Bogotá, 23 de junio de 2023

Señor Gobernador
CARLOS EDUARDO CAICEDO OMAR
GOBERNACIÓN DE MAGDALENA
Ingeniero (a)
JOSÉ RAMON IGLESIAS - DIRECTOR TICS
oficinatic@magdalena.gov.co
Santa Marta, Magdalena

Respetados señores:

DICITEC S.E.M. como parte de la oferta institucional de la **Federación Colombiana de Municipios** en aras de potenciar el desarrollo territorial, pone a disposición del país el apoyo y acompañamiento necesario para el desarrollo del proceso de la transición del protocolo IPv4 a IPv6 (Implementación protocolo IPv6), dándole acceso a los Municipios a nuestra amplia experiencia en estos procesos tecnológicos y a una reducción significativa de los costos asociados a ellos.

Dentro del plan de acción estuvo el contactarnos con el responsable del área de las tecnologías de la Información y las Comunicaciones TICs, de su Municipio, con el fin de sensibilizarlo sobre el tema y acordar un plan a seguir, así fue como en días pasados recibimos de ustedes la manifestación de apoyo para que nosotros les formalicemos una propuesta de **ACOMPAÑAMIENTO A LA IMPLEMENTACIÓN EL PROTOCOLO DE IPV6** para su Municipio.

Teniendo en cuenta lo anterior, hacemos llegar a usted nuestra propuesta formal adjunta a la presente, la cual incorpora el **beneficio ofrecido por la Federación Colombiana de Municipios** al separar **un (1) pool de direcciones IPV6** que se acondicione a la proyección de la **red municipal mínimo por los próximos 16 años**, lo cual significa que el Municipio tendrá su propio Pool de direcciones IPv6 y de esta forma tendrá independencia o autonomía frente al proveedor de Internet por cualquier cambio de este, evitando así todos los traumatismos que esto implica. Lo anterior significa igualmente un **ahorro de U$2.500** que corresponde al valor inicial de la membresía que el Municipio debería pagar a **LACNIC** y **U$10.200** correspondientes al valor de **U$600** anuales por cada uno de los próximos 16 años, que por la renovación debería pagar el Municipio a **LACNIC,** equivaliendo esto a un **ahorro** de más o menos **$58.174.985 Cincuenta y Ocho Millones Ciento Setenta y Cuatro Mil Novecientos Ochenta y Cinco Pesos** por los próximos **16 años**. Con este proceso igualmente la Entidad está provisionando las herramientas para el futuro desarrollo de las tecnologías de la información y las comunicaciones del Municipio.

Para atender cualquier inquietud que pueda generar la información brindada, tanto a ustedes como a cualquiera de los integrantes de su equipo de trabajo pueden comunicarse con nosotros a través del siguiente correo electrónico: **empresasmixtas@fcm.org.co, serviciostecnologicos@fcm.org.co, o municipios@ipv6spectrum.com**

Cordialmente,

ENRIQUE LÓPEZ
Gerente
CDFC-006-2022

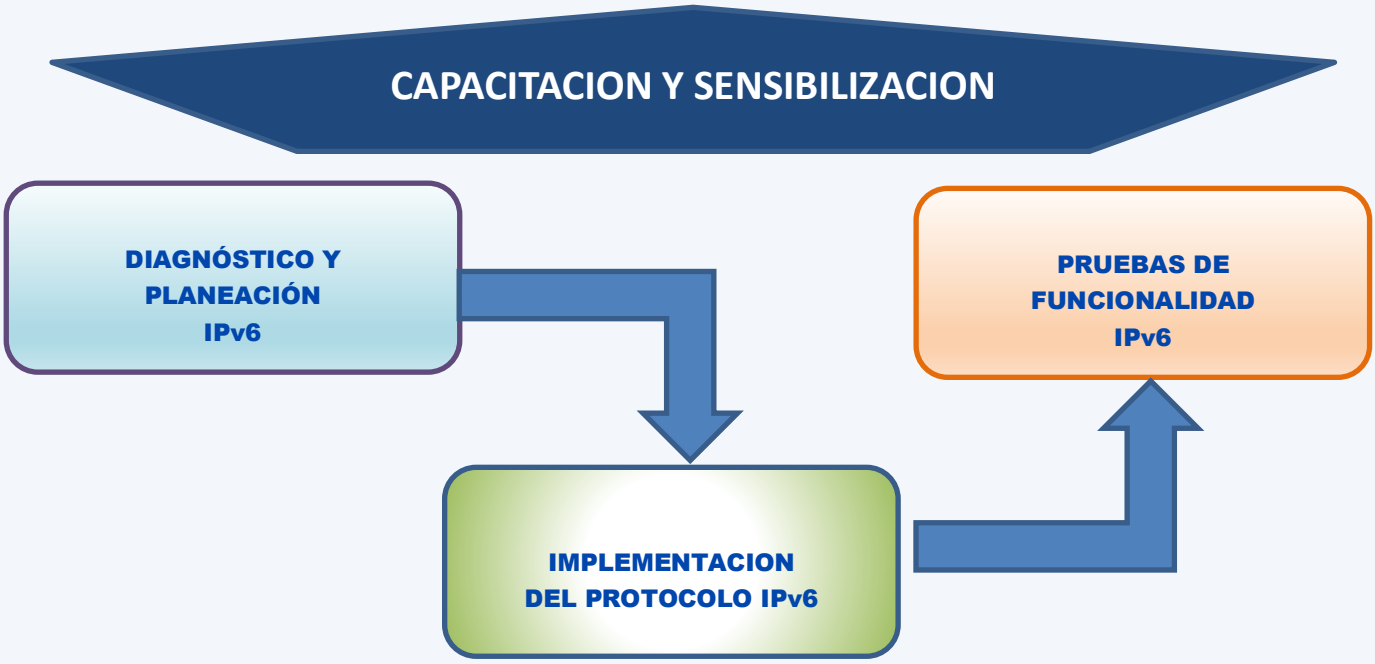
Propuesta de Asistencia Técnica Especializada

Propuesta para brindar asistencia técnica a la GOBERNACIÓN DE MAGDALENA, en la implementación del protocolo IPv6, por medio del acompañamiento y disposición de personal especializado y herramientas técnicas necesarias para la realización del diagnóstico, plan de implementación, transferencia de conocimiento, implementación y pruebas de funcionalidad (monitoreo).

Año 2023

Metodología – MINTIC – Fases Proceso

MODELO Guías No. 1 y 2 - Transición de IPv4 a IPv6 para Colombia / Aseguramiento Protocolo Ipv6



Objetivo

Celebrar un contrato interadministrativo que permita aunar esfuerzos, realizar el acompañamiento y brindar asistencia técnica mediante herramientas técnicas y el personal especializado en la realización del diagnóstico, el plan de implementación, la capacitación, la implementación y el desarrollo de pruebas de funcionalidad (monitoreo) del protocolo IPv6.

Alcance del Proyecto

En tal virtud, con el fin del desarrollo exitoso del proyecto en cuestión, **DICITEC S.E.M.** se compromete a llevar a cabo las siguientes actividades que se detallan en el alcance de la presente Propuesta:

- ✓ Realizar el Plan de Diagnóstico de la situación actual de los elementos de TI de la entidad.
- ✓ Determinar el grado de compatibilidad del inventario de TI (Hardware, Software).
- ✓ Determinar cuáles equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no pueden soportar IPv6, para determinar el grado de avance de IPv6.
- ✓ Realizar planeación de la transición de los servicios tecnológicos de la Entidad.
- ✓ Validar el estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.
- ✓ Establecer el protocolo de las pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos
- ✓ Analizar la nueva topología de la infraestructura y su funcionamiento.
- ✓ Identificar los esquemas de seguridad de la información y las comunicaciones bajo IPv4 e IPv6.
- ✓ Revisar y dejar consignado en el plan de direccionamiento IPv6, las políticas de enrutamiento y las políticas de seguridad y privacidad de IPv6 entre los segmentos de red internos.
- ✓ Ejecutar y configurar las pruebas piloto de IPv6
- ✓ Habilitar direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase.
- ✓ Configurar los servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.
- ✓ Configurar el protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.
- ✓ Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea la Entidad de acuerdo con los RFC de seguridad en IPv6.
- ✓ Acompañar y apoyar a la entidad en las reuniones con los proveedores de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.
- ✓ Analizar la información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.
- ✓ Preparar a los funcionarios de las Áreas de TI, de conformidad con los planes de capacitación establecidos por la entidad y establecer la sensibilización a las personas de toda la organización en especial a la Alta Dirección, a fin de dar a conocer el nivel de impacto en la implementación del nuevo protocolo.
- ✓ Realizar las pruebas y monitoreo de funcionalidad de IPv6.
- ✓ Realizar las pruebas de funcionalidad del nuevo protocolo utilizando las políticas de seguridad perimetral.
- ✓ Afinar las configuraciones de hardware, software y servicios de la Entidad.
- ✓ Elaborar un nuevo inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6

Obligaciones de DICITEC S.E.M.

Para dar cumplimiento al objeto de este proceso de **DICITEC S.E.M.** se compromete con la Entidad:

- ✓ Prestar la asistencia técnica objeto del contrato interadministrativo que sea celebrado de acuerdo con las condiciones de modo, tiempo, lugar y forma de pago especificadas en este, las cuales se convierten en requisitos mínimos.
- ✓ La solución debe Cumplir con el numeral 7.5.4.1 – XII de la Circular 038 de 2009, el cual cita textualmente "Implementar mecanismos para evitar el uso de información privilegiada, en beneficio propio o de terceros." Teniendo en cuenta que la Entidad tiene normalizado mediante políticas y estándares de seguridad de la información, el buen uso de la información privilegiada.
- ✓ Atender los requerimientos presentados por el supervisor del contrato como encargado del control y vigilancia de este y las demás que sean inherentes al objeto del contrato.
- ✓ Elaborar y entregar a la Entidad el plan de trabajo a realizar durante la duración del proyecto, el alcance y los resultados esperados.
- ✓ Asistir a las reuniones solicitadas por el Supervisor del Contrato en nombre de la Entidad, dejando constancia de estas en las actas correspondientes.
- ✓ DICITEC S.E.M. debe cumplir con las políticas de seguridad de la información establecidas por la Entidad.
- ✓ Asegurar que todos los cursos ofrecidos para la capacitación se realicen sobre las versiones finales entregadas a la Entidad.
- ✓ Cualquier cambio realizado sobre la infraestructura que se utilice para la prestación del servicio de DICITEC S.E.M, deberá ser notificado y autorizado previamente por la Entidad.
- ✓ La información que genere el proyecto será propiedad de la Entidad y será responsabilidad del proveedor el mantener la seguridad correspondiente sobre la misma, dado que el carácter de la información es confidencial.
- ✓ DICITEC S.E.M. debe presentar un plan de trabajo detallado del proyecto a realizarse por fases, el cual será definido en la reunión que llevará a cabo el Supervisor con DICITEC S.E.M. dentro de los cinco días siguientes a la suscripción del acta de inicio, igualmente se deberá identificar el alcance y los resultados esperados.
- ✓ DICITEC S.E.M. debe garantizar que toda la documentación que se genere en el proyecto se entregue en idioma español.
- ✓ Todos los elementos entregables serán entregados al supervisor del contrato en las oficinas de la Entidad o mediante comunicaciones electrónica.
- ✓ DICITEC S.E.M. debe realizar un diagnóstico de la situación actual de la Entidad, que permita definir el plan de trabajo a seguir.
- ✓ DICITEC S.E.M. debe proporcionar asesoramiento en el levantamiento y categorización de la información de los procesos en los que se requiera implementar la solución.
- ✓ DICITEC S.E.M. debe orientar y apoyar la definición de políticas que cubran las necesidades manifestadas por la Entidad.
- ✓ DICITEC S.E.M. debe entregar por escrito, con una semana de anticipación al comienzo de los cursos de capacitación, una relación donde se indique la experiencia del instructor en temas de IPv6. Eventualmente la Entidad podrá solicitar su reemplazo cuando así lo considere, circunstancia en la cual DICITEC S.E.M. dispondrá de una semana para presentar un nuevo candidato.
- ✓ Realizar en conjunto con el área de TIC de la Entidad el levantamiento de una matriz de asignación de responsabilidades en la que se involucren tanto las distintas áreas de la organización, como sus proveedores y el contratista que ejecuta el presente proyecto.
- ✓ Aplicar las RFC correspondientes a políticas de enrutamiento y seguridad de IPv6

FASES DEL PROYECTO DE IMPLEMENTACION DEL PROTOCOLO IPV6

Fase I – Diagnóstico - Planeación de IPv6

Obligaciones

1. Validar el inventario de activos de información de servicios tecnológicos de la Entidad y la interrelación entre ellos. Para esta actividad se requiere tener preparado el inventario de hardware y software, identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6. Para esta etapa se recomienda que para cada elemento del inventario de activos de información se pueda constatar con los fabricantes, y con los terceros si ha lugar, el cumplimiento de IPv6, a través de la certificación que avale el soporte del nuevo protocolo en las infraestructuras de TI.
2. Diseñar y afinar el plan de diagnóstico de IPv6 en la red de la Entidad con base en lo establecido en el inventario de activos de información.
3. Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en la Entidad; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI la Entidad de tal manera que la información recogida de esta tarea sea insumo para el inicio de la fase II de IPv6.
4. Validar el estado actual de los sistemas de información, los sistemas de comunicaciones, los sistemas de almacenamiento y evaluar la interacción entre ellos cuando se adopte el protocolo IPv6.
5. Presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no pueden soportar IPv6.
6. Adquirir el conocimiento sobre las políticas de enrutamiento entre los segmentos de red para IPv4, que tiene en la actualidad en funcionamiento la Entidad.
7. Identificar la configuración y todos los esquemas de seguridad de la red de comunicaciones y sistemas de información.
8. Hacer el análisis detallado del diseño de la red de comunicaciones actual (bajo IPv4) de la Entidad, con la finalidad de identificar claramente las configuraciones y los roles que juegan cada uno de los activos contenidos en los inventarios, proponiendo el nuevo diseño de red sobre IPv6.
9. 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 la Entidad.
10. Definir los lineamientos de implementación de IPv6 en concordancia con la política de seguridad de información y los controles de seguridad informática de la Entidad.
11. Llevar a cabo el recuento detallado de las características principales de las aplicaciones contenidas en el inventario que provea la Entidad, identificando aspectos técnicos como el lenguaje de programación en el que se desarrolló, qué tipo de bases de datos consulta, la arquitectura sobre la cual está desplegada y la forma en la que se integra con otras aplicaciones y los principales servicios de la red (DNS, DHCP y AD).
12. Planear el proceso de transición 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 (Local o en la nube), Validación del Servicio de la Central Telefónica, Sistemas Ininterrumpidos de Potencia, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información, NTP, Enrutamiento, Canales Electrónicos Transaccionales, Canales de comunicación y topología de red general y red de oficinas, servicios de movilidad, seguridad lógica, proveedores, IVR´s y cámaras Servicios de ambiente colaborativo.

13. Generar el plan detallado del proceso de transición de esta fase hacia IPv6 con base en el plan de diagnóstico y el diseño de la red de comunicaciones, mencionados en la fase anterior.
14. Tomar como base los procedimientos de implementación de estos servicios y las RFC3 aplicaciones identificadas en esta fase, con base en los estándares de IPv6.
15. Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el plan de transición.
16. Asignar un pool de direcciones para el Municipio.

Entregables contemplados (Detalle)

1. Informe de compatibilidad con el protocolo IPv6 de los inventarios de activos de TI - información, de equipos de comunicaciones y de aplicaciones de la Entidad, (Según el inventario de cada elemento de hardware y software Red de comunicaciones, sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros entregado por la Entidad).
2. Realizar el plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular para aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, dando resultado las recomendaciones para la adquisición de los elementos de comunicaciones, de cómputo y almacenamiento.
3. Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones (Que tan preparada se encuentra la Entidad en tema de adopción de IPv6).
4. Documento denominado Plan de Direccionamiento que será aplicado en la implementación del protocolo IPv6 en la infraestructura tecnológica de la Entidad. Este plan deberá contemplar la proyección de ajuste tecnológico programada para la Entidad a corto, mediano y largo plazo.
5. Documento denominado “Plan Técnico Implementación y/o Adopción del protocolo IPv6” (PTI) en el que se evidencie claramente la estrategia de implementación, el detalle de las configuraciones a aplicar en los equipos de comunicaciones a partir de la información recolectada en el Piloto Preliminar de Pruebas (PPP) Entidad.
6. Documento que define los lineamientos de implementación de IPv6 en concordancia con la política de seguridad de información y los controles de seguridad informática de la Entidad, basado en la Identificación y el análisis exhaustivo los potenciales riesgos de la implementación del protocolo IPv6 en la infraestructura tecnológica de la Entidad.
7. Documento de diseño detallado del plan de contingencia para la implementación que incluya una estrategia clara de Roll-Back o “Marcha atrás”.
8. Cronograma de Desarrollo del Piloto Preliminar de Pruebas (PPP) a ser llevado a cabo en la Entidad.
9. Documento de asignación a la Entidad del pool de direcciones IPv6 de acuerdo con las necesidades de ella y el resultado de la prospección de la red Municipal (Topología de la red proyectada) para los próximos 16 años.

Fase II - Implementación del Protocolo IPv6

Obligaciones

1. Diseñar con esta información el set de pruebas funcionales específicas para cada aplicación que irán contenidas en el Piloto Preliminar de Pruebas (PPP).
2. Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, equipos de cómputo, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 de la Entidad.
3. Preparar una zona controlada para realizar pruebas de funcionalidad del nuevo protocolo de comunicaciones IPv6, es importante aislar un segmento de red o crear un nuevo segmento de red, el cual debe permitir aceptar cambios y activaciones necesarias para confirmar la funcionalidad de IPv6 sin afectar el ambiente de producción de los usuarios.
4. Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet – ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral, desde el interior de las redes LAN, hacia

el exterior de las redes WAN a fin de garantizarla generación de tráfico de IPv6 ante la comunidad de Internet. La gestión, convocatoria y notificación a los proveedores de servicios de Internet – ISP es responsabilidad del contratante, toda vez que el contratista no tiene autonomía ni relación contractual con este tipo de proveedores, el cumplimiento de esta obligación por parte del contratista no está supeditado en ninguna medida al cumplimiento de los terceros mencionados – proveedores de servicio de internet (ISP).

5. Realizar el diseño de la nueva topología de la red con base en los lineamientos del nuevo protocolo IPv6 bajo 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 la Entidad.
6. 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, teniendo en cuenta el inventario de los activos de información de cada una de las infraestructuras de TI de la Entidad y teniendo en cuenta el diseño de la red bajo IPv6 previamente definido en la Fase I.
7. Ejecutar un Piloto Preliminar de Pruebas (PPP) que represente de la manera más fiel y simplificada la red de comunicaciones actual de la Entidad en un ambiente de pruebas aislado, con el objeto de evidenciar cómo se comportan los activos de información de la Entidad haciendo uso del nuevo protocolo bajo las configuraciones que estén vigentes en la actualidad. Este piloto incluirá las pruebas de funcionalidad de las aplicaciones de la Entidad que estén contenidas en los inventarios.
8. Ejecutar el Piloto Preliminar de Pruebas (PPP) en un ambiente de preproducción con el fin de afinar las configuraciones que deben ser aplicadas en la infraestructura de producción de la Entidad.
9. Diseñar y socializar el detalle de las configuraciones que deberán ejecutar los proveedores de conectividad (ISP) y de Infraestructura como servicio (IaaS) por solicitud de la Entidad a partir de los hallazgos evidenciados a partir de la ejecución del Piloto Preliminar de Pruebas (PPP) en el ambiente de preproducción y de acuerdo con la matriz de responsabilidades.
10. Activar las políticas de seguridad con la ejecución de pruebas de seguridad que permitan identificar vulnerabilidades derivadas de la implementación del protocolo IPv6 en la infraestructura tecnológica de la Entidad.
11. Ejecutar las pruebas del Plan de Contingencia para la Implementación que sean viables para garantizar que todos los escenarios están contemplados y los planes de roll back o “marcha atrás” funcionan adecuadamente.
12. Validar la funcionalidad en IPv6 de los siguientes servicios y aplicaciones de la Entidad sobre IPv6: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servicios Voz sobre IP, Servidores de Monitoreo, Servicios con sistema IPTV, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicios que soporten canales TDT, Servicio de Respaldo, Servicio de Comunicaciones Unificadas, Servicios VPN, Integración entre Sistemas de Información, Sistemas de Almacenamiento, Servicios de Administración de Red, Sistemas en la Nube y Sistema Ininterrumpido de Potencia
13. Documentar, acompañar y asegurar que la Entidad inicia la transición al protocolo IPv6 en coexistencia con IPv4 bajo la modalidad de transición endoble pila.
14. Actualizar el inventario de activos de información luego de implementado el protocolo Ipv6 y realizar el diseño de la nueva tecnología con base en los lineamientos del nuevo protocolo IPv6.

Entregables contemplados (Detalle)

1. Informe de resultados de las configuraciones realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento en el marco del piloto preliminar de pruebas.
2. Informe de análisis de riesgos de la implementación del protocolo ipv6.
3. Informe de resultados de las pruebas de seguridad y del plan de contingencia.
4. Plan de contingencia para implementación de protocolo ipv6.
5. Manuales escritos y en formato digital con recomendaciones de seguridad posteriores a la implementación.
6. Informe de resultados de las pruebas de preproducción y producción.
7. Documento con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta fase, incluye las configuraciones a realizar sobre el canal (canales) de comunicaciones con acceso a internet.

8. Documento denominado direccionamiento IPv6 definitivo aplicado a la infraestructura de red (Wan y Lan)

Fase III - Pruebas de Funcionalidad (Monitoreo)

Obligaciones

1. Ser soporte con el monitoreo de adopción del protocolo Ipv6 en coexistencia con IPv4.
2. Monitorear efectuando el debido seguimiento y certificación de afinamiento de la transición.
3. Monitorear el correcto funcionamiento de las configuraciones sobre equipos con el acompañamiento del equipo de soporte y administración de cada sistema por parte de la Entidad.
4. Realizar las pruebas de funcionalidad del nuevo protocolo utilizando las políticas de seguridad perimetral, de seguridad en redes locales, de servidores de cómputo, servidores de comunicaciones y equipos de comunicaciones, equipos de almacenamiento y presentar el informe de las pruebas realizada.
5. Monitorear el correcto funcionamiento en producción del entorno IPv4 (maquinas/ aplicaciones/redes, entornos que no fue posible migrar a IPv6), validando el correcto funcionamiento de cada uno de los componentes de la red, activos HD y SF, servicios, aplicaciones y plataformas TI, que debieron quedar en IPV4 validando su correcto y transparente funcionamiento con la plataforma migrada a IPv6.
6. Realizar la estabilización de la implementación a lo largo de esta fase.

Entregables contemplados (Detalle)

1. Reporte detallado del seguimiento, atendiendo los lineamientos establecidos en la guía No. 1 y 2 - transición de ipv4 a ipv6 para Colombia, o la versión más reciente del documento emitido por Mintic para el cumplimiento de esta obligación. Estos reportes deberán ser entregados durante el tiempo de ejecución (monitoreo, seguimiento y afinamiento de la transición y adopción).
2. Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación.
3. 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.
4. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.
5. Acompañamiento durante el mes siguiente a la ejecución de la fase de monitoreo, con el objetivo de verificar y realizar acciones que la puesta en marcha de esta versión exija. Esta actividad de acompañamiento se realizará con el acompañamiento del supervisor del contrato.

Fase – Capacitación

Obligaciones

1. Diseñar, proponer, ajustar y desarrollar para todos los funcionarios el plan de sensibilización del proyecto de implementación del Protocolo de IPv6 de la Entidad, estableciendo el objetivo general, los objetivos específicos, la metodología, el contenido temático, la duración, el material de formación y definición de los requisitos de cumplimiento de asistencia para ser certificado.
2. Diseñar, proponer, ajustar y desarrollar el Plan de Capacitación en IPv6 a los funcionarios del área de TIC de la Entidad, estableciendo el objetivo general, los objetivos específicos, la metodología, el contenido temático, la duración, el material de formación y definición de los requisitos de cumplimiento de asistencia para ser certificado por la entidad capacitadora.

Entregables contemplados (Detalle)

1. Plan de sensibilización para todos los funcionarios de la Entidad.
2. Plan de Capacitación al Programa de capacitación a los funcionarios de las áreas de TIC de la Entidad con fechas definidas.
3. Lista de asistencia que contenga la firma de asistentes y del DICITEC S.E.M., fecha y duración de la capacitación.
4. Material de estudio entregado a todos los funcionarios de la Entidad en medio digital.
5. Certificado de Asistencia de los funcionarios del área de TIC a la capacitación.

CONSIDERACIONES FINALES

1. Sí en la etapa de diagnóstico se encuentran activos o sistemas de la Entidad que no soporten o en donde no sea viable la implementación de IPv6 como por ejemplo entre otros que el Sistema Operativo o la Base de datos no sea compatible con IPv6, o porque no es posible que el ISP entregue la visibilidad en la Internet de IPS u otros casos, se dejaran documentadas las recomendaciones del caso y se entregarán las guías paso a paso de puesta a punto y capacitación, para que a futuro la Entidad pueda hacerlo cuando sus sistemas o activos sean compatibles con el protocolo IPv6.
2. Todas las actividades contempladas en el presente documento acatan las recomendaciones de organismos nacionales e internacionales como la UIT, ICANN, LACNIC, IETF, OECD, y de la versión más reciente del Manual de Gobierno en Línea, i), Guía de Transición de IPv4 a IPv6 para Colombia y ii) Guía de aseguramiento del Protocolo IPv6, en sus versiones de abril de 2021.

PLAZO DE EJECUCIÓN

Este proyecto de acuerdo con las experiencias previas requiere para su desarrollo un tiempo estimado de tres (3) meses desde la firma del acta y cubre las fases: Diagnóstico, plan de implementación, Implementación - Pruebas de Funcionalidad, Monitoreo del protocolo IPV6 y Capacitación.

PROPUESTA ECONÓMICA

VALORACION DEL PROYECTO	
Concepto	**Valor**
Fase I - Diagnóstico y Planeación de la Implementación IPv6	**$ 55.058.824**
Fase II - Implementación del Protocolo IPv6	**$ 61.941.176**
Fase III - Pruebas de Funcionalidad (Monitoreo)	**$ 13.764.706**
Capacitación	**$ 6.882.353**
Valor Proyecto	**$ 137.647.059**
IVA	**$ 26.152.941**

FORMA DE PAGO

Primer Pago equivalente al **40%** del valor a la presentación del Plan de Trabajo y Cronograma

Segundo y Último Pago equivalente al **60%** del valor al terminar el proceso previa Acta de Recibo a Satisfacción firmada por el supervisor del contrato.

VALORES AGREGADOS

BENEFICIOS GENERADOS POR DICITEC S.E.M	
1	1. Un (1) Pool de direcciones IPV6 requerido por la entidad. 2. Asignación por diecisiete (16) años del pool de direcciones requerido por la entidad.