DIAGNÓSTICO DE IPV4 A IPV6

ALCALDÍA DE PEREIRA

PROCESO

PROMOCIÓN DEL DESARROLLO ECONÓMICO

SUBPROCESO

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

ACTIVIDAD

GOBIERNO DIGITAL

Título:	DIAGNÓSTICO DE IPV4 A IPV6				
Sumario	El presente documento surge a partir de la aplicación del habilitador os lineamientos y estándares del “Dominio de Información”, adoptado en el Habilitador Transversal "Arquitectura TI" de la Política de Gobierno Digital del Ministerio de las Tecnologías de Información y Comunicaciones de la República de Colombia.				
Palabras Claves	Gobierno Digital Seguridad Digital IPv4 Ipv6				
Formato:	PDF		Lenguaje:	Español	
Dependencia:	Secretaría de Tecnologías de Información y la Comunicación				
Código:	N/A	Versión	1.0	Estado	En Aprobación
Categoría	Documento informativo: Implementación del habilitador transversal Seguridad y Privacidad. Guía de Transición de IPv4 a IPv6 para Colombia.				
	Componente:	TIC para el estado			
	Habilitador Transversal:	Seguridad y Privacidad			
	Lineamientos Estándares:	Modelo de Seguridad y Privacidad de la Información – Guía G20			
Asesor (es):	Magister Carlos Mario Arteaga Pacheco Contratista Prestación de Servicios Profesionales Especializados				
Autor (es):	Ingeniero Alejandro Pineda Muñoz Contratista Prestación de Servicios Profesionales				
Revisó:	Carlos Andrés Alvarez Palomino Director de Sistemas de Información y Servicios Digitales Alejandro Usma Vásquez Director de Infraestructura Tecnológica				
Aprobó:	Fredy Eduardo Ruano López Secretario de Tecnología de Información y la Comunicación				

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	03/12/2020	Emisión del documento

Tabla de contenido

1 INTRODUCCIÓN

Con este diagnóstico se pretende visualizar y conocer al detalle, el estado actual de toda la infraestructura tecnológica de la Alcaldía de Pereira y contar con un plan para la adopción del protocolo IPV6, teniendo en cuenta que a la fecha algunos dispositivos y equipos no soportan este nuevo protocolo, se pueden presentar problemas de compatibilidad afectando el correcto funcionamiento de los diferentes dispositivos conectados en la red de en la administración municipal, por lo que se pretende con este diagnostico conocer las falencias y necesidades para el plan de implementación.

2 CONCEPTOS

DHCPv6	Protocolo de Configuración Dinámica de Hosts para IPv6 con característica cliente-servidor y definido por la RFC 3315 de la IEFT, que proporciona una configuración administrada de dispositivos sobre redes IPv6.
DNS (Domain Name System):	*Sistema de Nombres de Dominio que contiene un sistema de nomenclatura jerárquica para equipos de computación, los DNS contienen una base de datos que tienen la función de indicar la IP que está asociada a un nombre de un sitio web (resolución de nombres).*
Encapsulamiento:	*Es un mecanismo usado en los túneles de comunicación hacia Internet que permiten contener paquetes IPv6 dentro de un paquete IPv4 y enviarlo por una red IPv4 o viceversa, ejemplos de esto son los encapsulamiento 6-en-4 o 4-en-6*
ICMP (Internet Control Messsage Protocol for IPv6):	El protocolo de mensajes de control ICMPv6, es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico, combina funciones que anteriormente estaban contempladas por varios protocolos tales como ICMP, IGMP y ARP, adicionalmente introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso en el ICMPv4.
IPsec (IP Security):	Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

RFC (Request For Comments):	Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos que han hecho llegar a la IETF -Engineering Task Force, sus recomendaciones para la valoración por el resto de la comunidad. Describen aspectos técnicos del funcionamiento de Internet y otras redes de comunicaciones, protocolos, procedimientos y comentarios o ideas para clarificar o corregir aspectos técnicos que garanticen buenas prácticas de trabajo.
Auditoría:	Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Bases de Datos Personales:	Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
Ciberespacio:	Es el ambiente tanto físico como virtual compuestos por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009)
Ciberseguridad:	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701)
Confidencialidad:	Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizada
Control:	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Datos Personales Mixtos:	Para efectos de este manual es la información que contiene datos personales públicos junto con datos privados o sensibles.
Datos Personales Privados:	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1581 de 2012, art 3 literal h)
Datos Personales Públicos:	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y

	sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
Datos Personales Sensibles:	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organización sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
Datos Personales:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, art 3)
Declaración de aplicación:	Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información - SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
Disponibilidad:	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera
Gestión de incidente de seguridad de la información:	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
Guía:	Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
Información Pública Clasificada:	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información:	Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
Integridad:	Propiedad de salvaguardar la exactitud y estado completo de los activos.
Ley de Habeas Data:	Se refiere a la Ley Estatuaria 1266 de 2008.
Ley de Transparencia y Acceso a la Información Pública:	Se refiere a la Ley Estatuaria 1712 de 2014.
Partes interesadas (Stakeholder):	Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Plan de tratamiento de riesgos:	Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implementar los controles necesarios para proteger la misma. (ISO/IEC 27000).
Política:	Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
Privacidad:	En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
Procedimiento:	Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.

Riesgo:	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000)
Seguridad de la información:	Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
Sistema de Gestión de Seguridad de la Información SGSI:	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, política, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
Tratamiento de Datos Personales:	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
Usuario:	Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información
Vulnerabilidad:	Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3 OBJETIVOS

- Definir claramente el plan de transición de ipv4 a ipv6.
- Analizar la situación actual de la Alcaldía de Pereira.
- Determinar un mecanismo de transición para la migración al nuevo protocolo.

4 INVENTARIO DE TI (HARDWARE, SOFTWARE)

4.1 INVENTARIO DE EQUIPOS DE CÓMPUTO

En la Alcaldía de Pereira en el segundo semestre del año 2020 realizo el diagnóstico de los equipos antiguos con el propósito de identificar cuáles deben ser reportados para determinar su destino final, debido al índice de obsolescencia tecnológica basado en las fechas de adquisición, características técnicas, estado de operación y reporte de incidentes técnicos. Por consiguiente, la cantidad de equipos de cómputo activos en la entidad tiende a disminuir si no se realiza la adquisición de nuevos equipos de cómputo.

Sistemas Operativos y versiones en la Alcaldía de Pereira sede central:

Los equipos de cómputo que se encuentran en la Alcaldía de Pereira cuenta con Sistema Operativo WINDOWS con versiones XP, VISTA, 7, 8, 8.1, 10; a continuación, se puede observar a detalle la cantidad de equipos con cada una de las versiones.

SISTEMA OPERATIVO	TOTAL
WINDOWS 10	471
WINDOWS 7	252
WINDOWS XP	52
WINDOWS 8	5
WINDOWS VISTA	3

Sistemas Operativos y versiones puntos vive digital:

PUNTO VIVE DIGITAL	SISTEMA OPERATIVO	TOTAL EQUIPOS
INEN FELIPE PEREZ	WINDOWS 8,1	30
LA BELLA	WINDOWS 10	27
LUCY TEJADA	WINDOWS 7	89
REMANZO	WINDOWS 8,1	33
SAN FERNANDO	WINDOWS 8,1	15
VILLA CONSOTA	WINDOWS 10	34
TECNICO SUPERIOR	WINDOWS 8,1	30

Sistemas Operativos y versiones comisarías de familia, corregidurías, inspecciones:

SISTEMA OPERATIVO	TOTAL EQUIPOS
WINDOWS 10	28
WINDOWS 7	48
WINDOWS XP	22

Teóricamente, todos los equipos de cómputo de la Alcaldía de Pereira soportan IPv6, pues Microsoft implementó este protocolo desde la versión Windows XP en adelante, sin embargo, no todas las versiones traen activo este soporte, este tipo de protocolo generalmente viene en las versiones PROFESSIONAL; en la mayoría de equipos se debe realizar la activación y configuración de manera manual.

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

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

4.2 EQUIPOS DE IMPRESIÓN

Se recomienda analizar las fichas técnicas de algunas impresoras, se encontró que fabricantes como HP señalan en ciertos modelos y tecnologías de impresoras láser soportan IPv6, a veces en el software de administración de estas impresoras no se encuentra la opción para habilitar y configurar el protocolo IPv6.

DEPENDENCIA	SUBDEPENDENCIA	MARCA	MODELO	SOPORTA IPV6
secretaria de desarrollo social y político	área legal y contractual	HP	LaserJet M2727nf	si
secretaría jurídica	control interno	HP	LaserJet Enterprise MFP M630	si
secretaria de seguridad y convivencia ciudadana	oficina de los abogados	HP	Color lasert Enterprise MFP M681	si
secretaria de desarrollo administrativo	bienes e inmuebles	HP	Laserjet 600m602	si
Secretaria de educación	cobertura	HP	LaserJet p3015	si
secretaria de infraestructura	dirección operativa parques y escenarios deportivos	HP	Laserjet p2055dn	si

4.3 EQUIPOS DE COMUNICACIONES

El total de switches y router, son compatibles con IPv6, son los equipos de comunicación más actualizados con los que cuenta la entidad.

4.4 SERVIDORES

El total de servidores tiene soporte IPv6 debido a que los Sistemas Operativos en los que se encuentran operando son compatibles con el nuevo protocolo, por lo que sugieren una fácil implementación de cualquier mecanismo de transición, Doble Pila.

Se cuenta con un total de 44 máquinas virtuales que soportan servicios como controlador de dominio, portal tributario entre otros servicios.

Inventario máquinas virtuales:

Nombre	Servicios	Sistema Operativo	Soporta IPv6
AD-1	Controlador de dominio	Win Server 2008 R2	Si
AD-2	Controlador de dominio	Win Server 2008 R2	Si
aire_portal	tributario.pereira.gov.co	Centos 7.4	Si
aire_portal_pru	Portal tributario pruebas	Centos 7.4	Si
antivirus	Antivirus endpoints	Win Server 2008 R2	Si
empece	Pagina emprendimiento Secretaria de Desarrollo y Competitividad	Ubuntu 16.04	Si
encifras	Pagina Pereira en Cifras	Ubuntu 14.04	Si
encifras-pru	Pagina Pereira en Cifras prueba	Ubuntu 14.04	Si
fs1	File Server	Win Server 2012	Si
fw-adm	Administracion reglas FW Interno	Win 7	Si
fwi	Filtro de paquetes red DC	Ubuntu 16.04	Si
glpi	Sistema de tiquetes	Ubuntu 16.04	Si
HelpPeople_Svr	Generador de PDFs	Win Server 2008 R2	Si
intranet	Intranet	Ubuntu 14.04	Si
Intrasem	Intranet Secretaria Educación	Centos 5.5	Si
juridica	Sistema de Juridica	Centos 6.4	Si
min1	Sistema documental	Ubuntu 16.04	Si
nas_infi	File Server	FreeNas 9.10	Si
nas-1	File Server ISOs	FreeNas 9.10	Si
nas-2	Archivos Comunicaciones	FreeNas 9.10	Si
nas-3	Control Interno Oportuno Sisben	FreeNas 9.10	Si
Oracle_prod	BDs SGI y SAIA producción	Oracle Linux 5.9	Si
oraserver_p	BDs SGI y SAIA pruebas	Centos 7.3	Si
oraserver1	BDs siif y fr12per	Centos 7.3	Si
oraserver2	SAIA migración	Centos 7.3	Si

Nombre	Servicios	Sistema Operativo	Soporta IPv6
OSC	Página web observatorio	Ubuntu 16.04	Si
proxy1	Proxy HTTP	Ubuntu 14.04	Si
Qlick	Digiturno	Win Server 2008 R2	Si
rural	Página web desarrollo rural	Win Server 2012	Si
saia	Saia Nuevo	Centos 7.6	Si
saia-app	Saia APP produccion	Centos 6.5	Si
saiaapp-pru	Saia APP pruebas	Centos 6.5	Si
sgi_pru	BD tributario de pruebas	Centos 7.3	Si
SIIF	Nuevo SIIF	Centos 7.3	Si
siproj-db	pgestiondoc (bd de SIPROJ)	RHEL 4	Si
Smart_VPN_Produc	recaudos.pereira.gov.co	Centos 5.9	Si
sondeox	Plataforma sondeox para gestión de vendedores informales. Vive digital. Registro Atención Emergencias de la DIGER .	Win Server 2008 R2	Si
Spark-DNS-doc	DNS server Documentación TI	Centos 6.4	Si
svr_vr_impresion	Print server	Win Server 2008	Si
Tributario1	app tributario	Centos 6.10	Si
vCenter60	Gestión infraestructura virtual	Suse Ent 11	Si
veeam	Gestión respaldos	Win Server 2008 R2	Si
vpnpruebas	recapru.pereira.gov.co	Centos 5.9	Si
win-apps	Formas Tributario App de Ingreso al Edif	Win 2003 Server	Si

Inventario servidores físicos:

Nombre	Descripcion	OS	IPV6
h1	Host virtualización #1	ESXi 6.0 2494585	Si
h2	Host virtualización #2	ESXi 6.0 2494585	Si
dl360	Host para Oracle BDs	ESXi	Si
dl380e	Host para Oracle WL	ESXi 6.0 9313334	Si
HP StoreEasy	NAS para respaldos	Windows Storage Server	Si
HP 3Par	SAN Producción		No
HP Eva	SAN Vieja		No
HP MSA	SAN iSCSI nueva		Si

4.5 APLICATIVOS

Se utilizan diferentes aplicativos y sistemas de información en las secretarías, que hacen parte de entidades gubernamentales a nivel Nacional y son éstas quienes tienen administración total sobre dichos aplicativos.

Con los aplicativos que corren sobre servidores con Sistemas Operativos compatibles con IPv6 no se tiene problema alguno en la implementación de técnicas para la coexistencia de los dos protocolos.

Inventario de aplicativos que dependen de la Secretaria TIC:

NOMBRE DEL APLICATIVO	FUNCION	LENGUAJE DE PROGRAMACION	MOTOR DE BASES DE DATOS	VERSIÓN IP	SOPORTE IPV6	ACTUALIZACIÓN
MIN Pereira	Sistema de Gestión Documental Inteligente	Php	MySQL	Dual Stack	Si	Si
SAIA	Sistema de Gestión Documental	Php	Oracle	IPv4		
SIIF Web	Sistema financiero	Java	Oracle	IPv4	No	Si
Portal Web	Página web institucional	HTML - JAVA-CSS	SQL Server	IPv4	No	Si
SIPROJ	Sistema de procesos judiciales	Javascript, Jquery	Oracle 10G	Dual Stack	Si	Si
SONDEOX	Sistema de encuestas parametrizadas	Javascript, Jquery, Php, Windev	PostgreSQL	Dual Stack	Si	Si
Denuncia Ciudadana	Sistema de atención a reportes de denuncias por parte de la ciudadanía	Php	MySQL	IPv4	Si	Si
Digiturno	Turnos de atención a la comunidad	Javascript, Jquery, Php, Windev	MySQL			

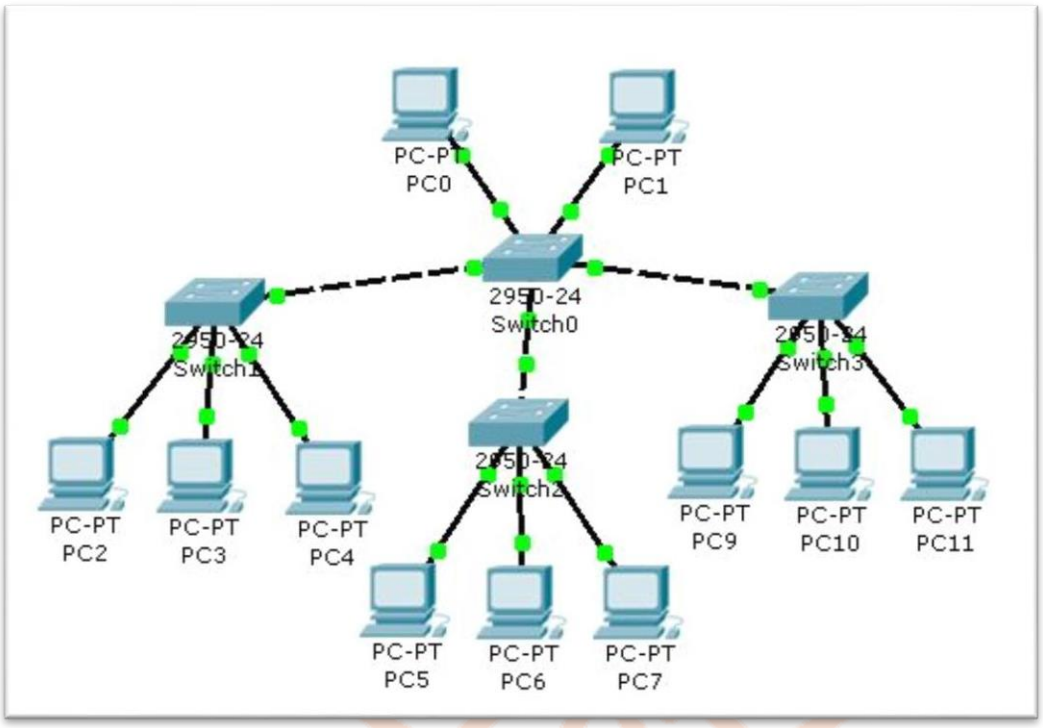
Inventario de aplicativos que dependen de otras dependencias de la Alcaldía:

NOMBRE DEL APLICATIVO	FUNCION	LENGUAJE DE PROGRAMACION	MOTOR DE BASES DE DATOS	VERSIÓN IP	SOPORTE IPV6	ACTUALIZACIÓN
AIREPLUS	Administración de los tributos municipales	PL-SQL, JAVA	Oracle	IPV4	SI	
SIABUC9 (sistema Integral automatizado de Bibliotecas de la Universidad de Tolima)	Con este software integral dispondrá de todas las herramientas necesarias para administrar de manera eficiente los procesos característicos de las Bibliotecas		Componente para gestión de bases de datos utiliza para crear, leer, actualizar y eliminar datos de una base de datos	IPV4	SI	
Llave del saber	Es un sistema de información para la generación y análisis de datos asociados a los servicios y acciones de las bibliotecas que participan de la Red Nacional de Bibliotecas Públicas,	. NET	PostgreSQL	Versión IPV4		
ADAS	Automatización de radio. emisora cultural de Pereira	C++	ACCES	IPV4	SI	SI
Memento data base(deportes)	Aplicativo permite diligenciar el formulario creado sin internet y luego mediante una sincronización con la cuenta asignada, sube los datos ingresados a la base de datos en el DRIVE.	GO	NOSQL	IPv6	SI	N/A
A luchar por Pereira(gobierno)	Recolectar las denuncias que presenta la comunidad	PHP, HTML	POSTGRES	SI	SI	SI
SISAA (Sistema de información socioeconómico y ambiental)	capturar información de uso de suelo actual de la zona rural, y registrar las intervenciones del personal técnico de la secretaria	PHP 7.0.33	POSTGRES	IPv4	NO	SI
Estratificación y Nomenclatura	Permite registrar la estratificación y nomenclatura del municipio de Pereira; generar certificados de estratificación y nomenclatura.	PHP	PostgreSQL	NO	NO	SI
Portal Geográfico del Municipio de Pereira	Geo portal para la consulta de cartografía y descarga de información normativa y cartográfica, además de generación de reportes	Phyton	Arcgis	No se	no	no
SISAP	Aplicativo para el registro de las actividades realizadas en el seguimiento de la salud Pública del Municipio de Pereira, vigilancia y control, aseguramiento	PHP	POSTGRES SQL	IPV4	SI	Si puede actualizarse
SEM	Aplicativo para el registro y seguimiento al sistema de emergencias medicas	PHP	POSTGRES SQL	IPV4	SI	Si puede actualizarse

5 ANÁLISIS DE LA NUEVA TOPOLOGÍA DE LA INFRAESTRUCTURA ACTUAL Y SU FUNCIONAMIENTO

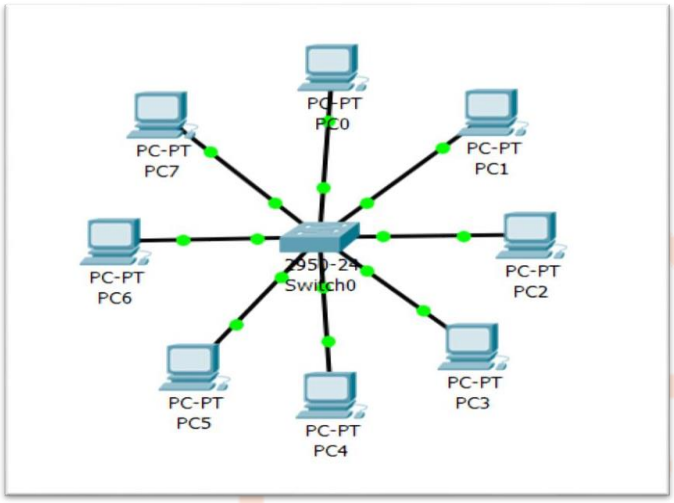
El funcionamiento de esta topología es igual a la topología en estrella.

La red de datos de la Administración Municipal de la Alcaldía de Pereira actualmente funciona bajo la topología de estrella extendida, con la diferencia que cada nodo puede ser el nodo principal de las demás máquinas, la topología en estrella extendida es jerárquica y busca que la información se mantenga local, como se observa en el diagrama.

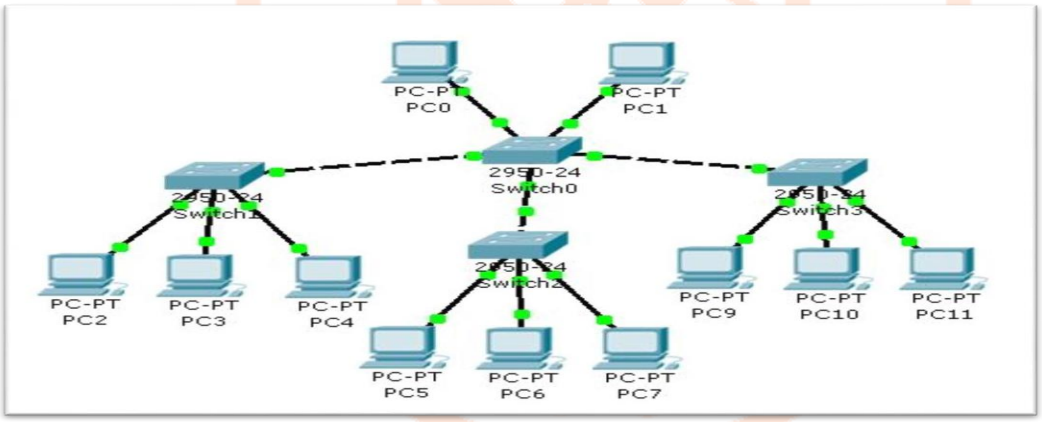


Todas estas sedes cuentan con **topología de red en estrella extendida, como lo son** Torre Central Séptimo piso y sótano, Palacio Nacional(centro de empleo, séptimo piso víctimas).

La Casa de Justicia de Cuba, cuenta con topología estrella:



UPVV Quinta con 14, Bombero, Centro Administrativo el Lago SISBEN, Parque del Café.



El proceso de enrutamiento lo hace el switch CORE ubicado en el quinto piso, el cual se encarga de distribuir por medio de fibra óptica a cada piso o sede

Puntos de red operando: 783 la información corresponde al número de equipos activos en la Alcaldía.

Categoría del cableado: categoría 5E, categoría 6 y 6A.

Diagrama de Red Sótano

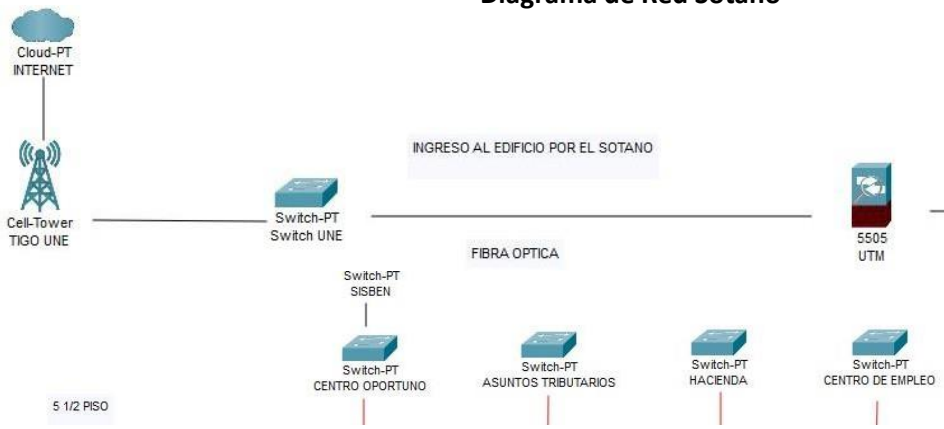
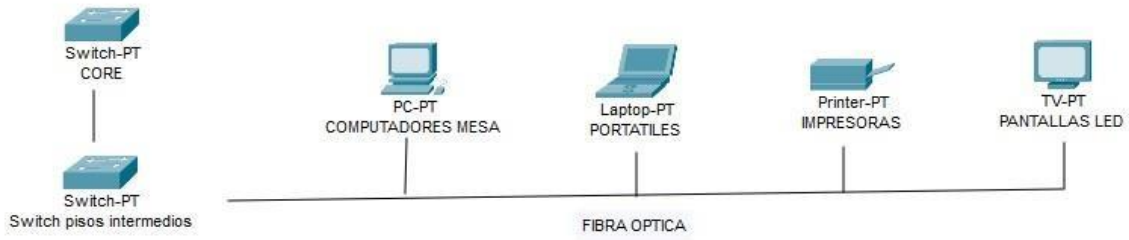


Diagrama de Red Pisos intermedios



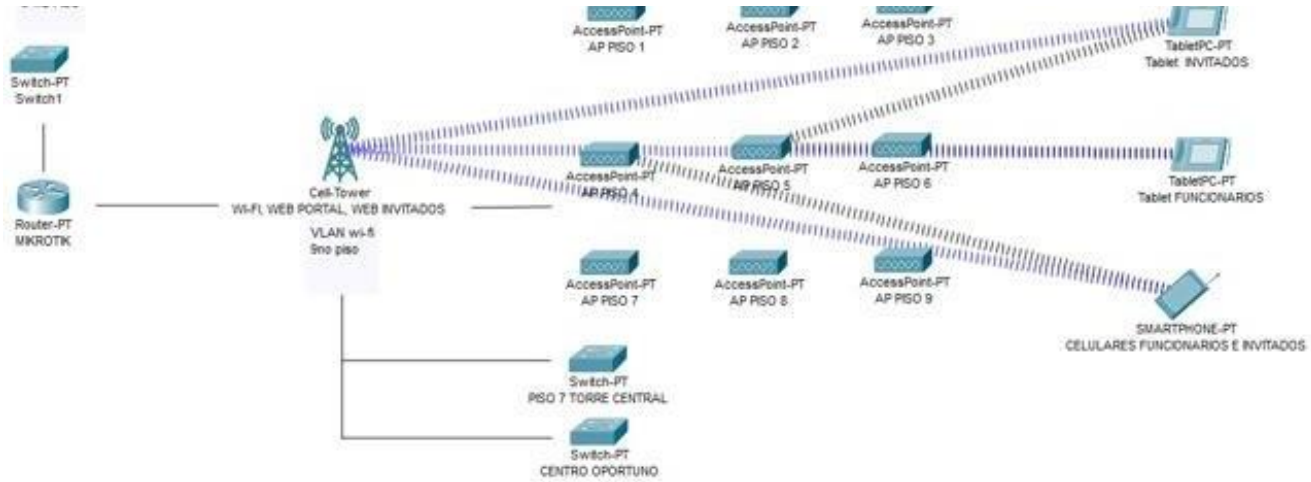
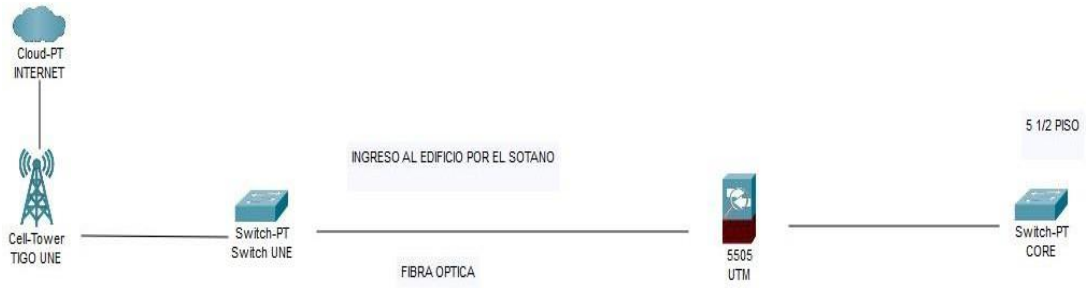
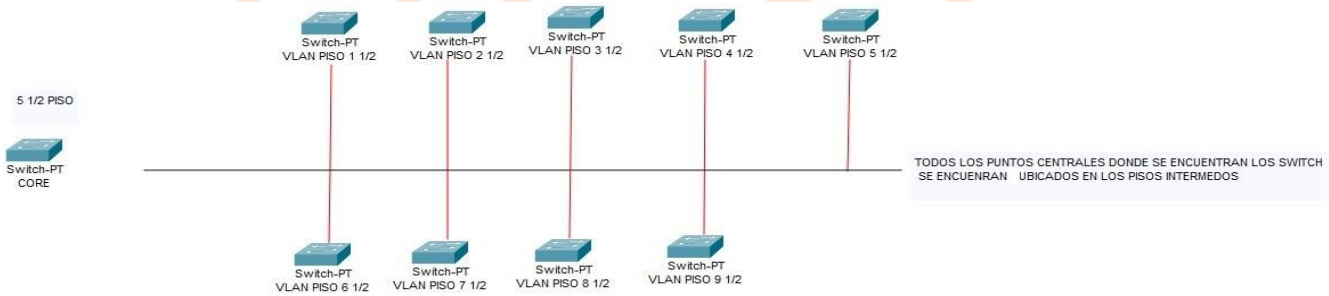


Diagrama de red desde la Alcaldía de Pereira hacia las sedes externas:
En este diagrama se muestra la distribución básica y general de la estructura de red de la alcaldía de Pereira y todas las sedes remotas que dependen la misma.

Empezamos por el diagrama de red inicial proveniente de la empresa TIGO UNE.

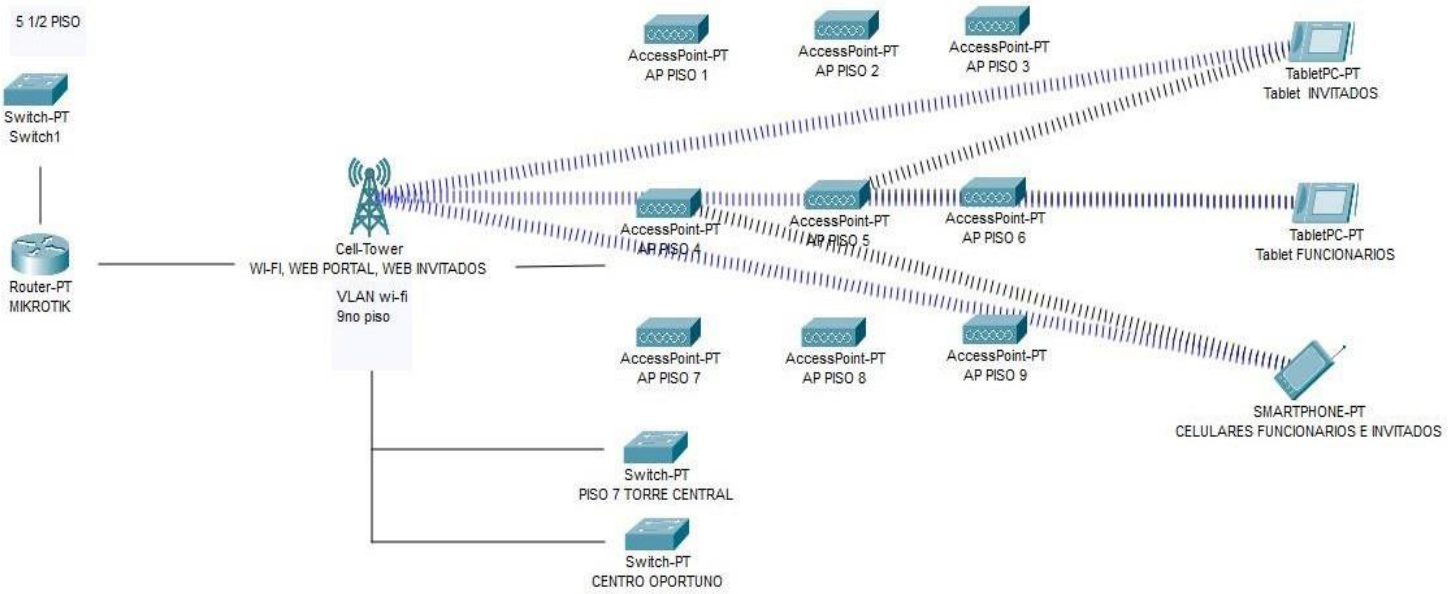


Continúa con la distribución de los pisos intermedios después de llegar por fibra óptica al piso 5 y medio que es donde se distribuye todo.

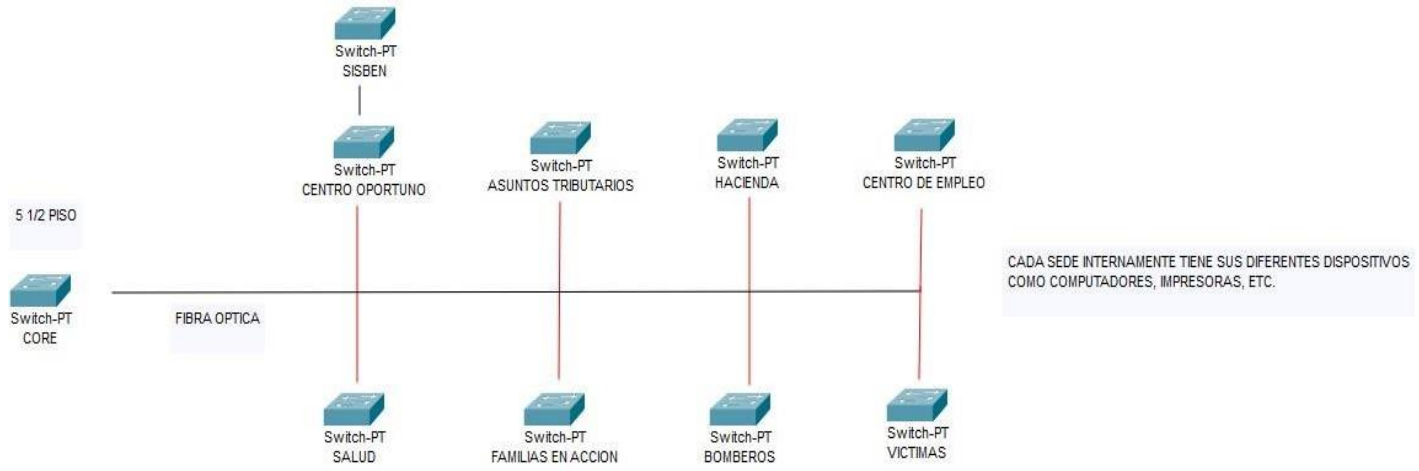


Después de llegar a cada piso intermedio, la red se distribuye por el piso dando posibilidad de conexión a diferentes equipos como se muestra a continuación.

Al interior del palacio no solo se presta el servicio de red de forma cableada, sino que también cuenta con una red Wi- fi que cubre la totalidad de los pisos, ofreciendo el servicio de red a funcionarios y a visitantes.



Por último la red no solo abarca la alcaldía, también brinda el servicio a diferentes sedes remotas de la misma como se muestra en la imagen a continuación



El Centro Administrativo Municipal entrega a su red direcciones IP dinámicas a través del protocolo DHCP, éste distribuye las 783 direcciones, de esta manera se asignan direcciones de manera aleatoria a cada uno de los host que hacen parte de la red, de manera contraria, se asignan direcciones estáticas a equipos servidores; por otra parte, no existe una segmentación de red establecida, no se encuentran determinadas subredes por áreas o departamentos, solo encontramos subredes por pisos.

Si se desea seguir entregando las IP a través de DHCP, se debe tener en cuenta que para la red trabajando en IPv6 este protocolo debe configurarse como DHCPv6, el cual permite a los servidores DHCP pasar parámetros de configuración como direcciones de red IPv6 a nodos IPv6. Ofrece la capacidad de asignación automática de direcciones de red reutilizables y flexibilidad de configuración adicional.

Este protocolo es una contraparte con estado de "Autoconfiguración de direcciones IPv6, Stateless", y se puede usar por separado o simultáneamente con este último para obtener parámetros de configuración automática. Si, por el contrario, se desea segmentar la red y establecer subredes, se debe tener presente que para IPv6 el procedimiento de segmentación es casi idéntico al realizado en IPv4.

En cuanto a las sedes externas la estructura de la red se organiza como VLANs que hacen parte de la red principal de la Alcaldía Municipal de Pereira.

6 PROTOCOLO DE PRUEBAS DE VALIDACIÓN DE APLICATIVOS, PLAN DE SEGURIDAD Y COEXISTENCIA DE LOS PROTOCOLOS

6.1 CARACTERISTICAS DEL NUEVO PROTOCOLO

El Protocolo de comunicaciones IPv6 Internet Protocol Versión 6, fue desarrollado por Steve Deering y Craig Mudge en el año 1994, y posteriormente fue adoptado por la IETF (Internet Engineering Task Force), adicionalmente IPv6 también es conocido como IPng (IP Next Generation). El nuevo protocolo tiene el propósito de reemplazar progresivamente el protocolo IPv4 actualmente en uso por la comunidad de Internet, en razón al limitado número de direccionamientos en IP que no hace posible su crecimiento en las redes y servicios; las características generales del nuevo protocolo son:

-Definido por la RFC (Request For Comments) 2460 de 1998.
-Tamaño del paquete 128 bits.
-Encabezado de base simplificado y de extensión.
-Identificación de flujo de datos, mejor calidad de servicio (QoS).
-Direccionamiento en Anycast, Multicast y Unicast.

Se recomienda La ejecución y configuración de las pruebas piloto de IPv6, se debe realizar bajo un proceso metódico que implique inicialmente la creación de una Red de Área Local Virtual (VLAN) de prueba sobre el Core de la red, que incluya diversos equipos y servicios de misión crítica que contemple entre otros, el análisis del comportamiento de software, el análisis del hardware en cada dispositivo, el análisis y comportamiento de estos en la red de comunicaciones, su comportamiento dentro de los aplicativos de la entidad, el análisis de cada servicio ofrecido y agregación de carga de tráfico sobre esta VLAN, teniendo en cuenta que las pruebas realizadas deben estar sujetas a las mejores prácticas y metodologías de transición a IPv6 conservando el criterio técnico de Doble Pila o Dual Stack. Una vez se tenga la certeza de que la VLAN de pruebas, ha soportado todo el proceso de pruebas de funcionalidad sobre un ambiente de tráfico en doble pila controlado; el siguiente paso es replicar esta VLAN."

6.2 PROTOCOLO DE PRUEBAS

El proceso de transición a IPv6 trae consigo cambios que pueden generar gran impacto no sólo en la red de datos sino en el desarrollo cotidiano de las actividades a las que se dedica la entidad, por ello es importante analizar previamente los siguientes riesgos que son algunos de muchos que se pueden correr y de esta manera buscar cómo evitarlos y/o determinar el modo de actuar cuando sucedan.

- ✓ Pérdida y/o fuga de información.
- ✓ Daños físicos en los equipos.
- ✓ No disponibilidad de repuestos.
- ✓ Incompatibilidad de hardware.
- ✓ Inestabilidad de las aplicaciones.
- ✓ Problemas de funcionamiento en los sistemas operativos.
- ✓ Fallas de instalación y conexión de los equipos de red.

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

6.3 PLAN DE SEGURIDAD

Cuando se configura IPv6 en una red, se está habilitando el acceso a través de una nueva capa de red. Esto hace que las reglas de seguridad perimetral existentes para IPv4, ya no sean válidas para IPv6. Pero la seguridad no es solamente la configuración del cortafuegos u otro equipamiento, también son procesos y procedimientos que han sido elaborados a través de los años que deben ser revisados y analizados. Lo importante es considerar que IP es la denominación del Protocolo Internet que involucra a los dos IPv4 e IPv6, lo que implica que esta distinción debe realizarse en los

procedimientos correspondientes.

El otro caso de interés es sobre el filtrado de multicast y en particular de multicast local al enlace. En IPv6 no existe dirección de difusión (o "broadcast"), y elementos como la autoconfiguración de direcciones, la detección de direcciones duplicadas y el descubrimiento de vecinos dependen del uso de multicast.

Los siguientes son los servicios que impactan en seguridad en la Alcaldía de Pereira al momento de iniciar el plan de implementación del nuevo protocolo IPv6:

- Directorio activo
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- Servicios Proxy • Dominio de red • Correo electrónico
- Mensajería Instantánea
- Telefonía
- Video Conferencia
- Servicio Web y Acceso a Internet
- Aplicaciones y bases de datos
- Equipos de comunicaciones fijos y móviles
- (Firewalls, servidores AAA (Authentication, Authorization and Accounting), NAC (Network Access Control)
- Canal de Comunicación de internet.

Dado que IPv6 contiene el protocolo, Internet Protocol Security- IPSec, la seguridad se establece de acuerdo a las características esenciales de este mismo, lo que permite que el paquete de IPv6 (de 128 bits) pueda salir a la red de internet completamente cifrado sin que tengan que intervenir procesos como la traslación de direcciones (NAT) o esquemas de encapsulamiento (Túneles) que reducen considerablemente el desempeño de las direcciones IP. Es importante desarrollar lineamientos de seguridad bajo la premisa de los pilares básicos de la seguridad de la información como son la Confidencialidad, la Integridad y la Disponibilidad.

6.3.1 DISPONIBILIDAD

La disponibilidad en soluciones bajo IPv6 se puede visualizar en la garantía de ofrecer a los usuarios de la Alcaldía de Pereira una alta disponibilidad en servicios bajo IPv6, se deben realizar configuraciones de enrutamiento para los sistemas de enrutamiento para el soporte simultáneo de ambos protocolos(IPv4- IPv6) a fin de mantener la continuidad del negocio y proteger las inversiones.

6.3.2 PRIVACIDAD

En IPv6 se pueden combinar dos esquemas de seguridad de IP para transmitir un paquete IPv6, por un lado la autentificación y por el otro la privacidad. Las técnicas se puedan

utilizar de acuerdo con el orden en que se apliquen esto dos servicios:

6.3.2.1 CIFRADO ANTES DE LA AUTENTICACIÓN
Este procedimiento sucede cuando el paquete IP es transmitido y autenticado en su totalidad, previo a un esquema de cifrado en los extremos. Primero se aplica la Carga de Seguridad Encapsulada - ESP a los datos que se van a proteger y después se incorpora el texto original al comienzo de la cabecera de autentificación IP.

6.3.2.2 ATENTICACIÓN ANTES DEL CIFRADO

La Cabecera de Autentificación se encapsula dentro del paquete IP interno. Este paquete interno es autentificado y protegido por el esquema de privacidad. Esta técnica sólo es adecuada para el Encapsulado de Carga Útil - ESP en modalidad de túnel. El método puede preferirse en virtud de que la cabecera de autenticación AH se protege por la Carga de seguridad encapsulada ESP y de esta forma es muy complejo que los mensajes del paquete sean interceptados y modifiquen el AH sin ser detectado.

7 PLANEACIÓN DE LA TRANSICIÓN DE LOS SERVICIOS TECNOLÓGICOS DE LA ENTIDAD

7.1 MECANISMOS DE TRANSICIÓN.

La versión 6 del Protocolo de Internet ha sido diseñada para que su implementación se realice en coexistencia con IPv4. A continuación, se describen algunas de las principales categorías de mecanismos que facilitarían dicha migración; estos pueden ser utilizados solos o en combinación y la migración puede ser realizada paso a paso, comenzando con un solo nodo, de igual manera puede darse el caso en el que la red completa sea migrada a IPv6 mientras que el proveedor de servicios siga utilizando IPv4, o puede darse el caso contrario.

Lo ideal para una transición de Ipv4 a Ipv6 es que ambos protocolos existieran en una red, por eso existen tres tipos de mecanismos la cual permite este tipo de red, pero con diferentes características del uno con el otro, pero los tres cumplen la misma función que a continuación se los detalla:

- Dual Stack (Doble pila)
- Túneles
- Traducción

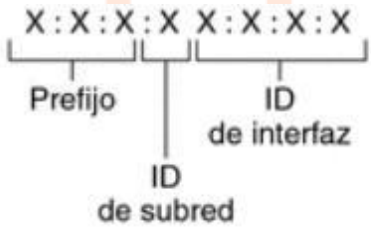
El Ministerio de las TIC recomienda en mecanismo Dual Stack (Doble pila) de esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la

conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4.

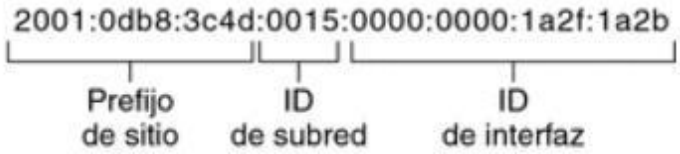
7.2 ESTRUCTURA DE LAS DIRECCIONES IPV6

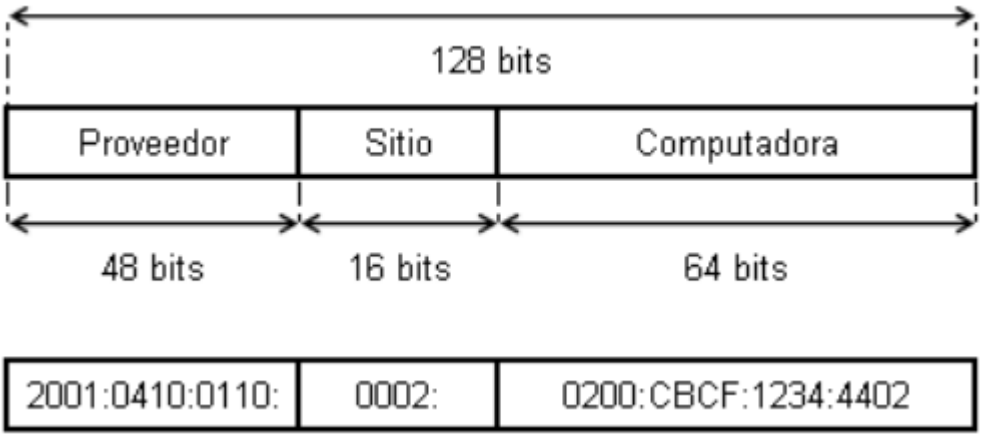
Las direcciones IPv6 tienen un tamaño de 128 bits, distribuidos en ocho campos de dieciséis bits representados por cuatro números hexadecimales cada uno y separados por dos puntos. En la figura se puede observar el formato de una dirección IPv6, los cuarenta y ocho primeros bits, es decir, los tres primeros campos contienen el prefijo de sitio, éste describe la topología pública y es el segmento que suelen asignar al sitio los ISP o RIR (Registro Regional de Internet). Los siguientes dieciséis bits lo ocupa el ID de subred y describe la topología privada, es asignado por el administrador de la red.

Los últimos sesenta y cuatro bits, o cuatro campos de la derecha, contienen el ID de interfaz y se puede configurar manual o automáticamente.



Ejemplo:





7.3 ESTRATEGIAS DE MIGRACIÓN A IPV6 STACK DOBLE

El método de stack doble es un método de integración en el que un nodo tiene implementación y conectividad para redes IPV4 e IPV6. Es la opción recomendada y requiere que se ejecuten IPV4 e IPV6 simultáneamente.

7.4 PLAN DE NUMERACIÓN

Se deben Ejecutar la configuración de las pruebas piloto de IPv6, con base en la realización de pruebas en los segmentos de red y VLANs creadas, con un número especial de usuarios que aprovechen la homogeneidad de la red, con servicios de filtrado, críticos a fin de evitar traumatismos en el normal funcionamiento de la red.

Se organizará por Distribución, es decir distribución por Servicios: Se basa en estimar los requisitos de direcciones de un determinado servicio o tecnología de acceso y su previsión de crecimiento para reservar suficientes direcciones, se utilizará el método Stack doble de integración en el que un nodo tiene implementación y conectividad para redes IPV4 e IPV6, el router y los switches se configuran para admitir ambos protocolos; el protocolo preferido es IPV6.

7.4.1 DIRECCIONAMIENTO ACTUAL Y SUGERENCIAS PARA IPV6

El Alcaldía Municipal entrega a su red direcciones IP estáticas, Si se desea entregar las IP a través de DHCP, se debe tener en cuenta que para la red trabajando en IPv6 este protocolo debe configurarse como DHCPv6, el cual permite a los servidores DHCP pasar parámetros de configuración como direcciones de red IPv6 a nodos IPv6. Ofrece la capacidad de asignación automática de direcciones de red reutilizables y flexibilidad de configuración adicional. Este protocolo es una contraparte con estado de "Autoconfiguración de direcciones IPv6, Stateless", y se puede usar por separado o simultáneamente con este último para obtener parámetros de configuración automática.

Si, por el contrario, se desea segmentar la red y establecer subredes, se debe tener presente que para IPv6 el procedimiento de segmentación es casi idéntico al realizado en IPv4.

7.4.2 NUMERACIÓN DE SERVIDORES

Para escoger el identificador de interfaz dentro de la red LAN que le corresponde a cada servidor se realiza generalmente numeración estática. La razón es apuntar a la máxima disponibilidad y evitar tener que realizar cambios ante problemas con la dirección de red. En el momento de escoger la dirección IPv6 estática a utilizar para un servidor se debe escoger una dirección fácil de recordar, como por ejemplo 2001:B36A:C2FE::1, esta opción facilita la operación pues hace más fácil el análisis de problemas ya que el espacio IPv6 es muy extenso y realizar barridos para buscar direcciones válidas en forma bruta o secuencial puede llevar un tiempo muy largo a menos que se cuente con registros de DNS. Por lo tanto, si un servidor tiene su registro en el DNS accesible públicamente, es menos importante utilizar direcciones aleatorias.

7.4.3 NUMERACIÓN DE TERMINALES

Para la numeración de terminales existen tres opciones que un administrador de red debe analizar:

Numeración manual. En este caso se debe numerar manualmente cada una de las terminales.

Numeración automática sin estado o sin servidor (“stateless” o “serverless”) utilizando el mecanismo “anuncios de encaminadores” (o “route advertisements”). Este mecanismo utiliza paquetes ICMPv6 y grupos de multicast locales a la interfaz. A través de este mecanismo se puede configurar la dirección IPv6, la longitud del prefijo y la ruta por defecto. Estas configuraciones se implementan en DHCPv6, particularmente a través de la opción sin estado (“stateless configuration”). Al no mantener estados, el administrador de la red no tendrá control sobre cuáles son las terminales que se conectan a la red IPv6. Cualquiera con acceso al medio común tendrá acceso.

Numeración automática con estados (“stateful”). En este caso la configuración de la dirección IPv6 se hace a través de DHCPv6 igualmente que con IPv4. De esta forma es posible definir un pool de direcciones o incluso asignar direcciones particulares para cada terminal. Utilizando DHCPv6 en su configuración con estados es posible realizar un control de acceso más estricto. Un parámetro que no se obtiene aún por parte de DHCPv6 es la ruta por defecto, por esto, aún cuando se utiliza DHCPv6 en modo con estados, es necesario utilizar el mecanismo de anuncio de encaminadores para obtener

la ruta por defecto.

7.4.4 CONFIGURACION DNS

Se recomienda mantener la utilización de los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6, de tal manera que la resolución de nombres de dominio se de en forma transparente tanto para Ipv4 como en IPv6, se exceptúa de esta regla los ambientes de prueba que se realicen sobre IPv6.

7.4.5 DESARROLLO DE SOFTWARE

De la misma manear que ocurre con IPv4, en Ipv6 se recomienda no usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías.

7.4.6 ENRUTAMEINTO DE LA RED

Disponer para las infraestructuras de TI, de varias zonas lógicas configuradas en el firewall, que estén segmentadas para cada uno de los servicios disponibles en la Entidad, a fin de garantizar la máxima protección una vez la red de comunicaciones comience a generar tráfico en IPv6.

7.4.7 TRANSICIÓN CON APLICATIVOS

Con los aplicativos que corren sobre servidores con Sistemas Operativos compatibles con IPv6 no se tiene problema alguno en la implementación de técnicas para la coexistencia de los dos protocolos, por el contrario, como no se tiene potestad alguna sobre alguno de los aplicativos, se recomienda trabajarlos como "nodos IPv4 Only", en donde se implementen métodos de traducción para que puedan soportar la técnica Doble Pila, esto mientras dura el proceso de migración y se tiene una comunicación directa con las entidades responsables de dichos aplicativos para saber cuándo éstos empiecen a trabajar sobre IPv6, si es el caso de que aún no estén implementados y/o trabajando ya con el nuevo protocolo.

7.5 POLÍTICAS DE ENRUTAMIENTO IPV6

El plan de enrutamiento para IPv6 no debe variar en demasía sobre lo que ya se hace en IPv4. En general para la administración tiene sentido que en IPv6 se mantenga la misma topología que en IPv4, pues el mantener dos topologías significaría incrementar el costo de operación del encaminamiento de la red y el aumento de incidentes.

Las opciones de enrutamiento en IPv6 son:

• Enrutamiento estático.

• Enrutamiento dinámico, en éste existen distintas categorías, como protocolos de vector distancia ó RIPNG (RIP Next Generation), protocolos de vector camino (“path vector”) ó BGPv4 y protocolos de estado de enlaces: ISIS o u OSPFv3.

7.6 SOLICITUD POOL DE DIRECCIONES ANTE EL ISP O ENTIDAD REGIONAL

Se recomienda utilizar bloques IPv6 propios, solicitados al ISP o recibidos directamente del RIR (Regional Internet Registry); es conveniente revisar nuevamente las políticas del registro; por ejemplo, en el caso de un proveedor de banda ancha que está utilizando direcciones IPv4 privadas (RFC1918) para sus clientes y desea reemplazar ese direccionamiento privado por direcciones IPv6 públicas (denominadas IPv6 globales), podrá hacer un requerimiento al registro pidiendo las direcciones IPv6 necesarias para ese cambio.

Se estima que para la Administración Municipal y en base al inventario de activos tecnológicos y de información se necesitan aproximadamente un pool de 1500 direcciones IPV6, En general y de acuerdo con toda la documentación consultada se ha decidido optar por de redes /64. Independiente del prefijo otorgado.

7.7 MONITOREO DE PRUEBAS

Las pruebas de funcionalidad (monitoreo) en IPv6 no solo debe ser tenido en cuenta en la fase de pruebas del modelo de transición de IPv4 a IPv6, sino que también debe permitir establecer el nivel de funcionamiento y criticidad de las redes IPv6 ya en operación, por lo que es necesario tener en cuenta la detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad y tener un plan de contingencias a la mano. Las siguientes son las variables a tener en cuenta a la hora de realizar monitoreo de los servicios de red en IPv6:

- Medición de tráfico sobre interfaces y dispositivos de red.
- Estado de servicios
- Estado de aplicaciones
- Actividad de los hosts y
- Canales de comunicación hacia Internet. Para ello es importante contar con herramientas de monitoreo, como por ejemplo analizadores de tráfico que provean análisis de interfaces de red, monitoreo de librerías de IPv6 y soporte sobre SNMP.

La Alcaldía de debe estar en capacidad de utilizar libremente las herramientas de test y/o de monitoreo una vez implementado IPv6, teniendo en cuenta que la complejidad de cada una de estas no es lo importante sino los resultados exitosos que arroje el mismo.

8 VALIDACIÓN DE ESTADO ACTUAL DE LOS SISTEMAS DE INFORMACIÓN, LOS SISTEMAS DE COMUNICACIONES, LAS INTERFACES Y REVISIÓN DE LOS RFC CORRESPONDIENTES.

Se precisa revisar los RFC de seguridad, en especial el RFC 4942 que hace referencia a las consideraciones de seguridad para el proceso de coexistencia y transición a IPv6.
Se requiere revisar el RFC 6177, cuya especificación técnica se refiere a las

recomendaciones que deben seguir los clientes para solicitar asignación de segmentos de IPv6 en el rango de /48 a /56.

Revisar los procedimientos de RFC de seguridad para la utilización del software de aplicativos, equipos de comunicaciones, redes, sistemas de cifrado, dispositivos móviles, entre otros.

Lista de RFC que aplican a la seguridad en IPv6:

- RFC 5619: Software Security Considerations, Agosto 2009
- RFC 5269: FMIP Seurity Distributing a Symectric Fast Mobile IPv6 (FMIPv6)
- RFC 4942: IPv6 Transition/Coexistence Security Considerations
- RFC 4218: Threats Relatiing To IPv6 Multihoming Solutions
- RFC 4891: Using IPsec To Secure IPv6 Tunnels
- RFC 4890: Recommendations For Filtering ICMPv6 Messages in Firewalls
- RFC 4864: Local Network Protection For IPv6
- RFC 4843: An IPv6 Prefix For Overlay Routable Cryptographic hash Identifiers (ORCHID) ♣ RFC 5213: Proxy Mobile IPv6
- RFC 4835: Cryptographic Algorithm Implementation Requeriments for Encapsulatiing Security Payload (ESP) and Authentication Header (AH)
- RFC 4487: Mobile IPv6 And Firewalls: Problem Statement
- RFC 4449: Securing Mobile IPv6 Route Optimization Using a Static Shared Key
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models Threats
- RFC 4301: Asociaciones de seguridad (SA). Security Architecture for the Internet Protocol. Soporte para IPsec-V2. (Hace obsoleto el RFC 2401)
- RFC 2401: Security Architecture for the Internet Protocol (Actalizado por RFC 3168), Soporte para IPsec-V2.
- RFC 4302: IP Authentication Header (Hace obsoleto RFC 2402)

- RFC 4877: Mobile IPv6 Operation with IKEv2 and the revised IPSec Architecture
- RFC 4581: Cryptographically Generated Addresses (CGA) extention field format (Actualiza el RFC 3972)

- RFC 4982: Support For Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA). (Actualiza el RFC 3972 errata)
- RFC 3414: User – Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 4807: IPSec Security Policy Database Configuration – MIB.
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 4718: IKEv2 Clarifications and implementation Guidelines

9 IDENTIFICACIÓN DE ESQUEMAS DE SEGURIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES.

La fase de implementación del protocolo IPv6 debe ser estructurado con base en los esquemas de seguridad de información, sobre los cuales se tengan contempladas las políticas de confidencialidad, integridad y disponibilidad de las Entidades.

Se requiere definir un plan de marcha atrás (Plan de Contingencias) para el caso de presentarse inconvenientes de indisponibilidad de los servicios, que atenten contra la seguridad de la información y de las comunicaciones en la Alcaldía de Pereira al momento de implementar el protocolo IPv6.

En el proceso de transición hacia el nuevo protocolo, revisar la seguridad de información de las infraestructuras de TI, la seguridad de IPv6 y el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio - DNS, Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Servicios Web y Sistemas de Gestión y Monitoreo.

Se recomienda mantener la utilización de los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6, de tal manera que la resolución de nombres de dominio se de en forma transparente tanto para Ipv4 como en IPv6, se exceptúa de esta regla los ambientes de prueba que se realicen sobre IPv6.

La implementación de IPv6 puede generar riesgos de seguridad de información, que impactan en los servicios de las entidades y pueden acarrear problemas; con el objeto de poder detectar estos riesgos se requiere hacer un análisis detallado que permita encontrar posibles vulnerabilidades y en efecto bajo IPv6 es necesario hacer esta labor debido a que el protocolo se apoya en otros protocolos como IPSec, HTTP, TCP, UDP o SIP.

Disponer para las infraestructuras de TI, de varias zonas lógicas configuradas en el firewall, que estén segmentadas para cada uno de los servicios disponibles en la Alcaldía de Pereira, a fin de garantizar la máxima protección una vez la red de comunicaciones comience a generar tráfico en IPv6.

Disponer del equipo humano idóneo necesario para verificar y monitorear los problemas de seguridad de información que surjan al momento de ejecutar las fases de implementación y pruebas de funcionalidad, cuya labor está bajo la responsabilidad del Director de infraestructura tecnológica de la Alcaldía de Pereira.

9.1 DIRECCIONAMIENTO IP

- Para el comportamiento del tráfico de IPv6, se requiere tener en cuenta el uso de las directivas de seguridad del protocolo IPsec, para ambientes que requieren atender solicitudes de servicios HTTP entre nodos IPv6.

- Considerar la revisión de los segmentos de bloque de direcciones en IPv6 y si estos se ha realizado por zonas lógicas de seguridad (Zonas Desmilitarizadas – DMZ) con base en las necesidades de operación de cada organización y estableciendo los criterios de seguridad correspondientes.

- La utilización de los bloques de direccionamiento en IPv6, deben acoger las políticas de seguridad y privacidad de la información permitiendo que el funcionamiento de las mismas sea transparente para los usuarios finales de la Entidad.

- Los planes de direccionamiento en IPv6 se deben realizar con base en los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.

- La utilización del direccionamiento IPv6 debe utilizarse en forma espaciada y no consecutiva como recomendación general a fin de evitar ataques de direccionamiento IP tanto del interior como del exterior en modalidad de “fuerza bruta”.

- Se recomienda crear VLANs (Redes de Área Local Virtuales) por separado dentro de las redes locales de las organizaciones para propósitos de pruebas de direccionamiento, tráfico, monitoreo y seguridad cuando se comience la fase de implementación del nuevo protocolo.

- En redes IPv6 los paquetes pasan por distintas etapas de enrutamientos, con el fin de mitigar el espacio de búsqueda de posibles atacantes de escaneo sobre las redes IPv6, por lo tanto se recomienda que los administradores de las redes utilicen herramientas de software de monitoreo para controlar posibles patrones de comportamiento de direccionamiento IP aún si el tráfico generado es dirigido (multicast) y se utiliza descubrimiento de vecinos (Neighbor discovery)4.

- Los paquetes IPv6, deben seguir las recomendaciones de seguridad de los paquetes IPv6, consistente en que estos contienen cabeceras de autenticación (AH, Authentication Headers) y encabezados de extensión de carga de seguridad encapsulada (ESP, Encapsulating Security Payload), en la cual el protocolo IPsec permite para cualquier nodo de IP el establecimiento de sesiones de seguridad de extremo a extremo.

9.2 PROTOCOLO IPSEC - INTERNET PROTOCOL SECURITY (IP SECURITY)

IPsec es un protocolo de seguridad definido por el estándar IETF5 desde 1999 y se basa en el RFC 4301, que establece las siguientes consideraciones: Según la IETF, “IPsec está diseñado para proporcionar interoperabilidad, de alta calidad, con seguridad basada en cifrado tanto para IPv4 como para IPv6. El conjunto de servicios de seguridad ofrecidos en IPsec, incluyen control de acceso, integridad sin conexión, autenticación de origen de los datos, detección y rechazo de repeticiones (una forma parcial de integridad secuencial), confidencialidad a través de cifrado y confidencialidad de flujo de tráfico limitado. Estos servicios se proporcionan en la capa 3, ofreciendo protección de manera estándar para todos los protocolos que pueden ser transportados a través de IP.

IPsec incluye una especificación para una mínima funcionalidad de firewall, ya que es un aspecto esencial de control de acceso en la capa IP. Las implementaciones son libres de implementar mecanismos de firewalls sofisticados exigidos por IPsec.”6 IPsec por lo tanto contiene las siguientes características:

- Integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores.

- IPsec es un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad; es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

- Así mismo, IPsec, es el protocolo para cifrado y autenticación IP el cual forma parte integral del protocolo IPv6. El funcionamiento de IPsec es obligatorio en IPv6 y se usa para asegurar el tráfico entre enrutadores BGP (Boundary Gateway Protocol); su uso se extiende para protocolos de enrutamiento tipo OSPFv3 (Open Shortest First Path).

- De acuerdo a lo anterior, el protocolo IPsec puede ser utilizado en diferentes escenarios a nivel de enrutamiento, por ejemplo con OSPFv3, que utiliza AH, la extensión de encabezados maneja ESP como un mecanismo de autenticación en lugar de la variedad de esquemas de autenticación y procedimientos definidos en OSPFv2; en IPv6 Móvil, donde esta especificación de protocolo es un proyecto de la IETF propuesto para usar IPSec para hacer obligatoria la autenticación de actualización; en Túneles, en la cual IPSec pueden ser configurado entre sitios (enrutadores IPv6) en lugar de que cada equipo utilice IPSec y finalmente administración de red, en la cual IPSec se puede utilizar para garantizar el acceso del enrutador para la gestión de la red.

9.3 REVISIÓN DE LOS RFC DE SEGURIDAD

Se precisa revisar los RFC de seguridad, en especial el RFC 4942 que hace referencia a las consideraciones de seguridad para el proceso de coexistencia y transición a IPv6.

Se requiere revisar el RFC 6177, cuya especificación técnica se refiere a las recomendaciones que deben seguir los clientes para solicitar asignación de segmentos de IPv6 en el rango de /48 a /56.

Revisar los procedimientos de RFC de seguridad para la utilización del software de aplicativos, equipos de comunicaciones, redes, sistemas de cifrado, dispositivos móviles, entre otros.

9.4 REDES PRIVADAS VIRTUALES - VPNS

En caso de que se presente varias conexiones privadas virtuales extremo a extremo que permiten intercomunicar dos o más redes locales (LAN); es importante tener presente el control del tráfico entre varios puntos de la red IPv6. En este orden de ideas, el tráfico IPv6 puede pasar por muchos recursos compartidos en una red de amplia cobertura, razón por la cual es necesario garantizar la seguridad del tráfico de las comunicaciones entre estas redes privadas virtuales con la utilización del protocolo IPSec.

9.5 SEGURIDAD DE IPV6 EN LOS CENTROS DE DATOS

Al momento de implementar IPv6, los centros de datos son los elementos importantes a revisar por ser los ejes centrales en la Alcaldía de Pereira, por lo tanto existen varias formas de introducir y operar IPv6 en Centros de Datos. Una forma es continuar con una operación IPv4 dentro del centro de datos y hacer algún tipo de translación en el borde (no recomendable de acuerdo a los lineamientos del gobierno), una segunda forma es usar la doble pila y una tercera es usar únicamente IPv6.

En resumen tenemos:

Translación de IPv4 en el borde: En este escenario el centro de datos mantiene su infraestructura interna en IPv4 y hace algún tipo de translación a IPv6 en el borde.

Pila Doble: Aquí encontramos pila doble a través todos los servicios del centro de datos o al menos en los que presentan servicios a usuarios. También puede encontrarse pila doble solo en el borde mientras que las conexiones internas son IPv4 o IPv6 únicamente.

Solo IPv6: Esta es generalmente la etapa final de la transición de un centro de datos a IPv6. Aquí encontramos IPv6 en todos los elementos del centro de datos. Para ofrecer servicios a los usuarios legados de IPv4 se utiliza algún tipo de translación en el borde.

9.6 LINEAMIENTOS DE SEGURIDAD EN LA NUBE BAJO IPv6

La seguridad en la nube en entornos tanto de IPv4 como de IPv6 deben responder a una estrategia de análisis para ambientes tanto físicos como lógicos que permitan a la Alcaldía de Pereira construir políticas adecuadas para su correcta administración e implementación en las infraestructuras de comunicaciones.

Es necesario presentar los lineamientos de seguridad en la nube a los distintos proveedores de comunicaciones de la nube considerando los siguientes aspectos:

Confección de un mapa de riesgos y sus implicaciones (Con el apoyo de los proveedores de servicios).
Establecimiento de control de identidad de usuarios.
Adopción de normas de protección de información.
Revisión de esquemas de virtualización (si existen).
Revisión de la infraestructura del tipo de nube que se requiere implementar para adecuarla a IPv6 (nube híbrida, federada, privada, pública, entre otras).
Adopción de retención de datos.
Acuerdos de Nivel de Servicio (ANS) con el proveedor del servicio.
Conexión a través de Redes Privadas Virtuales - VPNs.
Uso de claves complejas.
Almacenamiento de cifrado de la información.
Evaluación de los estándares de servicio.
Verificación de pruebas del servicio, es decir garantía de que los canales y servicios en la nube esté funcionando correctamente.
El proveedor de servicio contratado debe ofrecer gran reputación, esto debido a que la información en la nube puede estar en muchas partes del mundo.
Establecer acuerdos de confidencialidad de la información.

Recomendaciones antes de subir a la nube:

Hacer un análisis de la criticidad de la información (Activos de información, directorio activo, cuentas de correo, bases de datos importantes, entre otros).

Validar la calidad y las condiciones del servicio que ofrezca el proveedor de la nube.
Definir con claridad qué tipo de información debe ser publicada en la nube.
Verificar que información requiere ser almacenada en una estructura convencional.
Garantizar a los usuarios que la contratación de servicios con un proveedor en la nube sea de alta calidad y experiencia que apoye a la seguridad de la información.