

PLAN Y ESTRATEGIA DE TRANSICIÓN DE IPV4 A IPV6

SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2017

Página 1 de 10

Contenido

1.	INTRODUCCIÓN	3
2.	POR QUÉ IMPLEMENTAR IPv6?	4
3.	PLAN Y ESTRATEGIA DE TRANSICIÓN	5
3.1	Fase I. Planeación de IPv6	5
3.1.1	Entregables de esta Fase	6
3.1.2	Tabla de actividades de la Fase I – Planeación de IPv6	7
3.2	Fase II. Implementación del protocolo IPv6	7
3.2.1	Entregables de esta Fase	8
3.2.2	Tabla de actividades de la Fase II – Implementación de IPv6	9
3.1	Fase III. Pruebas de funcionalidad de IPv6	9
3.2.3	Entregables de esta Fase	10
3.2.4	Tabla de actividades de la Fase II – Implementación de IPv6	10

1. INTRODUCCIÓN

Las redes de telecomunicaciones han venido creciendo exponencialmente generando mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet que permiten establecer conexiones para cada elemento conectado a la red; estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final, así mismo en el año 1992 la Internet Engineering Task Force IETF1 a partir de diversos grupos de trabajo definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo protocolo de conectividad denominado IPv6 o Ipng (Next Generation Internet Protocol).

En ese orden de ideas el protocolo IPv6, hará posible que todos los dispositivos tecnológicos usados para la conexión a internet, tengan una dirección en IPv6, la cual facilitará la conectividad en banda ancha, ofreciendo mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

Así mismo, para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en 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 la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.²

Para entrar en el proceso de adopción de este nuevo protocolo, se recomienda realizar un inventario de los activos de información, revisar su actual infraestructura de computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente dentro de las entidades del estado.

2. POR QUÉ IMPLEMENTAR IPv6?

Los siguientes puntos son los beneficios que representa un proceso de transición de IPv4 a IPv6 que son importantes tener presente al momento de adoptar el nuevo protocolo con éxito; ellos son:

- La posibilidad de tener un mayor número de equipos conectados a la red de las entidades al ser implementada esta solución.
- Proceso técnicamente transparente para los usuarios de la red y sus distintos servicios dentro de las organizaciones.
- La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.
- Mejora de la seguridad de la red en virtud de la arquitectura del nuevo protocolo y sus servicios.
- Decremento de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores de no implementarse el nuevo protocolo en las entidades.
- Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.
- Gran número de direcciones IP para conexiones a Internet con el mundo exterior.
- Los Proveedores de servicio tendrán que hacer transición de sus soluciones al nuevo protocolo IPv6 y pensar en innovar a fin de ofrecer nuevos servicios a sus clientes, lo cual será ventaja para todas las entidades del Gobierno.

3. PLAN Y ESTRATEGIA DE TRANSICIÓN

3.1 Fase I. Planeación de IPv6

La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con el plan de diagnóstico de la infraestructura de TI de las Entidades.

Las siguientes son las actividades a tener en cuenta en esta fase:

- Elaborar y validar el inventario de Activos de Información de servicios tecnológicos de las entidades y su interrelación entre ellos. Para esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuáles equipos soportan IPv6, cuales requieren actualizarse y cuáles no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6.
- Analizar, diseñar y desarrollar el plan de diagnóstico del protocolo IPv4 a IPv6 en la red de las entidades del estado.
- Identificar la topología actual de la red y su funcionamiento dentro de la organización.
- Evaluar el grado de afinamiento del protocolo IPv6 a nivel de hardware y software con miras a preparar la nueva infraestructura de red de las entidades.
- Generar el plan detallado del proceso de transición de esta fase hacia IPv6.
- Planear la migración de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC de IPv6.
- Validar el estado actual de los sistemas de información, los sistemas de comunicaciones y evaluar la interacción entre ellos cuando se adopte el protocolo IPv6.
- Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no se pueden implementar a IPv6.
- Identificar la configuración y los esquemas de seguridad de la red de comunicaciones y sistemas de información.

- Se recomienda revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el firewall respectivo de cada entidad.
- Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de una validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en las Entidades; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de las entidades de tal manera que la información recogida de esta tarea sea insumo para la acometida de la segunda fase que es la implementación de IPv6.
- Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 por cada Entidad.
- Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros.
- Capacitar a funcionarios de las Áreas de TI de las Entidades de conformidad con los planes de capacitación establecidos, en el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto del nuevo protocolo.

3.1.1 Entregables de esta Fase

- Plan de trabajo para la adopción de IPv6.
- Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones.
- Documento que define los lineamientos al implementar la seguridad en IPv6 en concordancia con la política de seguridad de las entidades.
- Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de las Entidades y plan de sensibilización al total de funcionarios de las Entidades.

3.1.2 Tabla de actividades de la Fase I – Planeación de IPv6

La Supervigilancia tuvo en cuenta la siguiente tabla de actividades:

Fase I	Actividades Generales	Tiempo en meses de la actividad
Diagnóstico de la Situación Actual	Construcción del plan Diagnóstico	1
	Inventario de TI (Hardware, software)	1
	Análisis de nueva topología de la infraestructura actual y su funcionamiento	1
	Protocolo de pruebas de validación aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos	3
	Planeación de la transición de los servicios tecnológicos de la Entidad	2
	Validación de estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos y revisión de los RFC correspondientes.	2
	Identificación de esquemas de seguridad de la información y seguridad de los sistemas de comunicaciones	2

3.2 Fase II. Implementación del protocolo IPv6

La fase de implementación debe cubrir las siguientes actividades:

- Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la primera Fase del proceso de transición de IPv4 a IPv6 y teniendo en cuenta el inventario de los activos de información de cada una de las Entidades del Estado.

- Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en Doble Pila; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.
- Aplicar el modelo de transición de IPv6 en la red de la Entidad, permitiendo la coexistencia con los protocolos tanto IPv4 como IPv6 y la transición en doble pila.
- Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 en modalidad de doble pila; esta técnica permite que tanto los servicios de IPv4 como los servicios de IPv6 deben estar funcionando de manera independiente pero coexistente dentro de las Entidades
- Validar la funcionalidad de los siguientes servicios y aplicaciones de las Entidades sobre IPv6: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de respaldo, Servicio de Comunicaciones Unificadas, Servicios VPN, Integración entre Sistemas de Información, Sistemas de Almacenamiento, Servicios de administración de red.
- Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad (Servidores AAA, firewalls, NAC, y equipos perimetrales de conformidad con los RFC de seguridad en IPv6, se sugiere revisar los RFC de seguridad en IPv6 asociados.
- Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet para establecer la conectividad integral en IPv6 desde el interior de las redes LAN, hacia el exterior de las redes WAN a fin de garantizar que las entidades puedan generar tráfico de IPv6 normalmente.

3.2.1 Entregables de esta Fase

- Presentación del Informe del plan detallado de implementación del nuevo protocolo.
- Documento con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta fase.
- Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

3.2.2 Tabla de actividades de la Fase II – Implementación de IPv6

La Supervigilancia deberá tener en cuenta la siguiente tabla de actividades:

Fase II	Actividades Generales	Tiempo en meses de la actividad
Desarrollo del Plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase	2
	Configuración de servicios de DNS, VPN, otros.	1
	Configuración del protocolo IPv6 en Aplicativos, Sistemas de Comunicaciones, Sistemas de Almacenamiento.	3
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	2
	Coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6 hacia el exterior.	3

3.1 Fase III. Pruebas de funcionalidad de IPv6

Las pruebas de funcionalidad de esta fase deben cubrir las siguientes actividades:

- Realizar las pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la Entidad en un ambiente que permita empezar a generar tráfico de IPv6 de la entidad hacia Internet y viceversa.
- Realizar las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones.

- Al momento de las pruebas de funcionalidad se debe realizar el afinamiento de las configuraciones de hardware, software y servicios de las Entidades, con base en la información resultante de la fase II.
- Elaborar un inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

3.2.3 Entregables de esta Fase

- Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación.
- Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación.
- Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

3.2.4 Tabla de actividades de la Fase II – Implementación de IPv6

La Supervigilancia deberá tener en cuenta la siguiente tabla de actividades:

Fase II	Actividades Generales	Tiempo en meses de la actividad
Pruebas de funcionalidad de IPv6	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.	3
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	3
	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.	2

FUNCIONARIO O ANALISTA	NOMBRE	FIRMA	FECHA
Elaborado por	LYDA Rocio Gomez - Ingeniero Contratista Oficina de Informática y Sistemas		03/03/2017
Revisado por	Claudia Marcela Ladino Herrera- Jefe Oficina de Informática y Sistemas		