	INSTITUTO DE MOVILIDAD DE PEREIRA **NIT 816000558** **CONTROL DE LEGALIDAD** **FORMATO DE SEGUIMIENTO**
Versión: 0	**Vigencia: 07-2018**

ACTA DE SEGUIMIENTO No 10

FECHA DE SEGUIMIENTO:	02 DE DICIEMBRE DEL 2022
PERÍODO DE SEGUIMIENTO:	DEL 28 DE OCTUBRE AL 27 DE NOVIEMBRE DEL 2022
NOMBRE DEL CONTRATISTA:	GRUPO EMPRESARIAL EJETIC S.A.S
NÚMERO DE CONTRATO:	128-2022
TIPO DE CONTRATO:	PRESTACION DE SERVICIOS
VALOR TOTAL CONTRATO:	$ 18,794.997.oo
SUPERVISOR:	DANY ALEXANDER ORREGO CRUZ
FECHA INICIACIÓN DE CONTRATO:	28-01-2022
DURACIÓN CONTRATO:	NUEVE (09) MESES, SIN SUPERAR EL 31/12/2022
FECHA TERMINACIÓN CONTRATO:	27-10-2022
ADICION EN VALOR	$4.176.666
ADICION EN TIEMPO	DOS (02) MESES

OBJETO DEL CONTRATO
SEGUIMIENTO A LAS ACTIVIDADES DESARROLLADAS POR EL CONTRATISTA (Ver obligaciones del contratista)
ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO "SOFTWARE PARA LA ADOPCIÓN DE LA POLÍTICA DE GOBIERNO DIGITAL - SAPGD" Y CONTINUIDAD DE LA FASE I DEL PROYECTO DETRANSICIÓN DEL PROTOCOLO IPV4 AL PROTOCOLO IPV6 EN EL INSTITUTO DE MOVILIDAD DE PEREIRA
SEGUIMIENTO A LOS RIESGOS EXPUESTOS EN EL PRESENTE CONTRATO (Ver estudios previos y especificaciones tecnicas)

EVIDENCIA ANEXA
Se anexa factura de venta No. FE No 148

BALANCE DEL CONTRATO	
VALOR TOTAL	$ 18.794.997
VALOR ADICIONADO	$ 4.176.666
VALOR EJECUTADO	$ 18.794.997
VALOR A PAGAR	$ 2.088.333
VALOR POR EJECUTAR	$ 2.088.333

OBSERVACIONES:

FIRMA DEL SUPERVISOR
Número de Anexos:

FIRMA DEL CONTRATISTA

FACTURA ELECTRÓNICA DE VENTA

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE : 51ca21cb9580247949d7f56d5a04940031b16f75d7703231fbab31e3aa7d5e a4fb31d0118327575d8232505c49e149ef

Número de Factura: FE-148
Fecha de Emisión: 28/11/2022
Fecha de Vencimiento: 06/12/2022
Tipo de Operación: 10 - Estándar

Forma de pago: Crédito
Medio de Pago: Transferencia Débito Bancaria
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: GRUPO EMPRESARIAL EJETIC S.A.S
Nombre Comercial: GRUPO EMPRESARIAL EJETIC S.A.S
Nit del Emisor: 901251836
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal: R-99-PN
Responsabilidad tributaria: 01 - IVA
Actividad Económica: 6209

País: Colombia
Departamento: Risaralda
Municipio / Ciudad: Pereira
Dirección: CL 19 7 75 OF 211 ED BRAULIO LONDOÑO
Teléfono / Móvil: 3142281086
Correo: jorgem.valenciamesa@gmail.com

Datos del Adquiriente / Comprador

Razón Social: INSTITUTO DE MOVILIDAD DE PEREIRA
Nombre Comercial: INSTITUTO DE MOVILIDAD DE PEREIRA
Tipo de Documento: NIT
Número Documento: 816000558
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: O-23
Responsabilidad tributaria: 01 - IVA

País: Colombia
Departamento: Risaralda
Municipio / Ciudad: Pereira
Dirección: CR 14 17 60
Teléfono / Móvil: 3294920
Correo: sistemas@transitopereira.gov.com

Detalles de Productos

								IMPUESTOS				
Nro.	**Código**	**Descripción**	**U/M**	**Cantidad**	**Precio unitario**	**Descuento detalle**	**Recargo detalle**	**IVA**	**%**	**INC**	**%**	**Precio unitario de venta**
1	001 - Licencia de Uso de Software para la Adopción de la Política de Gobierno Digital del Estado Colombiano	Eje Básico - Licencia de uso del Software para la Adopción de la Política de Gobierno Digital, inscrito en la Dirección Nacional de Derecho de Autor mediante el Certificado: 137261, con Fecha Registro 19-feb-2019	NIU	1,00	$ 2.088.333,00	$ 0,00	$ 0,00					$ 2.088.333,00

Descuentos y Recargos Globales

Nro.	Tipo	Código	Descripción	%	Valor

Información Complementaria

Nro	Nombre Campo	Valor Campo

Anticipos

Nro	Valor	Fecha recibido

Referencias

Tipo de Documento Referencia	Número Referencia	Fecha Referencia

Notas Finales

Los servicios antes descritos son un servicio excluido de IVA de conformidad con los numerales 20 y 21 del Artículo 476 del Estatuto Tributario
Linea de negocio: Factura mes de Noviembre

Datos Totales

Documento validado por la DIAN 2022-11-28 12:39:16
Documento generado el: 2022-11-28 12:39:15
Generado por:Solución Gratuita DIAN Nit:800.197.268

MONEDA	COP
TASA DE CAMBIO	

Subtotal		2.088.333,00
Descuento detalle		0,00
Recargo detalle		0,00
Total Bruto Factura		2.088.333,00
IVA		0,00
INC		0,00
Bolsas		0,00
Otros impuestos		0,00
Total impuesto (=)		0,00
Total neto factura (=)		2.088.333,00
Descuento Global (-)		0,00
Recargo Global (+)		0,00
Total factura (=)	**COP $**	$ 2.088.333,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	83.533,32
Rete IVA	0,00
Rete ICA	0,00

Numero de Autorización: 18764037702388 Rango desde: 141 Rango hasta: 300 Vigencia: 2023-10-11

EJETIC
GRUPO EMPRESARIAL
Transformando la Sociedad

Tel:3142281086
Correo: gerencia@ejetic.com.co
Dirección:Calle 19 7-75 oficina 211 Edificio Braulio Londoño

Pereira, Diciembre 16 de 2022

Señores
INSTITUTO DE MOVILIDAD DE PEREIRA
Ciudad

ASUNTO: Certificación de pago de aportes al sistema de seguridad social y parafiscales

Para dar cumplimiento a lo previsto en el artículo 50 de la Ley 789 de 2002 y el artículo 23 de la Ley 1150 de 2017, el representante legal y el contador, se permiten certificar que:

GRUPO EMPRESARIAL EJETIC SAS NIT 901.251.836

Ha realizado los pagos de seguridad social y aportes parafiscales correspondientes y hasta este momento se encuentra a paz y salvo. Adicionalmente certifico que durante los últimos seis (6) meses calendarios legalmente exigibles, la empresa ha realizado el pago de los aportes anteriormente descritos exigidos por la Ley. **Esta certificación se presenta bajo la gravedad del juramente, entendiendo las implicaciones legales que esto conlleva.**

Mil gracias por la atención prestada, estaré atento a los requerimientos.

Atentamente,

JORGE MARIO VALENCIA MESA
Gerente
Grupo Empresarial Ejetic S.A.S.
Cel: 3142281086
E-mail: gerencia@ejetic.com.co

LEIDY ELIANA CUENCA MONTOYA
Contador
Grupo Empresarial Ejetic S.A.S.
Cel: 3044957018
E-mail: contabilidad@ejetic.com.co

ASOPAGOS s.a.

RAZON SOCIAL :	GRUPO EMPRESARIAL EJETIC SAS
IDENTIFICACION:	NI-901251836
COD. DEPENDENCIA O SUCURSAL:	0
NOM. DEPENDENCIA O SUCURSAL:	0
FECHA GENERACION REPORTE:	2022-12-27
FECHA LIMITE DE PAGO:	2022-12-12
FECHA DE PAGO:	2022-12-15
ENTIDAD DE PAGO:	BBVA COLOMBIA S.A.
PERIODO PENSION:	2022-11
PERIODO SALUD:	2022-12
NUMERO PLANILLA:	24980281
TOTAL COTIZANTES:	6
REFERENCIA DE PAGO (PIN):	24980281
TIPO DE PLANILLA:	E

CODIGO ENTIDAD	NIT	NOMBRE	NUMERO AFILIADOS	FONDO SOLIDARIDAD	FONDO SUBSISTENCIA	TOTAL INTERESES	VALOR PAGAR SIN INTERESES	VALOR PAGAR
EPS002	800130907	SALUD TOTAL	1	$ 0	$ 0	$ 100	$ 12.000	$ 12.100
EPS005	800251440	SANITAS	1	$ 0	$ 0	$ 300	$ 72.000	$ 72.300
EPS010	800088702	EPS SURA	2	$ 0	$ 0	$ 700	$ 203.200	$ 203.900
EPS018	805001157	SOS-EPS	1	$ 0	$ 0	$ 200	$ 40.000	$ 40.200
EPS042	900226715	COOSALUD	1	$ 0	$ 0	$ 100	$ 9.400	$ 9.500
Subtotal Salud		5	6	$ 0	$ 0	$ 1.400	$ 336.600	$ 338.000
230201	800229739	PROTECCION	2	$ 0	$ 0	$ 700	$ 197.400	$ 198.100
230301	800224808	PORVENIR	3	$ 20.000	$ 20.000	$ 3.000	$ 900.800	$ 903.800
25-14	900336004	COLPENSIONES	1	$ 0	$ 0	$ 1.000	$ 288.000	$ 289.000
Subtotal Pensión		3	6	$ 20.000	$ 20.000	$ 4.700	$ 1.386.200	$ 1.390.900
14-11	890903790	ARL SURA	6	$ 0	$ 0	$ 200	$ 44.200	$ 44.400
Subtotal ARL		1	6	$ 0	$ 0	$ 200	$ 44.200	$ 44.400
CCF44	891480000	COMFAMILIAR RISARALDA	6	$ 0	$ 0	$ 1.100	$ 336.600	$ 337.700
Subtotal CCF		1	6	$ 0	$ 0	$ 1.100	$ 336.600	$ 337.700
			Total a pagar	$ 20.000	$ 20.000	$ 7.400	$ 2.103.600	$ 2.111.000

FECHA DE PAGO DEL SIGUIENTE MES:	07/01/2023

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Certificado No:

9626497EDEA19DB1

LA REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

UNIDAD ADMINISTRATIVA ESPECIAL

JUNTA CENTRAL DE CONTADORES

CERTIFICA A:
QUIEN INTERESE

Que el contador público **LEIDY ELIANA CUENCA MONTOYA** identificado con CÉDULA DE CIUDADANÍA No 1093223832 de SANTA ROSA DE CABAL (RISARALDA) Y Tarjeta Profesional No 257885-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de Inscripción.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS ******************************
****
****

EL CONTADOR PUBLICO NO HA CUMPLIDO CON LA OBLIGACION DE ACTUALIZAR EL REGISTRO

Dado en BOGOTA a los 15 días del mes de Noviembre de 2022 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.

DIRECTOR GENERAL

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web www.jcc.gov.co digitando el número del certificado

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

257885-T



LEIDY ELIANA
CUENCA MONTOYA
C.C. 1093223832
RES. INSCRIPCION 268 DEL 17/05/2019
CORPORACION UNIVERSITARIA REMINGTON

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

268183 287431

Identificación Plástica S.A. 180942/0119

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

Esta tarjeta es el único documento que lo acredita como Contador Público de acuerdo con lo establecido en la Ley 43 de 1990. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (57)(1) 644 4450 o devolverla a la UAE – Junta Central de Contadores a la Carrera 16 No. 97- 46 Of.301 en Bogotá D.C.

FIRMA


REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA
NUMERO 1.093.223.832
CUENCA MONTOYA
APELLIDOS
LEIDY ELIANA
NOMBRES
Eliana Cuenca M
FIRMA
REPUBLICA DE COLOMBIA


FECHA DE NACIMIENTO 16-DIC-1993
SANTA ROSA DE CABAL
(RISARALDA)
LUGAR DE NACIMIENTO
1.49
ESTATURA
A+
G.S. RH
F
SEXO
11-MAY-2012 SANTA ROSA DE CABAL
FECHA Y LUGAR DE EXPEDICION
REGISTRADOR NACIONAL
CARLOS ARIEL SANCHEZ TORRES
INDICE DERECHO
P-2400600-00385628-F-1093223832-20120629
00304 10980A 1
38288171

PLAN DE CONTINGENCIA DEL PROCESO DE TRANSICIÓN DE IPv4 A IPv6

EJET!C
GRUPO EMPRESARIAL
Transformando la Sociedad

Tabla de contenido

1. OBJETIVOS 5

1.1. OBJETIVO GENERAL 5

1.2. OBJETIVOS ESPECÍFICOS 5

2. ALCANCE Y LIMITACIONES 5

3. DETERMINACIÓN DE INCIDENTES EN EL PROCESO DE TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 7

3.1. INCIDENTES GENERALES 7

3.2. Incidente Interno 7

3.2. INCIDENTES CONECTIVIDAD 9

3.2.1. Incidente 1 (Internet) 9

3.2.2. Incidente 2 (DNS) 9

3.2.3. Incidente 3 (LAN) 9

3.3. INCIDENTES SEGURIDAD 10

3.3.1. Incidente 1 (Tráfico Ipv6) 10

3.3.2. Incidente 2 (Seguridad Perimetral) 10

3.4. INCIDENTES SISTEMAS DE INFORMACIÓN Y APLICACIONES 10

3.4.1. Incidente 1 (Infraestructura) 10

3.4.2. Incidente 2 (Sistema Operativo) 10

3.4.3. Incidente 3 (Integración) 11

4. PROCEDIMIENTO DE ATENCIÓN DE INCIDENTES 11

4.1. CONECTIVIDAD 11

4.1.1 Tratamiento Incidente 1 (Internet) 11

4.1.2 Tratamiento Incidente 2 (DNS) 12

4.1.3. Tratamiento Incidente 4 (LAN) 12

4.2. SEGURIDAD 14

4.2.1. Tratamiento Incidente 1 (Tráfico Ipv6) 14

4.2.2. Tratamiento Incidente 2 (Seguridad Perimetral) 14

4.3. SISTEMAS DE INFORMACIÓN Y APLICACIONES 16

4.3.1. Tratamiento Incidente 1 (Infraestructura) 17

4.3.2. Tratamiento Incidente 2 (Sistema Operativo) 17

4.3.3. Tratamiento Incidente 3 (Integración) 18

5.1. INCIDENTES DE CONECTIVIDAD 19

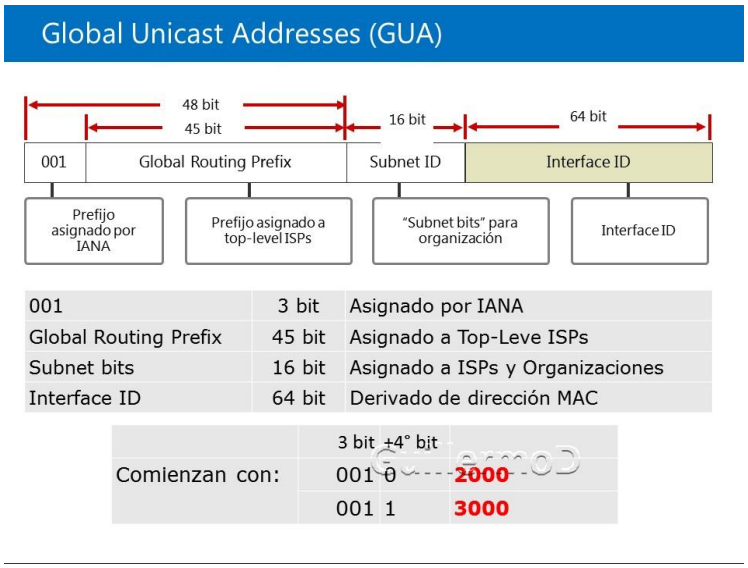
5.2. INCIDENTES DE SEGURIDAD 20

5.3. INCIDENTES DE SISTEMAS DE INFORMACIÓN Y APLICACIONES 20

DEFINICIONES

Direccionamiento GUA: Global Unicast Addresses (GUA): Este grupo de direcciones a direcciones públicas de Internet con protocolo IPv4. Con este direccionamiento desaparecen los procesos de NAT y las tablas de enrutamiento.

Figura 1 Tabla de enrutamiento



001	3 bit	Asignado por IANA
Global Routing Prefix	45 bit	Asignado a Top-Leve ISPs
Subnet bits	16 bit	Asignado a ISPs y Organizaciones
Interface ID	64 bit	Derivado de dirección MAC

	3 bit	+4° bit	
Comienzan con:	001	0	**2000**
	001	1	**3000**

Fuente: https://windowserver.wordpress.com/2013/09/25/aprendiendo-ipv6-clases-de-direcciones-ipv6/

Disponibilidad: Propiedad de la información y los recursos relacionados, los cuales deben estar disponibles y utilizables cuando se los requiera.

Evento: Es cualquier cambio de estado que tenga importancia para la gestión de uno o varios elementos de configuración (CI) o a su vez un servicio de TI.

ICMPv6: Descrito en el RFC 2463 **(**Request for Comments**),** es un protocolo de propósito múltiple que engloba funciones del protocolo IPv4, las cuales eran facilitadas por diversos protocolos como ICMP, IGMP o ARP. ICMPv6 está diseñado para realizar funciones tales como detectar y reportar errores que se encuentran durante el procesado de los paquetes, realizar diagnósticos, realizar funciones como Neighbor Discovery (equivalente a ARP) y detectar direcciones IPv6 de multidifusión (multicast), etc.

Incidente: El incidente es un evento que no forma parte de la operación estándar de un servicio y que causa interrupción del servicio o una reducción de su calidad.

Parches: Los parches son librerías de software empleadas para la corrección problemas o bugs en un sistema operativo o software específico.

Ping: Es una utilidad para el diagnóstico de conectividad que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes a través del protocolo ICMP con ICMP Echo Request y ICMP Echo Reply. Mediante esta utilidad se diagnostica el estado, velocidad y calidad de una red determinada.

Política: Es un conjunto de reglas para adoptar y mantener los niveles de seguridad.

Protocolo NDP: Es un protocolo de IPv6, definido en el RFC 2461 (Request for Comments), y equivalente al protocolo ARP Address Resolución Protocol (ARP) en IPv4, aunque también incorpora las funcionalidades de otros protocolos de esta versión, como ICMP Router Discovery e ICMP Redirect. Consiste en un mecanismo con el cual un nodo que se acaba de incorporar a una red, descubre la presencia de otros nodos en el mismo enlace, además de determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad acerca de las rutas a los vecinos activos.

Router Advertisement (RA): Es utilizado para el enrutamiento y la configuración automática de IPv6, los cuales utilizan esta información para aprender prefijos y parámetros de la red local.

Red LAN: (Red de área local) Es una red que conecta ordenadores en una red informática privada y su alcance se limita a un área reducida.

.

Red WAN: (Red de área amplia) Es una red de ordenadores que interconecta varias redes locales, sin la necesidad que se encuentren en una misma ubicación física.

Red WLAN: (Red de área local inalámbrica) Es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas.

Seguridad Perimetral: Es la integración entre elementos y sistemas para la protección de perímetros físicos y detección de tentativas de intrusión y su respectiva disuasión.

VLAN: (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

INTRODUCCIÓN

El Instituto de Movilidad de Pereira , dando cumplimiento a lo estipulado por el Ministerio de tecnologías de Información y las Comunicaciones (MINTIC) en la resolución 2710 de 2017 y tomando como guía el documento: “Guía de Transición de IPv4 a IPv6 para Colombia”, ha desarrollado el proyecto transición de protocolo IPv4 a IPv6 en la entidad. Lo anterior con el fin de incentivar el desarrollo de las TICs dentro de la organización y cumplir con la normatividad establecida para la vigencia actual.

En el entendido de que el desarrollo de este proyecto implica movimientos y procedimientos en la Infraestructura TIC, en los aplicativos y software en general que se manejan al interior de la entidad, es necesario establecer los procedimientos y actividades que se deben desplegar en caso de presentarse algún incidente que interfiera en el normal funcionamiento del componente TIC y que pueden llegar a impactar de forma significativa el desempeño de la entidad.

En el presente documento se identifican los posibles incidentes que se pueden presentar en la fase de implementación del proyecto de transición al nuevo protocolo, y se describen los procedimientos para cada caso para minimizar los impactos.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer los parámetros, procedimientos y actividades a realizar en caso de presentarse incidentes en la fase de implementación de la transición de IPv4 a IPv6, que puedan llegar a afectar el normal funcionamiento de los diferentes elementos o sistemas que componen la infraestructura de TI del El Instituto de Movilidad de Pereira.

1.2. OBJETIVOS ESPECÍFICOS

- Identificación de todos los posibles incidentes que se pueden presentar en el desarrollo de la fase de implementación sobre la infraestructura originados en la transición del protocolo IPv4 a IPv6 mediante Dual Stack, y su grado de impacto en el desempeño de la entidad.

- Definición de los procedimientos para minimizar el impacto en caso de presentarse cada uno de los posibles incidentes identificados durante la implementación.

- Especificar los elementos para documentar los incidentes y la aplicación de las acciones contempladas en este plan con los resultados que retroalimenten el proceso.

2. ALCANCE Y LIMITACIONES

El propósito de este documento es minimizar el impacto que se pueda generar al implementar el nuevo protocolo de internet IPv6 en El Instituto de Movilidad de Pereira, basado en un análisis detallado teniendo en cuenta las particularidades generales tanto a nivel externo, como interno y de infraestructura física conectividad, seguridad, sistemas de información y aplicaciones en El Instituto de Movilidad de Pereira, detectando los

posibles incidentes tanto de seguridad de la información como de seguridad informática, haciendo un análisis que permita encontrar posibles vulnerabilidades y en efecto bajo el protocolo IPv6 es necesario hacer esta labor debido a que IPv6 se apoya en otros protocolos como IPSec, HTTP, TCP, UDP o SIP.

Los ataques que se centran en comprometer redes lo hacen en tres áreas principales: el transporte (TCP/IP), el plano de control (principalmente protocolos de enrutamiento), y las aplicaciones que se ejecutan en hosts y servidores con conexiones de red. El despliegue de IPv6 incrementa la superficie de ataque en estas áreas mediante la inclusión de una nueva capa de transporte, nuevos planos de control (que aumenta la complejidad existente), añadiendo nuevos puertos abiertos y pilas de protocolos en los hosts y nuevos puntos de entrada en las aplicaciones.

Para este último es posible que se encuentren sistemas información y aplicaciones que presenten dependencias de integración entre otros servicios y limitaciones de IPs fijas configuradas a nivel de código fuente en cada aplicación al momento de implementar cambios como resoluciones de registros por nombre (Hostname vs IP) en los diversos módulos de programación usados en los servidores de aplicaciones, sobre los cuales se harían procedimientos específicos, como manejo de excepciones basadas en información del fabricante y encapsulado el protocolo de red IPv4 a través de equipos de red y de esta manera garantizar el uso efectivo de protocolo IPv6.

Debido a que se utiliza el método Dual Stack, el cual implica la convivencia de los protocolos IPv4 e IPv6, el cambio en los aplicativos no supone mayor traumatismo a nivel de sistema operativo y servicios, pero a nivel de integraciones y desarrollo de software es necesario la validación detallada, dado que en caso de detectarse una indisponibilidad, no se perdería conectividad al tener direccionamiento en IPv4 activo paralelamente.

Nota: El presente documento corresponde a un análisis preliminar que será complementado con los escenarios reales de contingencia, cuando se identifiquen las actividades detalladas del plan de implementación en el cual se definirían actividades puntuales de adopción del protocolo IPv6 con su correspondiente actividad de contingencia. Así mismo, es necesario documentar los incidentes presentados donde se

registren las acciones que se despliegan para cada caso y los resultados obtenidos en este ejercicio, los cuales determinarán la construcción de los procedimientos para el proceso de adopción del protocolo IPv6 con su respectiva solución documentada.

Unavez se cuente con este plan junto con el detalle de las contingencias, están se consolidarán y se actualizarán en una nueva versión de este documento.

3. DETERMINACIÓN DE INCIDENTES EN EL PROCESO DE TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6

3.1. INCIDENTES GENERALES

3.2. Incidente Interno

- **Contratación sin asistencia técnica.**

Compra de infraestructura tecnológica sin el control de los estándares necesarios para soportar el protocolo IPv6.

- **Pérdida de Información considerada crítica al interior del El Instituto de Movilidad de Pereira.**

Robo de información de la entidad por evento en la aplicación de políticas de Seguridad o eventos en la configuración de los elementos de seguridad Informática con el protocolo IPv6 que permiten el acceso desde el exterior de la entidad.

- **Evento en la infraestructura Tecnológica.**

Evento que afecte la infraestructura física o lógica de servidores vitales en la operación del servicio de la entidad, por ausencia de mantenimiento o mal manejo de los mismos.

- **Evento en Sistemas de Información.**

Falla por evento relacionado con la configuración y programación del protocolo IPv6 sobre el código fuente en aplicaciones o en bases de datos que maneja la entidad.

- **Ausencia de personal para la Operación de la Infraestructura Tecnológica.**

La falta de personal por enfermedad o por calamidad que imposibilita la correcta operación de las plataformas y equipos tecnológicos.

- **Mal uso de Hardware o Software.**

Evento por mal uso de Hardware o Software por parte de los funcionarios de la entidad por uso indebido, mal intencionado y/o por desconocimiento del protocolo IPv6.

3.1.2. *Incidente Externo*

- **Evento en el Sistema Eléctrico.**

Ausencia de fluido eléctrico por evento en el suministro de energía comercial o eventos en la operación de sistemas de respaldo de energía.

- **Caída de Servicios de Internet.**

Falla en el servicio por parte del proveedor ISP que suministra conexión a Internet.

- **Caída en el sistema de Comunicaciones de la Entidad.**

Evento en los sistemas de comunicaciones telefónico y de videoconferencia de la entidad por errores en las plataformas centralizadas de telefonía y/o videoconferencia posiblemente por problemas en la asignación de IP dinámica (DHCPv6), enrutamiento, permisos a nivel de seguridad perimetral, que entregan estos servicios.

- **Caída del servicio por Virus o Ataques Informáticos.**

Evento ocasionado por mala manipulación de las herramientas de seguridad o plataformas de aseguramiento de servidores donde se omitan políticas de seguridad con el protocolo IPv6, vitales en la operación de la entidad.

- **Afectación del servicio por Catástrofe Natural.**

Evento por la ocurrencia de un desastre natural el cual conlleva a la inoperatividad total o parcial de la infraestructura tecnológica del El Instituto de Movilidad de Pereira.

3.2. INCIDENTES CONECTIVIDAD

3.2.1. Incidente 1 (Internet)

Evento fortuito en la operación del proveedor de servicios de internet (ISP) al mantener en operación simultanea los protocolos IPv4 e IPv6, situación que podría afectar las comunicaciones y degradar la operación de los sistemas de información presentes en la entidad.

3.2.2. Incidente 2 (DNS)

Ausencia de los nuevos registros de recurso (AAAA) y/o actualización de los registros de tipo NS, PTR, SOA, etc. Como resultado de su omisión. Lo que podría traer como consecuencia errores en la resolución de nombres por tanto serios inconvenientes al intentar alcanzar los recursos por parte de los usuarios.

3.2.3. Incidente 3 (LAN)

Error en la configuración del protocolo NDP como consecuencia de la característica de autoconfiguración implícita en el protocolo IPv6. Tales errores pueden generar inconvenientes en la implementación que se haga sobre las interfaces de los equipos de red (Routers, Switches, Firewalls).

Las estaciones de trabajo de usuario final hacen uso del protocolo de mensajes ICMPv6 (Ra, Rs, Na, y Ns), los cuales se conectan a un segmento de red previamente configurado

en los equipos de capa 3, estas tendrán la posibilidad auto configurar una dirección IPv6 valida de tipo enlace local o enlace global.

3.3. INCIDENTES SEGURIDAD

3.3.1. Incidente 1 (Tráfico Ipv6)

Bloqueo de tráfico IPv6 por parte de los equipos de seguridad perimetral como consecuencia de la omisión de la labor de configuración o por errores en la configuración de los mismos como consecuencia de desconocimiento del protocolo IPv6.

3.3.2. Incidente 2 (Seguridad Perimetral)

Los equipos que se encuentran en la red interna podrán ser visibles en Internet a raíz de su configuración con el protocolo IPv6, lo que podría traer como consecuencia la generación de incidencias de seguridad para la infraestructura tecnológica, si la misma no se encuentra precedida por los dispositivos de seguridad perimetral (firewall, IPS, IDS, etc.). o si tales dispositivos no tienen la capacidad de filtrar paquetes IPv6.

3.4. INCIDENTES SISTEMAS DE INFORMACIÓN Y APLICACIONES

Este plan de contingencia está considerado para el total de aplicaciones y sistemas de información, para las cuales se presentará un plan de retorno en el caso de presentarse alguno de los siguientes incidentes que afecten la disponibilidad del servicio.

3.4.1. Incidente 1 (Infraestructura)

Con relación a la infraestructura se pueden presentar incidentes relacionados con temas de conectividad/seguridad que pueden repercutir directamente en la comunicación, imposibilitando el alcance de los servidores en donde residen los sistemas de información y aplicaciones.

3.4.2. Incidente 2 (Sistema Operativo)

Con relación a los sistemas operativos de los servidores donde residen los sistemas de información y aplicaciones se pueden presentar incidentes relacionados con la

configuración de módulos de kernel, configuración de interfaces de red, resolución de DNS y servicio NTP.

3.4.3. Incidente 3 (Integración)

Con relación a la integración entre los sistemas de información al momento de aplicar las configuraciones del protocolo IPv6, podrían generarse incidentes con afectación directa de: funcionamiento, dependencias de código, comunicaciones entre servidores web, bases de datos, datafile.

4. PROCEDIMIENTO DE ATENCIÓN DE INCIDENTES

4.1. CONECTIVIDAD

4.1.1 Tratamiento Incidente 1 (Internet)

Para mitigar esta situación se debe validar la correcta conexión entre la red del El Instituto de Movilidad de Pereira y la salida a Internet por medio del proveedor de Internet. Para este incidente es necesario el diagnóstico y evaluación a nivel de conectividad y seguridad perimetral con los respectivos especialistas a nivel Especialista de Networking , Se sugiere realizar los siguientes procedimientos:

- Revisar la conectividad a nivel del protocolo IPv6 entre los equipos de borde de la red del El Instituto de Movilidad de Pereira) y el extremo de conexión con la red del proveedor del servicio de internet.

- Revisar respuesta desde el equipo de borde de la red del El Instituto de Movilidad de Pereira hacia internet sobre el protocolo IPv6, para este caso se puede realizar pruebas hacia una página en internet ejemplo GOOGLE.

- Revisar traceroute hacia internet apuntando a una página externa a la entidad. (Podemos visualizar hasta donde se establece el ultimo salto) de esta manera validar la operatividad del equipo después del equipo que responde correctamente.

4.1.2 Tratamiento Incidente 2 (DNS)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación de los temas de conectividad y seguridad perimetral por parte del siguiente recurso humano: Especialista en Networking.

Se llevarán a cabo las siguientes acciones:

- Verificar desde la consola de DNS la existencia de los registros de recursos pertinentes.
- Verificar el direccionamiento IP asignado a los recursos.
- Ante la ausencia de registros de recursos asociados a servidores, servicios, aplicaciones. estos deberán ser creados de forma manual.
- Se realizarán pruebas de resolución de nombres, en el servidor DNS primario. Mediante la ejecución del comando nslookup desde la línea de comandos DOS.
- Realizar prueba básica de conectividad mediante la ejecución del comando ping desde la línea de comandos DOS.

4.1.3. Tratamiento Incidente 4 (LAN)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación de los temas de conectividad y seguridad perimetral por parte del siguiente recurso humano: Especialista en Networking.

Para mitigar esta situación se debe suprimir el envío de mensajes RA cuando se configuren las interfaces con direccionamiento IPv6 en Routers y Firewalls.

Al suprimir el mensaje "RA" se evita la autoconfiguración de las interfaces, de esta manera los administradores LAN pueden realizar pruebas con direccionamiento estático, esta situación permite realizar el despliegue del protocolo IPv6 de manera controlada. Después de configurar direccionamiento IPv6 en la interfaz del Routers, Firewall o interfaz de VLAN en Switch capa 3 con una dirección del segmento global asignado por LACNIC.

Es importante verificar que cada equipo tenga una o más direcciones IPv6 GUA válidas de un solo segmento de red. Después de la verificación se deben realizar las siguientes pruebas:

- Prueba Ping entre equipos del mismo segmento usando como destino las direcciones de enlace local.

- Prueba Ping entre equipos de distintos segmentos usando como destino las direcciones de enlace global.

- Prueba Ping entre equipos y servidores usando como destino las direcciones de enlace global.

. Conexión de escritorio remoto entre equipos del mismo segmento usando como destino las direcciones de enlace local.

- Conexión de escritorio remoto entre equipos del mismo segmento usando como destino las direcciones de enlace global.

- Pruebas de disponibilidad de servicios entre equipos y servidores usando como destino las direcciones de enlace global.

4.2. SEGURIDAD

4.2.1. Tratamiento Incidente 1 (Tráfico Ipv6)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación de la seguridad perimetral por parte del siguiente recurso humano: Especialista en Networking.

Se llevarán a cabo las siguientes acciones:

- Configurar las interfaces físicas del dispositivo de seguridad perimetral para que permitan el tránsito de paquetes IPv6.

- Permitir tráfico IPv6 en los diferentes dispositivos de seguridad perimetral a medida que se vaya realizando el despliegue en cada una de las sedes del El Instituto de Movilidad de Pereira) con el fin de corroborar el alcance del soporte IPv6 en cuanto ha filtrado de servicios se refiere.

- Permitir el Tráfico del servicio http y https para el protocolo IPv6 en la política del dispositivo de seguridad perimetral.

Después de realizar el procedimiento se deben realizar las siguientes pruebas:

- Corroborar que la política del dispositivo de seguridad perimetral permite el tráfico IPv6.

- Realizar pruebas de navegación a internet desde un equipo con direccionamiento IPv6.

- Realizar pruebas de acceso a aplicaciones desde un equipo con direccionamiento IPv6.

4.2.2. Tratamiento Incidente 2 (Seguridad Perimetral)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación de la seguridad perimetral por parte del siguiente recurso humano: Especialista en Networking

Se llevarán a cabo las siguientes acciones:

- Configurar las interfaces físicas del dispositivo de seguridad perimetral para que permitan el tránsito de paquetes IPv6.

- Configurar direccionamiento IPv6 GUA en los equipos que van a tener permisos de salida a internet.

- Realizar pruebas de navegación en el equipo conectado a internet.

- Permitir tráfico de servicios en la política configurada en el dispositivo de seguridad perimetral a medida que se vayan realizando las pruebas de navegación en internet con el fin de corroborar el alcance del soporte IPv6 en cuanto ha filtrado de servicios se refiere.

Después de realizar el procedimiento se deben realizar las siguientes pruebas:

- Prueba Ping hacia otros segmentos usando direcciones de alcance global GUA.

- Corroborar en primera instancia que la política del dispositivo de seguridad perimetral niega tráfico.

- Permitir el Tráfico del servicio ICMPv6 en la política del dispositivo de seguridad perimetral.

- Prueba Ping hacia otros segmentos usando direcciones de alcance global GUA y verificar que efectivamente son satisfactorias y que el dispositivo de seguridad perimetral las permite.

- Prueba de alcance WEB hacia otros segmentos usando direcciones de alcance global GUA.

. Corroborar en primera instancia que la política del dispositivo de seguridad perimetral niega tráfico.

- Escaneo de vulnerabilidades con el protocolo IPv6 sobre la red de pruebas.
- Permitir el Tráfico del servicio http y https en la política del dispositivo de seguridad perimetral.
- Prueba de alcance WEB hacia otros segmentos usando direcciones de alcance global GUA y verificar que efectivamente son satisfactorias y que el dispositivo de seguridad perimetral las permite.

NOTA: Realizar los mismos pasos para todos los servicios que se requiera.

En caso de que el dispositivo de seguridad perimetral no niegue el tráfico de algún servicio, se debe aplicar la política de seguridad de la información en la infraestructura para determinar el estado de criticidad de este servicio. Si el estado de criticidad es muy alto se debe deshabilitar el protocolo IPv6 en los equipos y servidores hasta que se garantice el filtrado de los paquetes con este servicio mediante parches o actualizaciones de software.

Esto se hace debido a que, si el dispositivo de seguridad perimetral no contempla dentro de su soporte con el protocolo IPv6, el filtrado de ciertos servicios generaría una vulnerabilidad de seguridad que puede ser aprovechada por atacantes para vulnerar la seguridad de la infraestructura.

4.3. SISTEMAS DE INFORMACIÓN Y APLICACIONES

Para la mitigación de los incidentes en la implementación del protocolo IPv6 es necesario la adopción de un plan de normalización del servicio el cual consiste en el restablecimiento de los parámetros físicos o lógicos, como se explica a continuación:

4.3.1. Tratamiento Incidente 1 (Infraestructura)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación de los temas de conectividad y seguridad perimetral por parte del siguiente recurso humano: Especialista en Networking - Administración de Sistemas Operativos Especialista en Aplicaciones y Responsable Aplicación – El Instituto de Movilidad de Pereira.

Se llevarán a cabo las siguientes acciones:

- Identificación de la falla con el fin de conocer desde que punto a nivel de comunicaciones no se están alcanzando los servidores y los sistemas operativos, respectivamente.

- Diagnóstico y evaluación a nivel de conectividad y seguridad perimetral.

- Solución, documentación y búsqueda de causa raíz para alimentar la base de conocimiento de la entidad con esto darle el correcto manejo a los incidentes que se relacionen con sistemas de información y aplicaciones.

4.3.2. Tratamiento Incidente 2 (Sistema Operativo)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación por parte del siguiente recurso humano: Especialista en Administración Sistemas Operativos - Especialista en Aplicaciones –Responsable Aplicación – El Instituto de Movilidad de Pereira.

Se llevarán a cabo las siguientes acciones:

- Es necesario ejecutar validaciones con el fin de diagnosticar, si la incidencia se presentó por configuración a nivel de módulos kernel, interfaz de red, respuesta de registro de DNS o problemas de sincronización de NTP.

. Para esto es necesario realizar la validación y diagnóstico de cada una de las partes que afectan el funcionamiento del sistema operativo.

4.3.3. Tratamiento Incidente 3 (Integración)

Ante la posible ocurrencia de dicho incidente, se precisa llevar a cabo un diagnóstico y evaluación por parte del siguiente recurso humano: Especialista en Administración Sistemas Operativos -Especialista en Aplicaciones y Responsable Aplicación – El Instituto de Movilidad de Pereira.

Se llevarán a cabo las siguientes acciones:

- Para la resolución de incidentes relacionados con integración entre sistemas de información, es necesario de ejecutar validaciones detalladas para identificar en que parte del sistema de información está la falla de funcionamiento, dependencia de servicio, código fuente y/o comunicaciones entre servicios web, base de datos y demás.

- Para estos casos el proceso de evaluación y diagnostico se hace con trabajo en conjunto entre el área de gestión informática, terceros dueños de las aplicaciones para de esta forma identificar las dependencias en cada uno de los escenarios.

- Finalmente, como apoyo a la resolución de los incidentes y gestión de los mismos, se cuenta con la hoja de vida de cada dispositivo basado en el historial de documentación de cada uno de los sistemas de información y aplicaciones.

5. PRUEBAS Y DOCUMENTACIÓN DE INCIDENTES

Para realizar la documentación de los incidentes que se presenten durante la implementación, se crea la carpeta INCIDENTES IMPLEMENTACIÓN PROTOCOLO IPv6 en la ruta:

(La ruta será la que la entidad tenga como servidor de almacenamiento de este tipo de documentos). Cada registro es un archivo de Word que se nombra: Incidente “XX”, donde

“XX “corresponde a un consecutivo que comienza en 01. Cada archivo debe contener la siguiente información:

- Fecha y hora de ocurrencia:
- Descripción del evento que provocó el incidente:
- Responsable de solución del incidente:
- Incidente previsto: SI No
- Descripción del Incidente:
- Servicios afectados:
- Grado de Afectación:
- Tiempo de afectación:
- Procedimientos aplicados:
- Solución:
- Resultados:

NOTA: El plan de contingencia que se presenta en este documento es una guía para mitigar los posibles inconvenientes que generalmente se derivan de implementaciones de protocolo IPv6, debido a que cada infraestructura tiene características únicas que las diferencian una de otra. Seguramente se van a presentar inconvenientes a lo largo del proceso de implementación del protocolo IPv6 en El Instituto de Movilidad de Pereira . Cada uno de los incidentes que se vayan presentando deben tener un protocolo de contingencia para su mitigación, el protocolo de contingencia que se genere, se va a usar para alimentar este documento, de esta manera al final del proceso de implementación se definirán todos los inconvenientes que se presentaron y un plan de mitigación consignado en este documento.

5.1. INCIDENTES DE CONECTIVIDAD

Se debe implementar un ambiente de pruebas para la simulación de escenarios similares a los configurados sobre la infraestructura tecnológica con miras a realizar las configuraciones

adecuadas sobre los equipos de conectividad, habilitando el protocolo IPv6 sobre este ambiente controlado. De esta manera en el momento de presentarse un incidente se tienen las herramientas para realizar las simulaciones y cambios adecuados para minimizar los INCIDENTES de ocurrencia.

5.2. INCIDENTES DE SEGURIDAD

A nivel de seguridad se deben contemplar un ambiente de pruebas controlado y con estricto monitoreo para minimizar la ocurrencia de incidentes que puede traer el despliegue del protocolo IPv6 y que pueden conllevar a diferentes tipos de ataques a la infraestructura tecnológica.

5.3. INCIDENTES DE SISTEMAS DE INFORMACIÓN Y APLICACIONES

Para ejecutar el plan de acción para restablecimiento de los parámetros configurados en la infraestructura física y en cada uno de los sistemas información. Es necesario la realización de pruebas en un ambiente idéntico al ambiente productivo, donde se implementará el protocolo IPv6 abarcando los frentes de conectividad, seguridad y sistemas de información, con el fin de no provocar incidentes sobre el estado actual funcional de los ambientes productivos.

De este modo alimentar el plan de excepciones de los sistemas de información y aplicaciones de que no soportaron el protocolo IPv6, así mismo, cabe aclarar que con este procedimiento se garantiza no tener afectación sobre los ambientes productivos y así garantizar la resolución de los dos protocolos IPv4 e IPv6.

PLAN DE DIAGNÓSTICO FASE I TRANSICIÓN A LA ADOPCIÓN DEL PROTOCOLO IPV6

EJET!C
GRUPO EMPRESARIAL
Transformando la Sociedad

Tabla de versiones

Versión	Fecha	Autor
1.0	24-MARZO-2022	Grupo EJETIC

Contenido

OBJETIVOS DEL ENTREGABLE **4**
Objetivo General **4**
Objetivos específicos: **4**
REQUERIMIENTOS ASOCIADOS AL ENTREGABLE **4**
DEFINICIONES **5**
PLANEACIÓN DE DIAGNÓSTICO **6**
ELEMENTOS CLAVE **8**
Herramientas **10**
Cronograma **10**
PLAN DE IMPLEMENTACIÓN **11**
ELEMENTOS CLAVE **12**
Recursos **12**
Herramientas **14**
Cronograma **15**
PLAN DE PRUEBAS DE FUNCIONALIDAD **15**
ELEMENTOS CLAVE **16**
Recursos **16**
Cronograma **18**

INTRODUCCIÓN

En concordancia con los objetivos de innovación tecnológica que exige el país, el INSTITUTO DE MOVILIDAD DE PEREIRA ha iniciado acciones para el proceso de transición del protocolo IPv4 a IPv6. El marco normativo sobre el cual las diferentes entidades de orden nacional deben adoptar implementar el protocolo de internet, se consigna en el documento "Plan de Trabajo para la Transición IPv6".

El proceso de adopción de IPv6 requiere de una planeación, de forma que cuente con una versión organizadas y detallada de los tiempos sobre los cuales se enmarca la implementación de dicho protocolo de internet, teniendo en cuenta que dentro del proyecto debe existir un periodo de transición sobre el cual las dos versiones (IPv4 e IPv6) deberán coexistir un tiempo importante. Es así como IPv6 se implementa como una actualización de software de los nodos IPv4 actuales, para luego desactivar paulatinamente las características de IPv4 hasta llegar a estar totalmente en el protocolo IPv6

Para realizar el proceso de adopción del nuevo protocolo, MinTIC recomienda realizar una serie de actividades de levantamiento de información y verificación sobre: el inventario de los activos de TI de información, e infraestructura de TI, los componentes de hardware y software existentes, los servicios, los sistemas de información, estándares y políticas; todo ello para determinar el impacto de adopción de IPv6, de forma que permita de forma armónica facilitar las actividades de planeación e implementación, procurando obtener una continuidad en la correcta ejecución de procesos y procedimientos definidos dentro de la clara identificación del negocio de la Entidad y con la adecuada implementación del protocolo IPv6 acorde a lo definido por el Ministerio de las TIC.
Este documento presenta el resultado de las actividades anteriormente descritas mediante un diagnóstico consolidado de los componentes de TI (Hardware y

Software), como también las recomendaciones, plan de direccionamiento IPv6, manejo de excepciones, informe de preparación, lineamientos de seguridad en IPv6, plan de migración de servicios tecnológicos y protocolo de pruebas.

OBJETIVOS DEL ENTREGABLE

Objetivo General.

Planear las fases necesarias para implementar la utilización del protocolo IPV6 en la red de comunicaciones en el INSTITUTO DE MOVILIDAD DE PEREIRA, para preparar el proceso de adopción del nuevo protocolo IPv6.

Objetivos específicos:

- Identificar las actividades necesarias para realizar el diagnóstico de la red, equipos de comunicaciones, servidores y aplicaciones.
- Elaborar la planeación de la implementación del protocolo en configuración Dual Stack (doble pila).
- Realizar la planeación de las actividades para el aseguramiento de la correcta y completa implementación del protocolo IPV6.

REQUERIMIENTOS ASOCIADOS AL ENTREGABLE

Este documento define la planeación de la transición; considerando el estado actual de la infraestructura Tecnológica del INSTITUTO DE MOVILIDAD DE PEREIRA, 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”.

De acuerdo con lo anterior el presente documento incluye los siguientes entregables:

- Plan de diagnóstico para la adopción de IPv6.
- Plan de implementación incluyendo lo requerido por MinTIC
- Plan de pruebas de funcionalidad de IPV6.

DEFINICIONES

Para el presente documento se consideran las siguientes definiciones:
Amenaza: (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de riesgos: (Inglés: Risk Analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Auditoría: (Inglés: Audit). 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: (Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.
Confidencialidad: (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Disponibilidad: (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
DHCPv6: (Protocolo Dinámico de Configuración de nodos)2 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.
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. 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 Provider3 Un Proveedor de Servicios de Internet asigna principalmente espacio 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.
Notación hexadecimal 4: 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.
Resolución de nombres: Obtención de una dirección a partir de un nombre. q) 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 RFCs, sin esperar a que sean STD.
Subred: Uno o más enlaces que utilizan el mismo prefijo de 64 bits.
Transición: Conjunto de mecanismos que permiten la integración de IPv6 en las redes con IPv4, básicamente doble-pila, túneles y traducción.

PLANEACIÓN DE DIAGNÓSTICO

Es la primera etapa en la transición y la más importante para la adopción del protocolo IPV6 en configuración Dual Stack (doble pila). Dentro de esta se realiza el inventario de activos de comunicación, servidores y aplicaciones que serán afectados en el proceso de transición.

En el presente capítulo se define el alcance de las actividades de diagnóstico:

- **Actividad 1:** Elaborar el inventario de activos de comunicaciones y servidores (Hardware)
- **Actividad 2:** Elaborar el inventario de soluciones y aplicaciones (Software)
- **Actividad 3:** Validar la capacidad y cumplimiento del hardware. Se puede abordar con un especialista o consultar con el fabricante o acudir a las fichas técnicas del hardware
- **Actividad 4:** Validar la capacidad del software base (Sistemas Operativos) Frameworks de desarrollo, soluciones y aplicaciones de utilizar IPv6. Se pueden abordar con funcionarios de soporte de aplicaciones, los terceros responsables o contratados para el mantenimiento del software o con los fabricantes o desarrolladores del software/solución
- **Actividad 5:** Construir el diagrama de arquitectura de Red (topología) con seguridad Informática.
- **Actividad 6:** Construir la arquitectura de enrutamiento actual de la red. Este diagrama debe estar alineado con el diagrama de topología de red
- **Actividad 7:** Elaborar el diagnóstico de la capacidad red, comunicaciones, servidores, soluciones y aplicaciones.
- **Actividad 8:** Definir la estrategia (mecanismos) de implementación del protocolo IPv6 considerando la topología de red, la capacidad de implementación de IPv6 en los equipos de comunicación, los servidores, la cantidad de renovaciones y adquisiciones requeridas, y la capacidad de las soluciones y aplicaciones.
- **Actividad 9:** Elaborar el plan de manejo de excepciones en donde se determine las decisiones para aquellas aplicaciones y activos de hardware que no soporten IPV6 y no se renueven.
- **Actividad 10:** Capacitar a los funcionarios, contratistas, administradores de infraestructura, administradores de servidores y aplicaciones en las actividades planeadas para el abordaje de la transición.

ELEMENTOS CLAVE

Para el desarrollo de las actividades definidas se requiere establecer los siguientes puntos:

- **Recursos.** Personal interno o externo mínimo requerido para el desarrollo de las actividades.
- **Herramientas.** Herramientas requeridas para el apoyo del desarrollo de las actividades establecidas
- **Cronograma.** tiempo proyectado para el desarrollo de las actividades establecidas.
- **Presupuesto.** Costos asociados a tiempos y recursos que permitan el desarrollo de las actividades para la adopción de IPv6.

Tabla 1. Tabla de asignación de recursos para Fase 1

Actividad	Nombre del Recurso	Ámbito	Recurso Interno	Recurso Externo	Responsable De la Actividad
Actividad 1	Elaborar el inventario de activos de comunicaciones	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 2	Elaborar el inventario de activos de computo	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 3	Elaborar el inventario de activos de Servicios en la nube	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 4	Elaborar el inventario de activos de Servicios Web	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto

Actividad 5	Elaborar el inventario de activos de servidores	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 6	Elaborar el inventario de soluciones y aplicaciones (Software)	Sistemas de Información	X	X	Funcionario Ejetic Funcionario instituto
Actividad 7	Elaborar el inventario de Bases de Datos	Aplicaciones y Bases de Datos	X	X	Funcionario Ejetic Funcionario instituto
Actividad 8	Validar la capacidad y cumplimiento del hardware	Equipos de Comunicaciones	X	X	Inge Fabián López Inge Mauricio Vargas
Actividad 9	Validar la capacidad del software base (Sistemas Operativos) Frameworks de desarrollo, soluciones y aplicaciones de utilizar IPv6.	Sistemas de Información	X	X	Funcionario Ejetic Funcionario instituto
Actividad 10	Construir el diagrama de arquitectura de Red (topología) con seguridad Informática	Seguridad TI	X	X	Funcionario Ejetic Funcionario instituto
Actividad 11	Levantamiento de la arquitectura de enrutamiento actual de la red	Equipos de Comunicaciones	X	X	Funcionario Ejetic Funcionario instituto
Actividad 12	Elaborar el diagnóstico de la capacidad red, comunicaciones, servidores, soluciones y aplicaciones.	Equipos de Comunicaciones	X	X	Funcionario Ejetic Funcionario instituto
Actividad 13	Definir la estrategia (mecanismos) de implementación del protocolo IPv6	Proveedores de Internet		X	Proveedor de servicio
Actividad 14	Elaborar el plan de manejo de excepciones	Seguridad TI	X	X	Funcionario Ejetic Funcionario instituto
Actividad 15	Capacitar a los funcionarios, contratistas	Equipos de Comunicaciones		X	Funcionario Ejetic

Herramientas

Las herramientas comprenden los elementos que se requieren como apoyo para el desarrollo de actividades establecidas en la fase 1 para la adopción de IPv6.

Tabla 2. listado de herramientas requeridas

Herramienta	Responsable Uso	Responsable Suministro	Actividad
Información	Funcionario instituto	Funcionario instituto	Actividad 1
Información	Funcionario instituto	Funcionario instituto	Actividad 2
Información	Funcionario instituto	Funcionario instituto	Actividad 3
Información	Funcionario instituto	Funcionario instituto	Actividad 4
Información	Funcionario instituto	Funcionario instituto	Actividad 5
Información	Funcionario instituto	Funcionario instituto	Actividad 6
Información	Funcionario instituto	Funcionario instituto	Actividad 7
Información	Funcionario instituto	Funcionario instituto	Actividad 8
Información	Funcionario instituto	Funcionario instituto	Actividad 9
Información	Funcionario instituto	Funcionario instituto	Actividad 10
Información	Funcionario instituto	Funcionario instituto	Actividad 11
Información	Funcionario instituto	Funcionario instituto	Actividad 12
Información	Funcionario instituto	Proveedor Internet	Actividad 13
Información	Funcionario instituto	Funcionario instituto	Actividad 14
Información	Funcionario Ejetic	Funcionario Ejetic	Actividad 15

Cronograma

El cronograma permite proyectar en una línea de tiempo las actividades que se han definido para el desarrollo de la fase 1 de la transición a la adopción a IPv6.

Tabla 3. Cronograma de desarrollo de actividades

Actividad	Fechas		Semanas							
	Inicio	Fin	1	2	3	4	5	6	7	8
Actividad 1	28/mar/22		X	X	X	X				
Actividad 2	31/mar/22		X	X	X	X				
Actividad 3	31/mar/22		X	X	X	X				
Actividad 4	31/mar/22		X	X	X	X				
Actividad 5	31/mar/22		X	X	X	X				
Actividad 6	31/mar/22		X	X	X	X				
Actividad 7	31/mar/22		X	X	X	X				
Actividad 8	31/mar/22		X	X	X	X				
Actividad 9	31/mar/22		X	X	X	X				
Actividad 10	31/mar/22		X	X	X	X				
Actividad 11	31/mar/22		X	X	X	X				
Actividad 12	31/mar/22		X	X	X	X				
Actividad 13	31/mar/22		X	X	X	X				
Actividad 14	31/mar/22		X	X	X	X				
Actividad 15	31/mar/22		X	X	X	X				

PLAN DE IMPLEMENTACIÓN

En esta etapa se planean las actividades en las cuales se implementa el protocolo IPv6 aplicando el enfoque Dual Stack; considerando la configuración de los activos de red, la renovación del hardware que no soporta IPV6, la modificación de las aplicaciones y aplicando las excepciones determinadas en la estrategia de implementación

En la presente sección se determinan la planeación de las siguientes actividades de implementación:

- **Actividad 1.** Diseño de la preparación y configuración de los sistemas de comunicaciones, servidores, soluciones y aplicaciones.
- **Actividad 2.** Diseño de los lineamientos de seguridad y adecuación de la política de seguridad de la información.
- **Actividad 3.** Realizar las adquisiciones y renovaciones de los equipos de hardware, soportes necesarios para la implementación
- **Actividad 4.** Realizar la modificación de la aplicaciones y soluciones para la utilización de IPV6

- **Actividad 5.** Realizar la adquisición de direcciones IPV6.
- **Actividad 6.** Realizar el diseño del alcance de prueba piloto.
- **Actividad 7.** Preparar planes de trabajo para la gestión de cambios.
- **Actividad 8.** Realizar la configuración de los equipos de comunicaciones y servidores.
- **Actividad 9.** Realizar la configuración de direccionamiento y enrutamiento de la red IPV6.
- **Actividad 10.** Ejecutar las pruebas unitarias de IPV6.

ELEMENTOS CLAVE

Para el desarrollo de las actividades definidas se requiere establecer los siguientes puntos:

- **Recursos.** Personal interno o externo mínimo requerido para el desarrollo de las actividades.
- **Herramientas.** Herramientas requeridas para el apoyo del desarrollo de las actividades establecidas
- **Cronograma.** tiempo proyectado para el desarrollo de las actividades establecidas.
- **Presupuesto.** Costos asociados a tiempos y recursos que permitan el desarrollo de las actividades para la adopción de IPv6.

Recursos

Los recursos para el proyecto son las personas con las capacidades requeridas para abordar la responsabilidad del seguimiento y desarrollo de actividades descritas dentro del plan de transición para la adopción de IPv6 en la entidad.

Figura 1. Ámbitos involucrados en la adopción del protocolo IPv6



Fuente: Cartilla guía de transición de ipv4 a IPv6, MINTIC, 2020.

Para el desarrollo del proyecto pueden existir dos tipos de recursos.

- **Recursos internos - Equipo base.** Personal idóneo que pertenece a la entidad, quienes se hacen responsables del seguimiento del cronograma establecido. Personal de la entidad en capacidad de desarrollar las actividades definidas para la presente fase.

- **Recursos externos.** Personal externo en capacidad de desarrollar las actividades definidas para la presente fase.

Tabla 4. Tabla de asignación de recursos para Fase 2

Actividad	Nombre del Recurso	Ámbito	Recurso Interno	Recurso Externo	Responsable de la Actividad
Actividad 1	Diseño de la preparación y configuración de los sistemas de comunicaciones, servidores, soluciones y aplicaciones.	Equipos de comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 2	Diseño de los lineamientos de seguridad y adecuación de la política de seguridad de la información.	Seguridad TI	X	X	Funcionario Ejetic Funcionario instituto

Actividad 3	Realizar las adquisiciones y renovaciones de los equipos de hardware necesarios para la implementación	Equipos de comunicaciones, cómputo y almacenamiento	X		Funcionario instituto
Actividad 4	Realizar la modificación de la aplicaciones y soluciones para la utilización de IPV6	Sistemas de Información	X		
Actividad 5	Realizar la adquisición de direcciones IPV6.	LACNIC		X	Funcionario Ejetic
Actividad 6	Realizar el diseño del alcance de prueba piloto.	Equipos de comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic
Actividad 7	Preparar planes de trabajo para la gestión de cambios.	Equipos de comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic
Actividad 8	Realizar la configuración de los equipos de comunicaciones y servidores.	Equipos de comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 9	Realizar la configuración de direccionamiento y enrutamiento de la red IPV6.	Equipos de comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic
Actividad 10	Ejecutar las pruebas unitarias de IPV6.	Equipos de comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic

Herramientas

Las herramientas comprenden los elementos que se requieren como apoyo para el desarrollo de actividades establecidas en la fase 1 para la adopción de IPv6.

Tabla 5. listado de herramientas requeridas

Herramienta	Responsable Uso	Responsable Suministro	Actividad
Presupuesto			Actividad 3
Presupuesto			Actividad 5
Rango Direcciones IP	Funcionario Ejetic	Funcionario Ejetic	Actividad 6

Cronograma

El cronograma permite proyectar en una línea de tiempo las actividades que se han definido para el desarrollo de la fase 1 de la transición a la adopción a IPv6.

Tabla 6. Cronograma de desarrollo de actividades

Actividad	Fechas		Semanas							
	Inicio	Fin	1	2	3	4	5	6	7	8
Actividad 1			X	X	X	X				
Actividad 2			X	X	X	X				
Actividad 3			X	X	X	X				
Actividad 4			X	X	X	X				
Actividad 5			X	X	X	X				
Actividad 6			X	X	X	X				
Actividad 7			X	X	X	X				
Actividad 8			X	X	X	X				
Actividad 9			X	X	X	X				
Actividad 10			X	X	X	X				

PLAN DE PRUEBAS DE FUNCIONALIDAD

En esta etapa se planean pruebas a realizar en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad que permitan evidenciar el correcto funcionamiento del protocolo IPv6 en los servicios implementados.
En la presente sección se determinan la planeación de las siguientes actividades de implementación:

- **Actividad 1.** Diseñar las pruebas de IPv6
- **Actividad 2.** Ejecutar las pruebas de comunicación IPv6 y las pruebas de seguridad informática.
- **Actividad 3.** Realizar el monitoreo de la comunicación utilizando IPv6.
- **Actividad 4.** Elaborar informe de resultados, identificando hallazgos y el impacto de los problemas detectados.

- **Actividad 5.** Diseñar y ejecutar los ajustes de configuración.
- **Actividad 6.** Realizar las pruebas finales.

ELEMENTOS CLAVE

Para el desarrollo de las actividades definidas se requiere establecer los siguientes puntos:

- **Recursos.** Personal interno o externo mínimo requerido para el desarrollo de las actividades.
- **Herramientas.** Herramientas requeridas para el apoyo del desarrollo de las actividades establecidas
- **Cronograma.** tiempo proyectado para el desarrollo de las actividades establecidas.
- **Presupuesto.** Costos asociados a tiempos y recursos que permitan el desarrollo de las actividades para la adopción de IPv6.

Recursos

Los recursos para el proyecto son las personas con las capacidades requeridas para abordar la responsabilidad del seguimiento y desarrollo de actividades descritas dentro del plan de transición para la adopción de IPv6 en la entidad.

Figura 2. Ámbitos involucrados en la adopción del protocolo IPv6



Fuente: Cartilla guía de transición de ipv4 a IPv6, MINTIC, 2020.

Para el desarrollo del proyecto pueden existir dos tipos de recursos.

- **Recursos internos - Equipo base.** Personal idóneo que pertenece a la entidad, quienes se hacen responsables del seguimiento del cronograma establecido. Personal de la entidad en capacidad de desarrollar las actividades definidas para la presente fase.

- **Recursos externos.** Personal externo en capacidad de desarrollar las actividades definidas para la presente fase.

Tabla 7. Tabla de asignación de recursos para Fase 3

Actividad	Nombre del Recurso	Ámbito	Recurso Interno	Recurso Externo	Responsable de la Actividad
Actividad 1	Diseñar las pruebas de IPv6	Equipos de Comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic
Actividad 2	Ejecutar las pruebas de comunicación IPv6 y las pruebas de seguridad informática	Seguridad TI	X	X	Funcionario Ejetic Funcionario instituto

Actividad 3	Realizar el monitoreo de la comunicación utilizando IPv6	Sistemas de Información		X	Funcionario Ejetic
Actividad 4	Elaborar informe de resultados, identificando hallazgos y el impacto de los problemas detectados	Sistemas de Información		X	Funcionario Ejetic
Actividad 5	Diseñar y ejecutar los ajustes de configuración	Equipos de Comunicaciones, cómputo y almacenamiento	X	X	Funcionario Ejetic Funcionario instituto
Actividad 6	Realizar las pruebas finales	Equipos de Comunicaciones, cómputo y almacenamiento		X	Funcionario Ejetic

Cronograma

El cronograma permite proyectar en una línea de tiempo las actividades que se han definido para el desarrollo de la fase 1 de la transición a la adopción a IPv6.

Tabla 7. Cronograma de desarrollo de actividades

Actividad	Fechas		Semanas							
	Inicio	Fin	1	2	3	4	5	6	7	8
Actividad 1										
Actividad 2										
Actividad 3										
Actividad 4										
Actividad 5										
Actividad 6										

PLAN DE DIRECCIONAMIENTO IPv6

EJETIC
GRUPO EMPRESARIAL
Transformando la Sociedad

EJETIC | GRUPO EMPRESARIAL

TABLA DE CONTENIDO

Pág.

DEFINICIONES 2

INTRODUCCIÓN 3

1. OBJETIVOS 5

2. CUADRO DE PREFIJOS /56 PARTIENDO DEL PREFIJO DE LACNIC ASIGNADO PARA ESTE PLAN DE DIRECCIONAMIENTO 5

2.1. DEFINICIÓN DEL DIRECCIONAMIENTO IPv6 8

2.2. ASIGNACIÓN DE PREFIJO IPv6 /56 PARA EL INSTITUTO DE MOVILIDAD DE PEREIRA 9

2.3. SEGMENTOS QUE SE VAN A USAR PARA DATACENTER Y WAN 10

ANEXOS ..... **Error! Bookmark not defined.**

DEFINICIONES

PREFIJO: Numero de bits contados de izquierda a derecha de una dirección IPv6, equivalente a la porción de red de una dirección IPv4.

IID: Interface ID o identificador de interface equivalente a la porción de Host de una dirección IPv4.

RIR: Registro Regional de Internet, es una organización que supervisa la asignación y registro de recursos de internet en una región especifica.

LACNIC: Latín América and Caribeña Network Information Centre, es el registro regional de internet para la zona de Latino América y el Caribe.

NIBBLE: Digito hexadecimal (0-F) de 4 bits de una dirección IPv6.

SEGMENTO: Porción de 16 bits de una dirección IPv6 compuesta por 4 nibbles, cada uno de los segmentos debe estar delimitado por ¨:¨ los valores de cada segmento oscilan entre :0000: y :FFFF:

SLAAC: Stateless Address Autoconfiguration, Auto configuración de direcciones IPV6 sin estado.

DHCPv6: Dinamic Host Configuration Protocol, protocolo de configuración dinámica de direcciones IPv6.

INTRODUCCIÓN

IPv6 es una realidad y la migración de IPv4 a IPv6 es imperativa para estar actualizado en temas de tecnologías TI. El ministerio de tecnologías de la información y las comunicaciones MINTIC mediante resolución 2710 de 2017 establece los lineamientos para la adopción del protocolo IPv6 en las entidades públicas de carácter nacional y territorial.

El Instituto de Movilidad de Pereira como entidad pública de carácter nacional debe realizar dicha adopción antes del 31 de diciembre de 2022. Para cumplir con este lineamiento se realiza un plan de numeración o direccionamiento IPv6 empleando un prefijo de documentación preliminar, como requisito fundamental para la solicitud de un prefijo IPv6 ante el registro de direcciones de internet para América latina y el Caribe (LACNIC). Este prefijo será segmentado con el fin de cubrir el direccionamiento IPv4 que actualmente tienen los segmentos de red del EL INSTITUTO DE MOVILIDAD DE PEREIRA, para que sean configurados en IPv6 y se logre la convivencia de los dos protocolos en Dual Stack.

El plan de direccionamiento significa básicamente la segmentación de un prefijo inicial, el prefijo inicial puede ser de documentación o el prefijo que asigne LACNIC. MINTIC en su reglamentación sugiere la generación de un plan de direccionamiento para la fase de planeación con un prefijo de documentación y otro plan de direccionamiento para la fase de pruebas de funcionamiento, este último debe usar el prefijo asignado por LACNIC. Para este documento se usará un prefijo asignado por LACNIC ajustado a las necesidades de direccionamiento de la entidad. Con IPv6 es posible cubrir el direccionamiento público y privado de una organización usando una sola red sumarizada, esta situación facilita el tráfico IPv6 debido a que se disminuye el tamaño de las tablas de enrutamiento de los equipos de capa 3. Para realizar una segmentación exitosa que garantice la implementación, la mejor practica es establecer la cantidad de segmentos IPv4 que actualmente funcionan en la infraestructura de la entidad, esta práctica indica el número exacto de VLANs que se van a cubrir con direccionamiento IPv6, además de establecer el número exacto de VLANs nuevas para usos específicos y los Backus que se necesiten en el proceso de implementación. Debido a la gran cantidad de subredes y hosts que puede

albergar cada uno de los prefijos /56 y /64 respectivamente se van a realizar asignaciones consecutivas, en caso de que se necesiten asignaciones para backup y redes especiales se realizara una asignación consecutiva desde el último segmento usado para segmentos principales. Por necesidades de direccionamiento se entiende el cubrimiento efectivo de cada una de las VLANs IPv4 que actualmente se usan en la infraestructura de la entidad, desde la fase de implementación cada una de estas VLANs quedara configurada con el mecanismo de transición DUAL-STACK o DOBLE PILA, este escenario brinda la posibilidad de realizar conexiones tanto en IPv4 como en IPv6 sin que se afecte el funcionamiento independiente de los protocolos.

Para determinar el tamaño de los prefijos que se van a usar, se deben tener en cuenta las siguientes consideraciones:

Las especificaciones de IPv6 recomiendan prefijos /64 para segmentos de red que alberguen HOSTS, debido al gran espacio disponible de direcciones IPv6. Es posible considerar un prefijo mayor al /64, depende de los administradores de red, esta práctica no es recomendada, porque puede presentar inconvenientes y se pierden características propias del protocolo IPv6 como SLAAC (stateless address autoconfiguration), el uso de prefijos superiores al /64 se puede pensar para los enlaces punto a punto. Por ejemplo, prefijos /126 y 127, estos prefijos son similares a los segmentos /30 y /31 que son usados para configurar enlaces punto a punto en IPv4. No es obligatorio, cada administrador puede usar la longitud de prefijo que se le facilite, puede usar prefijos /64 para los enlaces punto a punto. Los prefijos /128, se pueden usar de la misma manera que se usan los /32 en IPv4 para direcciones de loopback y definición de hosts específicos dentro de un segmento de red. El proceso de segmentación seguirá las recomendaciones y se generaran segmentos IPv6 para cada una de las VLAN IPv4 de la infraestructura con el rango de direcciones IPv6 validas disponibles.

OBJETIVOS

- Elaborar un cuadro de prefijos /56 partiendo del asignado por LACNIC para cubrir el direccionamiento de la entidad, para el caso un /48.

- Asignar un prefijo /56 al sitio de la entidad administrado por el ISP.

- Asignar los prefijos /56 necesarios para el Data Center principal de la entidad y los enlaces WAN, que para el caso es administrado por el ISP en una ubicación remota.

- Elaborar cuadros de prefijos /64 partiendo de los prefijos /56 que fueron definidos para los sitios.

1. CUADRO DE PREFIJOS /56 PARTIENDO DEL PREFIJO DE LACNIC ASIGNADO PARA ESTE PLAN DE DIRECCIONAMIENTO

Para el caso del El Instituto de Movilidad de Pereira, que cuenta con dos sedes donde el DATACENTER central se definió un prefijo /48 y la sede principal con un prefijo /49. Las razones por las cuales se eligió este prefijo son las siguientes:

- **Escalabilidad:** El Instituto de Movilidad de Pereira se encuentra en constante crecimiento y puede haber posibilidades en el futuro de construir o aliarse con nuevas sedes en diferentes ciudades del país, el subnetting del prefijo /48 a prefijos /56 dará la posibilidad de conectar 4096 sedes.

- **Asignación de recursos:** Cada digito hexadecimal de una dirección IPv6 contiene 4 bits y se denomina NIBBLE, LACNIC recomienda que la solicitud del prefijo se realice en limites binarios, esto significa que se deben solicitar prefijos múltiplos de

4 para garantizar NIBBLES completos y facilitar la segmentación del prefijo, por esta razón se realiza la solicitud de un prefijo /48

Este procedimiento se realizará en dos sede que tiene la entidad. La red del Instituto de Movilidad de Pereira se define como una gran estrella cuyo punto central es un DATA CENTER ubicado en el edificio de Torre central de Pereira. Este DATA CENTER se comunican con la sede administrativa ubicada Cl. 14 #17-60, Pereira, Risaralda a los equipos para solicitar servicios, recursos y salida a internet con permisos de seguridad , el prefijo /48 prefijo entregado para direccionamiento a todas las sedes del Instituto de Movilidad de Pereira con un enfoque escalable, este prefijo permite la construcción de nuevas sedes y la configuración de más VLANS.

Verificando las necesidades actuales del El Instituto de Movilidad de Pereira, existen redes, que no se encuentra segmentadas mediante VLANs, cuenta con direccionamiento IPv4 estático y máscara de Subred de 24 Bits, es necesario replicar un modelo adaptable en el protocolo IPv6.

Como primera medida, como parte del proyecto actual se realizó la solicitud formal ante el RIR (Regional Internet Registry - para el caso de Colombia LACNIC) del direccionamiento IPv6 global de acuerdo con los lineamientos dados por MinTIC.

Así mismo y de acuerdo con las indicaciones de MinTIC, la solicitud de este direccionamiento a LACNIC genera unos costos de membresía a partir del primer año por suscripción y membresía anual.

Después de realizar un proceso exitoso de solicitud de recursos ante LACNIC, el servicio nacional de aprendizaje EL INSTITUTO DE MOVILIDAD DE PEREIRA (EL INSTITUTO DE MOVILIDAD DE PEREIRA) cuenta ahora con un prefijo IPv6 propio. El prefijo que

fue asignado por LACNIC es: 2801:1ca::/48[1] notación abreviada de 2801:01ca:0000:0000:0000:0000:0000:0000/48

Un ejemplo de asignación de direccionamiento IPv6 completo partiendo del prefijo asignado por LACNIC puede ser:

2801:1ca: 0000:0000:12ab:34cd:56ef:7890

Rojo: Direccionamiento otorgado por RIR (Regional Internet Registry) o ISP (/32).
Azul: Direccionamiento de la organización (/48).
Verde: Subred de la organización (/56 o /64).
Negro: ID (Interface ID) Dirección individual del host (/128).

De acuerdo con el ejemplo y teniendo en cuenta los aspectos sobre IPv4 enumerados anteriormente, es recomendable hacer una asignación de red de la organización basados en /64 para redes IPv6, en donde tienen cabida las redes actuales y permite una amplia proyección a nuevas redes. (En el ejemplo esto corresponde al segmento de color **verde**).

La asignación del direccionamiento propio de la red, para el caso actual del El Instituto de Movilidad de Pereira, cuyo direccionamiento IPv4 es por ejemplo 192.168.0.XX y 192.168.XX.XX, entre otros, de acuerdo al RFC 1918 de la IETF, para IPv6 en el ejemplo corresponde al segmento **Azul**, donde se hace la definición de la red; cabe anotar que esta dirección, así como en IPv4, es un identificador único y particular dentro de las redes y su asignación es definitiva, porque nombra la red y si es cambiado posteriormente puede generar incidentes de conectividad.

En el segmento **Negro** se denota el direccionamiento propio de cada o host IID (Interface ID).

[1] :: Representa una cadena continua de segmentos IPv6 que contienen únicamente cero (0).

Por último, el segmento **Rojo** es asignado por el ente regulador (LACNIC) o el ISP y NO es modificable ya que representa las direcciones globales.

1.1. DEFINICIÓN DEL DIRECCIONAMIENTO IPv6

La definición del direccionamiento propio en IPv6 para la Entidad se realiza en el segmento de color **Azul** como en el ejemplo. Cabe recordar que estas direcciones son asignadas en hexadecimal con dígitos del 0 – 9 y caracteres A, B, C, D, E, F.

Aquí se puede colocar el direccionamiento a consideración propia de la entidad cuyo valor debe ser único, por ejemplo: ::**1234**. Es importante considerar que después de nombrado este debería ser un direccionamiento definitivo, ya que su modificación afecta equipos de comunicaciones, aplicaciones, bases de datos y demás activos de información en la red.

Para la definición de las subredes en IPv6 es necesario tener en cuenta las necesidades propias de la entidad en cuanto a crecimiento a nivel de subredes. A continuación, se presenta un ejemplo mediante el cual se contextualiza la manera en la que se podría hacer dicha asignación.

Para el caso del Instituto de Movilidad de Pereira se tomará un prefijo que contiene direcciones de alcance global GUA definidas en el RFC2373 de documentación, esto quiere decir que se va a tomar 2801:1ca::/32 como la base del direccionamiento.

2801:1ca::/32

Tomando como base el prefijo asignado por LACNIC se selecciona un prefijo que cumpla con las necesidades de direccionamiento del (EL INSTITUTO DE MOVILIDAD DE PEREIRA) . Las condiciones que debe cumplir el prefijo son las siguientes: Número suficiente de Direcciones IPv6 y que sea múltiplo de cuatro para que esté en limite binario y facilite la segmentación. Para el caso de la entidad se selecciona un prefijo /48

2801:1ca:000::/48

Para asignar direccionamiento a la sede, data center y segmentos de WAN se usarán prefijos /56

2801:1ca: 0000:00::/56

Para asignar direccionamiento a cada una de las VLANs se usarán prefijos /64

2801:1ca: 0000:0000::/64

Definidos estos segmentos se pueden definir direcciones IPv6 de este tipo:

2801:1ca: 0000:0000:12ab:34cd:56ef:7890/64

2801:1ca: 0000:0000:12ab:34cd:56ef:7890/128

Azul Prefijo /48 y **Verde** Subred desde /48 hasta /64

Negro: Corresponde al direccionamiento propio de cada host o IID (interface ID), esta porción de la dirección IPv6 se puede configurar de forma estática o usando SLAAC (autoconfiguración de direcciones con estado) o DHCPv6 (protocolo de asignación dinámica de direcciones IPv6).

PREFIJO ASIGNADO POR LACNIC	**2801:1ca::/48**

1.2. ASIGNACIÓN DE PREFIJO IPv6 /56 PARA EL INSTITUTO DE MOVILIDAD DE PEREIRA

En el Anexo 1.1. Direccionamiento IPv6 EL INSTITUTO DE MOVILIDAD DE PEREIRA - Prefijo LACNIC_v1.xls se puede observar de manera detallada la segmentación que se va a realizar.

Se puede observar de manera precisa el prefijo /56 principal de la sedes y la segmentación en prefijos /64 suficientes para cubrir la red de la institución . Es importante mencionar que se tendrán en cuenta segmentos para VLANs de prueba, VLANs disponibles en caso de que la entidad las requiera para desplegar.

El plan de direccionamiento también contempla segmentos /56 de back up en caso de que en un futuro se requiera direccionamiento adicional o sistemas de contingencia.

1.3. SEGMENTOS QUE SE VAN A USAR PARA DATACENTER Y WAN

Tabla 1 Segmento a utilizar para Datacenter y WAN

2801:1ca:0002:0700::	**WAN DATA CENTER**
2801:1ca:0002:0800::	**WAN SEDE PRINCIPAL**

el prefijo 2801:1ca:0002:0700::/56 hasta el prefijo 2801:1ca:0002:0800::/56, se usarán para la WAN DATACENTER, esta porción del espectro de direccionamiento brinda la posibilidad de generar al menos 250 redes /64, para la infraestructura de seguridad, DMZ servidores y los demás servicios que se presten en el DATACENTER principal.

Este direccionamiento se va a cubrir con prefijos /64 que parten de cada prefijo /56 del sitio, esto significa que cada sitio va a contar con 255 subredes /64,

Para el caso de los equipos que se van a configurar con direccionamiento estático, se puede hacer la asignación manual teniendo en cuenta la ubicación física y el direccionamiento IPV4.

En la fase 2 dentro del documento “Plan Detallado de Implementación” quedará el detalle de las direcciones IPv6 de cada dispositivo que actualmente tiene una dirección IPv4 estática a nivel de datacenter principal, rango DHCP.

EJET!C
GRUPO EMPRESARIAL
Transformando la Sociedad

Tel:3142281086
Correo: gerencia@ejetic.com.co
Dirección:Calle 19 7-75 oficina 211 Edificio Braulio Londoño

Pereira, noviembre 30 de 2022

Señores
INSTITUTO DE MOVILIDAD DE PEREIRA
Ciudad.

ASUNTO: Presentación noveno informe política de Gobierno Digital, Contrato de Prestación de Servicios IMP-CO-128-2022.

Cordial saludo.

De la manera más atenta nos permitimos remitirles, los documentos propios del octavo informe para el pago según lo estipulado en el Contrato de Prestación de Servicios IMP-CO-128-2022, cuyo objeto es: ACTUALIZACION, SOPORTE Y MANTENIMIENTO "SOFTWARE PARA LA ADOPCION DE LA POITICA DE GOBIERNO DIGITAL – SAPGD" Y CONTINUIDAD DE LA FASE I DEL PROYECTO DE TRANSICION DEL PROTOCOLO IPV4 AL PROTOCOLO IPV6 EN EL INSTITUTO DE MOVILIDAD DE PEREIRA.

Según lo estipulado en el contrato del asunto y fundamentados en lo estipulado en las cláusulas:

SEGUNDA. OBLIGACIONES DEL CONTRATISTA: 1. Servicio de Actualización, soporte y mantenimiento "Software para la Adopción de la Pol tica de Gobierno Digital – SAPGD", con almacenamiento en la nube bajo el modelo SAAS por un a o m s. 2. Realizar capacitación a los contratistas y funcionarios que se requieran en los temas relacionados con Gobierno Digital, sus actualizaciones y el uso del "Software para la Adopción de la Política de Gobierno Digital – SAPGD". 3.Desarrollar en el "Software para la Adopción de la Política de Gobierno Digital – SAPGD", la actualización del Plan Estratégico de Tecnologías de la Información – PETI. 4.Desarrollar en el "Software para la Adopción de la Política de Gobierno Digital – SAPGD", la actualización de la Arquitectura Empresarial de la entidad. 5. Desarrollar en el "Software para la Adopción de la Política de Gobierno Digital – SAPGD", la actualización de las políticas y estándares de TI. 6. Apoyar en la continuidad de la implementación de la fase I del proyecto de

Tel:3142281086
Correo: gerencia@ejetic.com.co
Dirección:Calle 19 7-75 oficina 211 Edificio Braulio Londoño

transición de IPv4 a IPv6 en el "Software para la Adopción de la Política de Gobierno Digital – SAPGD", para el Instituto de Movilidad de Pereira. Por ser un proceso de contratación Directa se requiere que cumpla con las siguientes recomendaciones técnicas: 1. Entregar a la entidad la licencia de uso por un a o de una Plataforma o Software para la Adopción de la Pol tica de Gobierno Digital del Estado Colombiano entregada en el 16 de diciembre del 2020. 2. Entregar el certificado de registro de soporte lógico de software expedido por el Ministerio del Interior – Dirección Nacional de Derecho de Autor del Libro 13 – Tomo 72 – Partida 61 de fecha de registro 19-Febrero- 2019. 3. Anexar dos o m s contratos, facturas de venta, actas de liquidación o certificaciones de contratos que sumados superen el monto del presente proceso, como también que se encuentren relacionados con el objeto o alcances.

CUARTA. FORMA DE PAGO: El Instituto de Movilidad de Pereira, cancela al Contratista 9 pagos mensuales, una vez se haga efectiva la prestación de los servicios requeridos y la respectiva entrega de la papelería donde se allegue constancia suscrita por el supervisor designado en la que se manifieste el cumplimiento de las obligaciones a cargo del contratista y se surtan los trámites administrativos correspondientes.

La empresa Grupo Empresarial Ejetic SAS remite:

- Cédula de ciudadanía Contadora Pública.
- Certificado Junta central de contadores
- Certificado de Paz y Salvo de Parafiscales.
- Tarjeta Profesional Contadora
- Factura de venta electrónica.

- **INFORME 9**

Dentro del desarrollo del contrato, Grupo Empresarial Ejetic SAS ha seguido las guías de transición y aseguramiento elaboradas por el MinTIC, en las cuales se detallan los lineamientos para garantizar la seguridad, integridad, disponibilidad, privacidad y otros elementos y poder avanzar en la migración a IPv6, en las entidades públicas del Estado Colombiano, adicionalmente se ha realizado un proceso de acompañamiento y conciencia ante la escasez de direcciones IPv4 frente a la entidad y la necesidad apremiante de desarrollar todo este proceso de transición en el Instituto de Movilidad de Pereira y así no presentar dificultades para seguir operando normalmente.

Tel:3142281086
Correo: gerencia@ejetic.com.co
Dirección:Calle 19 7-75 oficina 211 Edificio Braulio Londoño

Con base en lo anterior, la empresa Ejetic SAS a través de su sistema de información realizó en todo su proceso de acompañamiento la ejecución de dicho protocolo IPV4 a IPV6 cuyos documentos son:

- Plan de transición IPV6
- Plan de direccionamiento IPV6
- Plan de contingencia

La anterior información hace parte integral del presente informe y son anexos adjuntos.

Mil gracias por la atención prestada, estaré atento a los requerimientos.

Atentamente,

JORGE MARIO VALENCIA MESA
Gerente
Grupo Empresarial Ejetic S.A.S.
Cel: 3142281086
E-mail: gerencia@ejetic.com.co