CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS



Plan de Diagnóstico del Protocolo IPv6

Relación de Versiones

Versión	Fecha	Revisó	Aprobó
1	Diciembre 22 de 2023	Yorguin Gómez	

Tabla de Contenido

1. Justificacion 9

2. MARCO NORMATIVO 11

3. PLANTEAMIENTO DEL PROBLEMA 13

4. ALCANCE 15

5. Objetivos 16

5.1 OBJETIVO GENERAL 16

5.2 OBJETIVOS ESPECÍFICOS 16

6. ANÁLISIS DE LA INFRAESTRUCTURA 17

6.1 ARQUITECTURA DE RED DE COMUNICACIONES 17

6.2 INVENTARIO DE ACTIVOS DE TI DE TECNOLOGÍA 18

6.2.1 Análisis del documento de inventario de activos de TI. 20

6.2.2 Análisis del inventario de los Sistemas de información. 24

6.3 PLAN DE DIAGNOSTICO 25

6.3.1 Determinación de la Compatibilidad (Niveles mínimos de compatibilidad de IPv6 para los activos de TI). 27

6.3.2 Determinación de la Compatibilidad General de los Activos de TI: 31

6.3.3 Informe de equipos de Infraestructura (Servidores físicos, virtuales, almacenamiento y sistemas de información): 33

6.3.3.1 Informe de equipos de energía : 34

6.3.3.2 Informe de Equipos de Seguridad Informática: 34

6.3.3.3 Informe de Equipos de Seguridad Física: 35

6.3.3.4 Informe de Equipos de Usuario Final: 35

6.3.3.5 Informe de Sistemas Operativos: 38

6.3.3.6 Informe de Servicios (Directorio activo, DHCP y DNS) 39

6.3.3.7 Informe de Sistemas de Información: 39

6.3.3.8 Diagnóstico de aplicaciones 40

6.3.3.9 Recomendaciones para los sistemas de Información 42

7. PLAN DE TRANSICIÓN 43

7.1 MECANISMO DE TRANSICIÓN A UTILIZAR 43

7.2 PLAN DE DIRECCIONAMIENTO IPv6 43

7.3 PLAN DE MANEJO DE EXCEPCIONES 44

7.3.1 Para la infraestructura 44

7.3.2 Para equipos de Seguridad Física 44

7.3.3 Para los Sistemas de Información. 45

7.3.4 Para los activos de TI con compatibilidad desconocida 46

7.4 INFORME DE PREPARACIÓN (READINESS) 47

7.4.1 Solicitar el direccionamiento global al organismo regulador o proveedor de servicios de internet. 48

7.4.2 Revisión del Servidor DNS y Servidor DHCP IPv4 48

7.4.3 Preparación de los dispositivos de conexión a internet. 49

7.4.4 Preparación del servidor de direccionamiento DHCP IPv6. 50

7.4.5 Preparación de equipos de conectividad de red (actividad que realiza el operador contratado). 51

7.4.6 Preparación de servidores. 53

7.4.7 Preparación de equipos de usuarios final y otros tipos de host. 53

7.4.8 Preparación de los Sistemas de Información y Bases de Datos 54

7.5 RECOMENDACIONES GENERALES 56

7.6 LINEAMIENTOS DE IPv6 EN CONCORDANCIA CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 56

7.6.1 Herramientas sugeridas para la gestión de IPv6 60

7.6.1.1 Herramientas Open source 60

7.6.1.2 Herramientas Comerciales 60

7.6.2 Protocolo para diagnóstico e implementación de IPv6 en activos de TI desconocidos o descubiertos después del Diagnóstico 61

8. RECOMENDACIONES DE ADQUISICIÓN 64

9. TERMINOLOGÍA 65

REFERENCIAS 72

ANEXOS 73

Tabla de Figuras

Figura 1 Topología de Red - CAS 18

Figura 2 Clasificación de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por categoría 22

Figura 3 Cantidad de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por Tipo 23

Figura 4 Cantidad de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por impacto frente a IPv6 26

Figura 5 Compatibilidad general de los activos de TI con IPv6 31

Figura 6 Compatibilidad de IPv6 por Categoría 32

Figura 7 Estrategia de Implementación por Capas 47

Listado de Tablas

Tabla 1 Compatibilidad de Activos de TI con IPv6 20

Tabla 2 Determinación de la Compatibilidad 27

Tabla 3 Niveles de compatibilidad IPv6 29

Tabla 4 Compatibilidad Servidores HP 33

Tabla 5 Compatibilidad Servidores HP 34

Tabla 6 Equipos de cómputo totalmente compatibles 36

Tabla 7 Equipos Portátiles totalmente compatibles 36

Tabla 8.Impresoras CAS 37

Tabla 9 Sistemas Operativos compatibles con IPv6 38

Tabla 10 Inventario de aplicaciones 40

Tabla 11 Excepciones lenguajes de programación 45

Tabla 12 Lista de RFC sobre IPv6 59

Plan de Diagnóstico del Protocolo IPv6

1. JUSTIFICACION

A través de los años INTERNET ha estado en constante evolución en muchos aspectos como lo son el aumento de usuarios, aumento de recursos, el uso de servicios multimediales y lo que esto conlleva en cuanto a la determinación del consumo de ancho de banda, convirtiéndose de esta manera en una red que involucra una alta interactividad entre los usuarios que la acceden. Esto también trae consecuencias que como factores inciden en la actual estructura de red de las Entidades y que deben estar preparadas para incorporar nuevas tecnologías que involucren la modernización y a su vez permitan el desarrollo de las comunidades.

Atendiendo la situación de conectividad en materia de protocolo de internet, el Gobierno Nacional ha iniciado un proceso de innovación tecnológica, en el que las entidades del país deben adoptar el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Circular 002 del 6 de Julio de 2011 del Ministerio de Tecnologías de información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia bajo la Resolución 2710 de 2017 y la Resolución 1126 de 2021

La implementación del estándar de direcciones del Protocolo de Internet Versión seis (IPv6) permitirá que internet evolucione de cara al alto crecimiento de usuarios, así como al aumento en el número de dispositivos conectados y a la creciente demanda de servicios conectados al internet a nivel mundial; es por ello que el IPv6 es indispensable para el desarrollo de la sociedad de la información y del conocimiento. La implementación del protocolo IPv6 evitaría un atraso tecnológico en Colombia y además generaría un crecimiento en infraestructura, en el número de usuarios conectados y en

el incremento de oportunidades de negocios desde el uso del internet, entre otros; lo que permitiría a mediano plazo potenciar así el desarrollo del país de una forma constructiva e incluyente.

Cuando se habla de la nueva era con un mundo globalizado en donde cada vez es mayor el uso de aplicaciones que operan a través de la red INTERNET, nadie se pregunta cómo funciona esta red de redes simplemente se le exige como consumidores, y cada vez con mayor rigor y nivel de esta, teniendo en cuenta que los mecanismos en esta red implantados funcionen adecuadamente en todo momento. Si se considera, además que la introducción de aspectos clave como la movilidad, que es una de las funcionalidades que la informática y las telecomunicaciones han traído recientemente y le dan soporte a un gran porcentaje de la sociedad.

Lo anterior ha conllevado a que las Entidades Públicas actuales con redes IPv4 existentes, se vean en la tarea de proceder a la migración del protocolo de internet versión 4 a la versión 6, lo que implica tener que enfrentar el reto de identificar los factores que esto traiga como consecuencia y también contemplar el impacto al cambio. Por ello se determina una planificación para llevar a cabo la transición y poner en práctica las directivas protocolares de IPv6.

Este plan de Adopción del protocolo IPv6 contiene un plan técnico para que la Corporación Autónoma Regional de Santander - CAS lleve a cabo la migración y reduzca, así mismo, el mayor número de impactos negativos posibles. El plan de trabajo técnico identifica recursos humanos y financieros, así como las actividades necesarias para el logro de la migración y de la respectiva adopción.

Se puede afirmar que, actualmente, los dispositivos de red y equipos de cómputo de la Corporación Autónoma Regional de Santander - CAS están conectados a internet utilizando el protocolo IPv4 y que es casi imposible realizar el cambio de tecnología de manera inmediata; es por esto que se debe llevar una fase de transición en la que, se adopte al IPv6 a la infraestructura acorde a los lineamientos planteados por MINTIC.

2. MARCO NORMATIVO

Para los efectos del presente documento, se referencia la siguiente reglamentación:

Resolución 1126 (14 de mayo de 2021): Mediante la cual se modifica la resolución 2710:

- El plazo de adopción de las entidades estatales
- Modificación de los documentos "Guía de transición de IPv4 a IPv6 para Colombia" y "Guía para el aseguramiento del Protocolo IPv6", en el sentido de incorporar términos técnicos asociados a las nuevas tendencias y avances tecnológicos (Internet de las Cosas - IoT, Ciudades Inteligentes, Blockchain, etc.).

Resolución 2710 (3 de octubre de 2017): Mediante la cual se formulan y establecen:

- Las medidas para la adopción del Protocolo Internet Versión 6 (IPv6) en las entidades estatales de carácter nacional y las entidades territoriales.
- Las medidas para los Proveedores de Redes y Servicios de Telecomunicaciones con el fin de que habiliten tráfico y ofrezcan conectividad y servicios en IPv6 a las entidades a las que hace referencia la presente resolución.

Decreto 1078 de 2015: En cuyo artículo 2.2.9.1.2.2 define como instrumento el Manual de Gobierno en Línea, en donde se incluye el Modelo de Seguridad y Privacidad de la Información (MSPI). Se definen los lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

Circular 002 (6 de julio de 2011): En la cual se convoca a las entidades de la Administración Publica, Ramas y Organismos del Estado y al sector TIC para que en la compra y adquisición de sus infraestructuras (Hardware, Software, Almacenamiento, etc.), se exija obligatoriamente su compatibilidad con IPv6. Además, se invita a las entidades a diseñar y adoptar un plan de transición para la adopción de IPv6 en coexistencia con IPv4. Con la intención de lograr una transición a IPv6 segura y sin inconvenientes en las entidades.

Ley 1341 de 2009: Marco general del sector de Tecnologías de la Información y las comunicaciones.

Se considerarán como guía permanente entre otros los siguientes RFC (Request For Comments) emitidos por el IETF (Internet Engineering Task Force)[1]:

- **RFC1981 -** Descubrimiento del MTU de la ruta para IPv6
- **RFC2460** – Especificaciones básicas IPv6
- **RFC3315** – DHCPv6 client
- **RFC3484** – Selección direcciones por defecto
- **RFC3596** – Extensiones de protocolo para incorporar registros de recurso DNS IPv6
- **RFC4241** – Modelo de IPv4/IPv6 en Doble Pila para Adopción de los servicios de Internet
- **RFC4291** – Arquitectura de direccionamiento IPv6
- **RFC4862 -** IPv6 Stateless Address Autoconfiguration
- **RFC4941:** direcciones temporales
- **RFC6052 -** IPv6 Addressing of IPv4 IPv6 Translators
- **RFC6177** Asignación de direcciones IPv6 a sitios finales
- **RFC7719 -** DNS Terminology
- **RFC8305 -** Happy Eyeballs Version 2∫ Better Connectivity Using Concurrency
- **RFC8415 -** Dynamic Host Configuration Protocol for IPv6 ®DHCPv6

[1] http://ipv6now.com.au/RFC.php

3. PLANTEAMIENTO DEL PROBLEMA

La evolución tecnológica y el desarrollo de nuevos dispositivos inteligentes hacen que crezcan también los problemas relacionados con la estabilidad,compatibilidad, seguridad, conectividad y acceso a direcciones IP. Debido, entre otras razones, al creciente número de usuarios y de equipos que buscan conectarse al internet. Actualmente y desde 1981, los usuarios y equipos se pueden conectar al internet desde el Protocolo de Internet Versión 4 o IPv4. Sin embargo, la creciente demanda y la estructura con el que fue concebido el protocolo IPv4 ha requerido la utilización de la totalidad de direcciones disponibles y la cual fue agotado el pasado 19 de Agosto de 2020[2], lo que hace obligatorio realizar una migración al nuevo protocolo, es decir, al Protocolo de Internet Versión 6 (IPv6).

Migrar al protocolo IPv6 para que haya interoperabilidad y en un futuro un completo perfil de trabajo en un solo protocolo IP, requiere de unos cambios de infraestructura y demás procesos de actualización que involucran pruebas de integración y coexistencia entre el antiguo protocolo IPv4 y el nuevo IPv6 en la Corporación Autónoma Regional de Santander - CAS.

La migración de IPv4 a IPv6, según lo establece el MINTIC, se debe hacer de forma planeada y escalonada, con el fin de mitigar cualquier interoperabilidad entreaplicaciones que se pueda presentar durante el proceso. Ya que se tienen que utilizar ambos protocolos al mismo tiempo: IPv4 e IPv6 a través del intercambio de paquetes entre los mismos protocolos.

Se ha utilizado una asignación de direcciones mediante CIDR, así como la Traducción de direcciones de Red (NAT) que han intentado resolver este problema sin obtener mucho éxito, ya que en primera instancia no todos los enrutadores de la Corporación Autónoma Regional de Santander - CAS soportan CIDR, sin contar que existen aplicaciones que

[2] https://www.lacnic.net/4847/1/lacnic/agotamiento-de-ipv4:-lacnic-asigno-el-ultimo-bloque

requieren direcciones estáticas, por lo que NAT colabora en gran medida con estos casos. Otro aspecto para destacar es la seguridad misma que ha tomado un papel muy importante en el manejo de la información académica y financiera que es enviada a través de los medios electrónicos. IPv4 no fue diseñado para sea un protocolo seguro y muchas de las aplicaciones creadas para solucionar este problema de seguridad solo protegen la información en las capas de comunicación más altas (Aplicación y Transporte) haciendo vulnerable la información a ataques en la capa de Red. IPv6 por su parte se presenta como una solución viable a los problemas de la red se sistemas de la anteriormente mencionados, porque incluye entre otras mejoras, direcciones de 128 bits, en lugar de las direcciones de 32 bits de IPv4, incluyendo la seguridad sobre la capa de Red.

4. ALCANCE

Este documento es un diagnóstico y tiene como nombre "Plan de Diagnóstico IPv6" En cumplimiento de los requisitos del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) según el marco normativo.

Dentro del presente documento se desarrolla el diagnóstico del estado actual de la infraestructura Tecnológica de la Corporación Autónoma Regional de Santander - CAS para preparar el proceso de adopción del nuevo protocolo IPv6. Lo anterior siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) descritos en la "Guía de Transición de IPv4 a IPv6 para Colombia", numeral 7.1 "Fase I. Planeación de IPv6".

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Analizar, diseñar e implementar las actividades a realizar para la adopción del protocolo IPv6 en la Corporación Autónoma Regional de Santander - CAS en modo dual stack, para la operabilidad en la infraestructura y los servicios de la red, utilizando los dos protocolos, IPv4 e IPv6.

5.2 OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura donde se alojan los servicios informáticos conectados a Internet (equipos, aplicaciones y servicios informáticos) con el fin de diagnosticar su compatibilidad con IPv6.
- Elaborar y validar el inventario de activos de TI de información que permita mitigar problemáticas o desventajas posibles en la adopción de IPv6.
- Identificar y dar a conocer estrategias que se basen en lineamientos, buenas prácticas y recomendaciones para la adopción IPv6 establecidos por el MINTIC.
- Establecer un plan de trabajo que permita Implementar el protocolo para la interoperabilidad entre IPv4-IPv6 en Dual Stack, permitiendo operar la red LAN-WAN de la Corporación Autónoma Regional de Santander - CAS.
- Proporcionar las recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, en caso de que aplique.
- Documentar el plan de manejo de excepciones.
- Documentar los lineamientos de Implementación de IPv6 con concordancia con la política de seguridad de la información y los controles de seguridad informática de la entidad.
- Definir las directrices del plan de direccionamiento de IPv6 en la red de la Entidad.

6. ANÁLISIS DE LA INFRAESTRUCTURA

6.1 ARQUITECTURA DE RED DE COMUNICACIONES

La Arquitectura es el conjunto de elementos físicos de red de comunicaciones, su integración e interacción entre ellos, así como con los servicios de la entidad. Lo anterior teniendo en cuenta que el contexto del presente documento hace referencia únicamente a lo relacionado con la Transición a IPv6, donde la arquitectura de red de comunicaciones juega un papel fundamental para llevarla a cabo.

La topología de red de la Corporación Autónoma Regional de Santander - CAS está definida de la siguiente manera, inicialmente cuenta con tres (1) canal de comunicación para su conexión a internet suministrado por el proveedor de servicios de internet (ISP) CLARO y una red SDWAN que interconecta a las cinco (5) sedes de la entidad, cada uno estos enlaces están siendo conectados paulatinamente en un Firewall (Fortigate), que permite la utilización de unos servicios internos de la entidad e igualmente brindar seguridad informática a la red de datos, del equipo Firewall se tiene una conexión a un RouterSwitch que básicamente cumple la función de interconexión de los equipos y servicios de la Red LAN.

La entidad cuenta con varios segmentos de red, uno para que sede interconectada, en el cual están todos los equipos que utilizan los usuarios finales como impresoras, cámaras IP y equipos de cómputo, igualmente dentro de este segmento se utilizan varios Switches para la conexión de dichos equipos, este equipo se conecta directamente al equipo de borde Firewall, el cual se encarga de realizar el enrutamiento de paquetes según corresponda.

Para la comunicación a la red de internet de los equipos de la CAS, Se utiliza un equipo como el Firewall, el cual permite conexiones más seguras y mejor gestionadas; el equipo utiliza el pool de direcciones públicas que entrega el proveedor.

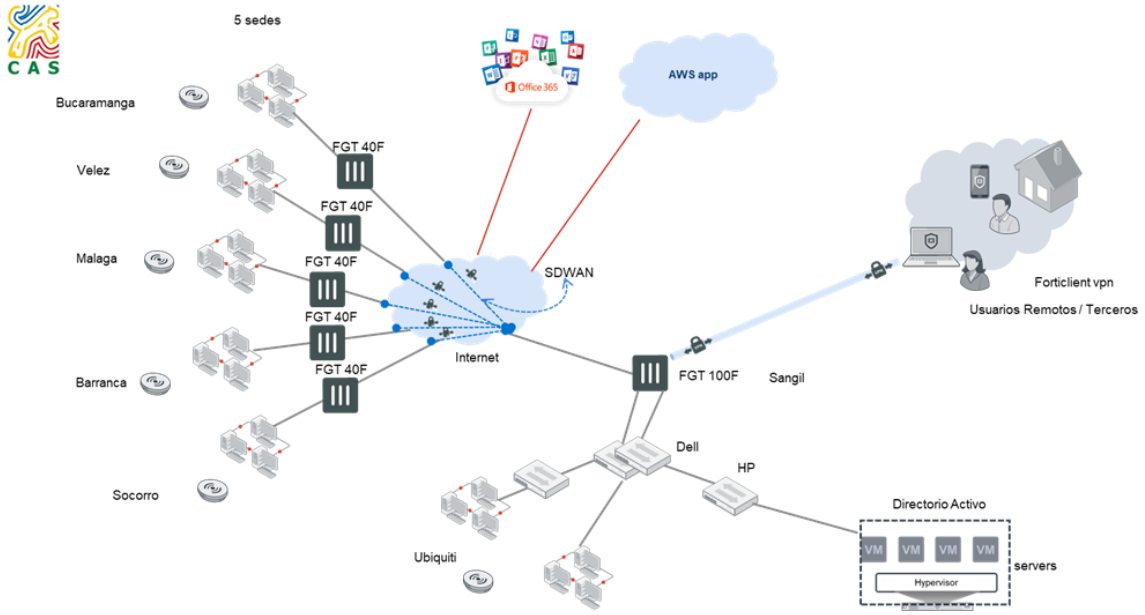


Figura 1 Topología de Red - CAS

6.2 INVENTARIO DE ACTIVOS DE TI DE TECNOLOGÍA

De acuerdo con la metodología utilizada para el diagnóstico de adopción del protocolo IPv6 en la Corporación Autónoma Regional de Santander - CAS, se realizó el levantamiento de información del inventario de activos de TI, donde se identificaron los siguientes tipos:

- **Equipos de Infraestructura (Servidores físicos, virtuales y almacenamiento):** Corresponden a los equipos servidores físicos, virtuales o de almacenamiento que proveen diferentes servicios a la Entidad, como por ejemplo los servicios de backup, almacenamiento, bases de datos o aplicaciones. En la actualidad, la entidad cuenta con un servidor físico que proveer los servicios dentro de la red.
- **Equipos de Energía:** Corresponden a todos los equipos que apoyan servicios en energía. Por ejemplo, el inventario relaciona las UPS (Uninterruptible Power Supply).

- **Equipos de Seguridad Física:** Corresponden a los equipos que son utilizados para el control de acceso físico como por ejemplo cámaras de video, NVRs, DVRs, o dispositivos biométricos con los que cuente la entidad.
- **Equipos de Seguridad Informática:** Estos equipos son aquellos que cumplen funciones de seguridad informática. Por ejemplo, firewalls, IPS, IDS, controladores de tráfico, y endpoint, entre otros. Lo anterior teniendo en cuenta solo los que son propiedad de la Corporación Autónoma Regional de Santander - CAS.
- **Equipos de usuario final:** Corresponden a todos los equipos que solicitan servicios en la red. Se relacionan equipos de cómputo, portátiles e impresoras de la entidad. Lo anterior basado en las marcas con las que cuenta la entidad.
- **Sistemas operativos:** La información de sistemas operativos se documentó en una hoja por separado dentro del inventario de activos de TI. Esta contiene la lista de sistemas operativos que tiene la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS actualmente y su respectiva evaluación de compatibilidad. Sin embargo, se aclara que los sistemas operativos son compatibles desde más de 10 años atrás. Los sistemas operativos que tiene la corporación AUTÓNOMA REGIONAL DE SANTANDER - CAS actualmente son totalmente compatibles con IPv6, después de realizada la validación.

Notas aclaratorias:

- Los activos de TI identificados se encuentran relacionados en el archivo F1-5 INVENTARIO TI – CAS - v1.xls
- El inventario de activos de TI contempla únicamente aquellos que son propiedad de la CAS. Esto fue acordado con la entidad dado que todos los equipos aprovisionados por el prestador de servicios, deberán ser compatibles con el protocolo IPv6. Por lo tanto, los equipos de comunicaciones y demás que son proporcionados por el operador, no hacen parte del diagnóstico.
- Para efectos de la incorporación eficiente de IPv6 se recomienda a la entidad que los equipos de usuario final obsoletos existentes sean reemplazados por aquellos que sean adquiridos.

6.2.1 Análisis del documento de inventario de activos de TI.

El documento de inventario de activos de TI, el cual se encuentra anexo al presente documento cuenta con la siguiente información en sus campos (Columnas), de acuerdo al tipo de activo el cual se encuentra separado por hojas dentro del mismo libro de Excel, así mismo se especifica si el campo es necesario para poder diagnosticar la infraestructura frente a la compatibilidad con IPv6:

Tabla 1 Compatibilidad de Activos de TI con IPv6

NÚMERO DE CAMPO	NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO	¿NECESARIO PARA EL DIAGNÓSTICO DE IPV6?
Equipo de Computo			
1	Equipo	Descripción del tipo de equipo de cómputo ejemplo, Computador, Servidor, SAN, Tableta, entre otros.	Si
2	Fabricante	Nombre del fabricante del equipo	No
3	Memoria	Descripción de la memoria RAM.	No
4	Procesador	Característica del procesador (Intel, AMD, de 32 /64 bits, etc).	No
5	Discos	Cantidad de discos y capacidad	No
6	Sistema Operativo	Descripción del sistema operativo que soporta el equipo de cómputo. (Windows, MacOS, Linux, etc)	Si
7	Versión	Versión del sistema operativo instalado	Si
8	Software Instalado		No
9	Rol / Dependencia	El papel que desempeña el equipo en la red de la Entidad. O Dependencia a la que está asignado	No
10	Versión IP	Versión IPv4 / IPv6.	Si
Impresoras			
1	Descripción	Breve descripción del tipo de impresora Ej: HP Photo Scaner	No
2	Marca	Nombre del fabricante de la impresora	Si
3	Modelo	Referencia y/o modelo de la impresora	Si
4	Puerto de Red	Especificar de la impresora cuenta con puerto de red	Si

NÚMERO DE CAMPO	NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO	¿NECESARIO PARA EL DIAGNÓSTICO DE IPV6?
5	Dependencia	Lugar y/o nombre de la dependencia a la que pertenece la impresora	No
6	Dirección IP	Dirección actual de la impresora	No
7	Versión IP	Versión IPv4 / IPv6.	Si
Equipos de Comunicación			
1	Equipo	Descripción del tipo de equipo de comunicaciones, ejemplo, switch, enrutador, firewall, modem, AP, DTE, NAC, etc.	Si
2	Marca	Describir la marca, ejemplo Fortinet, Cisco, Avaya, HP, Huawei, 3M, 3COM, etc.	Si
3	Modelo	Referenciar el modelo del equipo de comunicaciones.	Si
4	Sistema Operativo	Descripción del sistema operativo que soporta el equipo de comunicaciones.	No
5	Puertos Ethernet	Describir los puertos de Ethernet que soporta, ejemplo E0, S0, FE, FC, PoE, etc.	No
6	Rol	El papel que desempeña el equipo de comunicaciones en la red de cada entidad.	No
7	Versión IP	Versión IPv4 / IPv6	Si
8	Direccionamiento IP	Direccion IPv4/Ipv6.	Si
Equipos Servidores			
1	Tipo de Servidor	Si es un servidor de aplicaciones o de comunicaciones, de Bases de datos.	Si
2	Alojamiento	Describir si se encuentra en sitio, remoto en data center, en la nube, otro	No
3	Tipo Instalación	Físico, Virtual	Si
4	Sistema Operativo	Si es Windows, Linux, Solarix, etc.	Si
5	Versión del Sistema Operativo	Versión del Sistema Operativo y niveles de parcheo.	Si
6	Direccionamiento IP	Direccionamiento IPv4/Ipv6.	Si
7	Funcionalidad	El rol que cumple el servidor dentro de la organización.	No
Aplicaciones			
1	Aplicativo	Nombre del aplicativo	No

NÚMERO DE CAMPO	NOMBRE DEL CAMPO	DESCRIPCIÓN DEL CAMPO	¿NECESARIO PARA EL DIAGNÓSTICO DE IPV6?
2	Característica	Describir si el sistemas de información, programa o plataforma es de la entidad o de un tercero	No
3	Tipo	Indicar el tipo de funcionamiento del aplicativo (cliiente-Servidor, local, Web)	Si
4	Lenguaje de Programación	Lenguaje utilizado para el desarrollo del aplicativo.	Si
5	Responsable	Persona responsable del aplicativo, DBA, etc.	No
6	Componentes	Descripción de las partes que constituyen la aplicación y sus interfaces.	Si
7	Contrato	Descripción del soporte y/o mantenimiento sobre los Aplicativos de la Entidad si existe.	No
8	Soporte IPv6	Descripción si el aplicativo cumple o no con el protocolo IPv6.	Si

A nivel general la clasificación de activos de TI propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS es la siguiente:

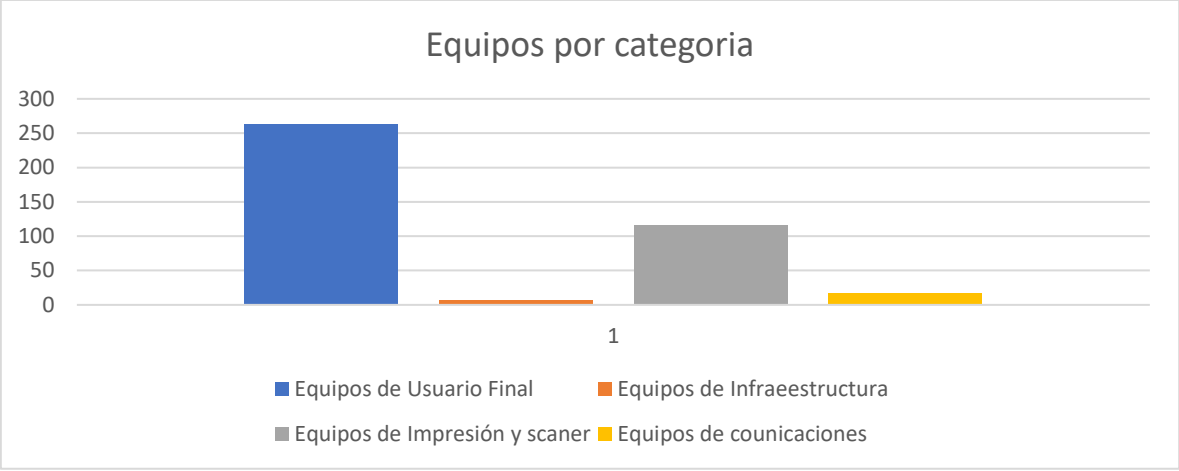


Figura 2 Clasificación de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por categoría

Fuente: Elaboración propia

La mayor cantidad de los equipos se concentra en los equipos de usuario final y de comunicaciones, que soportan la operación de la entidad. Con base en esta información se presenta a continuación la distribución de los activos de TI por tipo con el fin de identificar su segmentación.

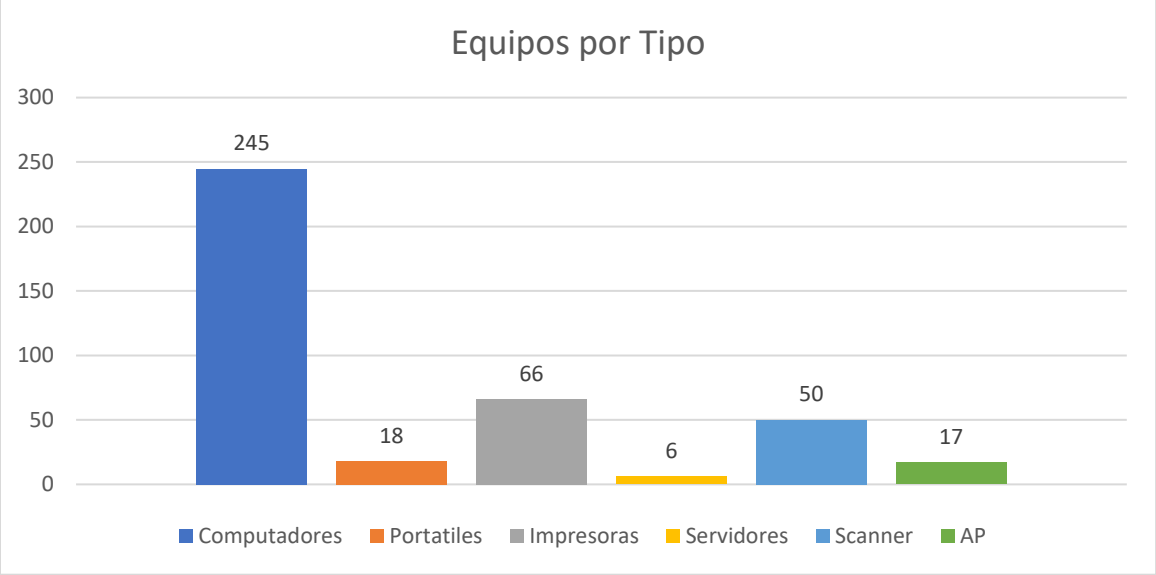


Figura 3 Cantidad de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por Tipo

Fuente: Elaboración propia

Como parte de la información recopilada por parte de la CAS, existe un inventario de equipos de usuario final que consigna la información de diferentes marcas y fabricantes, o en algunos casos, sin información. Esta información se agrega en el presente diagnóstico de forma general dado que se desea tener conocimiento sobre la compatibilidad de los equipos de usuario final que podrían o no reemplazarse. Sin embargo, esta información excluye equipos de contratistas, u otros, que serán reemplazados o que en la actualidad no existen en la red o simplemente son equipos que no tienen tarjeta de red y no aplica su compatibilidad. De todas formas, se presenta a continuación la distribución de estos equipos por cada uno de sus tipos.

La compatibilidad de estos equipos soporta el protocolo IPv6, dado que los equipos de usuario final que tiene la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS tienen sistemas operativos Windows recientes y por consiguiente se asume que permiten configurar IPv6.

Nota: Se agrega dentro del F1-5 INVENTARIO TI - CAS - v1 una pestaña con la información completa de equipos de usuario final actuales.

6.2.2 Análisis del inventario de los Sistemas de información.

A la fecha de creación del presente diagnóstico se han tomado las siguientes decisiones con respecto al inventario de Sistemas de Información:

- Se cuenta hasta el momento con 2 aplicaciones que hacen parte de los Sistema de Información misionales definidos e identificados por la CAS, los cuales serán sujetos al diagnóstico para la transición de IPv6, de igual manera se cuenta con (6) aplicativos identificados, propios de terceros con los que se cruza información de consulta o envío información como cumplimiento de las funciones propias de las diferentes áreas de la entidad.
- La CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS cuenta con un número importante de aplicaciones que son de uso, pero no tiene control sobre ellas. Por lo tanto, para efectos de la transición a IPv6, estas se manejarán como una bolsa de aplicaciones, que se mantendrán en IPv4 y se analizarán paulatinamente durante la etapa de Implementación.
- Para el diagnóstico no se tienen en cuenta aplicaciones de ofimática, de configuración de dispositivos, de edición de imágenes o similares, dado que estas son aplicaciones instaladas directamente en los equipos clientes, cuya compatibilidad es validada a través del sistema operativo y por lo tanto no son afectadas por el proceso de adopción IPv6.

NOTA: se recomienda siempre descargar las últimas versiones de las aplicaciones clientes, dado que cualquier aplicación previamente compilada que sea de más de 10 años atrás, podría no soportar IPv6.

Las aplicaciones identificadas, así como la lista de sistemas operativos se encuentran relacionadas en el Inventario de Sistemas de Información de IPv6, el cual es el documento *F1-5 INVENTARIO TI - CAS - v1.xls* al presente plan.

6.3 PLAN DE DIAGNOSTICO

Valoración del Impacto en los Activos de TI

Para establecer el valor del impacto en los activos de TI de información y los servicios con respecto a la afectación que podría tener como resultado de la implementación de IPv6, se utilizan los siguientes valores. Esta valoración indica el nivel de impacto que podría sufrir el activo de TI cuando se presente una afectación por causa de la implementación del protocolo IPv6.

Nota: Esta valoración no es una característica requerida, ni establecida por el MinTIC. Sin embargo, se utilizará como guía para los controles de cambio durante la implementación. Por lo tanto, durante la etapa de diagnóstico tendrá un valor inicial dado por la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS y posteriormente durante la etapa de implementación se actualizará respectivamente con cada control de cambio que vaya a realizarse. Por otro lado, la valoración de impacto se utilizará en el presente documento en el capítulo de Informe de Cumplimiento con el fin de poder especificar el nivel de impacto que tiene cada uno de los hallazgos identificados.

- **Impacto Alto** (Valoración 5): Afectación total de los servicios misionales de la entidad. Afectación del consumo de los servicios por los usuarios.
- **Impacto Medio**: (Valoración 3): Afectación parcial y moderada de los servicios de apoyo, No misionales, los cuales podrían generar quejas por parte de los ciudadanos.
- **Impacto Bajo**: (Valoración 1). Si el activo tiene alguna afectación, entonces la entidad puede seguir operando sin causar daño a las operaciones, servicios misionales o de apoyo.

La información anterior fue concertada con los funcionarios del área de tecnología de la Entidad, por cada uno de los activos de TI y servicios relacionados en el Inventario de activos de TI.

La distribución del impacto de los activos de TI es la siguiente:

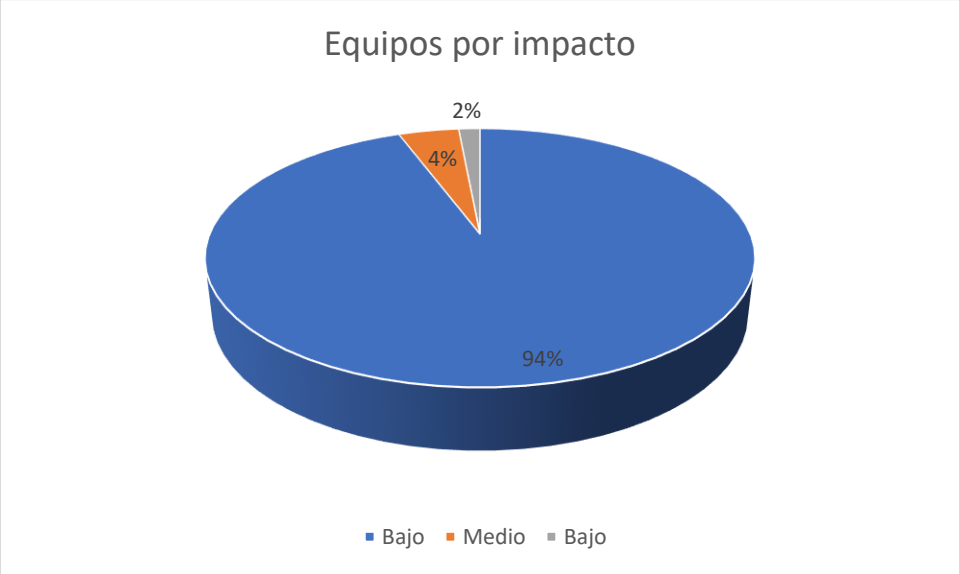


Figura 4 Cantidad de equipos propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS por impacto frente a IPv6

Fuente: Elaboración propia

Se puede identificar que existen 7 equipos que tienen criticidad Alta. Estos equipos corresponden al Equipo de Seguridad Informática (1) y Equipo Servidor (6). Sin embargo, los equipos clasificados con nivel "Medio" corresponden a equipos de comuniacaciones, los cuales, aunque están marcados con este nivel, tienen una importancia significativa frente a la implementación de IPv6 si son soporte de aplicaciones misionales. Por lo tanto, durante la etapa de implementación se tendrán en cuenta para reclasificar su criticidad según lo identificado en los controles de cambio o la naturaleza de las actividades de implementación.

Nota: Para la fase de implementación se tendrá en cuenta la "Guía de aseguramiento del protocolo IPv6", la cual indica los lineamientos técnicos de seguridad que deben aplicarse con cada cambio. Por lo tanto, la criticidad de los activos de TI estará articulada con el MSPI (Modelo de Seguridad y Privacidad de la Información) en su componente de seguridad, valorada en cuanto a confidencialidad, integridad y disponibilidad.

Informe de Cumplimiento de los activos de TI con IPv6

6.3.1 Determinación de la Compatibilidad (Niveles mínimos de compatibilidad de IPv6 para los activos de TI).

La compatibilidad de los activos de TI se define de acuerdo con los requisitos mínimos de IPv6 frente al tipo de activo y su funcionalidad. Esto dado que un equipo servidor que tiene direcciones IP estáticas y no requiere realizar ninguna acción adicional a recibir y enviar tráfico IPv6, podría tener la configuración básica de IPv6, y funcionar adecuadamente. Sin embargo, un enrutador, el cual, si requiere recibir y reenviar paquetes, descubrir equipos y manejar otro tipo de funcionalidades, requeriría implementar un RFC[3] como el de routing IPv6, SLAAC, u otros acordes con su función.

De acuerdo con lo anterior, se presenta la siguiente tabla, la cual incluye por tipo de activo el requerimiento mínimo de RFC que debería cumplir.

Tabla 2 Determinación de la Compatibilidad

TIPO DE DISPOSITIVO (VER ANEXO 2. INVENTARIO DE ACTIVOS DE TI IPV6)	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
Computadores de Escritorio y Portátiles Servidor de Almacenamiento Servidor Físico Servidor Virtual Impresoras	RFC de Nodo/Host: - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery - [RFC4443] ICMPv6 - [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection. Quoting from Section 5.4. - [RFC3484] Default Address Selection for IPv6.	Nodo/Host IPv6: Activo que implementa IPv6 y que no es un enrutador.	Marca y Modelo Revisión de fichas técnicas, manual de configuración o antigüedad de la Marca y Modelo de los activos de TI.

[3] Request for change. Nombre dado por el IETF para documentación técnica del protocolo IPv6.

TIPO DE DISPOSITIVO (VER ANEXO 2. INVENTARIO DE ACTIVOS DE TI IPV6)	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
	- [RFC3315] DHCPv6 - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS. - [RFC4213] Dual Stack		
DVR (Digital Video Recorder) NVR (Network Video Recorder) Cámara de Video UPS (Uninterruptible Power Suppy)	RFC de Nodo/Host exceptuando aquellos relacionados con adquisición de dirección IP automática. - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery - [RFC4443] ICMPv6 - [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection. Quoting from Section 5.4. - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS	Nodo/Host IPv6: Activo que implementa IPv6 y que no es un enrutador.	Marca y Modelo Revisión de fichas técnicas, manual de configuración o antigüedad de la Marca y Modelo de los activos de TI.
Appliances: Consola de administración centralizada de seguridad Descifrador de Tráfico Monitoreo de Tráfico Protección Endpoint	Debe soportar los RFC de Nodo/Host (Mencionados anteriormente) y los siguientes: - [RFC4301] Security Architecture for the Internet Protocol" - [RFC4303] ESP -[RFC4302] AH	Nodo/Host IPv6: Activo que implementa IPv6 y que no es un enrutador.	Marca y Modelo Revisión de fichas técnicas, manual de configuración o antigüedad de la Marca y Modelo de los activos de TI.
OTROS TIPOS DE ACTIVOS DE TI QUE APLICAN A LA CAS			
Sistemas operativos	Todos los RFC de Nodo/Host	Sistema Operativo que se comporta como Nodo/Host IPv6	Validación del sistema operativo según su antigüedad. Por ejemplo, versiones de Microsoft Windows desde Windows XP tiene la funcionalidad de IPv6
APIs	- [RFC3493] Basic Socket Interface Extensions for IPv6" - [RFC5014] "IPv6 Socket API for Source Address Selection"	Nodo/Host IPv6: Activo que implementa IPv6 y que no es un enrutador.	Validación de Sistema Operativo, Manejo de direcciones IP, Métodos de Interacción con otros sistemas, versión del motor de base de datos, versión del servidor web,

TIPO DE DISPOSITIVO (VER ANEXO 2. INVENTARIO DE ACTIVOS DE TI IPV6)	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
			adquisición de certificados digitales y lenguaje de desarrollo.

Finalmente se define la siguiente tabla con los niveles con los que se valoró la compatibilidad de los activos de TI que tiene actualmente la CAS:

Tabla 3 Niveles de compatibilidad IPv6

NIVEL		REQUISITOS MÍNIMOS	FUNCIÓN DEL EQUIPO
0	Sin compatibilidad: El equipo o aplicación no cuenta con funciones de IPv6.	No existen requisitos mínimos, el equipo o aplicación solo soporta IPv4.	Equipo o aplicación que desempeñe cualquier actividad o tarea.
1	Compatibilidad Elemental: El equipo permite que le sea configurada una dirección IPv6 de forma manual, pero no soporta Autoconfiguración ni DHCP. En algunos casos especiales no soporta Dual Stack.	RFC de Host - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmission rules. - [RFC4443] ICMPv6 - [RFC4213] Dual Stack	Nodo/Host IPv6: DVR (Digital Video Recorder) NVR (Network Video Recorder) Cámara de Video UPS (Uninterruptible Power Suppy)
2	Compatibilidad Estándar: El equipo soporta las características de IPv6 de autoconfiguración, DHCP, Dual Stack, mínimas para operar en un ambiente dual stack con asignación dinámica y estática.	RFC de Nodo - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery - [RFC4443] ICMPv6 - [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection. Quoting from Section 5.4. - [RFC3484] Default Address Selection for IPv6. - [RFC3315] DHCPv6 - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS.	Activo que implementa IPv6 y que no es un enrutador. Computadores de Escritorio y Portátiles Servidor de Almacenamiento Servidor Físico Servidor Virtual Impresoras

NIVEL		REQUISITOS MÍNIMOS	FUNCIÓN DEL EQUIPO
		- [RFC4213] Dual Stack	
3	Compatibilidad avanzada: El equipo soporta las configuraciones estándar y agrega otras funcionalidades (dependiendo del tipo de equipo) como seguridad, enrutamiento, multihoming y movilidad.	Soporte de los RFC de Compatibilidad estándar (Mencionados anteriormente) y los siguientes: - [RFC4301] Security Architecture for the Internet Protocol" - [RFC4303] ESP -[RFC4302] AH - [RFC 7157] - IPv6 Multihoming without Network Address Translation NAT64. - [RFC 3775] - Mobility Support in IPv6	Appliances: Consola de administración centralizada de seguridad Descifrador de Tráfico Monitoreo de Tráfico Protección Endpoint Routers Switches Balanceadores de carga Seguridad perimetral

Nota aclaratoria respecto a la determinación de la compatibilidad: Es importante tener en cuenta que el protocolo IPv6 ha sido implementado durante los últimos 20 años en todo el mundo. En Colombia, solo hasta hace unos 12 años, se ha venido adoptando por las entidades del Gobierno. Esto significa que, para los fabricantes de tecnología actuales, el protocolo IPv6 es una característica que ya se encuentra habilitada por defecto desde años atrás y que por consiguiente no es algo novedoso para incluir en sus fichas técnicas (datasheets). Por lo tanto, dentro de los documentos de referencia de los fabricantes como por ejemplo su ficha técnica (datasheet), o en sus sitios web, no se incluye la información de si el equipo es compatible o no con RFC específicos de IPv6, o en algunos casos si el equipo es compatible con este protocolo. Simplemente los fabricantes especifican en algunos casos el término "IPv6" dentro de su ficha técnica, o en sus manuales de configuración especifican la forma de configurar este protocolo. Por ejemplo, en algunos casos, el hecho de que el manual de configuración del equipo incluya una sección de configuración de IPv6 es indicación suficiente de que el equipo es compatible con el protocolo. Más aún, si el manual indica que es posible configurar IPv4 e IPv6 entonces se asume que el equipo soporta Doble Pila (Dual Stack).

6.3.2 Determinación de la Compatibilidad General de los Activos de TI:

A continuación, se presenta el nivel de cumplimiento de todos los activos de TI. Sin embargo, en los siguientes numerales se presenta en detalle para cada categoría de activos de TI sus respectivos hallazgos.

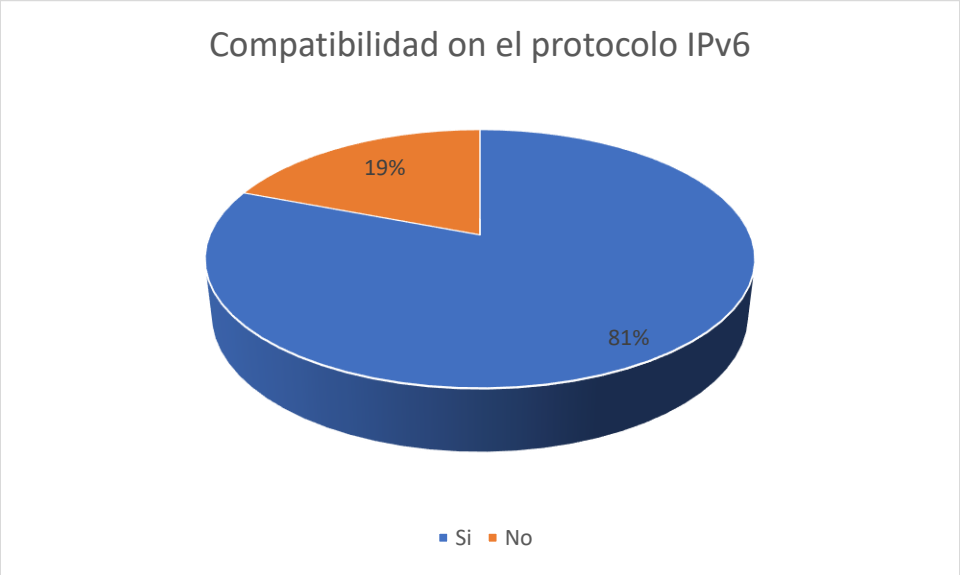


Figura 5 Compatibilidad general de los activos de TI con IPv6

Fuente: Elaboración propia

A continuación, se describe por categoría los activos de TI de acuerdo a su compatibilidad

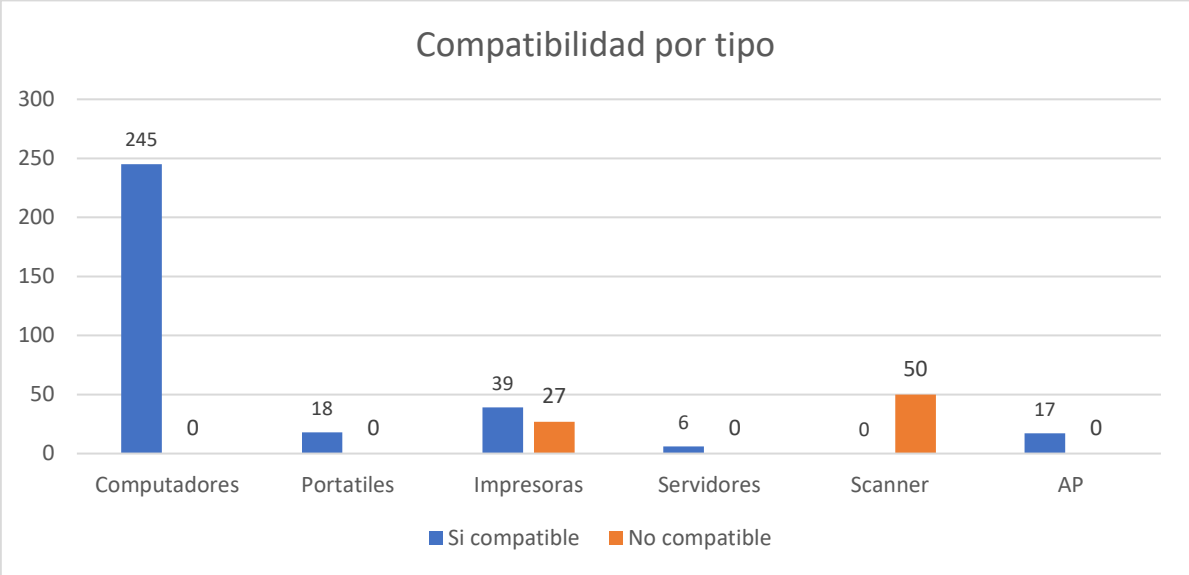


Figura 6 Compatibilidad de IPv6 por Categoría

Fuente: Elaboración propia

De acuerdo con la gráfica anterior, se pueden identificar equipos con nivel **"0. Sin compatibilidad"** todos estos son impresoras sin conexión a red y escanners; Finalmente el resto de equipos compatibles con el protocolo IPv6 que incluyen las siguientes cantidades: 245 equipos de escritorio, 18 portátiles, 39 impresoras, 6 servidores y 17 APs.

6.3.3 Informe de equipos de Infraestructura (Servidores físicos, virtuales, almacenamiento y sistemas de información):

De acuerdo con el levantamiento del inventario de activos de TI de información y después de la verificación de los documentos técnicos de los equipos servidores físicos se realizó el siguiente análisis para la adopción del protocolo IPv6.

Hallazgos

- Se identificó un servidor físico del fabricante HP. Por lo tanto, luego de consultar con la referencia de este tipo de equipos, se determina que el servidor físico de HP es totalmente compatible con el protocolo IPv6. Esto se puede validar en su manual de instalación y datasheet donde se indican sus configuraciones para IPv6. Los servidores requieren que su criterio de compatibilidad esté asociado únicamente con el nivel mínimo: "IPv6 Host".

  Servidores HP

Tabla 4 Compatibilidad Servidores HP

Proliant ML370 G6	https://support.hpe.com/hpesc/public/docDisplay?docId=c01709712&docLocale=en_US#N10013
Proliant DL 580 G5 E7330	https://support.hpe.com/hpesc/public/docDisplay?docId=c01154573&docLocale=en_US#N10011
ProLiant DL360 Gen10	https://buy.hpe.com/lamerica/es/compute/rack-servers/proliant-dl300-servers/proliant-dl360-server/servidor-hpe-proliant-dl360-gen10/p/1010007891

  Impacto: Bajo

  Servidores IBM

IBM System X3250 M3	https://lenovopress.lenovo.com/tips0803
IBM System X3500 M3	https://lenovopress.lenovo.com/tips0809

Impacto: Bajo

Servidores Lenovo

Tabla 5 Compatibilidad Servidores HP

Lenovo ThinkServer RD430	https://download.lenovo.com/pccbbs/thinkservers/rd430userguide_en.pdf

Impacto: Medio

6.3.3.1 Informe de equipos de energía :

De acuerdo con levantamiento del inventario de activos de TI de información referente a los equipos de energía, se realizó el siguiente análisis para la adopción del protocolo IPv6.

Hallazgos

- No se encontró equipos de energía como UPS que sean administrables vía red.

Impacto: Bajo

6.3.3.2 Informe de Equipos de Seguridad Informática:

De acuerdo con el levantamiento del inventario de activos de TI de información de la entidad y después de la verificación de los documentos técnicos de los equipos finales se realizó el siguiente análisis para la adopción del protocolo IPv6.

Hallazgos

- No se encontró equipos de energía como UPS que sean administrables vía red.

Impacto: Bajo

6.3.3.3 Informe de Equipos de Seguridad Física:

De acuerdo con el levantamiento del inventario de activos de TI de información de la entidad y después de la verificación de los documentos técnicos de los equipos finales se realizó el siguiente análisis para la adopción del protocolo IPv6.

Hallazgos

- No se encontró equipos de energía como UPS que sean administrables vía red.

Impacto: Bajo

6.3.3.4 Informe de Equipos de Usuario Final:

De acuerdo con el levantamiento del inventario de activos de TI de información de la entidad y después de la verificación de los documentos técnicos de los equipos finales se realizó el siguiente análisis para la adopción del protocolo IPv6.

Hallazgos

- Se identificaron 34 equipos de escritorio de marcas Hewlett Packard, Lenovo, Dell, HG y Compumax que son propiedad de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS y que son totalmente compatibles con IPv6. Estos equipos son compatibles por su hardware y por su sistema operativo Microsoft Windows 7 y 10.

Tabla 6 Equipos de cómputo totalmente compatibles

Marca	Cantidad
APPLE	1
DELL	29
HP	164
LENOVO	17
QBEX	26
Sin Marca	8

-

Tabla 7 Equipos Portátiles totalmente compatibles

Marca	Cantidad
HP	7
LENOVO	6
SAMSUNG	1
SONY	1
TOSHIBA	2
NA	1

- Se identificaron 63 impresoras de marca Epson, HP y Kyocera, de las cuales 27 de ellas no son compatibles ya que su conexión se hace a través de USB a un equipo de cómputo.
- La mayoría de impresoras compatibles con IPV6 actualmente no están siendo conectadas a red, puesto que gran parte de ellas vienen diseñadas para conexiones

inalámbricas y no se tiene implementado este tipo red de conexión en la CAS.

- Se identificaron 50 escáner de marca HP, actualmente no compatibles por estar asociados a u PC directamente

Tabla 8.Impresoras CAS

EPSON	**11**
L555	5
L575	6
HP	**53**
408DN	10
M130fw	3
M608	10
M806DN	2
P1006	3
P1102W	12
P1606DN	9
P2055dn	4
KIOCERA	**1**
FS-4300DN	1
ZEBRA	**1**
GC420	1

- Para el despliegue de configuraciones de IPv6 en estos equipos se utilizará DHCPv6 el cual ya está habilitado por defecto en el sistema operativo. Para las Impresoras el despliegue será por dirección IP estática, por lo tanto, no requiere funciones de DHCPv6.
- Con respecto a la compatibilidad de estos equipos, los sistemas operativos de los equipos tipo Desktop, Laptop y WorkStation son totalmente compatibles con el protocolo IPv6. Lo anterior dado que la mínima versión de sistema operativo es Windows XP, el cual es compatible. Por lo tanto, estos equipos tienen Compatibilidad 2. Estándar. Las Impresoras y scanner que tienen tarjeta de red son compatibles con el ultimo firmware instalado. Estos dispositivos tienen Compatibilidad 1 Elemental. Finalmente, los dispositivos como monitores, baterías, proyector, fuente, entre otros, son equipos que no tienen aplicación (N/A) con el protocolo IPv6 dado que no cuentan con tarjeta de red y por lo tanto no se evalúa dicha compatibilidad.

6.3.3.5 Informe de Sistemas Operativos:

De acuerdo con el levantamiento del inventario de activos de TI de información de la entidad se identificó que todos los sistemas operativos indicados dentro del Inventario de activos de TI son compatibles. Sin embargo, dado que puede haber usuarios finales dentro de la CAS que trabajen como Contratistas, estos usuarios podrían llegar a usar sus dispositivos (BYOD) móviles o sistemas operativos comerciales como MacOS. Por lo tanto, a continuación, se presenta la lista de sistemas operativos que son soportados para equipos móviles o portátiles que podrían llegar a usar los funcionarios de la entidad, contratistas y visitantes.

Tabla 9 Sistemas Operativos compatibles con IPv6

ID	SISTEMA OPERATIVO	VERSIONES SOPORTADAS CON IPV6
1	Microsoft Windows	Desde Windows XP son soportados. (En Windows XP hay que habilitarlo manualmente, en otras versiones ya viene habilitado por defecto)
		http://www.microsoft.com/ipv6
2	MacOS	Desde la versión 10.2 (Jaguar) soporta IPv6, es decir, soporta versiones: Panther, Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, Mavericks, Yosemite, El Capitán, Sierra, High Sierra, Mojave, Catalina, Big Sur y Monterey.
		http://developer.apple.com/macosx/
3	iPhone iOS	Desde la versión 4.1 soporta IPv6.
4	Android	Desde la versión 2.2 Android soporta IPv6
5	Linux	Todas las distribuciones pueden desarrollar manualmente un driver para IPv6.
		http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html

6.3.3.6 Informe de Servicios (Directorio activo, DHCP y DNS)

Respecto a lo relacionado con:

- Directorio activo
- Direccionamiento DHCP
- Servidor de nombre DNS

El desarrollo de la investigación realizada a la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS se tiene definido lo siguiente:

La infraestructura actual no cuenta con controladores de dominios definidos pertenecientes a la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS.

Por otra parte, a la fecha de presentación del documento no se cuenta con servidores DHCP en IPv4, en lo relacionado con la disponibilidad de las herramientas tratadas en la presente sección del documento.

Dentro de la infraestructura implementada actualmente por la CAS, no existe evidencia de un diseño con alta disponibilidad, como tampoco se encontró la disposición de certificados de seguridad, o en su defecto una entidad certificadora que apoyara lo relacionado con la asignación de dicha tarea de forma que los servidores dispuesto en los ambientes productivos pudieran ser consultados por el protocolo https. Este punto es de importancia para el proceso de implementación de IPv6 para la CAS.

En lo relacionado con la asignación de direcciones DHCP, Directorio Activo y DNS se identificó que dichas tareas no se encuentran aprovisionadas dentro de la CAS. Sin embargo, estos servicios será materia de evaluación y definición con la migración de protocolo IPv4 a IPv6, en caso de implementarse.

6.3.3.7 Informe de Sistemas de Información:

Teniendo en cuenta que, a la fecha de elaboración del presente documento, la corporación AUTÓNOMA REGIONAL DE SANTANDER - CAS ha facilitado un inventario de aplicaciones de

los Sistemas de Información compuesto inicialmente por 2 aplicaciones o Sistemas de Información identificados, la presente sección del documento se dividirá en dos frentes:

- Diagnóstico para las dos (2) aplicaciones de los Sistemas de Información.
- Restantes seis (6) aplicaciones de los Sistemas de Información dispuestos en el inventario por la CAS.

Por otra parte, y con el fin de brindar una mejor lectura del presente documento es importante que el lector tenga presente las siguientes consideraciones:

- La información correspondiente al levantamiento del software se construye teniendo en cuenta las siguientes fuentes de datos:
  - Inventario de Equipos Servidores de la Entidad.xlsx
  - Inventario de Aplicaciones de la Entidad.xlsx
- Las referencias estadísticas se construyen teniendo en cuenta dos items:
  - Item 1: a nivel de servidor (hardware)
  - Item 2: a nivel de Aplicación (Sistema de Información)

Lo anterior, con el fin de brindar una mejor base en la toma de decisiones sobre las diferentes estrategias que deben ser tenidas en cuenta para la implementación y/o migración de las aplicaciones y cuenten con el correcto requerimiento funcional por parte de la CAS.

6.3.3.8 Diagnóstico de aplicaciones

El diagnostico se hace sobre el siguiente inventario de aplicaciones:

Tabla 10 Inventario de aplicaciones

1	EPSs
2	ARLs
3	SIA OBSERVA
4	SIA CONTRALORIAS
5	SIA

6	SIRECI

Generalidades de las aplicaciones de los sistemas de información: El desarrollo de análisis descrito en la presente sección del documento se realiza teniendo en cuenta las siguientes variables de enfoque, con el fin de evaluar de una forma detallada la compatibilidad del inventario de aplicaciones en la implementación de IPv6:

- Sistema operativo y versión de sistema operativo.
- Lenguaje de programación y versión del lenguaje de programación.
- Motor de base de datos y versión del motor de base de datos.
- Servidor de aplicaciones, junto con su versión.
- Cadena de conexión a base de datos.
- Tipo de asignación IPv6.

Esta clasificación construida dentro del análisis busca apoyar al lector en el desarrollo del diagnóstico final para la implementación de IPv6, con el fin de identificar los sistemas o aplicaciones que requieran configuraciones o atenciones especiales en el momento de la implementación.

Hallazgos de aplicaciones: Como resultado del análisis y diagnóstico de la información provista respecto a las aplicaciones, se identificaron los siguientes hallazgos, los cuales sirven como conclusión al ejercicio realizado y detallado dentro del presente documento.

Para todas las aplicaciones, no se identificó públicamente información relacionada con la compatibilidad con IPv6. En lo relacionado a los siguientes ítems:

- Método de asignación IP
- Certificado de seguridad máquina servidor de aplicaciones
- Certificado de seguridad servidor base de datos
- Certificado de seguridad Middleware

Sin embargo, estas aplicaciones al estar publicadas por cada uno de los entes responsables de sus sistemas de información en internet, son compatibles con IPv6 asegurados a través de la configuración Dual Stack.

Tipo de asignación IPv6: Teniendo en cuenta la gran diversidad sistemas de información existentes, desarrollados en distintos lenguajes de programación y motores de base de datos, como también en el software servidores de aplicaciones, de forma que la implementación de protocolo IPv6 no genere traumatismos en su implementación se proponen la asignación de IPv6 según sea el caso:

- Dual Stack
- Tunneling
- Asignación IP

La configuración Doble Pila (Dual Stack) se recomienda para las aplicaciones sobre las cuales no se tuvo mayor cantidad de datos y que aportaron en los valores de incertidumbre en todas las estadísticas.

Por su parte, la configuración Doble Pila, se recomienda para las aplicaciones sobre las cuales existen versiones en lenguajes de programación muy viejos o sin soporte encontrado.

6.3.3.9 Recomendaciones para los sistemas de Información

El resultado del análisis preliminar presenta que el Sistema Operativo es compatible con una configuración IPV6.

En cuanto a los lenguajes de programación, y según las distintas versiones sobre los cuales fueron construidas las aplicaciones, es importante que en las actividades relacionadas con la implementación en ambientes productivos y/o tareas de migración se cuente con la correcta configuración requerida para que dichas aplicaciones no presenten errores en puesta en operación de las mismas.

7. PLAN DE TRANSICIÓN

Aunque se cuenta con el documento de Plan de Transición, a continuación, se presentan diferentes aspectos de Transición que hacen parte del Plan de Diagnóstico.

7.1 MECANISMO DE TRANSICIÓN A UTILIZAR

De acuerdo con las condiciones de la infraestructura, los Sistemas de Información actuales y acorde con los lineamientos definidos por MinTIC, el mecanismo de transición recomendado para la **Corporación Autónoma Regional de Santander - CAS** es **Doble Pila (Dual Stack),** ya que este provee las opciones para la coexistencia IPv4/IPv6 y para la desactivación progresiva del protocolo IPv4.

Se recomienda la lectura de los siguientes enlaces de referencia para la adopción del mecanismo de transición Dual Stack:

- https://www.ietf.org/rfc/rfc4241.txt
- https://www.MINTIC.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

7.2 PLAN DE DIRECCIONAMIENTO IPV6

Con el fin de cubrir todos los aspectos y recomendaciones para la asignación del direccionamiento IPv6 dentro de la CAS, se presenta anexo al presente documento el "F1-4 Plan de Direccionamiento IPv6 CAS v1.xls**",** el cual contiene el análisis realizado sobre la topología física de red de la entidad y la propuesta de direccionamiento a implementar.

7.3 PLAN DE MANEJO DE EXCEPCIONES

De acuerdo con los hallazgos identificados durante el proceso de diagnóstico se hacen las siguientes recomendaciones para el manejo de excepciones.

Nota: Los niveles mínimos de compatibilidad con IPv6 para los activos de TI propios de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS se establecen en el numeral "6.3.1. Determinación de la Compatibilidad (Niveles mínimos de compatibilidad de IPv6 para los activos de TI)"

7.3.1 Para la infraestructura

Recomendaciones:

- Si bien el sistema operativo del servidor soporta IPV6, se recomienda realizar una migración a un sistema más actual, puesto que la versión implementada en el servidor no tiene a disposición más actualizaciones de su sistema, Igualmente se recomienda realizar todas las actualizaciones posibles de los controladores de las tarjetas de red.

7.3.2 Para equipos de Seguridad Física

Excepciones:

- Para el caso de tener cámaras de video IP con conexión a NVR estas deberán mantenerse en IPv4 hasta que se pruebe durante la implementación su configuración con IPv6. Por lo tanto, debe seguirse el protocolo de diagnóstico para equipos con compatibilidad Desconocida.

Recomendaciones:

- Seguir el protocolo definido para los activos de TI con Compatibilidad desconocida.

Ver numeral: 7.3.4. Para los activos de TI con compatibilidad desconocida.

7.3.3 Para los Sistemas de Información.

Excepciones:

Dado que el desarrollo del diagnóstico presentó que algunos de los lenguajes de programación implementados pueden encontrarse en versiones muy anteriores a las vigentes, o en algunos casos sin soporte por las casas fabricantes, se sugieren lo siguiente:

Tabla 11 Excepciones lenguajes de programación

LENGUAJE DE PROGRAMACIÓN	EXCEPCIÓN A IMPLEMENTAR
Delphi	Asignar IPv4 fija
Java versiones anteriores a 6	Asignar IPv4 fija
Otro lenguaje de programación	Asignar IPv4 fija

Recomendaciones:

- Depurar los Jobs, Procedimientos almacenados y todo elemento de software que invoque a una aplicación, modificando aquellos que utilizan la dirección IP de los servidores, cambiándola por los nombres de los mismos.
- Intervenir las bases de datos para las aplicaciones desarrolladas internamente, evaluando y depurando de igual manera la modificación de llamados por IP a llamados por nombres de servidores.
- Validar las aplicaciones que gestionen datos como direcciones IPv4, con el fin de realizar los cambios necesarios en los campos de las tablas, tanto en su tipo como en su tamaño. El cambio de 32 a 128 bits afecta significativamente el almacenamiento de datos.
- De igual forma es importante tener en cuenta que las aplicaciones que se desarrollen

internamente podrán definir variables dentro del código que pueden tener implicaciones en el momento de almacenar direcciones IPv6.

7.3.4 Para los activos de TI con compatibilidad desconocida

Si se detectan activos de TI con compatibilidad desconocida, de los cuales no se cuenta con la información necesaria para poder determinar si el activo cumple o no con los requisitos mínimos del protocolo IPv6, El tratamiento estándar para estos equipos es mantenerlos en el protocolo IPv4. Esto no genera ningún riesgo o impacto para la entidad, dado que, si bien se está llevando a cabo una "transición", donde coexisten los protocolos IPv4 e IPv6 simultáneamente, el tratamiento en el peor de los casos, para un equipo que tiene compatibilidad desconocida es mantenerlo en IPv4. Por lo tanto, el equipo seguirá operando tal cual cómo opera actualmente. Es decir, no se modifica absolutamente nada de su configuración o estado actual. Sin embargo, es importante seguir los siguientes pasos:

- Determinar la información relevante del equipo para poder consultar con el fabricante su compatibilidad. Esto deberá realizarse ingresando directamente a la configuración del equipo, para ver si es posible identificar algún dato que permita determinar la compatibilidad con IPv6.
- Si no se cuenta con información alguna, entonces se debe realizar la verificación en ambiente de pruebas con alguno de los equipos, con el fin de revisar directamente su panel de configuración e identificar si tiene opción de configuración de IPv6.
- En caso de no poder cumplir con ninguna de las opciones anteriores y no poder determinar la compatibilidad con IPv6, entonces se deberá mantener la configuración del equipo en IPv4 hasta que pueda ser reemplazado por uno compatible.

7.4 INFORME DE PREPARACIÓN (READINESS)

El informe de preparación contempla los aspectos técnicos necesarios para poder realizar la implementación. Sin embargo, la estrategia propuesta incluye realizar la transición a través de capas de acuerdo con la Figura 10

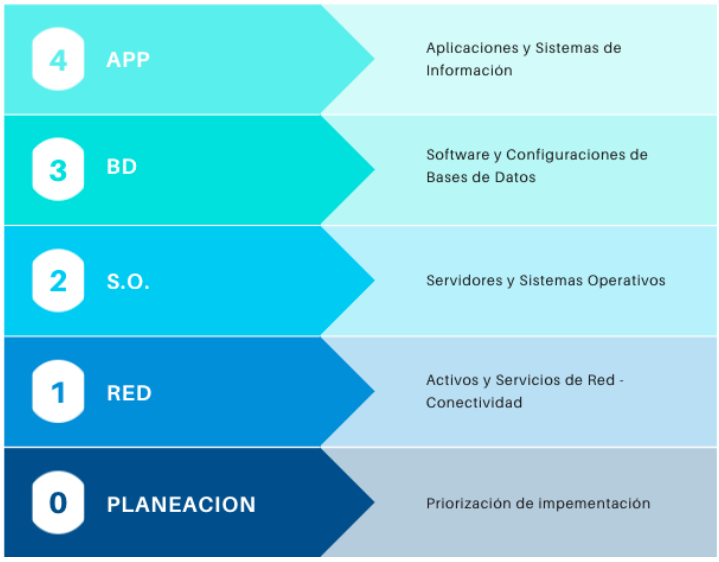


Figura 7 Estrategia de Implementación por Capas

Fuente: Elaboración propia

Para efectuar la implementación se deben realizar las siguientes actividades y en el siguiente orden especifico. Lo anterior basado en los resultados del Análisis de la información de activos de TI recopilada. La priorización para la implementación se define de acuerdo con los siguientes criterios:

- Prioridad a los servicios con criticidad Alta, Media y Baja.
- Orden de implementación por Capa (0. Planeación, 1. Red, 2.SO, 3.BD, 4.APP)

Nota: Todo el proceso de preparación debe ser acompañado por los proveedores de servicios, hardware y software de la Entidad.

7.4.1 Solicitar el direccionamiento global al organismo regulador o proveedor de servicios de internet.

Remitirse a la Sección 7.2 Plan de direccionamiento.

Teniendo en cuenta que el Ministerio TIC, recomienda en su última Guía de Transición (Abril de 2021) a cada una de las Entidades, la solicitud previa del bloque de direcciones de IPv6 ante LACNIC, con el fin de preparar la implementación con estas direcciones.
Aun cuando las ventajas de tener sus propias direcciones, LACNIC al momento de la redacción del presente documento entrega a clientes finales, un bloque /48, el cual resulta muy amplio para una entidad como la Corporación Autónoma Regional de Santander - CAS, el cual puede realizar su adopción con un bloque /64 que puede suministrar el proveedor de servicio.

7.4.2 Revisión del Servidor DNS y Servidor DHCP IPv4

Para una apropiada adopción del protocolo IPv6, es recomendable hacer una revisión sobre el servidor de DNS consistente en:

- Verificación de correspondencia de nombres con direcciones IPv4.
- Eliminación de registros DNS duplicados y obsoletos.
- Creación de objetos DNS que no estén registrados o que tengan problemas de registro DNS.

Para el caso interno se recomienda la implementación de un DNS que soporte los servicios que actualmente utiliza la entidad.

Así mismo, teniendo en cuenta que se tendrá una coexistencia entre dos protocolos, es necesario hacer la revisión del servidor de asignación automática de direcciones IPv4 (servidor DHCP), en los siguientes aspectos.

- Verificación de los registros de direcciones IPv4 duplicados.
- Verificación de registros de direcciones IPv4 obsoletos.
- Eliminación de registros no coherentes.

- Verificación de asignación correcta de los hosts en sus VLAN correspondientes.
- Revisión de las asignaciones estáticas

En el caso de los segmentos de red que actualmente son manejados a través de direccionamiento estático, se implementará un servicio de DHCPv6 que asigne las respectivas IP a hosts de usuario final.

7.4.3 Preparación de los dispositivos de conexión a internet.

La preparación de los dispositivos requiere tener presente varias de las consideraciones expuestas hasta ese momento, estas son:

- Haber adquirido un direccionamiento IP global.
- Contemplar el mecanismo de transición seleccionado.
- Haber definido el plan de direccionamiento IPv6.
- Contemplar que en este momento la mayoría de los sitios de internet en América Latina aún se comunican con direccionamiento IPv4, por lo tanto, es necesario mantener activo el protocolo IPv4.

Para la configuración de enrutadores, se tienen el siguiente escenario:

Escenario 1: Direccionamiento Global entregado por el RIR. En este se debe contemplar los siguientes aspectos:

- Solicitar al ISP realizar la configuración global asignada por el RIR.
- Replicar la configuración en el enrutador pasivo (Backup). Esto si el proveedor lo entrega.
- Mantener el direccionamiento IPv4 actual, para evitar incidentes con los servicios publicados.
- Realizar pruebas de conectividad sobre IPv6.

Para la configuración del Firewall, se deben tener en cuenta los siguientes aspectos:

- Activar las características IPv6 para el dispositivo.
- De acuerdo con el plan de direccionamiento, asignar direcciones IPv6 estáticas a las interfaces de red del dispositivo.

- Verificar la gestión del dispositivo a través del direccionamiento IPV6 asignado. Se puede usar una interfaz de prueba para la administración y gestión del dispositivo, una vez las pruebas por esta interfaz sean satisfactorias, se puede realizar la configuración en la interfaz principal.
- Realizar la configuración para la comunicación con los enrutadores del ISP.
- Configurar ACL de prueba para conectividad a Internet a través de IPv6.
- Realizar pruebas de conectividad IPV6 Firewall / enrutador y viceversa.
- Replicar la configuración al Firewall pasivo (Backup), en caso de contar a futuro con un equipo en alta disponibilidad.

Nota: En esta instancia, aún no se hace publicación de los servicios sobre IPv6, por lo tanto, se deben mantener aseguradas las ACL tanto para IPv6 como para IPv4.

7.4.4 Preparación del servidor de direccionamiento DHCP IPv6.

Para la preparación del servidor de direccionamiento IPv6 (DHCP IPv6) se deben tener en cuenta las siguientes consideraciones:

- Haber adquirido un direccionamiento global (temporal o definitivo) emitido por su RIR (LACNIC).
- Tener pre-configurados los dispositivos de conexión a internet (Router, Firewall, entre otros).
- Haber definido un plan de direccionamiento IPv6 acorde con la topología de red de la entidad.
- Depurar previamente el DNS y el servidor DHCP IPv4.

Teniendo en cuenta que en la Corporación Autónoma Regional de Santander - CAS, el manejo de direcciones IPv4 se hace estáticamente, la configuración del servidor que se habilite debe considerar:

- Activar las características IPv6 en el servidor que maneja DHCP.
- Asignar una dirección IPv6 estática, acorde con el plan de direccionamiento IPv6.
- Registrar la dirección IPv6 estática en el servidor de DNS (Recuerde que esta

dirección no es modificable ya que a través de esta los clientes de la red encontraran la dirección del servidor DNS IPv6).

- Si las características se encuentran activas, revise si la configuración del servidor DHCP cuenta con ámbitos activos de TI en IPv6.
- Cree un ámbito DHCP IPv6 de pruebas para su topología de red teniendo en cuenta las consideraciones dadas en el Plan de direccionamiento IPv6.
- Configurar las opciones de enrutamiento en el ámbito de la entidad.
- Crear un entorno de pruebas para validar la correcta asignación de direcciones IPv6. Si las pruebas son satisfactorias crear los ámbitos necesarios de acuerdo con su topología y su plan de direccionamiento.
- Establecer los dispositivos manejados por el DHCP IPv6 que requieran direccionamiento estático.
- De acuerdo con las recomendaciones dadas en el plan de direccionamiento establecer una dirección estática convirtiendo la dirección IPv4 en su correspondencia Hexadecimal IPv6.

7.4.5 Preparación de equipos de conectividad de red (actividad que realiza el operador contratado).

Para la preparación tenga en cuenta las siguientes consideraciones:

- Activar las características de IPv6 para sus dispositivos de red, de acuerdo con el mecanismo de transición definido (Dual Stack).
- Asignar un direccionamiento IPv6 estático para la gestión, acorde a la naturaleza de red a la que corresponde el dispositivo.
- Verificar la gestión del dispositivo a través del direccionamiento IPV6 asignado.
- De acuerdo con el plan de direccionamiento y la topología actual de red, se deben crear las VLAN IPv6 en el Switch de Core.
- Crear las reglas de enrutamiento necesarias de tráfico IPv6.
- Configurar las ACL IPv6 similares a las IPV4 existentes.
- Configurar los puertos del Switch de Core para permitir el tráfico de las VLAN IPv6 entre los Switches internos y los dispositivos de conectividad de red e Internet.

- Configurar los Switches internos de acuerdo a las VLAN IPv6 creadas en el Switch de Core y realice la configuración de los puertos según los requerimientos del dispositivo.
- Se recomienda utilizar un Switch de pruebas antes de la configuración definitiva, para verificar la correcta asignación de direccionamiento IPv6 en los Host de la red.
- Luego de pruebas y/o correctivos, replicar la configuración en los demás Switches.
- Realizar una activación temporal del protocolo IPv6 en equipos aleatorios clientes de una VLAN seleccionada, para la verificación de conectividad IPv6, esto requiere desactivación temporal de IPv4 en esos mismos equipos.
- Hacer un monitoreo del comportamiento de la conectividad en IPv6 durante un tiempo que se considere prudente.
- Restaurar las configuraciones IPv4 realizadas para las pruebas.

Nota: Dichas pruebas son para conectividad y comunicaciones, aún no existe configuraciones IPv6 para servidores y aplicaciones.

Para la red Wireless, se debe considerar en la configuración:

- Configurar la controladora Inalámbrica para su gestión a través de IPv6.
- Activar las características que permitan el uso del mecanismo de transición.
- Configurar una dirección IPv6 estática en la controladora.
- Realizar pruebas de conectividad IPv6 hacia el dispositivo.
- Mantener activa la configuración IPv4 del dispositivo.
- Configurar las VLAN correspondientes en IPv6 para los clientes inalámbricos.
- Configurar los puertos de la controladora para permitir el tráfico de las VLAN IPv6.
- Realizar pruebas de conectividad de los clientes inalámbricos y verificar la correcta asignación de direcciones IPv6 en dicho cliente.

7.4.6 Preparación de servidores.

Siendo los servidores la columna vertebral de la infraestructura, donde se soportan las operaciones críticas de la entidad, es necesario tener consideraciones especiales para esta:

- Verificar que los dispositivos de red de los servidores soportan, son compatibles y se encuentran actualizados para su operación en IPv6.
- Acorde al análisis de criticidad IPv6, es necesario establecer un plan ordenado de asignación de direcciones para estos dispositivos.
- Validar la compatibilidad de los sistemas operativos de los servidores con IPv6.
- Verificar la correcta asignación de direcciones en los servidores de DNS y DHCP IPv4.
- Activar las características de IPv6 en cada uno de los sistemas operativos de los servidores.
- Asignar una dirección IPv6 estática, de acuerdo con el plan de direccionamiento.
- Verificar la conectividad del servidor en IPv6.
- Verificar el correcto registro del servidor en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6.

Nota: Siempre se deberá mantener activo el protocolo IPv4 durante las pruebas.

Otras consideraciones: gran parte de la infraestructura de servidores soporta las aplicaciones de la entidad, bases de datos, archivos e información crítica para la entidad, es por ello que la activación de las características IPv6 se realizará de manera gradual evitando impactos en la continuidad del negocio, por lo tanto, se deben abrir ventanas de mantenimiento específicas para estas configuraciones y pruebas.

7.4.7 Preparación de equipos de usuarios final y otros tipos de host.

- Verificar que los dispositivos de red, de los equipos cliente, soportan, son compatibles y se encuentran actualizados para su operación en IPv6.

- Acorde al análisis de criticidad IPv6 (Bajo/Medio/Alto), es necesario establecer un plan ordenado de asignación de direcciones para estos dispositivos.
- Validar la compatibilidad de los sistemas operativos de los equipos cliente con IPv6.
- Verificar la correcta asignación de los equipos cliente en los servidores de DNS y DHCP IPv4.
- Activar las características de IPv6 en cada uno de los sistemas operativos de los equipos cliente.
- Asignar una dirección IPv6 automática, de acuerdo al plan de direccionamiento.
- Verificar la conectividad de los equipos cliente en IPv6.
- Verificar el correcto registro de los equipos cliente en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6.

7.4.8 Preparación de los Sistemas de Información y Bases de Datos

Para los sistemas de información

- Iniciar el proceso de actualización de aplicaciones desarrolladas en lenguajes de programación NO compatibles con IPv6. Para el caso de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS no se cuentan con lenguajes de programación no compatibles. Sin embargo, cada vez que se vaya a desarrollar una aplicación se deben tener en cuenta las mejores prácticas de desarrollo para incluir IPv6.

  http://long.ccaba.upc.es/long/045Guidelines/LONG_Trans_app_IPv6.pdf
  https://www.arin.net/knowledge/preparing_apps_for_v6.pdf

- Actualizar la tabla de Host de los documentos de conexión de las aplicaciones con las nuevas direcciones IPv6 de los servidores de aplicaciones. De igual forma es recomendable realizar el cambio del direccionamiento por el nombre correspondiente del host registrado dentro del DNS IPv6.
- Elaborar un plan de implementación IPv6 para las aplicaciones de acuerdo con la criticidad dada en el inventario de activos de TI IPv6.

- Configurar en los documentos conexión o conectores de aplicación con base de datos, el nombre del host que se invocará.
- En los escenarios donde las aplicaciones no puedan trabajar IPv4 e IPv6 simultáneamente (Capa de Aplicación), se deben separar los entornos de la aplicación para que cada uno se comunique mediante su respectivo protocolo. Recordar: La actualización de la aplicación debe hacerse en ambos entornos.
- Antes de poner en producción una aplicación modificada para IPv6, crear un ambiente de pruebas y cerciórese que arroja los resultados esperados.
- Evitar alterar las aplicaciones en producción.
- Crear copias de rCASldo antes de cualquier modificación.

Para Bases de Datos

- Crear una copia de seguridad de las bases de datos.
- Actualizar la tabla de Host, con las direcciones IPv6 correspondientes.
- Actualizar los Jobs, Procedimientos almacenados y toda configuración de base de datos que invoque a una aplicación, modificando acorde a la tabla de Host actualizada.
- Para las Bases de Datos, crear una copia de seguridad, realizar las configuraciones para IPv6 en un entorno de pruebas, modificando acorde a la tabla de Host actualizada.
- Validar los modelos de bases de datos con el fin de determinar si existen campos dentro de las tablas que deban modificarse, ya sea en su tamaño o en su tipo. Lo anterior para el almacenamiento de variables que tengan datos de dirección IPv6.

Para las conexiones Cliente / Aplicación

De acuerdo con la manera en que se invoque a la aplicación, tener en cuenta:

- Para las Aplicaciones WEB, hacer el llamado a través del nombre del Host, ya que a través de la dirección IP puede generar inconvenientes. Es importante tener en cuenta que si se desea acceder a una aplicación por su dirección IPv6 se debe usar la sintaxis adecuada de la dirección entre corchetes: [ ].
- Para las Aplicaciones Cliente/Servidor, actualizar orígenes de datos, documentos conexión o cualquier otro tipo de conector que la aplicación tenga, para que esta se

realice a través de nombre de Host. En caso de que los clientes compilados ya tengan direcciones IP quemadas en el código, se recomienda recompilar la aplicación con el nombre del servidor en vez de la dirección IP.

- Para las unidades mapeadas, hacer el llamado de las unidades de red compartidas invocando directamente el nombre del Host donde se encuentra el recurso.

7.5 RECOMENDACIONES GENERALES

- Capacitar a todo el personal implicado en la gestión y manejo del protocolo IPv6.
- Socializar ante la organización el plan de implementación de IPv6.
- Todos los procesos de adquisición tecnología a futuro deben exigir la compatibilidad con IPv6.
- Aunque el porcentaje de compatibilidad de los equipos con IPv6 es importante, se deben tener en cuenta que todos los nuevos equipos deben adquirirse con compatibilidad en IPv6.
- Validar el plan técnico de implementación con el fin de determinar las actividades y fechas en las que deben llevarse a cabo dichas actividades de implementación.

7.6 LINEAMIENTOS DE IPV6 EN CONCORDANCIA CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que el protocolo IPv6, por sus características, ofrece un alto nivel de seguridad, así mismo dependiendo del mecanismo de transición seleccionado, es necesario hacer el aseguramiento de la infraestructura de red con las políticas definidas para esta. Por lo tanto, se definen los siguientes lineamientos de IPv6 que abarcan no solo los temas de implementación del protocolo IPv6 sino también aspectos de seguridad de la información.

- Para la Corporación Autónoma Regional de Santander - CAS, el mecanismo de transición propuesto es Doble Pila (Dual Stack), teniendo en cuenta que los equipos de comunicaciones soportan el mismo.

- El mecanismo Doble Pila conlleva a que las políticas de seguridad y configuración de los dispositivos en IPv6 deben ser similares a las existentes en IPv4, con el fin de no afectar la arquitectura de seguridad de red.
- Es necesario tener en cuenta que las vulnerabilidades de seguridad pueden presentarse en los siguientes escenarios:
    - Heredarse desde IPv4
    - Comportarse diferente en IPv6
    - Generarse nuevas en IPv6.

  De acuerdo con lo anterior, es recomendable actualizar y reforzar la arquitectura de red con respecto a las nuevas vulnerabilidades que puedan surgir en aspectos como:

    - Control de acceso (ACL, Privilegios en redes IPv4, que se transfieran a IPv6)
    - Segmentación de redes
    - Creación de VLANs
    - Implementar una DMZ para la infraestructura
    - Características de seguridad de DNS, DHCP, ND en IPv6. Validar que los equipos de red implementen los RFC de seguridad.
    - Realizar el filtrado de paquetes en firewall de acuerdo con las recomendaciones del siguiente RFC: https://tools.ietf.org/html/rfc4890
- Con base en los esquemas de seguridad de la información se debe implementar el protocolo IPv6 teniendo en cuenta los criterios de Confidencialidad, Integridad y disponibilidad definidos en las políticas de la entidad.
- Se debe definir un plan de contingencias en el caso de presentarse indisponibilidad de los servicios.
- Generar la documentación que contemple los aspectos de seguridad de entorno a los sistemas de comunicación, sistemas de información y sistemas de almacenamiento, que surjan del proceso de implementación de IPv6.
- Definir un plan de direccionamiento con el prefijo asignado por LACNIC o el proveedor de servcio, que cubra todas las VLAN definidas para la entidad. Usuarios finales, punto a punto, servidores, seguridad física, administración entre otras. Tener en cuenta todos los tipos de direccionamiento.
- Segmentar el bloque de direcciones en zonas lógicas que cubran la estructura de red que tienen la entidad.
- Generar el ambiente de pruebas respectivo que permita probar las funcionalidades

más críticas para el despliegue del protocolo. Por ejemplo: DNS, DHCP, Firewall, Aplicaciones, enrutamiento, navegación a internet, usuarios finales, entre otros.

- Para el firewall se deben duplicar los objetos para que tengan asignada direcciones IPv4 y Direcciones IPv6. Esto garantiza que el equipo pueda ser alcanzado por ambos protocolos.
- De igual forma para los equipos de seguridad, todas las políticas deberán incluir los objetos IPv6 previamente configurados. En este caso se hace la observación de que dado que todo el prefijo IPv6 quedará anunciado en internet es indispensable que se haga una configuración apropiada de seguridad en los equipos perimetrales.
- Asignar el segmento de host de las direcciones IP de forma automática por EUI-64. Lo anterior para permitir que se puedan reconocer los equipos evaluados en las actividades de monitoreo.
- Asignar direccionamiento estático a todos los equipos servidores y dispositivos que están fuera del alcance del DHCP.
- Dado que el proyecto de despliegue de IPv6 se realizará a través de una transición, se deben mantener los equipos y sistemas de información en ambos protocolos. Posteriormente, cuando los informes de monitoreo muestren resultados sobre el uso de IPv6, se podrá evaluar la desactivación paulatina del protocolo IPv4.
- Las configuraciones que se realicen en los equipos deberían quedar documentadas y actualizadas constantemente con el fin de mantener registro de los cambios en IPv6 realizados a la entidad.
- Por cada cambio realizado se debe verificar que los aspectos de seguridad quedan aplicados y no se generan nuevas vulnerabilidades en la red.
- Todo cambio para la configuración de IPv6 deberá realizarse ya sea en ventana programada o en ambiente de pruebas antes de poderlo desplegar en ambiente de producción.
- Se recomienda sensibilizar y capacitar a todos los funcionarios y contratistas de la entidad en aspectos técnicos y gerenciales del proceso de transición. Esto permite que los usuarios finales tengan conocimiento de los beneficios que entrega la migración.
- Definir un funcionario de la entidad que se encuentre encargado de IPv6 dentro de la entidad. Este funcionario estará encargado de revisar la transición, el monitoreo, la inclusión de nuevos equipos y la aplicación de los aspectos de seguridad del protocolo IPv6.

- Aplicar las buenas prácticas de seguridad recomendadas en los siguientes RFC de seguridad: 2401, 2402, 2406, 2408.

Tabla 12 Lista de RFC sobre IPv6

RFC	NOMBRE	CONTENIDO
2401	Arquitectura de Seguridad para el Protocolo Internet	Este documento especifica un protocolo de Internet en vías de estandarización para la comunidad de Internet. Este documento especifica la estructura fundamental de IPec. La meta de la arquitectura es proporcionar diversos servicios de seguridad para el tráfico en la capa IP, en ambientes IPv4 e IPv6. Este documento describe las metas de tales sistemas, sus componentes y cómo estos se adaptan en el ámbito IP. Este documento también describe el servicio de seguridad proporcionado por los protocolos IPec, y como estos servicios se pueden emplear en ambientes IP. Este documento no trata todos los aspectos de la arquitectura IPec. Fuente: https://www.rfc-es.org/rfc/rfc2401-es.txt
2402	Cabecera de Autentificación IP	La Cabecera de Autentificación IP (Authentication Header - AH) se usa para proporcionar integridad sin conexión y autenticación del origen de datos para datagramas IP ("autentificación" a partir de ahora), y para proporcionar protección contra reenvíos. Fuente: https://www.rfc-es.org/rfc/rfc2402-es.txt
2406	Carga de Seguridad IP Encapsulada (ESP)	La cabecera de Carga de Seguridad Encapsulada (ESP) está diseñada para proporcionar un conjunto de servicios de seguridad en IPv4 y en IPv6. ESP es usado para proporcionar confidencialidad, autentificación del origen de los datos, integridad sin conexión, un servicio de anti-replay (una forma parcial de integralidad de secuencia) y confidencialidad limitada del flujo de tráfico. Fuente: https://www.rfc-es.org/rfc/rfc2406-es.txt
2408	Internet Security Association and Key Management Protocol (ISAKMP).	Este documento describe un protocolo utilizando los conceptos de seguridad necesarios para establecer asociaciones de seguridad y llaves criptográficas en un ambiente de internet. Fuente: https://www.ietf.org/rfc/rfc2408.txt

7.6.1 Herramientas sugeridas para la gestión de IPv6

Existen diferentes tipos de herramientas para efectuar la gestión del protocolo IPv6, entre estas se propone evaluar tanto herramientas Open source como herramientas comerciales. A continuación, se describen algunas de ellas:

7.6.1.1 Herramientas Open source

- **GestiónIP:** Software web automatizado para la gestión de direccionamiento IPv4 e IPv6. La herramienta permite efectuar la planeación jerárquica de asignación de direccionamiento IP. Tiene funciones de descubrimiento de red, búsquedas, filtros y un sistema de gestión de VLAN automáticas.
- http://www.gestioip.net/
- **TeamIP:** Solución web 2.0 que permite la gestión del direccionamiento de red IPv6. Tiene una interfaz simple y robusta para la planeación de transición y administración del direccionamiento IPv4/IPv6 de acuerdo con las mejores prácticas de gestión de red.
- https://www.combodo.com/teemip-194
- **6Connect:** Es un producto comercial, pero tiene versión libre disponible. Permite realizar cálculos de direccionamiento IPv6 e IPv4 para los CAScios de direccionamiento asignados o no asignados. Se encuentra integrada con las APIs de ARIN y RIPE para la asignación de direcciones. Realiza consulta de DNS reverso a las IP asignadas de forma automática, soporte para DNSSEC.
- https://www.6connect.com/6connect-provision/

7.6.1.2 Herramientas Comerciales

- **Infoblox IP Address Management:** Gestión de red y direccionamiento IPv6/IPv4. Planeación de la asignación y distribución de direcciones IP con integración para ambientes VMware y Microsoft.
- https://www.infoblox.com/products/ddi/
- **BlueCat Address Manager:** Esta herramienta es robusta para la gestión de direccionamiento IP, permitiendo tomar control de redes complejas y dinámicas.

Cuenta con servicios Core, workflow y automatización que pueden gestionar cualquier dispositivo conectado dentro de la red desde un panel de control. Provee inteligencia de red y supervisión entre dispositivos puede mejorarse la seguridad de la red garantizando conectividad constante.

- https://www.bluecatnetworks.com/solutions/
- **SolarWinds IP address manager:** Esta herramienta ayuda en la planeación de la migración de IPv4 a IPv6 bajo la creación de múltiples escenarios de prueba antes de una migración real. Permite adicionar, editar y eliminar redes y subredes para IPv4 e IPv6, así como identificar los equipos que trabajan en Dual Stack. Es posible crear grupos de direcciones IPv4/IPv6 para la organización de dispositivos y áreas, así como crear y editar direcciones individuales, rangos o prefijos en IPv4 e IPv6.
- http://www.solarwinds.com/ip-address-manager

Como resultado de las herramientas mencionadas anteriormente, la entidad podrá revisar las opciones, probarlas o consultar sobre otro tipo de herramientas a discreción. Sin embargo, de las opciones presentadas anteriores se recomienda usar:

- Open source: GestiónIP
- **Comercial:** SolarWinds IP address Manager

Se listan a continuación algunos sitios que podrían ser de ayuda en la gestión de IPv6:

- https://www.manageengine.com/products/oputils/IPv6-address-management.html
- https://www.ultratools.com/IPv6Tools
- https://getIPv6.info/display/IPv6/IPv6+Management+Tools
- http://www.networkworld.com/article/2288768/infrastructure-management/tools-cure-ip-address-management-headaches.html

7.6.2 Protocolo para diagnóstico e implementación de IPv6 en activos de TI desconocidos o descubiertos después del Diagnóstico

Si bien la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS podría llegar a desconocer la existencia de equipos o sistemas de información en su infraestructura, se define a continuación el protocolo para tratar este tipo de activos de TI desconocidos,

con el fin de que sean diagnosticados e incluidos dentro del plan de implementación para la Transición a IPv6.

Este protocolo aplica para todas las etapas de la transición a IPv6 (Diagnóstico, Implementación y Monitoreo) y en los siguientes casos:

- Si se identifica un equipo (hardware) o Sistema de información (software) que la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS no había identificado previamente.
- Si durante la implementación se descubre un equipo o sistema de información que genera afectación al proceso de transición y que no se tenía identificado. Por ejemplo, un dispositivo de enrutamiento, Switch o equipo no informado que al desplegar IPv6 es descubierto a causa de la afectación del despliegue y por lo tanto requiere modificar el plan de implementación.
- Aplicaciones que se encuentran clasificadas como Bolsa de Aplicaciones, las cuales serán revisadas previamente a su implementación del protocolo.
- Nuevas aplicaciones adquiridas por parte de la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS o del Operador.

Protocolo:

De acuerdo con lo anterior se deben seguir las siguientes actividades:

- Inclusión del activo identificado dentro del inventario de activos de TI (hardware o aplicaciones).
- Identificación del nivel de compatibilidad con IPv6. Dependiendo del tipo de dispositivo, deberá evaluarse si solo necesita la configuración básica de IPv6 Host, Forward o Dual Stack.
- Determinar si se deben genera excepciones para el dispositivo. Esto en caso de que no sea compatible.
- Determinar cuáles serían los requisitos de preparación para la adopción del protocolo IPv6.
- Identificar dentro del plan de Implementación la actividad donde se debe incluir este

activo con el fin de que aplique la misma actividad o ventana de implementación.

- Incluir el activo dentro del plan de Implementación para que sea desplegado IPv6 en dicho dispositivo.
- Si el activo corresponde a una actividad que ya se ha implementado previamente, entonces se creará una nueva actividad dentro del plan con fecha posterior y se tratará de manera consecutiva con las demás actividades según lo planeado previamente.
- En caso de que el activo se identifique como parte de una falla en el despliegue, entonces se dará prioridad a la transición de este activo antes de continuar con la actividad que falló.
- Si existe más de un activo identificado simultáneamente como desconocido, pero no genera retrasos en la implementación, entonces estos se agruparán y se trabajarán en conjunto (actividades mencionadas anteriormente).

Como resultado de estas actividades el activo debe quedar incluido dentro del inventario de activos de TI, con el protocolo IPv6 desplegado en caso de que aplique, o en su defecto incluido dentro del Plan de Implementación para que sea configurado y migrado en el protocolo IPv6 según lo planeado.

En caso de que durante la implementación se detecte que un equipo o sistema de información que se tenía planeado migrar a IPv6 ya no se encuentre disponible o se haya dado de baja se deben realizar seguir las siguientes actividades:

- Actualizar el inventario de activos de TI
- Ajustar los planes técnicos de implementación donde se incluían dichos activos de TI.

Nota: La bolsa de Sistemas de información, es decir, aquella lista de aplicaciones que la CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS desconoce actualmente deberá ser trabajada acorde a los mismos pasos mencionados. Sin embargo, su despliegue en IPv6 será validado previamente por el grupo de IPv6 de la entidad con el fin de determinar si se despliegan de forma separada o en grupo, como un paquete, dentro del marco del Plan de Implementación definido.

8. RECOMENDACIONES DE ADQUISICIÓN

Como resultado del diagnóstico a continuación se presentan las recomendaciones de adquisición de infraestructura o software que permiten complementar el proceso de transición a IPv6.

- Para la infraestructura de comunicaciones se recomienda la adquisición de un Router de Core, puesto que, aunque el equipo actual soporta IPV6, tiene baja capacidad de procesamiento, lo que podría provocar mayor latencia en las comunicaciones.
- Adquirir una herramienta de control de IPv6. Esto permite gestionar el direccionamiento IPv6 de la entidad y administrarlo adecuadamente. Si bien inicialmente la asignación se realizará partiendo del plan de direccionamiento, es importante que a futuro se contemple la adquisición de dicha herramienta.
- Se recomienda que todos los contratos de adquisición de nuevas tecnologías, hardware y software incluyan la política de IPv6, la cual debe exigir que todos los equipos y software sean compatibles y desplegados en IPv6 cumpliendo con los requisitos técnicos mínimos que defina la CAS, así como los lineamientos de seguridad de IPv6 en general.

9. TERMINOLOGÍA

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

AUDITORÍA: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

AUTENTICACIÓN: Provisión de una garantía de que una característica afirmada por una Entidad es correcta.

BASE DE DATOS: Tecnología de la información que permite la estructuración de forma adecuada de los datos a través de la construcción de relaciones de sus elementos.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

DIRECCIÓN IP: Representación numérica que identifica una interfaz en particular de manera exclusiva en una red de datos.

DIRECCIONAMIENTO IPV6: Es una etiqueta numérica del paquete usada para identificar una interfaz de red que provee una conexión entre nodos de una red sobre IPv6, esto facilita el enrutamiento de los paquetes entre distintos hosts.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

DHCPv6 (Protocolo Dinámico de Configuración de nodos)[4]: Protocolo de configuración con estado ("stateful") que proporciona direcciones IP, direcciones de los servidores DNS y otros parámetros de configuración.

DIRECCIÓN: Identificador único asignado a nivel de la capa de red a una interfaz o conjunto de ellas, que puede ser empleado como campo de origen o destino en datagramas IPv6.

DNS (Sistema de nombres de dominio, Domain Name System): Sistema jerárquico de almacenamiento y el protocolo asociado para almacenar y recuperar información que permite vincular nombres y direcciones IP.

DOBLE-PILA (DUAL-STACK): Mecanismo de coexistencia IPv4/IPv6, mediante el cual un nodo incorpora tanto la pila IPv4 como la pila IPv6.

INFRAESTRUCTURA TECNOLÓGICA: Conjunto de elementos de hardware y software sobre el que se asientan los servicios de una organización.

IP: Protocolo Internet

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.

[4] Las definiciones (g) a (m) Tomadas de http://www.IPv6.es/es-ES/Glosario/

IPEC (seguridad del Protocolo de Internet, Internet Protocol security): Conjunto de estándares que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPEC soporta autenticación a nivel de Entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección anti-repeticiones.

IPv4: Protocolo de Internet versión 4.

IPv6: Protocolo de Internet versión 6.

ISP – INTERNET SERVICE PROVIDER[5]: Un Proveedor de Servicios de Internet asigna principalmente CAScio de direcciones IP a los usuarios finales de los servicios de red que éste provee. Sus clientes pueden ser otros ISPs. Los ISPs no tienen restricciones geográficas como lo tienen los NIRs.

LACNIC: Organización internacional no gubernamental con sede en Uruguay cuya función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región de América Latina y el Caribe.

LENGUAJE DE CONSULTA ESTÁNDAR (SQL): Lenguaje de programación dentro del cual se establecen las reglas para la estructura, consulta y presentación de datos e información.

LENGUAJE DE PROGRAMACIÓN: Conjunto de reglas sintácticas que permiten la construcción de aplicaciones y/o Sistemas de Información

MECANISMOS DE TRANSICIÓN A IPV6: Los protocolos IPv4 e IPv6 no son compatibles y para la migración a IPv6 debe mantenerse la coexistencia de ambos protocolos por un tiempo determinado en lo que se logra la total migración a IPv6. La clave para una migración exitosa consiste en poder utilizar ambos protocolos en la red hasta que todos los

[5] Tomado de http://www.lacnic.net/web/lacnic/manual-1

servicios sean migrados a IPv6. La mayoría de los nodos de Internet van a necesitar utilizar ambos protocolos por mucho tiempo, lo que requiere la definición e implementación de mecanismos de transición a IPv6. Esos mecanismos de transición pueden agruparse en tres grandes categorías: (Doble Pila, Traductores, Tunneling).

A pesar de las ventajas que ofrecen cada uno de estos mecanismos, la esencia principal de todos ellos es el mecanismo de Doble Pila.

De acuerdo a las recomendaciones de MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) y organismos internacionales como LACNIC el mecanismo que garantiza con eficiencia la coexistencia de ambos protocolos (IPv4 e IPv6) es el de Doble Pila. Este será por tanto el mecanismo que se considerará para la implementación del Protocolo Internet Versión 6 (IPv6) al interior de la institución.

MOTOR DE BASE DE DATOS: Herramienta tecnológica que permita la gestión de la información a través de la implementación de las reglas establecidas por el lenguaje SQL y la relación de entidades

NOTACIÓN HEXADECIMAL[6]: Notación empleada para expresar direcciones IPv6 en forma literal. La dirección de 128 bits es dividida en 8 bloques de 16 bits cada uno. Cada bloque se expresa como un número hexadecimal y éstos están separados del siguiente por medio del ":". Los ceros situados a la izquierda de cada bloque pueden ser omitidos. Ejemplo de una dirección IPv6 unicast: 2001:DB8:1234:ABCD:789:EF01:0:1.

POLÍTICAS DE SEGURIDAD: Son aquellas reglas y procedimientos definidos por una organización con el propósito de preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información.

POLÍTICAS DE ENRUTAMIENTO: El enrutamiento basado en políticas proporciona una herramienta para reenviar y enrutar paquetes de datos basados en las políticas definidas

[6] Las definiciones (o) a (s) Tomadas de http://www.IPv6.es/es-ES/Glosario/

por los administradores de red. En efecto, es una manera de que la política invalide las decisiones del protocolo de enrutamiento. El enrutamiento basado en políticas incluye un mecanismo para aplicar selectivamente políticas basadas en la lista de acceso, el tamaño de los paquetes u otros criterios. Las medidas que se toman pueden incluir el enrutamiento de paquetes en rutas definidas por el usuario, el establecimiento de la precedencia, el tipo de bits de servicio, etc.

PREFIJOS IPV6: Representan un rango o bloque de direcciones IP consecutivas. Que deberán solicitarse formalmente ante organismos autorizados para su asignación en cuyo caso la organización será propietaria indefinidamente de tal bloque de direcciones o podrá recibirse de un Proveedor de Servicios de Internet con la diferencia de que tal direccionamiento no pertenecerá a la organización.

PROTOCOLO DE PRUEBAS: Programa sistemático de verificación e inspección diseñado y ejecutado para el control de calidad de la tecnología y operación de un equipo, proceso o servicio. Así como condiciones de seguridad y fiabilidad.

PROTOCOLO DE INTERNET: Conjunto de reglas para el emisión y recepción de datos a través de un canal de internet.

PROTOCOLO IPV4: Es la cuarta versión del Protocolo de Internet, es un protocolo de interconexión de redes. Utiliza direcciones de 32 bits que limitan el CAScio de direcciones a 42.934.967.296 direcciones.

PROTOCOLO IPV6: es la nueva versión del Protocolo de Internet (Internet Protocol -IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s con el IETF (Internet Engineering Task Force). Destinado a sustituir al Protocolo Internet Versión 4. IPv6 amplía el número máximo de direcciones de Internet al manejar un tamaño de dirección IP de 128 bits a diferencia de su antecesor IPv4 que maneja un tamaño de dirección IP de 32 bits.

PROVEEDOR DE SERVICIOS INTERNET: Empresas que proporcionan servicios de conexión a Internet y temas relacionados.

PRUEBAS DE FUNCIONALIDAD: Proceso mediante el cual se valida la funcionalidad de un sistema.

REDES PRIVADAS VIRTUALES – VPN: (Virtual Private Network): Es una tecnología de acceso que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

RESOLUCIÓN DE NOMBRES: Obtención de una dirección a partir de un nombre.

RFC: Petición de Comentarios, Request For Comments. Paso previo de un documento estándar de Internet (STD), aunque en la actualidad, los fabricantes implementan en sus productos RFC, sin esperar a que sean STD.

RIR: Regional Internet Registry: Los Registros de Internet Regionales (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir los recursos de Internet dentro de las respectivas regiones.

SEGMENTOS DE RED: Resultado de dividir una red de datos con el propósito de aumentar el número de nodos conectados a ella.

SERVICIO WEB: Herramienta de software que permite la interoperabilidad entre sistemas o herramientas tecnológicas, de forma que garanticen la comunicación de escritura o lectura de datos.

SISTEMAS DE INFORMACIÓN: Conjunto de mecanismos ordenados como lenguaje de programación, base de datos, interfaz, servicio web, que tienen como fin la administración de datos e información para su procesamiento y entrega.

SISTEMAS DE COMUNICACIÓN: Conjunto de dispositivos interconectados para el transporte y entrega de información.

SUBRED: Uno o más enlaces que utilizan el mismo prefijo de 64 bits.

TOPOLOGÍA DE RED: Es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (ejemplo: computadores, impresoras, servidores, switches, enrutadores, etc.) se interconectan entre si sobre un medio de comunicación.

a). Topología física: Se refiere al diseño actual del medio de transmisión de la red.

b). Topología lógica: Se refiere a la trayectoria lógica de una señal a su paso por los nodos de la red.

REFERENCIAS

- Resolución 2710 del 2017. Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Modelo de Seguridad y Privacidad de la Información. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Transición de IPv4 a IPv6 para Colombia. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en

- https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Aseguramiento del Protocolo IPv6. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en
- https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

ANEXOS

- Anexo 1. Topología de Red General

- Anexo 2. Inventario de Activos TI - Diagnostico IPv4 a IPv6 CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER - CAS V1

- Anexo 3. Plan de Direccionamiento IPv6 Corporación Autónoma Regional de Santander - CAS v1