptiva que establece una guía para el desarrollo del tema. El estudio plantea una serie recomendaciones para mejorar en el desempeño y el correcto funcionamiento de los sistemas de información en concordancia con las buenas prácticas para el aseguramiento del protocolo IPv6 en la infraestructura tecnológica de la organización.
Palabras clave: *Doble Pila, Direccionamiento IP, Protocolo, Nueva Generación, Internet.*

Abstract

The main objective of this document is to analyze the state of the secure implementation of the IPv6 protocol in a public entity of district order. The study addressed the qualitative research methodology that allows us to collect several types of information, theoretical texts, and descriptive evidence to help us establish a guide for the development of the topic. The study proposes a series of recommendations to improve the performance and correct operation of information systems in accordance with good practices for the assurance of the IPv6 protocol in the technological infrastructure of the organization.
Keywords: *Dual Stack, IP Addressing, Protocol, New Generation, Internet.*

I. INTRODUCCIÓN

[1] Nació en Fusagasugá, Colombia. Candidato a Especialista en Seguridad de la Información de la Fundación Universitaria Los Libertadores, Especialista en Telecomunicaciones de la Universidad Piloto de Colombia e Ingeniero de sistemas de la Universidad Antonio Nariño. EMAIL: jcpinerosg@libertadores.edu,co, Es certificado como: Cisco CCNP Enterprise, Cisco CCNP Security, Palo alto PCNSA, Fortinet NSE4, IPv6 Fórum Network/Security Engineer Gold, Auditor Interno ISO 27001:2013, ITIL Fundations v3/v4, Cobit 5, Microsoft MCSA Windows Server 2012/2016, Microsoft Azure Network Engineer Associate, Microsoft Windows Server Hybrid Administrator Associate, VMware VCP 5.0/6.0/6.7 entre otros, con más de 15 años de experiencia en múltiples roles como administrador de infraestructura, especialista en redes y seguridad, consultor en redes y seguridad, oficial de seguridad de la información, gerente de infraestructura, subdirector de infraestructura en empresas públicas y privadas del resorte financiero, estatal, educativo y fabricantes en tecnología.

2 Nació en Bogotá, Colombia. Candidato a Especialista en Seguridad de la Información de la Fundación Universitaria Los Libertadores, Ingeniero de sistemas de la misma Universidad. EMAIL: jaortizp@libertadores.edu.co Con más de 15 años de experiencia en múltiples roles como administrador de infraestructura, desarrollador e ingeniero de soporte en empresas públicas y privadas. Actualmente administrador de sistemas Linux de la Personería de Bogotá.

3 Nació en Bogotá, Colombia. Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniero en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@libertadores.edu.co. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios además docente universitario en varias universidades.

En la actualidad las tecnologías de la información en las entidades gubernamentales del país presentan una constante evolución por la gran cantidad de servicios prestados a la comunidad mediante el uso de herramientas sistematizadas, en el contexto de las nuevas dinámicas en el compartir de la información digital, es necesario, establecer pautas que puedan servir de apoyo para mejorar la percepción en la Seguridad de la Información por parte del público en general.

Para la adopción del protocolo IPv6 se requiere de una planeación adecuada, de tal manera, que se cuente con una organización detallada de los tiempos requeridos para dicha implementación. Durante este proceso, es importante recalcar que las dos versiones (IPv4 e IPv6) deberán coexistir durante un tiempo mientras se logra el cambio; es fundamental, conocer a qué vulnerabilidades podríamos estar expuestos para aplicar las mejores prácticas y estándares, disminuyendo las implicancias de seguridad del nuevo protocolo sobre la infraestructura de red de la entidad.

Se debe tener en cuenta, que las entidades del orden nacional y distrital están en la obligación de apropiarse de las mejores prácticas para los sistemas de información y así, cumplir con el objetivo de prestación del servicio con una plataforma tecnológica segura mediante la utilización del protocolo IPv6.

Un ámbito importante para lograr este objetivo es: recopilar, estudiar y desarrollar una estructura para la aplicación de las buenas prácticas en Seguridad de la Información recomendadas por los entes nacionales o internacionales, que son los encargados de emitir las estrategias para la protección de la información que se transmite por un sistema de información usando el protocolo de comunicaciones IPv6.

La información abordada en este documento fue recopilada bajo la observancia y resguardando la privacidad de los datos de acuerdo con lo que se establece la ley colombiana 1712 de 2014 en el marco general de la Transparencia y del Derecho de Acceso a la Información Pública, se debe tener en cuenta que, la información tratada en este documento es catalogada como pública, según el artículo 19 de la ley en mención, por temas de manejo interno en la entidad y por la criticidad de la información se tomará la generalidad de los datos, modificando algunos ítems para que no sea identificado ningún componente tecnológico fuera del ámbito académico.

En ese orden de ideas, este documento presentará el referente teórico abordado para el estudio, la metodología implementada, los resultados, la discusión y conclusiones generadas para la correcta implementación del protocolo en la entidad.

II. MARCO CONCEPTUAL

A. PROTOCOLO IPV6.

El protocolo de internet versión 6 también llamado IPv6 es la nueva generación para la transmisión de la información por la red global Internet usada hoy en día. Este protocolo permite que todos los dispositivos conectados a internet puedan intercambiar datos. Actualmente, la versión más utilizada es la versión 4 (IPv4) que tiene muchas limitaciones para la puesta en marcha de todas las capacidades que pueden prestar las nuevas tecnologías de la información y para solventar este inconveniente, entre muchos otros, se liberó la nueva versión IPv6, (6NET, 2005, p. 17).

Cabe aclarar que la versión IPv4 se usa aproximadamente desde la década de 1980, sin embargo, en los ambientes tecnológicos es conocida por su limitación en la asignación de nuevas direcciones y por no haber sido desarrollado considerando la transmisión segura de la información. Esta situación originó que, en América Latina, por ejemplo, el bloque de direcciones IPv4 disponibles se agotara en agosto de 2020, según datos de LACNIC (la organización que administra las direcciones IP en la región). Este agotamiento de direcciones IPv4 obligó a que la organización internacional encargada de la normalización de estándares tecnológicos Internet Engineering Task Force (IETF) en el año 1990 desarrollara el nuevo protocolo de Internet IPv6 y su migración comenzó desde su lanzamiento en junio de 2012.

En consecuencia, las principales mejoras que se integraron en Ipv6, son las siguientes:

- *Dirección Ipv6 de 128-bits.*

En lugar de permitir direcciones IP de 32-bits en su formato, por ejemplo, 192.168.120.250 separadas por punto (.), Ipv6 permite utilizar direcciones IP de 128-bits separadas por dos puntos, agrupadas en 8 campos con tamaño de 16-bits representados por 4 dígitos hexadecimales, una dirección IPv6 puede ser del siguiente tipo: 2008:DB80:CAFÉ:0123:ABCD: 2345:0000:1111.

Con el incremento del direccionamiento IP en tamaño a 2^{128} o 3.4×10^{38} trillones de diferentes direcciones IP que se pueden asignar, es un número que en la concepción del cerebro humano no puede ser establecido, pero se puede comparar como el espacio que ocuparía un grano de arena IPv4 en cualquier playa de un planeta IPv6, (Hagen, 2014, p. 40).

- *Nuevo formato para la cabecera del protocolo IPv6.*

El encabezado del protocolo IPv6 se ha reducido a (40 bytes) fijos donde se han eliminado o renombrado campos del protocolo IPv4, pero guardando y mejorando las características en el funcionamiento, se redujo de 14 encabezados en IPv4 a solo 8 encabezados en IPv6, cabe aclarar que no está dentro del alcance de este documento tratar con profundidad cada una de las opciones de los encabezados.

Tabla 1.
Encabezado Protocolo IPv4.

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live		Protocol	Header Checksum
Source Address (32 bits)			
Destination Address (32 bits)			
Options		Padding	

Nota: *Elaboración propia con datos del libro (6NET, 2005, p. 21).*

Tabla 2.
Encabezado Protocolo IPv6.

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address (128 bits)			
Destination Address (128 bits)			

Nota: *Elaboración propia con datos del libro (6NET, 2005, p. 21).*

Los paquetes IPv6 están compuestos por el campo de la cabecera y el campo de la información o datos que se transmiten. El campo de la cabecera como se mencionó en IPv6 es fijo de 40-bytes y contienen las direcciones IP de origen y destino con tamaños de 128-bits cada una, la versión de IP (versión) de 4-bits, clase de tráfico (traffic class) de 8-bits encargada de dar prioridad al paquete, etiqueta de flujo onflow control) de 20-bits encargada de dar calidad de servicio, longitud del campo de datos (payload length) de 16-bits, cabecera siguiente (next header), de 8-bits y límite de campos (hop limit) o el tiempo de vida del paquete. El campo de datos con los que se transportan la información del paquete de tamaño normal (64kb) o el paquete con la opción jumbogram, (6NET, 2005, p. 22).

- *Seguridad Nativa para IPv6.*

En Ipv6 el protocolo de seguridad en internet (Internet Protocol Security IPsec), es obligatorio, fue integrado desde el origen durante el diseño y desarrollo de las especificaciones de IPv6, abarca las políticas de confidencialidad, integridad y autenticación para los paquetes transmitidos en la red. La diferencia con IPv4 (aunque también funciona con Ipsec), es que se debe utilizar en complemento con soluciones de terceros para su correcta integración. La tecnología (IPsec) asegura y protege la comunicación de extremo a extremo sin importar el dispositivo que origina o recibe la transmisión del paquete IPv6 en la red o redes de comunicaciones, (6NET, 2005, p. 246).

- *Calidad de servicio (Quality of Service QoS) en IPv6.*

La calidad de servicio en IPv6 se implementa en la etiqueta de Flujo (Flow Label) en el encabezado del protocolo. Esta opción permite dar alta prioridad a los paquetes que se envían a un destino en cierto rango de tiempo, por ejemplo, la transmisión del tráfico de telefonía VoIP que no soporta retardos en la emisión de los paquetes, sobre el tráfico de video que soporta retardo en la transmisión de datos, sin afectar el desempeño.

- *Autoconfiguración (Auto-configuration) IPv6.*

IPv6 tiene la habilidad de facilitar la configuración automática del direccionamiento mediante el uso de las opciones de configuración “stateful” que permite utilizar el Dynamic Host Configuration Protocol (DHCP) externo que almacena las entradas de las direcciones IP asignadas a un dispositivo y la configuración “stateless” que no utiliza un servidor DHCP externo para la asignación del direccionamiento IP a un nodo, (Hagen, 2014, p. 28).

- *Nuevos Encabezados de Extensión, (Extension Headers) en IPv6.*

Los encabezados de extensión son las opciones adicionales que permite al protocolo IPv6 procesar los paquetes de información que se transmiten en la red de manera más eficiente, estos encabezados se encadenan y pueden estar presentes en su totalidad o parcialmente, de acuerdo con la necesidad que se presente en ese momento al realizar la transmisión de los datos, para el protocolo IPv6 se definieron 6 encabezados de extensión que se enumeran de acuerdo con el orden encadenado por IPv6 durante la transmisión de un paquete.

1) *Encabezado de Salto (Hop-by-Hop Options Header):* Encargado de transportar la información que debe ser procesada por todos los nodos a lo largo del camino, por ejemplo, las características de los protocolos de enrutamiento como distancia administrativa, métrica entre otros, (Hagen, 2014, p. 80).
2) *Encabezado de Enrutamiento (Routing Header):* Similar al que utiliza IPv4, es el encargado de establecer la secuencia de saltos, nodos, dispositivos que el paquete de datos debe cruzar antes de alcanzar su destino, (Hagen, 2014, p. 82).
3) *Encabezado de Fragmentación (Fragmentation Header):* Envía los paquetes fragmentados (máximo tamaño del paquete transmitido o MTU) en IPv6, su funcionamiento es similar a IPv4, divide el paquete si es mayor al tamaño permitido, le asigna un identificador y luego vuelve a ensamblar cuando se necesite, (Hagen, 2014, p. 85).
4) *Encabezado de Autenticación (Authentication Header AH):* Se utiliza en complemento con IPsec para proveer autenticación y garantizar la integridad de los paquetes trasmitidos, (Hagen, 2014, p. 217).
5) *Encabezado de Encapsulamiento de Seguridad del Paquete (Encapsulating Security Payload ESP Header):* encargado de aportar autenticación y cifrado para los paquetes trasmitidos, (Hagen, 2014, p. 220).
6) *Encabezado de Opciones Destino (Destination Options Header):* Contiene las opciones que deben ser procesadas por el nodo destino del paquete, como por ejemplo la verificación de los saltos, la carga útil del paquete, (Hagen, 2014, p. 88).

- *Nueva versión del Internet Control Message Protocol (ICMP) para IPv6.*

Protocolo de comunicaciones que se ubica en la capa 2 (data link / enlace) del modelo de interconexión OSI (Open System Interconection Model), es el encargado de reportar los errores, realizar diagnóstico y establecer los mensajes de información de las características de la red. Fue definido para IPv6 como ICMPv6 y forma parte directa de las especificaciones desarrolladas para el estándar de IPv6. Es el pilar fundamental para el funcionamiento de las herramientas IPv6 como el descubrimiento de vecinos (Neighbor Discovery) que ayuda a determinar la MAC del nodo de red, encontrar los routers vecinos, determinar los prefijos de la red IPv6, encontrar direcciones IP duplicadas entre otras funcionalidades, también es importante para los mecanismos de autoconfiguración IP “stateless”, el descubrimiento de la menor unidad de transmisión MTU (Maximun Transmit Unit) durante la transmisión del paquete de datos, (Hagen, 2014, p. 95).

- *Tipos de direcciones IPv6.*

Para finalizar esta breve explicación del protocolo IPv6 y su importancia en la actualidad, es necesario, conocer los diferentes tipos de direcciones IPv6 que existen y sus principales características.

- Direcciones tipo *Unicast:* Son las direcciones que identifican una interfaz en un dispositivo electrónico que utilice IPv6, de modo que un paquete enviado a otro dispositivo que también utilice IPv6 con una dirección unicast lo recibirá, también se puede entender como una transmisión de información punto a punto o uno a uno.

  Dentro de las direcciones unicast se pueden encontrar las direcciones "Global" que son las encargadas de transmitir los datos entres las redes de comunicaciones o también llamadas enrutables en internet (ejemplo 2800:ffff:cd::1111/48). Las direcciones "Enlace Local" utilizadas para los ámbitos locales en la comunicación del protocolo IPv6 (ejemplo FE80:/64, loopback ::1) y las direcciones "ULA" (Unique Local Address) que son direcciones enrutables en internet que deben ser utilizadas en ambientes locales en vínculo con las direcciones globales (ejemplo FC00::/7), las direcciones "ULA" se consideran obsoletas, (6NET, 2005, p. 31).

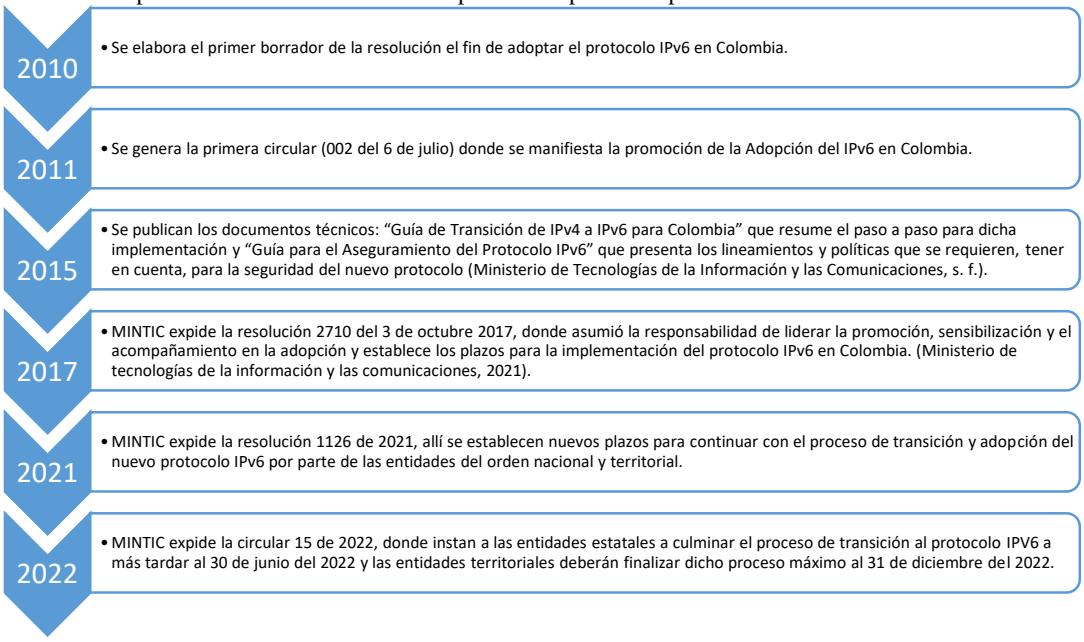
- Direcciones tipo Anycast: Se identifica como una asociación de interfaces que permite enviar a una dirección anycast un paquete a la interfaz o interfaces más cercanas de acuerdo, con la medida del protocolo de enrutamiento utilizado, también es conocida como una transmisión de uno a uno de muchos, (6NET, 2005, p. 32).

- Direcciones tipo *Multicast:* También son un conjunto de interfaces, pero el paquete transmitido se entrega a todas las interfaces asociadas a esa dirección, es conocida como una transmisión de uno a muchos, (6NET, 2005, p. 33).

B. MARCO NORMATIVO IPV6 EN COLOMBIA.

Con el fin de lograr la innovación tecnológica que exige el país, las entidades del estado deben adherirse en el proceso de conversión del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la circulares, decretos, manuales, resoluciones y demás guías establecidas por el MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) que buscan promover la adopción de IPv6 en Colombia y que desde 2009, ha venido liderando esta transición y busca que proveedores, entidades del gobierno y sector privado, decidan migrar hacia allá (ver figura 1).

Figura 1
Línea de tiempo de la normativa de MINTIC para la adopción del protocolo IPV6 en Colombia



Nota: Datos obtenidos del sitio de MINTIC

C. ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN

- **NORMA ISO 27002/IEC VERSIÓN 2022.**

Con la implementación de esta guía se pueden establecer los controles que son la base de evaluación de riesgos de los activos más importantes de la empresa, la ISO 27002:2022 se puede utilizar para apoyar la implantación del SGSI en cualquier tipo de organización, pública o privada y no sólo en las empresas de tecnología.

Su principal objetivo es definir directrices y principios generales para iniciar, realizar, conservar y optimizar la gestión de la seguridad de la información en una organización, también incluye la selección, ejecución y administración de los controles, tomando en consideración los entornos de riesgo encontrados.

La norma ISO 27002 ofrece diferentes recomendaciones de las mejores prácticas en gestión de seguridad de la información definida en el estándar como "la preservación de la confidencialidad, integridad y disponibilidad". Se encuentra organizada en 93 controles y dividida en 4 cláusulas que se enfocan hacia la aplicación controles.

- **ESTÁNDAR INTERNACIONAL EN SEGURIDAD INFORMÁTICA DEL "NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)", EN SU DOCUMENTO "GUIDELINES FOR THE SECURE DEPLOYMENT OF IPV6".**

El Instituto Nacional de Normas y Tecnología (NIST) desarrolló un marco para la mejora de la seguridad cibernética en infraestructuras críticas conocido como NIST Cibersecurity Framework que utiliza un lenguaje común para gestionar y reducir los riesgos de ciberseguridad, así como, proteger su información, este fue inicialmente emitido en los Estados Unidos en febrero de 2014 y a la fecha se encuentra disponible la

versión 1.1 emitida en abril de 2.018, comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

Este marco recopila las mejores prácticas de las normas y estándares internacionales y las agrupa según semejanza, contempla un conjunto de actividades, resultados y referencias informativas comunes en la infraestructura crítica y proporciona una orientación detallada para generar perfiles únicos, que mediante su uso, ayudan a alinear las actividades de ciberseguridad con sus requisitos, tolerancias de riesgo y recursos proporcionando un mecanismo para comprender las características y peligros en ciberseguridad.

El Núcleo del Marco consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar las cuales brindan un conjunto de actividades que buscan lograr resultados específicos de ciberseguridad, no es una lista de comprobación de las acciones a realizar, muestra los resultados clave de ciberseguridad identificados por la industria como útiles para gestionar el riesgo.

Los niveles de implementación permiten catalogarse en un umbral predefinido en función de las practicas modernas de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones propias.

III. METODOLOGÍA

Esta investigación se desarrolló en tres etapas: la primera, el levantamiento de la información; la segunda, un diagnóstico de la situación actual de una entidad distrital seleccionada, y finalmente el estudio de la información recopilada y los estándares en seguridad de la información seleccionados.

- **Primera Etapa: Levantamiento de Información.**

En esta fase se realizan las actividades para la consecución de la información necesaria para alcanzar el objetivo que se desarrolla en este documento. El levantamiento de la información fue realizado personalmente basado en el conocimiento y acceso que se tiene a la infraestructura de redes y servidores de la entidad, ejecutando los comandos necesarios para obtener los datos de dispositivos de red, servidores y demás elementos que componen la estructura tecnológica

- **Segunda Etapa: Diagnostico de la Situación Actual.**

En esta fase se realizó el diagnóstico de la situación para seguridad de la información del servicio IPv6 para los componentes antes identificados, de la subred servidores y los servicios base seleccionados en la entidad.

- **Tercera Etapa: Estándares en Seguridad de la Información.**

En esta fase se realizó el análisis de las dos normas (ISO/IEC 27002:2022 y NIST Cibersecurity Framework) utilizadas para generar las recomendaciones a la entidad, con el fin de asegurar el protocolo IPv6.

IV. RESULTADOS Y DISCUSIÓN.

- **Levantamiento de Información.**

La consecución de los datos que se utilizaron como insumo para realizar el análisis y la elaboración de este documento, fueron tomados de la fuente directa que origina la información, una entidad pública de orden distrital.

Pese a que la información obtenida, se clasifica como pública, al no contar con la autorización oficial para su divulgación se realizará ofuscación de los datos sensibles que no permita identificar la entidad o la información utilizada durante la elaboración del documento.

- **Segunda Etapa: Diagnostico de la Situación Actual.**

1. *Tabla direccionamiento IPv6 para la subred de servidores entidad.*

Actualmente, la entidad tiene asignado un pool de direccionamiento IPv6 de tipo global o enrutable en internet con el prefijo de red /64 con el proveedor de comunicaciones Empresa de Telecomunicaciones de Bogotá (ETB) en la ciudad de Bogotá y sólo una red virtual (virtual LAN), con un solo direccionamiento IPv6 con prefijo /64 asignado para todos los servidores de la infraestructura tecnológica en la entidad.

Tabla 3.
Direccionamiento IPv6 subred de servidores.

Prefijo IPv6	Direccionamiento	Descripción
Proveedor	2800:26XX:004D::/48	Pool de direccionamiento IPv6 global que asigno el proveedor a la entidad.
Subred servidores	2800:26XX:004D:0X00::/64	Subred /64 asignada para el segmento de los servidores de aplicación de la entidad.

Nota: *Elaboración propia con datos seleccionados de la entidad para el estudio IPv6.*

Se debe aclarar que todos los servicios de “Out Band Management” (OBM) llamados servicios administradores fuera de banda, ejemplos: “on board administrator”, consolas de gestión de switches SAN, direcciones IP de administración de sistemas de virtualización (KVM o Hyper-v, sistemas de control ambiental, etc.), también se están ejecutando sobre la misma red de los servidores de aplicación de la entidad.

2. *Servicios base tecnológicos utilizados para el ejercicio académico.*

Se realiza la selección de los siguientes servicios base (servicio base, son las aplicaciones que para cualquier tipo de negocio o entidad que utilicen elementos de tecnología, son necesarios para el funcionamiento inicial de cualquier servicio que se preste interno en la compañía o externo a los clientes), entre estos, podemos encontrar los controladores de dominio, el conmutador (switch) de la granja de servidores, la página web de la entidad, etc.

Tabla 4.
Servicios base seleccionados estudio IPv6.

#	Servicio	Sistema Operativo	Nombre Máquina	Dirección IPv4 / IPv6	Descripción
1	DNS	Windows Server 2016 STD x64	dc-tt.uaxxx.gov.co	192.168.2X0.89/24 2800:26XX:4D:2X0::89/64	Este servicio se presta la resolución de nombres contra direcciones IP en la red interna de la entidad.
2	AD/DC	Windows Server 2016 STD x64	dc-tt.uaxxx.gov.co	192.168.2X0.89/24 2800:26 XX:4D:2X0::89/64	Servicio encargado de establecer la autenticación centralizada para los usuarios de la entidad.
3	DHCP	Windows Server 2016 STD x64	dc-tt2.uaxxx.gov.co	192.168.2X0.20/24 2800:26 XX:4D:2X0::20/64	Provee el direccionamiento IPv6 automático para los usuarios de la entidad.
4	NAS / SAN	HPE EVA 4400	sas-srv.uaxxx.gov.co	192.168.2X0.225/24 2800:26 XX:4D:2x0::225/64	Elemento de cómputo donde se almacena la información digital y algunos servidores virtuales de la entidad.
5	Switch granja servidores	HPE 5130	HPE	192.168.2X0.3/24 2800:26 XX:4D:2X3::3/64	Dispositivp de red que proporciona la conectividad a los equipos máquinas tipo servidor que están en el centro de cómputo de la entidad.

Nota: *Elaboración propia con datos seleccionados de la entidad para el estudio IPv6.*

3. *Estudio de las metodologías en seguridad de la información y seguridad informática seleccionadas.*

Se decide usar la norma internacional ISO/IEC 27002 en su versión 2022 por ser un estándar internacional reconocido y aceptado a nivel mundial y la guía en seguridad del protocolo IPv6 de la NIST al ser un organismo acreditado en la comunidad internacional en tecnología que avalan las buenas prácticas en la Seguridad de la Información e Informática.

Controles de la ISO/IEC 27002:2022 utilizados para el ejercicio académico.

En el desarrollo de este documento se utilizarán cinco (5) controles de la norma ISO/IEC 27002:2022, que fueron seleccionados teniendo en cuenta el criterio, conocimiento y la experticia adquirida a través del tiempo, de acuerdo con el resorte de la información recopilada.

A continuación, se describen los controles y numerales que fueron seleccionados de la norma ISO/IEC 27002:2022, con estos controles y numerales se efectúa el análisis para cada uno de ellos y de acuerdo con los resultados obtenidos, se aplican los contenidos aprendidos para generar las recomendaciones en el aseguramiento del protocolo IPv6 en la entidad.

Control 8.17 “Sincronización de reloj”.

Este numeral es el encargado de recomendar las actividades que se deben implementar en la infraestructura tecnológica que facilite establecer las pautas para la correcta configuración de los sistemas de sincronización de la hora en los sistemas informáticos. Permitiendo correlacionar los eventos que se puedan presentar cuando ocurra un incidente en seguridad. De los cinco (5) ítems analizados para este control fueron seleccionados cuatro (4) para utilizarlos en la metodología de estudio, pueden ser verificados en la tabla mostrada a continuación.

Tabla 5.
Control 8.17 ISO/IEC 27002 – 2022.

8.17. Sincronización del reloj

Tipo de control	Información Propiedades de seguridad	La seguridad cibernética conceptos	Capacidad Operacional	Dominios de seguridad
#Detectivo	#Integridad	#Proteger #Detectar	#Seguridad_información_ Administración_eventos	#Protección #Defensa

Control

Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.

Propósito

Permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y respaldar las investigaciones sobre incidentes de seguridad de la información.

Guía	Seguridad IPv6
3. Se debe utilizar dos fuentes externas de sincronización confiable al mismo tiempo para evitar variación.	Se utiliza para emitir recomendaciones en seguridad sobre IPv6.
4. No es recomendable utilizar múltiples servicios de sincronización externos como locales, en este cao se debe monitorear cada servicio para mitigar los riesgos derivados de las diferencias.	
5. La configuración correcta de los relojes de las computadoras es importante la precisión de los registros de eventos, que puedan ser necesarios para las investigaciones o como evidencias en casos legales y disciplinarios. Los registros de auditoria inexactos pueden dificultar dichas investigaciones y dañar dicha evidencia.	

***Nota**: Elaboración propia con datos seleccionados de la norma, (ISO/IEC, 2022, p.108).*

Control 8.20 “Seguridad de redes”.

Este numeral permite establecer las recomendaciones que se deben seguir para proteger correctamente las redes y los dispositivos de red que son los encargados de realizar la transmisión de la información que circula por la red de comunicaciones de la entidad. De los quince (15) ítems analizados para este control fueron seleccionados nueve (9) para utilizarlos en la metodología de estudio, pueden ser verificados en la tabla mostrada a continuación.

Tabla 6.
Control 8.20 SGSI ISO/IEC 27002 – 2022.

8.20. Seguridad de redes.

Tipo de control	Información Propiedades de seguridad	La seguridad cibernética conceptos	Capacidad Operacional	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Integridad #Disponibilidad	#Proteger #Detectar	#Sistema_seguridad_red	#Protección

Control

Las redes y dispositivos de red deben protegerse, administrase y controlarse para proteger la información en los sistemas y aplicaciones.

Propósito

Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.

Guía	Seguridad IPv6
1. El tipo y nivel de clasificación de la información que la red puede soportar.	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.
2. Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red.	
3. Mantener la documentación actualizada, los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores).	
4. Separar la responsabilidad operática de las redes de las operaciones del sistema TIC cuando corresponda (ver 5.3)	
5. Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes públicas, redes de terceros o redes inalámbricas para proteger los sistemas y aplicaciones conectados (ver 5.22, 8.24, 5.14 y 6.6). También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y las computadoras conectadas a la red.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
6. Registro y monitoreo adecuados para permitir el registro y detección de acciones que puedan afectar o son relevantes para la seguridad de la información (ver 8.16 y 8.17).	
7. Coordinar estrechamente las actividades de gestión de la red para optimizar el servicio a la organización como para garantizar que los controles se apliquen de forma coherente en toda la infraestructura de procesamiento de la información.	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.
8. Sistemas de autenticación de red.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
9. Restringir y filtrar la conexión de los sistemas a la red (por ejemplo, usando firewalls).	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.
10. Detectar, restringir y autenticar la conexión de equipos y dispositivos de red.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
11. Endurecimiento de los dispositivos de red.	
12. Segregar las subredes de administración de red a otro tráfico de red.	
13. Aislar temporalmente subredes criticas (por ejemplo, DMZ, honeypot) si la red está bajo ataque.	
14. Deshabilitar protocolos de red vulnerables.	
15. Las organizaciones deben garantizar que se apliquen controles de seguridad adecuados al uso de redes virtualizadas o definidas por software.	

***Nota**: Elaboración propia con datos seleccionados de la norma, (ISO/IEC, 2022, p.111).*

Control 8.21 “Seguridad de los servicios de red”.

Numeral encargado de emitir todas las recomendaciones para establecer las tareas que pueden ayudar a asegurar el transporte de la información digital de los sistemas de información por la red de datos de la entidad, sin diferenciar sí la transmisión de esta información utiliza el protocolo IPv4 o IPv6. De los diez (10) existentes en el control fueron seleccionados nueve (9) para utilizarlos en la metodología de estudio, pueden ser verificados en la tabla mostrada a continuación.

Tabla 7.
Control 8.21 ISO/IEC 27002 – 2022.

8.21. Seguridad de los servicios de red.

Tipo de control	Información Propiedades de seguridad	La seguridad cibernética conceptos	Capacidad Operacional	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_seguridad_red	#Protección

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben identificarse, implementarse y monitorearse.

Propósito

Para garantizar la seguridad en el uso de los servicios de red.

Guía	Seguridad IPv6
1. Las redes y los servicios de red a los que se permite acceder.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
2. Requisitos de autenticación para acceder a los diversos servicios de red.	
3. Procedimiento de autorización para determinar quién puede acceder a que redes y servicios en red.	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.
4. Administración de redes y controles tecnológicos y procedimientos para proteger el acceso a conexiones de red y servicios de red.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
5. Hora, ubicación y otros atributos del usuario al momento del acceso.	
6. Seguimiento del uso de los servicios de red.	
7. Tecnología aplicada para la seguridad de los servicios de red, como autenticación, encriptación y controles de conexión a la red.	
8. Parámetros técnicos requeridos para la conexión segura a los servicios de red de acuerdo con las normas de seguridad y conexión a la red.	
9. Almacenamiento en cache (por ejemplo, en una red de entrega de contenido y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en cache de acuerdo con los requisitos de rendimientos, disponibilidad y confidencialidad.	
10. Procedimiento para el uso de servicios de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.	

***Nota**: Elaboración propia con datos seleccionados de la norma, (ISO/IEC, 2022, p.112).*

Control 8.22 “Segregación de redes”.

Se establecen los mecanismos recomendados para realizar una diferenciación de los servicios que circulan en la red de datos de la entidad, mediante la división lógica de dominios de red físico o lógicos. De los tres (3) ítems analizados fueron seleccionados dos (2), para aplicarlos en la metodología de estudio, pueden ser verificados en la tabla mostrada a continuación:

Tabla 8.
Control 8.22 ISO/IEC 27002 – 2022.

8.22. Segregación de redes.

Tipo de control	Información Propiedades de seguridad	La seguridad cibernética conceptos	Capacidad Operacional	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_seguridad_red	#Protección

Control

Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en las redes de la organización.

Propósito

Para dividir la red en límite de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales.

Guía	Seguridad IPv6
1. Las redes en dominios de red separados de lo público y lo privado, o niveles de confianza, criticidad y sensibilidad (por ej., dominio acceso público, dominio escritorio domino servidores, sistemas de alto riego, etc.).	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
2. Política de seguridad especifica para cada dominio de red de acuerdo con el control de acceso necesario.	
3. Tratamiento especial para redes inalámbricas.	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.

***Nota**: Elaboración propia con datos seleccionados de la norma, (ISO/IEC, 2022, p.113).*

Control 8.23 “Filtrado web”.

Tabla 9.
Control 8.23 ISO/IEC 27002 – 2022.

8.23. Filtrado Web.

Tipo de control	Información Propiedades de seguridad	La seguridad cibernética conceptos	Capacidad Operacional	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Sistema_seguridad_red	#Protección

Control

El acceso a los sitios web externos debe administrase para reducir la exposición al contenido malicioso.

Propósito

Para dividir los sistemas contra el malware y evitar el acceso a los recursos web no autorizados.

Guía	Seguridad IPv6
1. Las organizaciones deben reducir los riegos de que su personal acceda a sitios web peligrosos. La organización está en la obligación de identificar y bloquear los sitios web peligrosos para los usuarios.	Se utiliza parcialmente para emitir recomendaciones en seguridad IPv6 para el ámbito de ls subred de servidores.
2. Establecer las políticas sobre uso seguro y apropiado de los recursos en línea.	
3. Tratamiento especial para redes inalámbricas.	No se utiliza para el análisis porque es un procedimiento ya implementados en la entidad.

***Nota**: Elaboración propia con datos seleccionados de la norma, (ISO/IEC, 2022, p.114).*

Este numeral posibilita las actividades que se deben establecer para proteger los sistemas de información que están publicados por medio se servicios web en la red interna o externa de la entidad. De los tres (3) ítems analizados se seleccionó uno (1) para aplicarlos en la metodología de estudio, pueden ser verificados en la tabla mostrada a continuación.

Numerales seleccionados del estándar “Guidelines for the secure Deployment of IPv6” del National Institute of Standars and Technology (NIST).

Se seleccionan los siguientes numerales del documento para ser trabajos en concordancia y sincronía con las demás buenas prácticas en seguridad seleccionadas, a continuación, se realiza la mención de cada uno de ellos.

Para el tercer capítulo del documento nombrado “*3. IPv6 Overview (Descripción General de IPv6*”), se trabaja el siguiente numeral.

3.2.1 IPv6 Address Assignments, (Asignamiento del direccionamiento IPv6)

En este numeral sirve para realizar el diseño correcto del espacio para el direccionamiento IPv6 en la entidad, que se adecúe y sea óptimo en su implementación y funcionamiento. También, se tratan las recomendaciones para la correcta asignación del direccionamiento IPv6 mediante el uso de las estrategias de movimiento entre nibbles a la izquierda, al centro o a la derecha, para así, surtir un espacio de direccionamiento eficientemente, (NIST, 2008, p. 34).

Para el sexto capítulo del documento nombrado "*6. IPv6 Deployment (Descripción general de IPv6)*", con la información contenida en los puntos seleccionados de la norma se establecerá un campo más amplio para realizar las recomendaciones para la implementación del protocolo IPv6 que actualmente está ejecutándose en la entidad, en relación, con los temas de seguridad informática y de la información, a continuación, se describen de forma general los literales de cada uno de los numerales seleccionados.

6.1 Security Risks (Riesgos de Seguridad).

Capítulo de la norma donde se mencionan las características en los posibles ataques en la red de datos que se pueden efectuar mediante el uso del protocolo IPv6.

6.1.1 Attacker comunity (Ámbito de Ataque).

Se pueden encontrar como las amenazas en seguridad se están adaptando a la nueva tecnología que se está utilizando para el protocolo IPv6 y ahora no solo, es necesario, proteger las redes que se publican en internet con IPv4 si no también con IPv6. Con el fin de evitar ataques, es necesario que, la entidad establezca los controles para mitigar la amenazas en seguridad internas o externas, (NIST, 2008, p. 123).

6.1.3 Vulnerabilidades en IPv6 (Vulnerabilities in IPv6)

Se pueden encontrar fallas durante la Implementación del protocolo IPv6 en la integridad o la confidencialidad y como IPsec resuelve este problema, aunque no es la solución definitiva para todos los casos, por ejemplo, los ataques de hombre en el medio se pueden seguir realizando en redes IPv6 aprovechando las nuevas características, también se pueden explotar las vulnerabilidades en la ejecución del protocolo IPv6 en sistemas operativos "Legacy". IPv6 al no utilizar ARP (Address Resolution Protocol) para la resolución de direcciones MAC (Media Control Access) contra las direcciones IP y utilizar ICMP para el descubrimiento de la mayoría de las funcionalidades básicas de la red es un blanco para que los atacantes exploten vulnerabilidades en el protocolo IPv6 por falencias en las configuraciones en seguridad, (NIST, 2008, p. 125).

Para finalizar, se deben tener en cuenta, las vulnerabilidades que se puedan presentar al realizar el diseño del direccionamiento IPv6 y los problemas que las opciones de autoconfiguración, DHCPv6 con la intrusión de servidores DHCP (no permitidos) en la red IPv6, enfocando todas las lecciones aprendidas implementado las buenas prácticas en seguridad que permitan reducir la superficie de ataque en IPv6.

6.1.4 Operación Dual (Dual Operations).

Al tener implementación de doble pila IPv4/IPv6 ya sea por el método seleccionado para realizar la implementación de IPv6 o porque existan aplicaciones que solo funcionan con la pila IPv4, se aumenta la complejidad para la administración de la infraestructura de red en la entidad, aumentan las configuraciones a realizar, adquirir elementos de cómputo compatibles con las dos pilas de protocolo y establecer controles para mitigar los riesgos asociados a cada tipo de ataque según el tipo de protocolo IPv4/IPv6, (NIST, 2008, p. 126).

6.2 Seguridad del Direccionamiento (Addressing Security).

Capítulo de la norma donde se establece como una correcta definición para el plan del direccionamiento IPv6 en la entidad puede facilitar de múltiples formas la implementación de medidas para disminuir las amenazas en la seguridad y privacidad de la información.

6.2.1 Plan de Direccionamiento (Numbering Plan).

Se establecen las pautas para que la entidad implemente un plan de asignación para el direccionamiento IPv6, la entidad deberá contar con el prefijo /48 para que soporte hasta 65.535 subredes con prefijo /64, el plan de numeración debe manejar un modelo de numeración que permita realizar la entrega de los segmentos de red de manera ordenada y

localizando los espacios mediante el uso de direccionamientos con los prefijos /48, /56 o /64. El uso de un buen modelo de direccionamiento IPv6 facilitará la configuración de las características en seguridad en los dispositivos de seguridad o los dispositivos de enrutamiento externo, (NIST, 2008, p. 127).

6.2.2 Direccionamiento Jerárquico para asegurar la Segmentación de Red Segura (Hierarchical Addressing to Support Security Segmentation).

La asignación del direccionamiento IP es diferente para los protocolos IPv4 que para IPv6, se debe tener en cuenta que, para el protocolo IPv6 la configuración de las subredes puede soportar un número gigantesco de direcciones que pueden ser asignadas a un dispositivo o usuario, lo que permite "desperdiciar" espacios de direcciones sin problemas. Para ayudar a facilitar esta configuración se debe utilizar un modelo de direccionamiento jerárquico que se base en la segmentación y no en la cantidad de direcciones IP, también que tenga en cuenta, los requerimientos en seguridad, el aislamiento de los ambientes, la protección de sitios, enlaces, dispositivos, etc. Algunos métodos utilizados para la segmentación del espacio IPv6 son: subredes con numeración secuencial, números de vlans (virtual lans), números de Sistema Autónomo (AS), numeración de los segmentos IPv4, localizaciones físicas, unidades de negocio, o combinación entre algunas o todas las mencionadas. El diseño seleccionado debe simplificar la seguridad y la administración de los recursos o servicios que se transmitan sobre la infraestructura IPv6, (NIST, 2008, p. 128).

6.2.4 Administración del Direccionamiento (Address Management).

Se deben considerar las implicaciones en seguridad para los mecanismos como: la administración del direccionamiento, la autoconfiguración y la configuración manual. Los tres escenarios definidos tienen sus ventajas y desventajas de acuerdo al modelo de negocio que tenga la organización en ese momento, para la entidad en cuestión se está utilizando el método DHCPv6 statefull que permite la asignación del direccionamiento IPv6 automático de manera centralizada, evitando el uso de direcciones generadas por EUI-64 que pueden ocasionar riesgos de seguridad o por asignación manual que, aunque el método es bueno por lo extenso de los espacios en IPv6, sólo es recomendable para los servicios que necesiten tener asignada siempre la misma dirección IP, (NIST, 2008, p. 129).

6.4 Entornos de Doble Pila IPv4/IPv6 (Dual Stack IPv4/IPv6 Environments).

Capítulo de la norma donde se mencionan las características de los posibles inconvenientes en seguridad en la red de datos cuando se implementa mal la tecnología Doble pila para los protocolos IPv4 e IPv6.

6.4.1 Despliegue Ambiente de Doble Pila (Deployment of a Dual Stack Enviroment).

Se debe aclarar que la pila de protocolo IPv4 no es compatible con la pila del protocolo IPv6, esto quiere decir que el tráfico que se envía por IPv4 no puede ser procesado por IPv6 y la transmisión realizada en IPv6 no puede ser procesada por IPv4. Por eso se definió el modelo de transición Dual-Stack o también llamado doble pila, que permite a los dispositivos procesar los paquetes que se generan por IPv4 o IPv6 al mismo tiempo. A nivel de capa 2, se puede utilizar un tag de VLAN para separar los tráficos, pero en capa 3 la división del tráfico se configura de acuerdo a la necesidad y al tipo de protocolo de enrutamiento que se esté utilizando, al tener implementado este modelo de transición se pueden presentar inconvenientes como: mantener tablas de enrutamiento diferentes para IPv4/IPv6, protocolos de enrutamiento para cada uno, implementación en seguridad para cada uno, calcular el ancho de banda para cada tipo de tráfico de acuerdo con el protocolo utilizado, características en seguridad en los dispositivos tipo firewall, AAA, NAS, configuraciones en los servidores de nombre DNS relacionados con IPv6, (NIST, 2008, p. 132).

6.4.2 Direccionamiento en Ambiente de Doble Pila (Addressing in Dual Stack Environment).

El procesamiento de las tareas que se general por IPv4/IPv6 son cubiertas por cada uno, independiente de la tecnología de transición, para la asignación del direccionamiento IP automático, se debe tener en cuenta que el servicio DHCPv4, es diferente en su funcionamiento al DHCPv6 y cada uno debe tener su propio servicio configurado, (NIST, 2008, p. 132).

6.4.3 Implicaciones en Seguridad para Despliegues en Doble Pila (Security Implications of a Dual Stack Environment)

Al utilizar este método de transición, los dos protocolos IPv4 e IPv6 amplían la superficie de ataque porque se deben asegurar las dos pilas del protocolo que funcionan diferente y pueden generan vulnerabilidades en el proceso de interacción entre ellas, (NIST, 2008, p. 133).

A). Diagnóstico de la seguridad del servicio IPv6 en la entidad.

Como resultado de haber realizado el estudio de la información recopilada en el numeral anterior, se establece el siguiente diagnóstico sobre la implementación de las buenas prácticas en seguridad de la información para el protocolo IPv6 en la entidad para los siguientes ítems.

1. Diagnóstico subred servidores IPv6.

Al efectuar el estudio de la información que fue recopilada con las tablas del direccionamiento IPv6, por donde se transmite la información que es procesada por los sistemas de cómputo de la entidad, se encontró lo siguiente: en cuanto a la configuración implementada con miras al funcionamiento del protocolo de comunicaciones IPv6 de forma segura de acuerdo con los estándares internacionales.

El proveedor de telecomunicaciones le facilitó a la entidad un prefijo de red /48 IPv6 de tipo global para el uso e implementación del protocolo IPv6, aun así, se debe aclarar que, aunque se ahorra en costos económicos, al recibirlo del proveedor, se corre el riesgo que al cambiar de ISP (Internet Service Provider) a futuro, se deba realizar de nuevo las configuraciones, ya que este prefijo de red no pertenece a la entidad sino a la empresa proveedora, que le presta el servicio.

La entidad cuenta con un pool de direccionamiento IPv6 global con prefijo de red /48, dividido o segmentado de la forma básica, no por eso segura, en segmentos de tamaño /64 resultado 65535 redes cada una con un espacio para la asignación de direccionamiento IP con un prefijo /64 para la entidad. Esta forma de segmentar un pool IPv6 es la más insegura (no se recomienda en el diseño porque no permite la correcta gestión del direccionamiento ni su aseguramiento), además de no ser sencilla su administración, se realizó así, para facilitar la implementación y por temas de desconocimiento del personal asignado.

La implementación actual del protocolo IPv6 en la entidad se llevó a cabo mediante el modo de convivencia con la infraestructura que se ejecuta en IPv4, como beneficio no se interrumpe el servicio que se ejecuta en IPv4, como desventaja la transición hacia IPv6 es lenta y la sobrecarga en el cómputo de los dispositivos de red es más alta para el procesamiento de los paquetes en simultánea para IPv4 e Ipv6.

La subred de servidores utilizada en la entidad con el método para la segmentación del pool o prefijo IPv6, fue la número #513 de las 65535 redes disponibles del pool /48 asignado por el proveedor de telecomunicaciones, este segmento de red IPv6 es: “2800:26XX:004d:0X00::/64”, como se puede observar para la selección de este segmento de red, para los servidores de la entidad se realizó una asociación entre el tercer octeto de la dirección IPv4 “192.168.X00.0/24”, con el cuarto grupo de nibbles

(en el contexto IPv6 es la agrupación de 4 bits que genera un carácter hexadecimal de la dirección de red), de la dirección IPv6, se debe aclarar que la asignación aunque correcta en su funcionamiento, la lógica no corresponde cien por cien en la definición ya que en IPv4 los valores son decimales y en IPv6 hexadecimales, a continuación se explica:

Tabla 10.
Asociación direccionamiento IP actual.

	Decimal	Hexadecimal
Tercer Octecto IPv4	200	00c8
Cuarto Grup IPVv6	200	512

Nota: *Elaboración propia.*

No se encuentran separados en su estructura lógica los servicios y ambientes de producción, desarrollo y pruebas ya que se utiliza la misma subred para todos los servidores por donde se transmite la información de la entidad.

No solo el tráfico de la de la subred de servidores está siendo transmitido por este segmento, sino que además se encuentra configurado otro tipo de dispositivos en este este espacio de direccionamiento IP que debería ser exclusivo para los servidores de cómputo de la entidad como: teléfonos, sistemas de control ambiental, sistemas biométricos, usuarios finales, etc.

El dispositivo de red switch donde están conectados todos los dispositivos físicos de cómputo (servidores), está implementado por defecto en la virtual lan (VLAN) 1 sin configurar alguna característica en seguridad para IPv4 o IPv6.

Para finalizar, se pudo establecer que las configuraciones realizadas para la implementación del protocolo IPv6 en la entidad, son por defecto, que definen los fabricantes para cada uno de los servicios que se ofrecen, que no establecen las pautas mínimas en la configuración para asegurar la transmisión de los datos por los sistemas de información por la red con el protocolo IPv6.

2. *Diagnóstico servicios base seleccionados IPv6*

Realizado el análisis a la implementación del protocolo IPv6 en los servicios básicos de la entidad, se observó la reserva y asignación de un pool de direcciones en una subred 64.

Tabla 12.

Direccionamiento IPv6 subred de servidores.

Prefijo IPv6	**Direccionamiento**	**Descripción**
Proveedor	2800:26XX:004D::/48	Pool de direccionamiento IPv6 global que asigno el proveedor a la entidad.
Subred servidores	2800:26XX:004D:0X00::/64	Subred /64 asignada para el segmento de los servidores de aplicación de la entidad.

Nota: Elaboración propia

Después de realizar la implementación del protocolo IPv6 en la infraestructura de la entidad, todos los dispositivos están funcionando en modo Dual Stack, está implementación modifica la manera en que los dispositivos interactúan entre sí, debido a que todos los hosts que lo tengan configurado en su tarjeta de red darán prioridad al tráfico IPv6 siempre y cuando el servicio que se esté solicitando responda peticiones en IPv6, esto es un problema cuando se realizan las configuraciones por defecto, como se llevaron a cabo en la entidad ya que se generarán conexiones constantes mientras el

servidor responda por el protocolo que tiene mayor prioridad, cuando el dispositivo al que desee hacer conexión no conteste inducirá un bloqueo en la solicitud y aparecerá como no disponible afectando la operación, para evitar esto se debe configurar de manera que si no logra conexión usando el protocolo IPv6 pase al protocolo IPv4 de manera automática sin afectar la respuesta y el resultado final de la petición.

Configuraciones de un Servidor DHCP IPv6 recomendadas

Se encontró un manual con las configuraciones recomendadas para un servidor DHCP con protocolo IPv6 y que nombramos a continuación.

DHCPv6 es un método para asignar automáticamente direcciones IPv6 a clientes de red. Cuando se habilita IPv6 para una interfaz de confianza u opcional, puede habilitar el servidor DHCPv6 en la interfaz, para asignar direcciones IPv6 a clientes que se conectan.

No puede utilizar estas direcciones IP de propósito especial en la configuración. DHCPv6:

- Las direcciones IP que comienzan con 2002, a no ser que los bits 17-48 especifiquen una dirección IPv4 válida.
- Direcciones IP que comienzan con FE80, ya que esto especifica una dirección local de enlace
- Direcciones IP que comienzan con FEC0, ya que esto especifica una dirección local de sitio
- Direcciones IP que comienzan con FF, ya que esto se utiliza para direcciones multicast de IPv6

Ajustes del Servidor DHCPv6 recomendada

Puede configurar el servidor DHCPv6 en una interfaz de confianza, opcional o personalizada de modo que el servidor DHCP pueda asignar direcciones y prefijos a los clientes IPv6 que se conectan.

Cuando se configura una interfaz para usar un servidor DHCPv6 debe agregar por lo menos, una entrada al Grupo de Direcciones o al Grupo de Prefijos.

Configuración del grupo de direcciones DHCPv6 recomendada

El Grupo de Direcciones define las direcciones IPv6 que el servidor DHCP puede asignar a clientes DHCPv6 que se conectan.

Sí se ha habilitado Delegación de Prefijo de Cliente DHCPv6 para una interfaz externa, el cuadro de diálogo Agregar Rango de Direcciones incluirá una casilla de selección Utilizar delegación de prefijo que puede seleccionar para utilizar el prefijo delegado en el rango de direcciones.

Configuración del grupo de prefijos DHCPv6 recomendada

El Grupo de Prefijos define los prefijos IPv6 que el servidor DHCP puede asignar a clientes DHCPv6 que se conectan.

Configuración de reservas DHCPv6 recomendada

Se debe hacer lo siguiente:

- Agregar una dirección o un prefijo reservado para la entidad.
- Las direcciones reservadas deben estar en un rango configurado en el “Grupo de Direcciones”.
- Un prefijo reservado debe estar en un rango configurado en el “Grupo de Prefijos”.

- Sólo realizar una reserva por dirección IP, prefijo o ambos para el mismo cliente.
- Para reservar un prefijo para otro Firebox que se conecte, especificar el DUID de la interfaz externa del cliente DHCP en la reserva de prefijo.
- Sí se ha habilitado Delegación de Prefijo de Cliente DHCPv6 para una interfaz externa, el cuadro de diálogo Agregar IP y Prefijo Reservados por DUID incluirá una casilla de selección, puede seleccionar esta casilla de selección para utilizar el prefijo delegado en la dirección IP reservada.

Habilitación de una confirmación rápida recomendada
Para obtener direcciones IPv6 de un servidor, el cliente DHCPv6 puede utilizar un intercambio rápido de dos mensajes (solicitar, responder) o un intercambio de cuatro mensajes (solicitar, anunciar, requerir, responder). Por defecto, el cliente DHCPv6 utiliza el intercambio de cuatro mensajes. Para usar el intercambio de dos mensajes, se habilita la opción de Confirmación Rápida en Firebox y en el cliente. Activamos la casilla de selección Confirmación Rápida para permitir el servidor DHCP para usar el intercambio rápido de dos mensajes y asignar una dirección IP.

Configuración de las caducidades de direcciones IPv6 recomendada
Los ajustes de caducidad IPv6 controlan la extensión de vida durante la cual una dirección IPv6 se mantiene válida y la duración en tiempo de la dirección. Para cambiar la configuración predeterminada, cambie los valores para Caducidad Válida y Caducidad Preferida donde la válida debe ser superior o igual a la preferida.

Configuración de servidores DHCPv6 DNS por interfase recomendada
Por defecto, cuando está configurado un servidor DHCP, su Firebox proporciona la información DNS y WINS configurada. Para especificar información diferente cuando distribuya direcciones IPv6, puede agregar servidores DNS en los ajustes DHCPv6 para la interfaz y allí agregar las direcciones IP de hasta tres servidores DNS. (Watchguard, 2022)

El funcionamiento del servicio DNS se basa en una arquitectura cliente/servidor, donde el cliente realiza consultas por RRs a los Servidores Recursivos.

Al recibir consultas, los Servidores Recursivos las encaminan a los Servidores Autoritativos y de acuerdo con la respuesta recibida, continúan el encaminado de las consultas para otros Servidores Autoritativos hasta obtener una respuesta satisfactoria. Dentro de la estructura jerárquica de los DNS, los Servidores Autoritativos responden las consultas sobre las zonas o dominios por los cuales poseen autoridad o una referencia en caso de que conozcan el camino para la respuesta, o una negación en caso de que no la conozcan.

Para que el DNS trabaje con la versión 6 del protocolo de Internet, algunos cambios fueron definidos en el RFC 3596.

En el plan de Implementación IPv6 entregado a la entidad se especificó el prefijo y direcciones IPv6 para cada dispositivo y cada segmento de red, sin embargo, el protocolo IPv6 se encuentra activado por defecto en la mayoría de los sistemas en donde fue configurado, utilizando la dirección Link-local para llevar a cabo la conexión en la capa de red.

Para la implementación de nuevos dispositivos de red, equipos de seguridad y cualquier elemento con funcionalidades de capa 3, es muy importante contar con el soporte para el protocolo IPv6. Se recomienda verificar que las nuevas adquisiciones de

estos dispositivos cumplan con los RFC relacionadas con IPv6 para la función específica. (RFC 8415, RFC 3315, RFC 3596, RFC 4472, RFC 4339)

Recomendaciones relacionadas con el diseño de la subred de servidores la entidad.

Teniendo en cuenta lo extenso del tema seleccionado en el desarrollo de este documento y la cantidad en el detalle de los numerales que se seleccionaron de las normas ISO/IEC 27022 y la Guía de Aseguramiento del protocolo IPv6 de NIST, se toma la decisión de realizar un modelo para la actualización de la arquitectura de la subred de servidores con la que actualmente cuenta la entidad.

La presentación de este nuevo modelo para la arquitectura de la red de servidores tiene como meta exponer de manera practica como con el estudio realizado y los resultados obtenidos en el desarrollo de este ejercicio académico se pueden aplicar con el apoyo de los conocimientos adquiridos y así facultar a la entidad en la mejora de la seguridad informática y la seguridad de la información de la infraestructura tecnológica.

Ahora se relacionan los puntos de convergencia entre las metodologías que se utilizaron para realizar el estudio y desarrollo de esta actividad.

ISO/IEC 27002 – 2022	NIST, Guidelines for the secure Deployment of IPv6
Control 8.22 Segregación de redes.	IPv6 Address Assignments, (Asignamiento del direccionamiento IPv6)
1. Las redes en dominios de red separados de lo público y lo privado, o niveles de confianza, criticidad y sensibilidad (por ej., dominio acceso público, dominio escritorio domino servidores, sistemas de alto riego, etc.).	3.2.1. IPv6 Address Assignments, (Asignamiento del direccionamiento IPv6). 6.2. Addressing Security (Seguridad del Direccionamiento). 6.2.1. Numbering Plan (Plan de Direccionamiento). 6.2.2. Hierarchical Addressing to Support Security Segmentation (Direccionamiento Jerárquico para asegurar la Segmentación de Red Segura).
Ítems de convergencia entre las metodologías de estudio.	
Como parte fundamental del diseño de la nueva arquitectura para el direccionamiento IPv6 es necesario tener claro el tamaño de los espacios o dominios que se van a definir, para evitar que falten o sobren recursos cuando se asigne el nuevo esquema del direccionamiento IPv6, se debe realizar de acuerdo con los servicios tecnológicos que actualmente o en un futuro próximo estarán soportando los servicios en la entidad.	
Se debe diseñar e implementar un modelo jerárquico (estructura secuencial tipo árbol) para la arquitectura de red, independiente del protocolo IPv4 o IPv6 que se esté utilizando, este puede ser definido por características tales como; ubicación geográfica, ambientes de trabajo, roles de la entidad, pisos de trabajo, roles de seguridad, números de red secuenciales, tags o identificadores de vlans, o en combinación de estas u otras opciones. Al establecer un modelo jerárquico para el asignamiento del direccionamiento IPv6, se le permitirá a la entidad hacer rastreable la información que circula por la red de datos de acuerdo con el direccionamiento IP utilizado.	
En lo posible no replicar el plan de direccionamiento IPv4 que esta implementado en la entidad con el del protocolo IPv6, un claro ejemplo del porque no realizar esta equivalencia es la diferencia sideral entre los tamaños que manejan cada uno de los protocolos, con IPv4 un espacio de 32bits y con IPv6 un espacio de 128bits, por otro lado, la numeración decimal de IPv4 contra la numeración hexadecimal de IPv6, entre muchas otras.	
Se deben establecer dominios de red separados para el ambiente de servidores de cómputo, en este caso específico se podría utilizar el modelo de subredes de desarrollo, producción, pruebas, además de realizar la precisión de un dominio de red para la administración de los dispositivos fuera de banda.	
Los dominios de seguridad deben estar restringidos por elementos de seguridad lógica mas avanzados tipo firewall / UTM que permita establecer filtros o políticas entre los ambientes de red dimensionados, el alcance de las recomendaciones socializadas en este documento se enmarca en la capa 3 (red) del modelo OSI (Open System Model), que se utiliza para definir la estructura en la actividad de datos que circulan por la red.	

Determinados los puntos que se van a tomar como base de acuerdo con las metodologías de estudio, el paso a seguir es iniciar el proceso para la edificación del nuevo esquema de direccionamiento IPv6 para la subred de servidores que utiliza en la actualidad la entidad.

Se debe mencionar que existen varios métodos para elaborar los esquemas de direccionamiento IPv6, aunque no está en el alcance de este estudio profundizar sobre la definición y /o uso de cada una, si es bueno mencionarlas para establecer más adelante la razón del porque se utilizara la técnica de para el asignamiento del direccionamiento IPv6 basada en los límites de nibbles (nibble es la agrupación de 4 bits representado por un carácter hexadecimal).

Técnica de asignación sin segmentación IPv6: Se utiliza el total del direccionamiento facilitado por el proveedor sin usar algún método de asignación jerárquica, tomando como ejemplo el prefijo de la entidad “2800:26xx:004d::/48”, se establecen 65536 redes IPv6 disponibles para su uso.

Tabla 13		
Asignación IPv6 entidad		
Total IPv6:	/128	(/48 (isp) - /16 (cliente) - /64 (user))
Prefijo IPv6 entidad:	/48	(/16 (cliente) - /64 (user))
Espacio IPv6 cliente:	/16	65536 redes de cada una con tamaño /64 (2^{64})
Nota: Elaboracion propia		

Esta es la forma en la que se asignó el direccionamiento IPv6 en la entidad y que actualmente está en producción.

red 1: 2800:26xx:004d:0000::/64
red servidores: 2800:26xx:004d:0200::/64
……
……
red 65536: 2800:26xx:004d:ffff::/64

Técnica de asignación por equivalencia IPv4 a IPv6: es la técnica que hace una translación directa del direccionamiento IPv4 al direccionamiento IPv6: este método se menciona por cultura general pero no se debe utilizar porque mantener la relación directa entre IPv4 e IPv6 para no es posible, sin embargo, se puede mapear la dirección IPv4 en los últimos 32bits de la dirección IPv6, por ejemplo.

Tabla 14	
Mapeo direcciones IPv4 e IPv6	
Dirección IPv4:	192.168.200.20/224
Dirección IPv6:	2800:26xx:004d:ffff:ff:ee:192.168.200.20
Nota: Elaboracion propia	

Técnica de asignación por etiquetas de vlan (Virtual lans): con este procedimiento se realiza un mapeo directo de los tags (identificadores) de vlan que existen actualmente en la infraestructura contra el nuevo direccionamiento IPv6, por ejemplo.

Si utilizamos el identificador de vlan (tag) 45, la relación con IPv6 seria de la siguiente forma:

Tabla 15	
Relación IPV6 en la VLAN 45	
vlan:	45
red 1:	2800:26xx:004d:0045::/64
red 1:	2800:26xx:004d:4500::/64
Nota: Elaboracion propia	

Se debe aclarar que el número 45 decimal es diferente al número 45 hexadecimal (decimal 69).

Técnica de asignación por movimiento de bits a la izquierda, centro, derecha: este método se utiliza el cálculo de potencia 2 para realizar el asignamiento del direccionamiento IP, ya no se depende de un nibble (2^4) para realizar esta tarea, por ejemplo.

Tabla 16								
Cálculo para asignacion de direccionamiento IP								
Asignamiento por nibbles:	/48	/52	/56	/60	/64			
Asignamiento por 2bits:	/48	/50	/52	/56	/58	/60	/62	/64
Asignamiento por bit:	/49	/50	/51	…	…	…	63	/64
Nota: Elaboracion propia								

Técnica de asignación por límites de nibbles: Se realiza la segmentación para la asignación del direccionamiento IP usando múltiplos de 4 bits (nibble), dando como resultado que se puedan usar prefijos de red siempre pares y múltiplos de 4, por ejemplo.

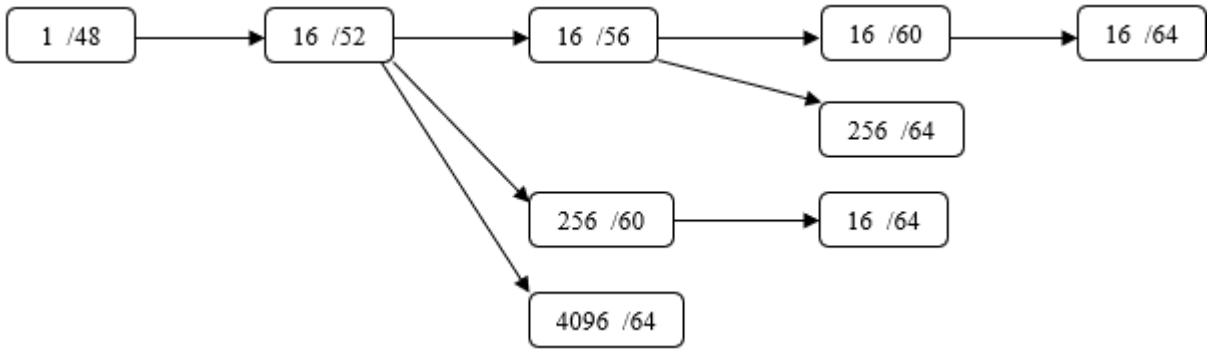
Tabla 17			
Segmentación para la asignación de direccionamiento IP usando múltiplos de 4 bits			
Prefijo	/48		
Prefijo	/52	/48 + 4bits	(1 nibble)
Prefijo	/56	/48 + 8bits	(2 nibbles)
Prefijo	/60	/48 + 12bits	(3 nibbles)
Prefijo	/64	/48 + 16bits	(4 nibbles)
Nota: Elaboracion propia			

usando esta metodología se gana una lectura del prefijo de red más amigable para el administrador de red ya que es fácil asociar el esquema de direccionamiento IP con la lectura que le da el ser humano, también posibilita que la estructura jerárquica sea identificada sin problemas y se logre verificar rápidamente en el caso que se tenga que realizar alguna tarea para solucionar inconvenientes.

Después de realizar una breve introducción de las técnicas que se pueden utilizar para realizar el asignamiento del direccionamiento IPv6 y estableciendo que la metodología de segmentación de red por nibbles es la óptima, se establecerá a continuación el nuevo el esquema de direccionamiento IPv6 para la entidad.

Requerimientos:

Tabla 27.
Visualización de los prefijos IPv6



***Nota**: Elaboración propia con datos seleccionados del libro (Coffeen, 2015, p. 78).*

La entidad actualmente cuenta con 3 sedes, incluyendo la principal y dos sucursales.

Se establece la necesidad de implementar los ambientes de pruebas, desarrollo producción1, produccion2, produccion3, administración (management), usuarios-vpn, red MPLS, entre otras, con posibilidad de crecimiento para actualizar la infraestructura de red del centro de cómputo donde se encuentra alojada la red de datos de los servidores.

Para iniciar el ejercicio de diseño del nuevo esquema de direccionamiento IPv6 se realiza la selección por niveles de agrupación, por ubicación física (sedes) y con el uso de los identificadores de las vlans que se están utilizando actualmente en la infraestructura tecnológica.

Nivel 0.

Información con el prefijo IPv6 facilitado por el proveedor de telecomunicaciones ISP (Internet Service Provider), Empresa de Telecomunicaciones de Bogotá (ETB).

2800:26ff:004d::/48

Nivel 1.

Se comienza con la segmentación de red para la asignación el direccionamiento IPv6 mediante el uso de un nibble completo (4bits), ofreciendo para el diseño la posibilidad de seleccionar un espacio de $2^4 = 16$ subredes disponibles con prefijo /52, este espacio se utilizará para cada una de las sedes o zonas geográficas donde se ubiquen los servicios tecnológicos de la entidad.

Tabla 18

Segmentación de la red para cada sede de la entidad

red 1	2800:26ff:004d:0000::/52	libre para uso
red 2	2800:26ff:004d:1000::/52	libre para uso
red 3	2800:26ff:004d:2000::/52	sede principal galerías
red 4	2800:26ff:004d:3000::/52	libre para uso
red 5	2800:26ff:004d:4000::/52	libre para uso
red 6	2800:26ff:004d:5000::/52	libre para uso
red 7	2800:26ff:004d:6000::/52	libre para uso
red 8	2800:26ff:004d:7000::/52	libre para uso
red 9	2800:26ff:004d:8000::/52	sede archivo central
red 10	2800:26ff:004d:9000::/52	sede archivo general
red 11	2800:26ff:004d:a000::/52	libre para uso
red 12	2800:26ff:004d:b000::/52	libre para uso
red 13	2800:26ff:004d:c000::/52	libre para uso
red 14	2800:26ff:004d:d000::/52	sedes MPLS
red 15	2800:26ff:004d:e000::/52	libre para uso
red 16	2800:26ff:004d:f000::/52	libre para uso

Nota: Elaboracion propia

El resultado de este primer nivel de segmentación da como resultado que se utilizaran cuatro (4) prefijos /52 para satisfacer las necesidades del direccionamiento IPv6 en las sedes de la entidad, con la posibilidad de tener en reserva trece (13) prefijos /52 para cuando el crecimiento de la red así lo requiera.

Tabla 19

Segmentación de la red para cada sede de la entidad

red 3	2800:26ff:004d:2000::/52	sede principal galerías
red 9	2800:26ff:004d:8000::/52	sede archivo central
red 10	2800:26ff:004d:9000::/52	sede archivo general
red 14	2800:26ff:004d:d000::/52	sedes MPLS

Nota: Elaboracion propia

Nivel 2.

Al tener un espacio de direccionamiento IPv6 tan amplio para cada una de los cuatro (4) prefijos /52 (cada uno con la posibilidad de configurar 4096 subredes con un tamaño en el prefijo o subredes /64) seleccionadas en la etapa 1, se toma la decisión de realizar otro nivel de segmentación con el uso de otro nibble (4bits) en el prefijo /52 base del nivel 1, este nuevo nivel es definido para establecer un diseño que permita la adición de puntos físicos como edificios al sitio geográfico, esto da como resultado 16 prefijos /56 para cada uno de los prefijos /52 y cada prefino /56 con 256 prefijos /64. A continuación se muestra cómo queda esta segmentación para la sede principal de la entidad, este ejercicio para la definición del esquema de direccionamiento aplica de igual forma para cada uno de los prefijos /52 del Nivel 1.

Tabla 20		
Subredes nivel 1		
red 3	2800:26ff:004d:2000::/52	sede principal galerías
Nota: Elaboracion propia		

Tabla 21		
Subredes nivel 2		
red 1	2800:26ff:004d:2000::/56	
red 2	2800:26ff:004d:2100::/56	
red 3	2800:26ff:004d:2200::/56	edificio principal galerías
red 4	2800:26ff:004d:2300::/56	
red 5	2800:26ff:004d:2400::/56	
red 6	2800:26ff:004d:2500::/56	
red 7	2800:26ff:004d:2600::/56	
red 8	2800:26ff:004d:2700::/56	
red 9	2800:26ff:004d:2800::/56	
red 10	2800:26ff:004d:2900::/56	
red 11	2800:26ff:004d:2a00::/56	
red 12	2800:26ff:004d:2b00::/56	
red 13	2800:26ff:004d:2c00::/56	
red 14	2800:26ff:004d:2d00::/56	
red 15	2800:26ff:004d:2e00::/56	
red 16	2800:26ff:004d:2f00::/56	
Nota: Elaboracion propia		

De acuerdo con la metodología utilizada se selecciona un prefijo /56 para cada una de Los edificios de la entidad, cada uno de estos prefijos /56 contiene 256 prefijos con tamaño del direccionamiento IPv6 con prefijo /64, los otros espacios de direccionamiento se dejan para para crecimiento o servicios futuros.

Tabla 22		
Red edificio principal prefijo 56		
red 3	2800:26ff:004d:2200::/56	edificio principal galerías
Nota: Elaboracion propia		

Nivel 3.

Este es el último nivel para la segmentación del espacio de direccionamiento IPv6 que se le va a distribuir a la entidad, se utilizaran cada uno de los prefijos /56 generados en el nivel 2, cada uno de estos prefijos /56 tiene disponible para su uso una cantidad de 256 prefijos o subredes con un tamaño /64, que se asociaran para usarse con la topología capa 2 (vlans) o una posible asociación o equivalencia en IPv4 si fuese necesario.
capa 2 (vlans) y su equivalencia en IPv4.

Tabla 23		
Subred nivel 1		
red 3	2800:26ff:004d:2000::/52	sede principal galerías
Nota: Elaboracion propia		

Tabla 24		
Subred nivel 2		
red 3	2800:26ff:004d:2200::/56	edificio principal galerías
Nota: Elaboracion propia		

Tabla 25		
Subredes nivel 3		
red 1	2800:26ff:004d:2200::/64	
red 2	2800:26ff:004d:2201::/64	
red 3	2800:26ff:004d:2202::/64	subred pruebas
red 4	2800:26ff:004d:2203::/64	subred desarrollo
red 5	2800:26ff:004d:2204::/64	subred producción1
red 6	2800:26ff:004d:2205::/64	subred producción2
red 7	2800:26ff:004d:2206::/64	subred producción3
red 8	2800:26ff:004d:2207::/64	
red 9	2800:26ff:004d:2208::/64	
red 10	2800:26ff:004d:2209::/64	subred administración
red 11	2800:26ff:004d:220a::/64	subred usuarios vpn
red 12	2800:26ff:004d:220b::/64	subred MPLS
red 13	2800:26ff:004d:220c::/64	
……..		
……..		
……..		
red 252	2800:26ff:004d:22fb::/64	
red 253	2800:26ff:004d:22fc::/64	
red 254	2800:26ff:004d:22fd::/64	
red 255	2800:26ff:004d:22fe::/64	
red 256	2800:26ff:004d:22ff::/64	
Nota: Elaboracion propia		

Como se pudo evidenciar al realizar este ejercicio donde se define la arquitectura jerárquica para el espacio de direccionamiento IPv6, facilitando la descripción y comprensión de la secuencia utilizada para el modelo desarrollado.

Como punto final se presenta un ejemplo para la asignación del direccionamiento IPv6 con equivalencia con los identificadores o tag de vlan capa 2.

Tabla 26.
Visualización de los prefijos IPv6

Nombre	Subred IPv4	tag vlan	subred IPv6	Observación
Asignación directa IPv4 a IPv6 hexadecimal				
pruebas	192.168.202.0/24	202	2800:26ff:004d:2202::/64	n/a
desarrollo	192.168.203.0/24	203	2800:26ff:004d:2203::/64	n/a
producción1	192.168.204.0/24	204	2800:26ff:004d:2204::/64	n/a
producción2	192.168.205.0/24	205	2800:26ff:004d:2205::/64	n/a
producción3	192.168.206.0/24	206	2800:26ff:004d:2206::/64	n/a
administración	192.168.209.0/24	209	2800:26ff:004d:2209::/64	n/a
usuarios vpm	192.168.210.0/24	210	2800:26ff:004b:220a::/64	n/a
mpls	192.168.211.0/24	211	2800:26ff:004d:220b::/64	n/a
Asignación indirecta IPv4 a IPv6 hexadecimal				
otros	192.168.10.0/24	10	2800:26ff:004d:220a::/64	10 decimal = a hexa
otros	192.168.55.0/24	55	2800:26ff:004d:2237::/64	55 decimal = 37 hexa
otros	192.168.111.0/24	111	2800:26ff:004d:226f::/64	111 decimal = 6f hexa
otros	192.168.240.0/24	240	2800:26ff:004d:220b::/64	240 decimal = 0b hexa
otros	192.168.199.0/24	199	2800:26ff:004d:22c7::/64	199 decimal = c7 hexa

***Nota**: Elaboración propia.*

V. CONCLUSIONES

Cuando hablamos de seguridad en IPv6 es necesario mencionar el IPSec (Internet Protocol Security), a través del cual se busca garantizar la seguridad de los datos usando técnicas como el cifrado de la información evitando que se pueda ver la trama enviada, la autenticación garantiza e informa de donde viene un determinado paquete, la integridad de los datos para saber si han sido modificados o no, etc.

Básicamente los protocolos de seguridad en internet fueron crearon para impedir el acceso no autorizado a la información encontrada dentro de una red corporativa. Sin embargo, hay diferentes formas de vulnerar dichas restricciones, debido a que muchas redes manejan las comunicaciones entre los equipos de una red como texto sin formato, gracias a esto una persona con las habilidades necesarias y pudiéndose conectar a la red físicamente, podría extraer información confidencial.

Es importante recordar que, aunque IPv6 es un protocolo que optimiza algunos aspectos vulnerables de la versión anterior, no se debe dejar de lado las buenas prácticas de seguridad y correcta administración de una red y de los componentes de estas.

Para nuestra entidad, que cuentan con conexiones privadas virtuales punto a punto (VPN), es aconsejable que se tenga en cuenta todo el control de tráfico entre todos los puntos posible de la red IPV6, es imprescindible utilizar IPsec para que se encargue de la seguridad de todo el tráfico generado por las comunicaciones entre las VPNs.

El monitoreo es necesario en el establecimiento de los niveles de funcionamiento y criticidad de la red con IPV6 en su servicio activo. Para ello es requisito prevenir aquellos problemas que se puedan presentar, así como detectar y diagnosticar fallas,

también tener en cuenta definir las acciones para solventar incidencias de seguridad y generar planes de contingencia para la entidad.

Cuando se realice el monitoreo de los servicios de red que cuentan con IPV6, es necesario tener claridad sobre los siguientes ítems:

- El estado de las aplicaciones y de los servicios activos.
- La medición correcta de los dispositivos conectados a la red y sobre las interfaces.
- Los canales disponibles para la comunicación externa y la actividad de cada elemento que interviene en la comunicación.
- Contar con herramientas precisas y eficientes de monitoreo y análisis de tráfico de la red con IPV6 que generen graficas sobre el comportamiento de las interfaces y demás dispositivos.

Cuando se configura la doble pila, un dispositivo posee la capacidad de soportar el protocolo IPV4 y el protocolo IPV6, pero las reglas de seguridad que se aplican para la seguridad y el tráfico indeseado en IPV4, no funciona de igual forma en IPV6, por lo que la entidad deberá adoptar estrategias que permitan controlas este tipo de situaciones.

Una de las recomendaciones que también sugiere el Ministerio de Tecnologías de la Información y la Comunicación (Mintic), es la deshabilitación de los protocolos de red que no se encuentran en uso. En la mayoría de los casos, el nuevo Hardware tiene el servicio IPV6 activado por defecto, sin embargo, es necesario suspenderlo cuando se identifiquen problemas en el Core de la red, que puedan causar problemas en las operaciones y la infraestructura de la entidad.

VI. REFERENTES BIBLIOGRÁFICOS

[1] |6NET Consortium. (2005). An IPv6 Deployment Guide. Buselas, Bélgica: 6NET Consortium.

[2] ALONSO, J. C. (10 de Septiembre de 2017). http://lacnic.net//index.html. Obtenido de LACNIC: http://www.labs.lacnic.net/site/sites/default/files/060-ipv6-direccionamiento-lacnic-03.pdf

[3] Blanchet, M. (2006). Migrating to IPv6 A Practical Guide to Implementing Mobile and Fixed Networks. Quebec, Canada: Jhon Wiley & Sons Ltd.

[4] Coffeen, T. (2015). IPv6 Address Planning

[5] Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). Guidelines for the Secure Deployment of IPv6 (Vols. 800-119). Gaithersburg, Maryland, USA: NIST, National Institute of Standars and Tecnology.

[6] Hagen, S. (2014). IPv6 Essentials, Integrating IPv6 Your IPv4 Network. Unit States of America: O´reilly.

[7] Hogss, S. (2009). IPv6 Security. Indianapolis, USA: Cisco Press.

[8] Institute for Scientic Information . (2021). Global Research Report. América Latina: América del Sur y Central, México y el Caribe. Clarivate Analytics.

[9] ISO/IEC 2022. (2022). ESTÁNDAR INTERNACIONAL ISO/CEI 27002 (Tercera Edición 2022-02 ed.). Vernier, Ginebra, Suiza: ISO/IEC 2022. Obtenido de www.iso.org.

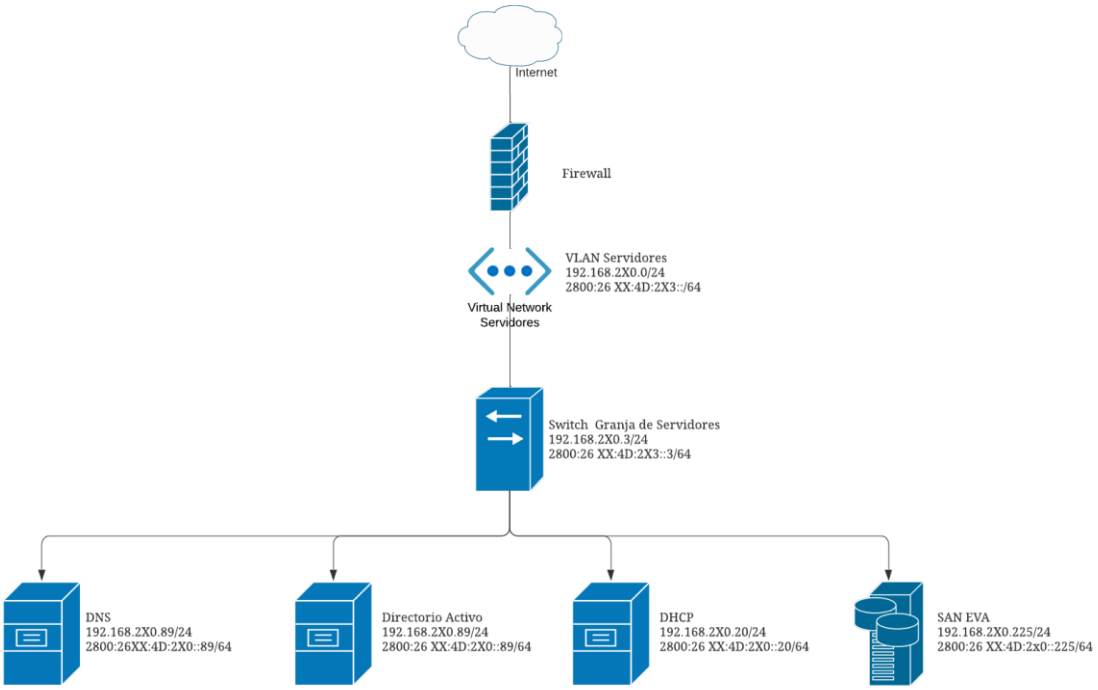
[10] Jorge Bejarrano, A. B. (2014). Transición de IPv4 a IPv6 para Colombia Guia N° 20. Bogota, Colombia: Ministerio de las TICS, MINTIC.

[11] Ministerio de Tecnolgías de la Información y las Comunicaciones. (2017). Resolución Número 2710 de 2017. Bogotá, Bogotá, Colombia: MinTIC.

[12] Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Resolución Número 1126 de 2021. Bogotá, Bogotá, Colombia: MinTic.
[13] (Vol. Guía 2). Bogotá, Bogotá, Colombia: MinTIC.
[14] MinTIC, V., & Dirección de Gobierno Digital. (2021). Guía para el Aseguramiento del protocolo IPv6.
[15] NIST, N. I. (2008). A Profile for IPv6 in the U.S. Government – Version 1.0, Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD: NIST Special Publication 500-267.
[16] Rooney, T., & Dooley, M. (2013). Ipv6 deployment and management. New Jersey: IEEE Press, Wiley.
[17] Society, t. I. (1998). Internet Protocol, Version 6 (IPv6) Specification RFC2460. USA, USA, USA.
[18] Stephen NightinGale, E. J. (2009). USGv6 Test Methods: General Description and Validation, National Institute of Standards and Technology. National Institute of Standards and Technology: NIST, National Institute of Standars and Technology.
[19] Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.). MINTIC Colombia - Documentos IPv6. MINTIC Colombia. Recuperado 12 de mayo de 2022, de https://mintic.gov.co/portal/inicio/Micrositios/Documentacion-sobre-IPv6/Documentos-IPv6.
[20] (Ministerio TIC expide resolución que modifica los lineamientos para la adopción del protocolo IPv6 - Ministerio TIC expide resolución que modifica los lineamientos para la adopción del protocolo IPv6, s/f)
[21] Ministerio TIC expide resolución que modifica los lineamientos para la adopción del protocolo IPv6 - Ministerio TIC expide resolución que modifica los lineamientos para la adopción del protocolo IPv6. (s/f). MINTIC Colombia. Recuperado el 4 de junio de 2022, de https://mintic.gov.co/portal/inicio/Sala-de-prensa/176075:Ministerio-TIC-expide-resolucion-que-modifica-los-lineamientos-para-la-adopcion-del-protocolo-IPv6
[22] Watchguard (2022). Configurar un Servidor DHCP IPv6. Recuperado de: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/networksetup/ipv6_dhcp_server_c.html

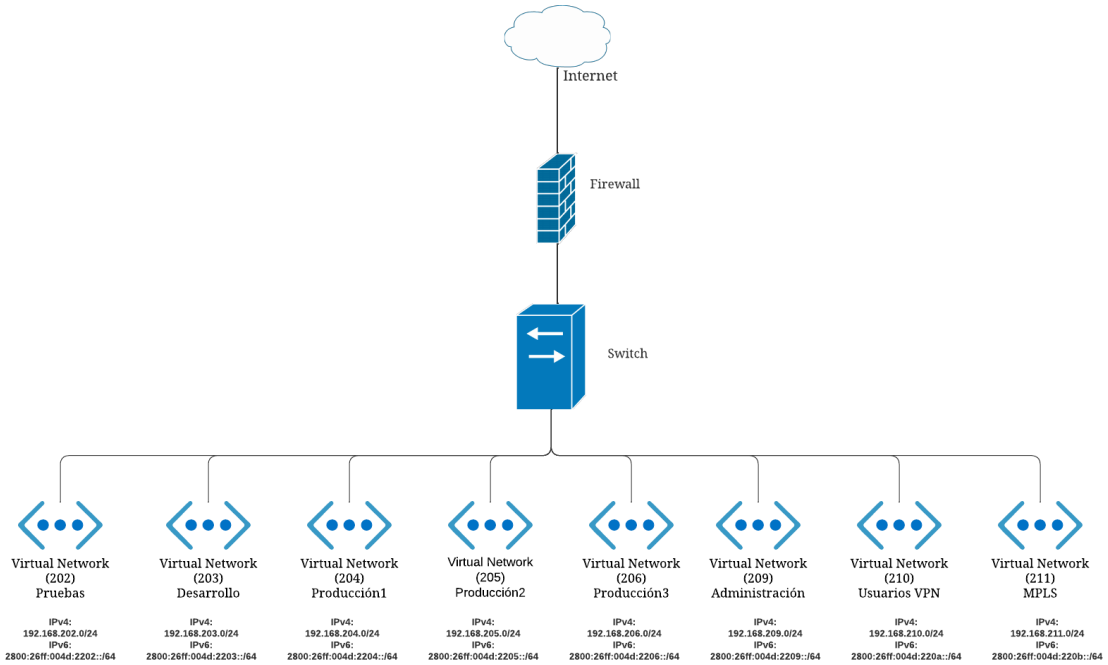
VII. APÉNDICES

Apéndice 1
Estado actual IPv6



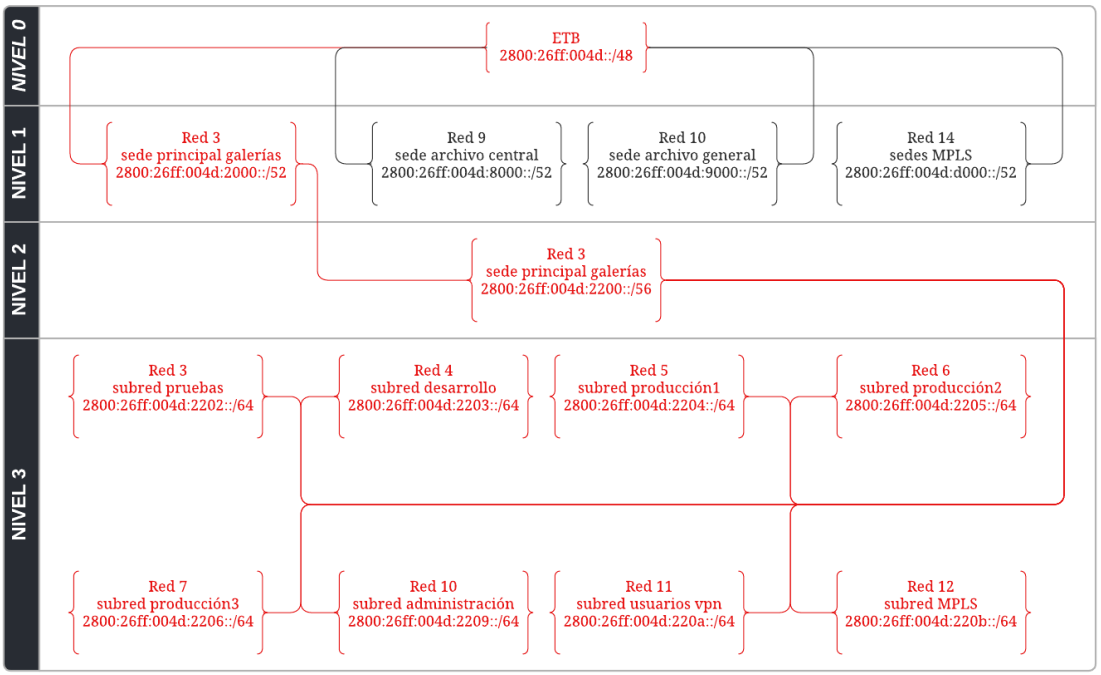
***Nota**: Elaboración propia.*

Apéndice 2
Arquitectura IPv6 sugerida



***Nota**: Elaboración propia.*

Apéndice 3
Esquema direccionamiento IPv6 sugerido



***Nota**: Elaboración propia.*