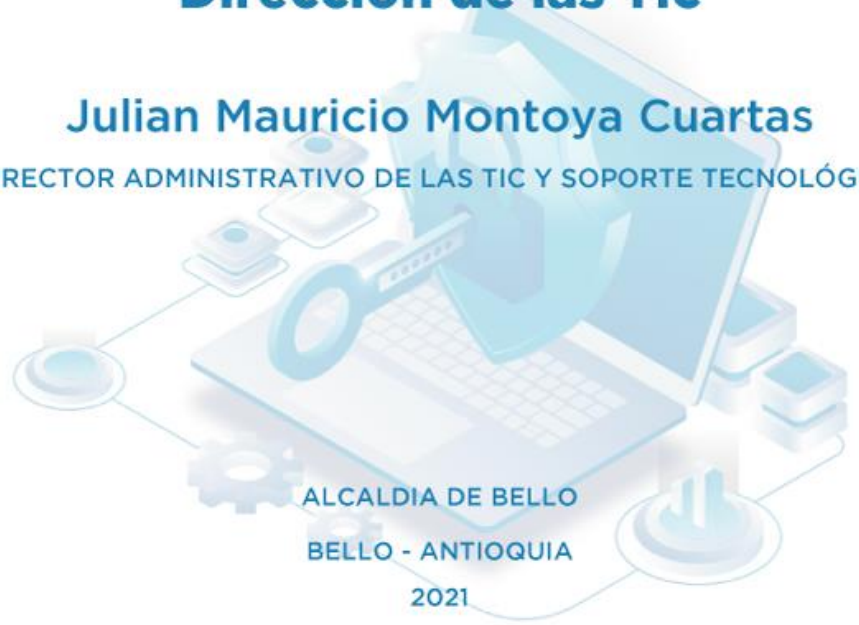
Código:	D-GR-06
Versión:	01

Plan de tratamiento de Riesgos de la seguridad de la información Vigencia 2021 - 2023

Dirección de las Tic

Julian Mauricio Montoya Cuartas

DIRECTOR ADMINISTRATIVO DE LAS TIC Y SOPORTE TECNOLÓGICO



ALCALDIA DE BELLO

BELLO - ANTIOQUIA

2021

1. INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos de Seguridad de la Información da cuenta de una serie de procedimientos que la Alcaldía Municipal de Bello realizará a fin de implementar la estrategia de gobierno digital alrededor del componente de seguridad y privacidad de la información y gestión de los riesgos, cuyo principal objetivo es proteger los derechos de los usuarios de la entidad, mitigar los riesgos, y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

En la situación actual que viven los sistemas de información es obligatorio implementar unas estrategias a nivel interno que pueda salvaguardar la información sensible de la entidad para que se pueda cumplir todo lo misional y que los procesos funcionen con normalidad. Es de vital importancia para cada entidad acogerse a la política de gobierno digital, teniendo en cuenta que tiene todos los lineamientos y estandarizaciones para que cada entidad pueda cumplir y tener una hoja de ruta clara en estos aspectos.
La política de Gobierno Digital expedida por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un estado y ciudadanos competitivos, proactivos innovadores, que generen valor público en un entorno de confianza digital. Teniendo en cuenta lo anterior, la implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.
El documento denominado Modelo de Seguridad y Privacidad de la Información, MSPI, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, nos indica que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

2. OBJETIVOS

Objetivo General

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad de la Información que permita mitigar los riesgos informáticos de la entidad sobre los activos de las tecnologías de la información que soportan los servicios internos y externos del municipio de Bello desde el enfoque de ciberseguridad y prevención de eventos de seguridad, en función de garantizar la estabilidad de los sistemas a los ciudadanos y usuarios.

Objetivos Específicos

- Gestionar los eventos de seguridad de la información para detectar y clasificar con eficiencia los incidentes de la alcaldía municipal.
- Cumplir con la normatividad colombiana y de la política de Gobierno digital.
- Administrar los riesgos de seguridad y privacidad de la información.
- Definir los principales activos a proteger en la alcaldía del municipio de Bello.
- Identificar las principales amenazas que afectan a los activos.

3. ALCANCES Y LIMITACIONES

ALCANCES

Lograr el compromiso de la alta dirección de la Alcaldía Municipal para emprender

la implementación plan de gestión del riesgo en la seguridad de la información.

- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.
- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

LIMITACIONES

Los recursos presupuestales necesarios para para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Alcaldía Municipal de Bello.

4. GESTIÓN DE RIESGOS

IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.
La alcaldía Municipal de Bello, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos

informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la alcaldía Municipal de Bello, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

DEFINICION GESTIÓN DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DESEGURIDAD DE LA INFORMACIÓN

Figura 1 Proceso para la administración del riesgo.

IDENTIFICACIÓN DEL RIESGO

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

SITUACION NO DESEADA

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, porintromisión
- Incendio en las instalaciones de la empresa por desastre natural o de maneraintencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información

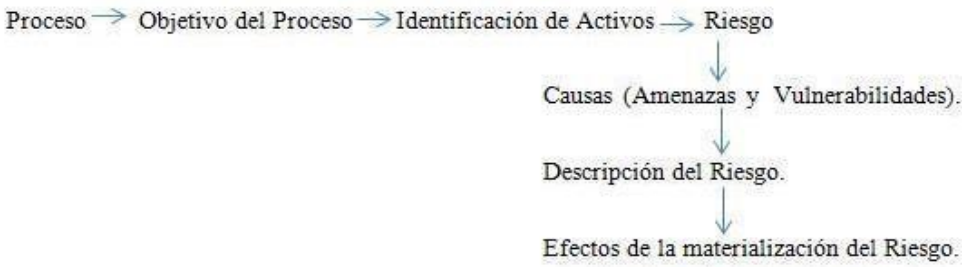
5. ORIGEN DEL PLAN DE GESTION

Debido al riesgo de pérdida de información es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.
El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las alcaldías y entidades públicas en el país. Es por ello necesario que la alcaldía municipal de Bello cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma alcaldía.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto unservicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridadde la información.

IDENTIFICACIÓN DEL RIESGO



6. ANALISIS DE VULNERABILIDAD

DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Alcaldía de Bello se encontraron otras

amenazas e impactos como los siguientes:

- La red de internet implementada no es la más adecuada. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes, el internet lento y la perdida de señal afecta de forma directalos tiempos de producción laboral y desempeño de las funciones.

- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de la Alcaldía.

- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

- Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidosafectan los activos de información y de informática.

- Las UPS existentes tienen inconvenientes y por ende generan desconexiones eléctricas en los servidores, caídas y podrían ocasionar perdida de información.

- En algunos papeles reutilizables se encontró información que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- En algunas secretarías de la alcaldía no existen los equipos de cómputo suficientespara el uso de la totalidad de su personal. Existe un riesgo de pérdida de informaciónya que deben compartir los recursos informáticos.

- La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.

- No hay control para el uso de memorias portátiles en los equipos de la Alcaldía, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en la alcaldía.

- Existe desconocimiento con respecto a la instalación de dispositivos de red como routers inalámbricos o switches, esto requiere un acompañamiento de personal de tecnología para tener una asesoría técnica y una buena configuración.

- No existe personal de las TIC encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la

informaciónpara la Alcaldía.

- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.
- No existe un plan de continuidad que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la alcaldía. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores).

7. PROPUESTA DE SEGURIDAD

- Implementar controles de seguridad para operar los sistemas en la alcaldía con buenas prácticas y orientado al cumplimiento de la política de gobierno digital.

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.

- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.

- Socializar las políticas de seguridad y privacidad de la información con el personal de la alcaldía.

- Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.

- No compartir los usuarios y las contraseña ya que son intransferibles y de uso personal.

- Implementar un nube o servidor compartido para guardar la información laboral de cada funcionario de la alcaldía municipal.

- Asignar la función para dirigir la creación y el control de un sistema de seguridad y privacidad de la información en la Alcaldía junto con otras actividades propias del área.

8. PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- Capacitar al personal en el almacenamiento de copias de seguridad de la información local manejada en las diferentes secretarías.

- Obtener una nube dedicada para la información de la alcaldía con el fin de tener un respaldo en caso de accidentes en los servidores.

- Contar con un plan alternativo que asegure la continuidad de la actividad en caso que ocurran incidentes graves.

- Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un

  Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

9. PLAN DE CONTINUIDAD

- Socializar con los directivos, secretaría general y oficina de las TIC la importancia del Plan de Continuidad de la seguridad de la información, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización

de los eventos identificados.

- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red

- Detectar el riesgo y plantear controles y efectuar las implementaciones respectivas (Mitigar Riesgos).

- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

- Política de copia de seguridad de datos, procedimientos de almacenamiento fuera de la alcaldía.

- Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

IDENTIFICACIÓN DE LOS RIESGOS PARA LA ALCALDÍA DE BELLO

ACTIVO	RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Bases de datos de nómina	Pérdida de la integridad	Pérdida de datos por modificación, alteración y eliminación de información de la base de datos de nómina de entidad.	**Información**	**1.**Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario **2.**Gestión deficiente de las contraseñas **3.**Tablas de contraseñas sin protección	Pérdida de Dinero, Retraso en el pago de nómina, Demandas por incumpliendo de salarios, Plan tortuga funcionarios, Generación de desconfianza a los ciudadanos.
Servidor de base de datos	Pérdida de confidencialidad	Acceso no autorizado al servidor	Hardware	Ausencia de un eficiente control de cambios en la configuración	Deficiente control de cambios en la configuración Explotación de vulnerabilidades por falta de actualizaciones se seguridad y hardening
	Pérdida de confidencialidad	Acceso no autorizado al servidor, donde se encuentran los datos de los contribuyentes para el pago de impuestos.	Hardware	**1.**Conexiones de red pública sin protección **2.**Arquitectura insegura de la red **3.**Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	**1.** Desconfianza ciudadanos, robo de información, cifrado de información (Ramsonware) **2.** Robo de información, activación de malware, escalamiento de privilegios, modificación y eliminación de datos.

ACTIVO	RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Servidor Portal Web	Pérdida de disponibilidad	Servidor fuera de servicio, impidiendo que los usuarios autorizados no tengan acceso.	**Hardware**	**1.**Arquitectura insegura de la red **2.**Ausencia de mecanismos de monitoreo	Impedimento para la descarga de los formatos y demás documentos.
Servidores de datos, equipos de cómputo, discos duros externos	**Pérdida de disponibilidad**	Perdida de disponibilidad a los servidores por obsolencia o daño de hardware, equipos o discos de respaldo	**Hardware**	1. **Obsolecencia de equipos** 2. **Desconexiones de la red eléctrica.** 3. **Descargas eléctricas sin regulación.**	**Perdida de información, daño físico, falta de disponibilida de la información.**
Servidores de datos y de servicios web.	**Falta de acceso**	Descargas de Software, descargas de adjuntos en correo electrónico, Ataques de denegación del servicio.	**Hardware**	**Falta de controles de seguridad, desconocimiento de los usuarios en buenas prácticas de seguridad, exposición de servicios web sin controles, ejecución de software malicioso.**	**Perdida o secuestro de datos, perdida de información sensible, detrimento patrimonial para la entidad (Ransomware).**
Página web, servidores de datos, servidores web.	**Falta de servicio eléctrico.**	No acceso a los servicios por una caída en la red eléctrica, caída del servicio en el proveedor de internet, falta de redundancia eléctrica o UPS.	**Hardware**	**Inconvenientes en la red de electricidad, falta de una UPS, inconveniente con los anillos de Internet o del servicio.**	**Inconvenientes con la comunidad por falta de servicios, detrimento patrimonial, sanciones económicas.**

10. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

- El análisis permitió identificar que se desconocen y poco se cumplen las políticas de
- seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:
-
- Socialización y capacitación de temas de Seguridad.
- Generar un Ambiente con la seguridad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.
-

11. PLAN DE CAPACITACIÓN

- Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

- Detectar los requerimientos tecnológicos. Determinar objetivos de capacitación para el personal

- Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.

- Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad

- Evaluar los resultados de cada actividad.

12. PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existentes actualmente por la IPv6 debido a que algunos equipos informáticos de la alcaldía de Bello no soportan la nueva versión de IP.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En ese orden de ideas, este documento, presenta los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas organizaciones del Estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país.

Para abordar esta temática se empezará por comentar que desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando una 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 elementos 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, hace 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.

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.

Así mismo, para atender esta necesidad inminente de innovación tecnológica en el país, el Mintic, mediante este instrumento, desea proyectar los lineamientos necesarios para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del estado, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Circular 002 de Julio de 2011, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

Finalmente, el mismo documento, será el apoyo al plan guía de acompañamiento, que facilitará las acciones necesarias para la adopción del nuevo protocolo en las entidades del país, partiendo de la fase inicial de diagnóstico de las infraestructuras de TI (Hardware y el Software), hasta la fase final que contemple la implementación y el monitoreo del nuevo protocolo en las distintas instituciones.

Planeación de IPv6

La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con el inventario de activos de información y se consolida con el plan de diagnóstico de las infraestructuras de TI de las Entidades; para ello se recomienda tener en cuenta el modelo de referencia para la adopción de IPv6, de la gráfica 1.

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 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.
• Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de las entidades del estado con base en lo establecido en el inventario de activos de información.
• 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 las Entidades; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI las entidades de tal manera que la información recogida de esta tarea sea insumo para el inicio de la fase II de IPv6.
• Identificar la topología actual de la red y su funcionamiento dentro de la organización y con base en esto, proponer el nuevo diseño de red sobre IPv6.
• 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 los anteriores puntos.
• 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, Servicios de ambiente colaborativo; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC3 de IPv6.

• 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.

• 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 soportar IPv6.

• Identificar la configuración y todos los esquemas de seguridad de la red de comunicaciones y sistemas de información.

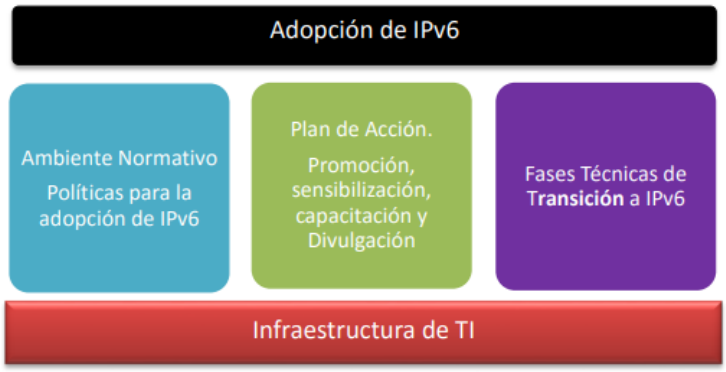
• Revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el firewall respectivo de cada entidad, se recomienda en todo caso revisar los RFC correspondientes a políticas de enrutamiento y seguridad de IPv6.

• 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 por cada Entidad. 3 RFC: “Request For Comments” Solicitud de Comentarios: para documentar requerimientos técnicos

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

• 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.
• Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el plan de transición.
• Preparar a los funcionarios de las Áreas de TI, de conformidad con los planes de capacitación establecidos por cada entidad para el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto en la implementación del nuevo protocolo, de conformidad con el siguiente modelo de referencia de adopción de IPv6.
• Las entidades deberán entrar en sincronización y operación con los ISP (Proveedores de Servicios de Internet) con el fin de definir las estrategias de enrutamiento de IPv6 nativo.



Gráfica 1. Modelo de Referencia para la Adopción de IPv6

13. ENTREGABLES DE ESTA FASE

- Plan de trabajo para la adopción de IPv6 en toda la organización.
- Plan de diagnóstico que debe contener los siguientes componentes:
    - Inventario de TI (Hardware y software) de cada Entidad diagnosticada. o Informe de cumplimiento de IPv6 por cada elemento de hardware y software (Red de comunicaciones,

sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros).

- Recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6.
- Informe con el plan de direccionamiento en IPv6 o 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 o 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).
- 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 las entidades.

Fuente: guía de transición MINTIC

En la actualidad la alcaldía de Bello se encuentra en la fase de planeación, con el inventario de activos, equipos, servidores y dispositivos de infraestructura. También con la gestión de la membresía y la proyección de la compra del pool de direcciones IPV6.

14. NOTAS DE CAMBIO

Elaboró:	Julián Mauricio Montoya Cuartas – Director TIC	Fecha:	2021-09-15
Revisó:	Julián Mauricio Montoya Cuartas – Director TIC	Fecha:	2021-09-15
Aprobó:	Julián Mauricio Montoya Cuartas – Director TIC	Fecha:	2021-09-15