



El futuro digital
es de todos

MinTIC

Guía 2

Guía para el Aseguramiento del Protocolo IPv6

MinTIC – Viceministerio de Transformación Digital
Dirección de Gobierno Digital
Abril de 2021

ADOPCIÓN IPv6

Karen Abuninen Abuchaibe – Ministra de Tecnologías de la Información y las Comunicaciones

Germán Camilo Rueda Jiménez – Viceministro de Transformación Digital

Aura Maria Cifuentes Gallo – Directora de Gobierno Digital

Gersson Jair Castillo Daza – Subdirector de Estándares y Arquitectura de TI

Fernando Alirio Contreras Sánchez – Equipo IPv6

Elkin Giovanni Romero Maturana – Equipo IPV6

Versión	Observaciones
1.0.0	Borrador Inicial
2.0.0	Revisión Jorge Bejarano
3.0.0	Versión ajustada Ing. Fernando Contreras
4.0.0	Versión ajustada Ing. Fernando Contreras
5.0.0	Versión ajustada Ing. Fernando Contreras
6.0.0	Versión ajustada Ing. Fernando Contreras
7.0.0	Versión ajustada Equipo IPv6
7.0.1	Actualizaciones Equipo IPv6 – Jordi Palet

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:

sopORTECCC@mintic.gov.co



Esta guía de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons

Atribución 4.0 Internacional

Tabla de Contenido

1. Derechos de Autor	6
2. Audiencia	7
3. Introducción	8
4. Justificación	9
5. Objetivos Específicos	10
6. Términos y Definiciones	11
7. Características de IPv6.....	14
8. Lineamientos de Seguridad para IPv6	15
8.1 Lineamientos generales.....	15
8.2 Direccionamiento IP	17
8.3 Protocolo IPsec – Internet Protocol Security (IP Security)	18
8.4 Estructura del IPsec	20
8.5 Revisión de los RFC de Seguridad	20
8.6 Redes Privadas Virtuales – VPNs	20
8.7 Monitoreo de IPv6.....	21
8.8 Seguridad de IPv6 en los Centros de Datos.....	21
9. Pilares de la seguridad de la información en IPv6.....	23
9.1 Confidencialidad	23
9.1.1 Confidencialidad en Modo Transporte.....	24
9.1.2 Confidencialidad en Modo Túnel	24
9.2 Integridad	24
9.3 Disponibilidad	25
9.4 Privacidad	25
9.4.1 Cifrado antes de Autenticación	26
9.4.2 Autenticación antes del Cifrado	26
9.4.3 Riesgos a la Privacidad.....	26
9.5 Servicios Impactados en Seguridad	26
10. Análisis de Riesgos.....	29
10.1 Valoración del Activo de Información	29
10.2 Gestión del Riesgo para el proceso de transición de IPv4 a IPv6	30
10.3 Hacking Etico	30
10.3 Pruebas de penetración en redes IPv4/IPv6	31

11. Lineamientos de seguridad en la nube bajo IPv6	33
12. Recomendaciones para mitigar riesgos en IPv6	35
12.1 Reconocimiento de los riesgos de las configuraciones de Doble Pila	35
12.2 Des-habilitación y bloqueo de IPv6	36
12.3 Traducción de direcciones de red	36
12.4 Ataques en ambientes IPv6	36
12.5 Riesgos de utilización de túneles de IPv6 a IPv4	37
12.6 Escaneo en redes IPv6	38
13. RFCs de seguridad en IPv6.....	39
14. Conclusiones.....	41
15. Anexo 1	43
15.1 Sistema RPKI para Recursos Numéricos Asignados en la Región (LACNIC)	43
15.1.1 Actividades de Estandarización	43
15.1.2 Función de Certificación de Recursos (RPKI)	43
15.1.3 Especificaciones de la RFC 4593 – Generic threats to routing protocols.....	44
16. Anexo 2	46
16.1 Resumen del BCOP	46
16.2 Transfondo del BCOP / Historia.....	46
16.3 Texto del BCOP	47
16.3.1 Requisitos para “equipamiento de seguridad en la red”	47
17. Referencia.....	50

Tablas

- Tabla 1. Valoración de Activos de Información 29
- Tabla 2. Gestión del Riesgo para el Proceso de Transición 30
- Tabla 3. Hacking Ético..... 30
- Tabla 4. Ejemplo Hacking Ético..... 30

1. Derechos de Autor

- Todas las referencias a los documentos de adopción del protocolo IPv6, cuentan con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Subdirección de Estándares y Arquitectura de Tecnologías de la Información – Dirección de Gobierno Digital.

2. Audiencia

- Sujetos obligados de las disposiciones contenidas en el Artículo 2 Ámbito de aplicación de la Resolución 2710 de 3 de octubre de 2017, las entidades de que trata el Artículo 2.2.9.1.1.2 del Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que requieran adoptar el protocolo IPv6, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial y la Subdirección de Estándares y Arquitectura de TI de la Dirección de Gobierno Digital.

3. Introducción

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 y políticas que se requieren tener en cuenta en el marco de la seguridad del protocolo IPv6, en las distintas infraestructuras de Tecnologías de la Información y las Comunicaciones que las Entidades del Estado, teniendo en cuenta su aplicación en todo el ciclo de desarrollo que sigue el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar el proceso de adopción de IPv6 bajo un buen esquema de seguridad informática y con un nivel de impacto altamente positivo para todas las organizaciones del país.

4. Justificación

- El Ministerio de las Tecnologías de la Información y las Comunicaciones, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial y la Subdirección de Estándares y Arquitectura de TI, pone a disposición de las entidades, la siguiente guía la cual permite a éstas, contar con una línea base para el análisis, desarrollo e implementación del protocolo IPv6, de conformidad con los lineamientos establecidos en la Resolución 2710 de octubre de 2017.

5. Objetivos Específicos

- Presentar un marco de referencia sobre lineamientos de seguridad en IPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y pruebas de funcionalidad del proceso de transición de IPv4 a IPv6 en cada una de las Entidades del Estado, para adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación de los diferentes organismos del Estado.

6. Términos y Definiciones

- Presentar un marco de referencia sobre lineamientos de seguridad en IPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y pruebas de funcionalidad del proceso de transición de IPv4 a IPv6 en cada una de las Entidades del Estado, para adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación de los diferentes organismos del Estado.

- **Análisis de riesgos:** Proceso que comprende la identificación de activos de información y las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del mismo.

- **Confidencialidad:** La información debe ser accesible solo por aquellas personas autorizadas.

- **DHCPv6 (*Dynamic Host Configuration Protocol*):** Protocolo de Configuración Dinámica de Hosts para IPv6 con característica cliente-servidor y definido por la RFC 8415 de la IETF, que proporciona una configuración administrada de dispositivos sobre redes IPv6.

- **Dirección IPv6:** Es un identificador numérico único configurado en una interfaz de red que provee una conexión entre nodos de una red sobre IPv6, y facilita el enrutamiento de los paquetes entre distintos hosts.

- **Disponibilidad:** Capacidad de garantizar que tanto la información como los servicios van a estar accesibles y utilizables en todo momento.

- **DNS (*Domain Name System*):** Sistema de Nombres de Dominio que contiene un sistema de nomenclatura jerárquica para equipos de computación. Los DNS contienen una base de datos que tienen la función de indicar la IP que está asociada a un nombre de un sitio web (Resolución de nombres).

- **Encapsulamiento:** Es un mecanismo usado en los túneles de comunicación que permiten contener paquetes IPv6 dentro de un paquete IPv4 y enviarlo por una red IPv4 o viceversa, ejemplos de esto son los encapsulamientos 6in4 o 4in6.

- **ICMPv6 (*Internet Control Messsage Protocol for IPv6*):** El protocolo de mensajes de control ICMPv6, es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes

y para realizar otras funciones de la capa de Internet como el diagnóstico, combina funciones que anteriormente estaban contempladas por varios protocolos tales como ICMP, IGMP y ARP, adicionalmente introduce algunas mejoras.

IPv6: Es la nueva versión del Protocolo de Internet (Internet Protocol - IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90 en el IETF (*Internet Engineering Task Force*). Hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en sustitución de IPv4.¹

IPsec (IP Security): Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

Integridad: La información y sus métodos de procesamiento deben ser completos y exactos con la finalidad de protegerlos por tener valor para las organizaciones.

Protocolo de Comunicaciones: Conjunto de convenciones y reglas a procedimientos que permiten el intercambio de la información entre diferentes elementos de red.

RFC (*Request For Comments*): Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos aprobadas por el IETF - Engineering Task Force. Describen aspectos técnicos del funcionamiento de Internet y otras redes de comunicaciones, protocolos, procedimientos y comentarios o ideas para clarificar o corregir aspectos técnicos que garanticen buenas prácticas de trabajo.

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

RPKI (*Resource Public Key Infrastructure*): Es el mecanismo estándar de IETF de Certificación de Recursos, cuyo objetivo es la emisión de material criptográfico que permita a sus miembros, demostrar digitalmente que poseen el derecho de uso de direcciones IPv4 e IPv6.

SNMP (*Simple Network Management Protocol*): Es un protocolo Simple de Administración de Red de capa de aplicación, que facilita el intercambio de información de administración entre

¹ Fuente: <http://portalipv6.lacnic.net/que-es/>

dispositivos de red, siendo un componente de la suite de protocolos de Internet como se define en la IETF.

7. Características de IPv6

- El Protocolo de comunicaciones IPv6 Internet Protocol Version 6, fue desarrollado por Steve Deering y Craig Mudge en el año 1994, y posteriormente fue adoptado por la IETF (Internet Engineering Task Force), inicialmente también conocido como IPng (IP Next Generation). El nuevo protocolo tiene el propósito de reemplazar progresivamente el protocolo IPv4 actualmente en uso por la comunidad de Internet, en razón al limitado número de direcciones de IPv4 que no hace posible su crecimiento en las redes y servicios. Las características generales del nuevo protocolo son:
 - ✓ Definido por la RFC (Request For Comments)² 2460 de 1998.
 - ✓ Actual estándar bajo el RFC 8200 de julio de 2017.
 - ✓ Tamaño del paquete 128 bits.
 - ✓ Encabezado de base simplificado y de extensión.
 - ✓ Identificación de flujo de datos, que facilita nuevos mecanismos de calidad de servicio (QoS).
 - ✓ Direccionamiento Anycast, Multicast y Unicast.
 - ✓ Puede incorporar mecanismos de IPSec (IP Security) al protocolo, ofreciendo mejoramiento de las capacidades de autenticación y privacidad de los datos que transmite porque los paquetes que proceden de un origen son los indicados en la cabecera de autenticación, mientras que en IPv4, los paquetes pueden venir de orígenes distintos a los indicados en la cabecera.
 - ✓ Fragmentación y re-ensamblado exclusivamente entre origen y destino.
 - ✓ Conectividad Extremo a Extremo.
 - ✓ Interacción con nodos vecinos a través del protocolo ICMP (Internet Control Message Protocol for IPv6).
 - ✓ Mecanismos de seguridad avanzada sobre los datos transmitidos.
 - ✓ Espacio de direccionamiento de 340 Sextillones (asimilable a 340 trillones de direcciones por pulgada cuadrada, 670 mil billones de direcciones por metro cuadrado).
 - ✓ Extensibilidad.

² RFC: "Request For Comments" Solicitud de Cambios ante una labor técnica de emergencia

8. Lineamientos de Seguridad para IPv6

8.1 Lineamientos generales

- ✓ La fase de implementación del protocolo IPv6 debe ser estructurada con base en los esquemas de seguridad de información, sobre los cuales se tengan contempladas las políticas de confidencialidad, integridad y disponibilidad de las Entidades
- ✓ Dentro de la fase de planeación, se recomienda definir un plan de marcha atrás (Plan de Contingencias de IPv6) para el caso de presentarse inconvenientes de indisponibilidad de los servicios ya sea porque algunos elementos no cumplen con IPv6 o porque dada su configuración inicial pueden atentar contra la seguridad de los sistemas de información y de las comunicaciones de las Entidades al momento de implementar el protocolo IPv6, ver la Guía de transición de IPv4 a IPv6 para Colombia³
- ✓ En el proceso de transición hacia el nuevo protocolo, es importante revisar la seguridad de información de las infraestructuras de TI, la seguridad informática de IPv6 y el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio - DNS, Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC8415 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Sistemas de almacenamiento, Servicios Web y Sistemas de Gestión y Monitoreo.
- ✓ Se debe mantener la utilización de los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6, de tal manera que la resolución de nombres de dominio sea transparente en las dos versiones del protocolo IP. Se exceptúa de esta regla los ambientes de prueba que se realicen sobre IPv6.
- ✓ Para el caso de las aplicaciones, al igual que ocurre con IPv4, en IPv6 se recomienda no usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías.
- ✓ Se debe garantizar que los dispositivos, servicios y aplicaciones son capaces de funcionar con IPv6-only, manteniendo los mismos niveles de seguridad que en doble-pila.

³ https://www.mintic.gov.co/portaf/604/w3-article-5903.htm?_noredirect=1

- ✓ Se recomienda diseñar y desarrollar aplicaciones totalmente parametrizadas de tal manera que cualquiera de estas pueda funcionar con las dos versiones de IP, y siempre que sea posible, de forma automática, dependiendo del DNS.
- ✓ Generar la documentación necesaria que contemple los aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surjan del desarrollo de la implementación de IPv6.
- ✓ La implementación de IPv6 puede generar riesgos de seguridad de información, que impactan en los servicios de las entidades y pueden acarrear problemas; con el objeto de poder detectar estos riesgos se requiere hacer un análisis detallado que permita encontrar posibles vulnerabilidades y en efecto bajo IPv6, es necesario hacer esta labor debido a que el protocolo se apoya en otros protocolos como IPSec, HTTP/S, TCP, UDP o SIP.
- ✓ Disponer para las infraestructuras de TI, de varias zonas lógicas configuradas en el firewall, que estén segmentadas para cada uno de los servicios disponibles en la Entidad, a fin de garantizar la máxima protección una vez la red de comunicaciones comience a generar tráfico en IPv6.
- ✓ Disponer del equipo humano idóneo necesario para verificar y monitorear los problemas de seguridad de información que surjan al momento de ejecutar las fases de implementación y pruebas de funcionalidad, cuya labor está bajo la responsabilidad del Director de Seguridad de la Información – CISO (Chief Information Security Officer) o del que haga sus veces y del equipo de trabajo de seguridad de las Áreas de TI de cada Entidad.
- ✓ La verificación y el entendimiento de los componentes de seguridad diseñados para el protocolo IPv6, son claves para evaluar, monitorear y mejorar el desempeño de los servicios y aplicaciones bajo IPv6, cuando estos empiecen a generar tráfico en los canales de IPv6. En este sentido el documento sobre “Política para la adopción de IPv6 en Colombia, estructuración y definición de Cintel y Mintic del año 2012”, dice:

“Se debe dar paso a la transición de IPv4 a IPv6 como una herramienta para mejorar las condiciones de seguridad nacional y la seguridad de la información. Siempre que la adopción de IPv6 facilita las tareas de monitoreo y refuerza los protocolos de seguridad nacional, dado que con IPv6 cada usuario, cada equipo, cada terminal móvil puede recibir, de forma estática, una dirección IP que lo identifica, lo cual hace posible establecer con certeza la ubicación y el origen de la comunicación y permite adoptar medidas de seguridad que redundarán en beneficios para todos.”

Así mismo el protocolo IPv6 debido a su gran cantidad de direcciones disponibles, no tiene como política manejar direcciones IP públicas o privadas, ya que por su naturaleza son direcciones globales – *Global Unicast Address* - (GUA), por lo que elimina toda clase de

elementos que permite “esconder” direcciones IP públicas en la comunicación (como uso de NATs Network Address Translation – Traducciones de red), lo cual parece minimizar los riesgos de intrusión en la red; sin embargo, lo anterior no quiere decir que el protocolo IPv6 sea más seguro que IPv4, aunque una adecuada implementación incrementa la protección de las redes. Además, al no requerir NATs, se puede utilizar IPsec, extremo-a-extremo, incrementando los niveles de seguridad en la red.”⁴

- ✓ Se recomienda al equipo de seguridad de cada entidad consultar el RFC 7721 y draft-ietf-opsec-v6, que establecen consideraciones de seguridad y privacidad al momento de utilizar IPv6.

8.2 Direccionamiento IP

- ✓ Para el comportamiento del tráfico de IPv6, se requiere tener en cuenta el uso de las directivas de seguridad del protocolo IPsec, para ambientes que requieren atender solicitudes de servicios HTTP/S entre nodos IPv6.
- ✓ Considerar la revisión de los segmentos de bloque de direcciones en IPv6 y si este se ha realizado por zonas lógicas de seguridad (Zonas Desmilitarizadas – DMZ) con base en las necesidades de operación de cada organización y estableciendo los criterios de seguridad correspondientes.
- ✓ La utilización de los bloques de direccionamiento en IPv6, deben acoger las políticas de seguridad y privacidad de la información permitiendo que el funcionamiento de las mismas, sea transparente para los usuarios finales de la Entidad.
- ✓ Los planes de direccionamiento en IPv6 se deben realizar con base en los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.
- ✓ Se requiere tener en cuenta dentro de la configuración de los firewalls que, si se requieren hacer pruebas de monitoreo de estado en el tráfico de IPv6, este debe hacerse mediante descubrimiento de vecinos (*ND – Neighbor Discovery*), esto en ocasión a que las interfaces de IPv6 no usan ARP como es normal en IPv4.
- ✓ La utilización del direccionamiento IPv6 debe realizarse en forma espaciada, no consecutiva y en la medida de lo posible aleatoria, como recomendación general, a fin de evitar ataques de direccionamiento IP tanto del interior como del exterior en modalidad de “fuerza bruta”.

⁴ Documento Política para la Adopción del IPv6 en Colombia, estructuración y definición, numeral 12.10, página 72, 73, 2012, Contrato 947 Mintic, Cintel, año 2012.

- ✓ Se recomienda crear VLANs (Redes de Área Local Virtuales) por separado dentro de las redes locales de las organizaciones para propósitos de pruebas de direccionamiento, tráfico, monitoreo y seguridad cuando se comience la fase de implementación del nuevo protocolo.
- ✓ En redes IPv6 los paquetes pasan por distintas etapas de enrutamientos, con el fin de mitigar el espacio de búsqueda de posibles atacantes de escaneo sobre las redes IPv6, por lo tanto, se recomienda que los administradores de las redes utilicen herramientas de software de monitoreo para controlar posibles patrones de comportamiento de direccionamiento IP aún si el tráfico generado es no-dirigido (multicast) y se utiliza descubrimiento de vecinos (Neighbor Discovery)⁵.
- ✓ Los paquetes IPv6, deben seguir las recomendaciones de seguridad de los paquetes IPv6, consistente en que estos contienen cabeceras de autenticación (AH, Authentication Headers) y encabezados de extensión de carga de seguridad encapsulada (ESP, Encapsulating Security Payload), en la cual el protocolo IPsec permite para cualquier nodo de IP el establecimiento de sesiones de seguridad de extremo a extremo.
- ✓ Es necesario hacer una clasificación de reglas de firewall, teniendo en cuenta servicios por puertos, por aplicaciones, por ambientes web y por red, dado que las reglas de IPv4 dentro del firewall deben seguir trabajando en paralelo con las reglas de IPv6.
- ✓ Los servicios u objetos de IPv4 deben tener una equivalencia con los servicios u objetos de IPv6, teniendo en cuenta que IPv4 trabaja con máscaras de subred para calcular su tamaño, mientras que IPv6 lo hace siempre con prefijos /64 para cada segmento de red o VLAN, que es independiente de las máscaras de IPv4.

8.3 Protocolo IPsec – Internet Protocol Security (IP Security)

IPsec es un protocolo de seguridad definido por el RFC 4301 del estándar IETF⁶ desde 1999, que establece las siguientes consideraciones:

Según la IETF, "IPsec está diseñado para proporcionar interoperabilidad, de alta calidad, con seguridad basada en cifrado tanto para IPv4 como para IPv6.

⁵ Más información de este tipo de ataques característicos en el RFC 4941.

⁶ IETF (Internet Engineering Task Force) o Grupo de Trabajo de Ingeniería de Internet, entidad que regula las propuestas y los estándares de Internet, conocidos como RFC

El conjunto de servicios de seguridad ofrecidos en IPsec, incluyen control de acceso, integridad sin conexión, autenticación de origen de los datos, detección y rechazo de repeticiones (una forma parcial de integridad secuencial), confidencialidad a través de cifrado y confidencialidad de flujo de tráfico limitado.

Estos servicios se proporcionan en la capa 3, ofreciendo protección de manera estándar para todos los protocolos que pueden ser transportados a través de IP.

IPsec incluye una especificación para una mínima funcionalidad de firewall, ya que es un aspecto esencial de control de acceso en la capa IP. "Las implementaciones son libres de implementar mecanismos de firewalls sofisticados exigidos por IPsec."⁷

IPsec por lo tanto contiene las siguientes características:

- ✓ Integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores.
- ✓ IPsec es un componente opcional dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad e integridad; es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.
- ✓ Así mismo, IPsec, es el protocolo para cifrado y autenticación IP el cual forma parte integral del protocolo IPv6. El funcionamiento de IPsec es clave en IPv6 y se usa para cifrar el tráfico entre enrutadores BGP (Boundary Gateway Protocol); su uso se extiende para protocolos de enrutamiento tipo OSPFv3 (Open Shortest First Path).
- ✓ De acuerdo a lo anterior, el protocolo IPsec puede ser utilizado en diferentes escenarios a nivel de enrutamiento, por ejemplo con OSPFv3, que utiliza AH, la extensión de encabezados maneja ESP como un mecanismo de autenticación en lugar de la variedad de esquemas de autenticación y procedimientos definidos en OSPFv2; en IPv6 Móvil, donde esta especificación de protocolo es un proyecto de la IETF propuesto para usar IPsec para hacer obligatoria la autenticación de actualización; en Túneles, en la cual IPsec pueden ser configurado entre sitios (enrutadores IPv6) en lugar de que cada equipo utilice IPsec y finalmente administración de red, en la cual IPsec se puede utilizar para garantizar el acceso del enrutador para la gestión de la red⁸.

⁷ Fuente: <https://tools.ietf.org/html/rfc4301>

⁸ Tomado de <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>

8.4 Estructura del IPsec

- ✓ El protocolo contiene un primer encabezado llamado Cabecera de Autenticación – Authentication Header (AH), el cual provee integridad y autenticación del origen y protección contra duplicados. La Autenticación de Encabezado IPsec protege la integridad de la mayoría de los campos de encabezado de IPv6, excepto aquellos que cambian sobre los enrutamientos, de la misma forma como lo hace el campo “Límite de Salto” del paquete adicionalmente el AH autentica el origen por medio de un algoritmo de cifrado.
- ✓ El segundo encabezado llamado “Encapsulado de Seguridad de Carga Útil” - IPsec (ESP – Encapsulating Security Payload), el cual provee confidencialidad, autenticación del nodo origen, integridad interna del paquete y protección contra duplicación.

8.5 Revisión de los RFC de Seguridad

- ✓ Se precisa revisar los RFC de seguridad, en especial el RFC 4942 que hace referencia a las consideraciones de seguridad para el proceso de coexistencia y transición a IPv6.
- ✓ Se requiere revisar el RFC 6177 y RIPE690, cuya especificación técnica se refiere a las recomendaciones que deben seguir los clientes para solicitar asignación de segmentos de IPv6 en el rango de /48 para cada “sitio” en el caso de Entidades.
- ✓ Como se mencionó anteriormente, se recomienda a cada entidad consultar el RFC 7721 y draft-ietf-opsec-v6, que establecen consideraciones de seguridad con IPv6
- ✓ Revisar los procedimientos de RFC de seguridad para la utilización del software de aplicativos, equipos de comunicaciones, redes, sistemas de cifrado, dispositivos móviles, entre otros.
- ✓ Teniendo en cuenta los activos de información de las Entidades, se requiere clasificar las aplicaciones de acuerdo con una matriz de riesgos que permita determinar los niveles de seguridad de estas. Para este punto es necesario revisar los RFCs que indican las recomendaciones a seguir con respecto a la seguridad en las aplicaciones⁹.

8.6 Redes Privadas Virtuales – VPNs

⁹ Ver www.mintjic.gov.co/ipv6

En caso de que en las Entidades tengan como parte de su diseño una o varias conexiones privadas virtuales extremo a extremo que permiten intercomunicar dos o más redes locales (LAN); es importante tener presente el control del tráfico entre varios puntos de la red IPv6. En este orden de ideas, el tráfico IPv6 puede pasar por muchos recursos compartidos en una red de amplia cobertura, razón por la cual es necesario garantizar la seguridad del tráfico de las comunicaciones entre estas redes privadas virtuales con la utilización del protocolo de seguridad.

8.7 Monitoreo de IPv6

Las pruebas de funcionalidad (monitoreo) en IPv6 no solo deben ser tenidas en cuenta en la fase de pruebas del modelo de transición de IPv4 a IPv6, sino que también debe permitir establecer el nivel de funcionamiento y criticidad de las redes IPv6 ya en operación, por lo que es necesario tener en cuenta la detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad y tener un plan de contingencias a la mano.

Las siguientes son las variables a tener en cuenta a la hora de realizar monitoreo de los servicios de red en IPv6:

- ✓ Medición de tráfico sobre interfaces y dispositivos de red.
- ✓ Estado de servicios
- ✓ Estado de aplicaciones
- ✓ Actividad de los hosts y
- ✓ Canales de comunicación hacia Internet.

Para ello es importante contar con herramientas de monitoreo, como por ejemplo analizadores o balanceadores de tráfico que provean análisis de interfaces de red, monitoreo de librerías de IPv6 y soporte sobre SNMP.¹⁰

Cada Entidad debe estar en capacidad de utilizar libremente las herramientas de prueba y/o de monitoreo una vez implementado IPv6, teniendo en cuenta que la complejidad de cada una de estas no es lo importante sino los resultados exitosos que arroje el mismo.

8.8 Seguridad de IPv6 en los Centros de Datos

¹⁰ SNMP: Simple Network Management Protocol - Protocolo Simple de Administración de Red

Al momento de implementar IPv6 en las organizaciones, los centros de datos son los elementos importantes para revisar por ser los ejes centrales de todas las operaciones tecnológicas de la empresa, por lo tanto, tal y como se menciona en muchas entidades, "Existen varias formas de introducir y operar IPv6 en Centros de Datos". Una forma es continuar con una operación IPv4 dentro del centro de datos y hacer algún tipo de traducción en el borde (no recomendable de acuerdo con los lineamientos del gobierno)¹¹; una segunda forma es usar la doble pila y una tercera es usar únicamente IPv6.

En resumen, tenemos:

- Traducción de IPv4 en el borde: En este escenario el centro de datos mantiene su infraestructura interna en IPv4 y hace algún tipo de traducción a IPv6 en el borde.
 - Doble-pila: Aquí encontramos doble-pila a través todos los servicios del centro de datos o al menos en los que presentan servicios a usuarios. También puede encontrarse doble-pila solo en el borde mientras que las conexiones internas son IPv4 o IPv6 únicamente.
 - Solo-IPv6: Esta es generalmente la etapa final de la transición de un centro de datos a IPv6. Aquí encontramos IPv6 en todos los elementos del centro de datos. Para ofrecer servicios a los usuarios legados de IPv4 se utiliza algún tipo de traducción en el borde.
- El uso de estos escenarios no es necesariamente en la forma secuencial descrita y tampoco ninguna es el mejor, el más correcto o el recomendado. Cada uno ofrece diferentes beneficios y desventajas que deben ser analizados para seleccionar la mejor opción, sin embargo, el agotamiento de IPv4 hace inviable mantener IPv4 y por ello a menudo es recomendable IPv6-only con traducción en el borde, preservar sin costo adicional los servicios y aplicaciones legendarias de las entidades de forma transparente.

La mayoría de los aspectos de seguridad de IPv6 se aplican a los centros de datos, los cuales pueden encontrarse en el documento que aparece en¹². Sin embargo, un aspecto importante son los ataques a *Neighbor Discovery Protocol* (NDP). Este ataque es similar a los ataques de ARP de IPv4 y el atacante puede llenar el caché de vecinos y consumir la memoria del enrutador resultando en la inhabilidad de éste para reenviar paquetes.¹³

11 Ver Guía de Transición de IPv4 a IPv6 para Colombia, <http://www.mintic.gov.co/portal/604/w3-article-5903.htm>

12 Operational Security Considerations for IPv6 Networks, draft-ietf-opsec-V6. Chittimageni, K., Kaeo, M., And E.Vyncke.2013

13 Tomado de http://portalipv6.lacnic.net/wp-content/uploads/2015/02/ipv6_operadores_red-tablets.pdf, IPv6 para operadores de red, Alejandro Acosta, Santiago Aggio y otros; Internet Society ISO-AR Capítulo Argentina, pág. 83

9. Pilares de la seguridad de la información en IPv6

Dado que IPv6 permite extremo a extremo el protocolo, Internet Protocol Security- IPSec, la seguridad se establece de acuerdo con las características esenciales de este mismo, lo que permite que el paquete de IPv6 (de 128 bits) pueda salir a la red de Internet completamente cifrado sin que tengan que intervenir procesos como la traducción de direcciones (NAT) que reducen considerablemente el desempeño de las direcciones IP y no deberían ser considerados, dado que estos conceptos no son la naturaleza del IPv6. Debido al gran número de direcciones IPv6 para atender el despliegue de nuevos servicios en la comunidad de Internet, es necesario aplicar lineamientos de seguridad tal y como se realizan actualmente con IPv4 en aplicaciones y servicios, porque a pesar de que las entidades comienzan a desplegar tráfico en IPv6, los constantes ataques de los hackers no se hacen esperar. Por lo tanto, es importante desarrollar políticas de seguridad bajo los pilares básicos de la seguridad de la información que son: la Confidencialidad, la Integridad y la Disponibilidad.

9.1 Confidencialidad

- La Confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.¹⁴
- Desde el punto de vista de la estructura del protocolo mismo, el paquete IPSec, maneja dos protocolos de seguridad; de un lado uno relacionado con la Cabecera de Autenticación (AH), encargado de proporcionar autenticidad de los datos, integridad y no repudio y por el otro lado el Encapsulado de Carga Útil (ESP), consistente en proporcionar confidencialidad mediante el cifrado de los datos.
- Este último, el Encapsulating Security Payload (ESP) de la cabecera de IPv6 puede utilizar un algoritmo de cifrado encargado de proporcionar integridad, autenticidad, y confidencialidad de la información.
- Es preciso tener en cuenta que el uso de la Cabecera de Autenticación del paquete datagrama IPv6, genera aumento de latencia de las comunicaciones, esto debido principalmente al cálculo de la

¹⁴ http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad

información de autenticación por parte del nodo origen y el cálculo de comparación de la información de autenticación por el nodo destino de cada datagrama IPv6.

Tanto la AH, como el ESP, son instrumentos para el acceso de datos con base en la distribución de flujo de tráfico de paquetes y claves cifradas. Estos métodos permiten trabajar en dos modalidades, a tratar en los siguientes puntos.

9.1.1 Confidencialidad en Modo Transporte

Al generar tráfico, las cabeceras de IP están al descubierto, por lo cual es posible saber con quién se están comunicando los nodos dentro del flujo de información, aunque existe confidencialidad en los datos, ver siguiente esquema:

Paquete IPv6 una vez aplicado el campo Cabecera de Autenticación AH.

Cabecera IP de Origen	Saltos del paquete	Cabecera de Autenticación AH	Destino del paquete	TCP	Datos
-----------------------	--------------------	------------------------------	---------------------	-----	-------

9.1.2 Confidencialidad en Modo Túnel

En este modo se cifra la cabecera IP y se crea una nueva (se encapsula), con la dirección del enrutador de tal manera que con este elemento se puede saber a qué red se envía la información, aunque no necesariamente a que usuarios, ver siguiente esquema:

Paquete IPv6 después de aplicado el campo Cabecera de Autenticación AH.

Nueva Cabecera IP	Cabecera de Extensión	Cabecera de Autenticación AH	Cabecera IP de Origen	Cabecera de Extensión	TCP	Datos
-------------------	-----------------------	------------------------------	-----------------------	-----------------------	-----	-------

9.2 Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad consiste en mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.¹⁵

¹⁵ http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad

Desde el punto de vista del paquete IPv6, la integridad apunta a relacionar la Cabecera de Autenticación (AH) y el Encapsulado de Seguridad de Carga Útil (ESP), con la integridad de los datos asegurando los datos al momento de generar tránsito de paquetes a través de la red IPv6.

Complementariamente a lo anterior, dentro de la estructura del paquete IPv6, la AH permite proporcionar integridad y autenticidad de los datos por medio de una función de autenticidad cifrada sobre los datagramas de IPv6 que se hace por medio de una clave de autenticación.

El esquema de funcionamiento para proveer seguridad se establece cuando el nodo origen procesa la información de autenticidad antes de enviar el paquete cifrado de IPv6 por la red y el nodo receptor chequea la información autenticada cuando la recibe; el Campo Límite de Saltos (Hop Limit), contenido en la estructura del paquete IPv6, puede ser omitido en el cálculo de la autenticidad en razón a que este evalúa constantemente los número de saltos de ruteo producidos en la red y no el tiempo de vida de los mismos sin afectar la seguridad de los datos.

Los algoritmos de autenticación utilizados en el campo de Cabecera de Autenticación podrían producir no repudio (es decir que tanto las claves del nodo origen como del nodo destino se utilizan en el cálculo de la autenticidad)¹⁶, esta característica no es nativa de todos los algoritmos de autenticación que pueden utilizarse en el campo de Cabecera de Autenticación de IPv6.

9.3 Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.¹⁷

La disponibilidad en soluciones bajo IPv6, se puede visualizar en la garantía de ofrecer a los usuarios finales una alta disponibilidad en servicios y aplicaciones bajo IPv6, sin embargo es necesario prever que los servicios de las redes tanto a corto como a mediano plazo se establezcan en coexistencia con los protocolos IPv4 y IPv6, lo cual implica que las entidades tendrán que tener configurados los sistemas de enrutamiento para el soporte simultáneo de ambos protocolos a fin de mantener la continuidad del negocio y proteger las inversiones.

9.4 Privacidad

¹⁶ No repudio es la propiedad que tiene un nodo receptor de ser capaz de verificar que el nodo emisor dice ser el que envió una información, aun cuando el emisor pudiera negar posteriormente haber enviado la información

¹⁷ http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad

En virtud de que los procesos de traducción de direcciones de red, o NAT (Network Address Translation); en IPv4 no existen, surge el problema de mantener la privacidad en los accesos de IPv6, para ello es necesario plantear niveles y servicios de privacidad de IPv4 en IPv6.

En IPv6 se pueden combinar dos esquemas de seguridad de IP para transmitir un paquete IPv6, por un lado, la autenticación y por el otro la privacidad. Las técnicas se puedan utilizar de acuerdo con el orden en que se apliquen esto dos servicios de la siguiente manera:

9.4.1 Cifrado antes de Autenticación

- Este procedimiento sucede cuando el paquete IP es transmitido y autenticado en su totalidad, previo a un esquema de cifrado en los extremos. Primero se aplica la Carga de Seguridad Encapsulada - ESP a los datos que se van a proteger y después se incorpora el texto original al comienzo de la cabecera de autenticación IP.

9.4.2 Autenticación antes del Cifrado

- La Cabecera de Autenticación se encapsula dentro del paquete IP interno. Este paquete interno es autenticado y protegido por el esquema de privacidad. Esta técnica sólo es adecuada para el Encapsulado de Carga Útil - ESP en modalidad de túnel. El método puede preferirse en virtud de que la cabecera de autenticación AH se protege por la Carga de seguridad encapsulada ESP y de esta forma es muy complejo que los mensajes del paquete sean interceptados y modifiquen la AH sin ser detectado.

9.4.3 Riesgos a la Privacidad

- Como se había expresado al comienzo del punto 7.4, con la desaparición de la traducción de direccionamientos de red, o NAT (*Network Address Translation*); comúnmente utilizado en IPv4, surge el riesgo de mantener la privacidad en los servicios de acceso de IPv6, para ello es necesario plantear mejores niveles y servicios de privacidad de IPv4 en IPv6.

9.5 Servicios Impactados en Seguridad

- Los siguientes son los servicios que impactan en la seguridad de las Entidades al momento de iniciar el plan de implementación del nuevo protocolo IPv6:

- ✓ Directorio Activo
- ✓ DNS (Domain Name System)

- ✓ DHCP (Dynamic Host Configuration Protocol)
 - ✓ Servicios Proxy
 - ✓ Dominio de red
 - ✓ Correo electrónico
 - ✓ Mensajería Instantánea
 - ✓ Telefonía IP
 - ✓ Video Conferencia
 - ✓ Servicio Web y Acceso a Internet
 - ✓ Aplicaciones y bases de datos
 - ✓ Equipos de comunicaciones fijos y móviles
 - ✓ Equipos de seguridad (Firewalls, Servidores AAA (Authentication, Authorization and Accounting), NAC (Network Access Control))
 - ✓ Canal de Comunicación de Internet.
- Los requerimientos de seguridad son inherentes al protocolo mismo en especial de la capa de enrutamiento IP, donde IPv6 ha realizado un gran labor de seguridad con la estructura del paquete, pero los demás aspectos de seguridad que son del entorno de las redes y servicios de comunicaciones, requieren seguir trabajando con políticas de seguridad informática bien robustas y mejoradas tal y como se definen actualmente para IPv4; del mismo modo la implementación de IPv6 deberá hacerse bajo el establecimiento de una conexión extremo a extremo, en razón al gran número de direcciones disponibles sobre las cuales ya no son requeridos los mecanismo de NAT (Network Access Translation) que permitían la optimización de direcciones públicas en forma directa para IPv4 y los mecanismos de encapsulamiento (Túneles) que se manejaban de las direcciones en IPv4; a este respecto podemos recoger lo afirmado en el documento de "Adopción de IPv6 en Colombia, Documento de Política" de Cintel, que dice que ".....debe señalarse que el regreso a la conectividad extremo-a-extremo también redundo en mejoras a la seguridad de la red, toda vez que la implementación del protocolo IPv6 permite incorporar el protocolo IPsec (Seguridad

IP), y por el tamaño de las redes IPv6 es mucho más difícil encontrar agujeros de seguridad en una subred, por lo que en principio se reducirá el número de intrusiones en la red.”¹⁸

¹⁸ Tomado de “Política para la adopción del IPv6 en Colombia, Estructuración y Definición, Mintic, Cintel, Contrato No. 947 de 2012, página 12.”

10. Análisis de Riesgos

- El riesgo se define como el nivel de impacto en las operaciones de la entidad y sus activos, o individuos, como resultado de la operación de un proceso de negocio según el impacto potencial de una amenaza y la probabilidad de que dicha amenaza sea una realidad.
- La gestión del riesgo es el proceso de identificación, evaluación y toma de acciones efectivas para la reducción de los riesgos a un nivel aceptable. Se incluye la valoración del riesgo; el análisis costo-beneficio; la evaluación, selección e implementación de controles de seguridad.
- Las razones fundamentales para implementar un proceso de gestión del riesgo sobre los sistemas de TI de las entidades son:
 - Mitigación de los impactos negativos sobre los procesos misionales y de negocio.
 - La necesidad de contar con información de base para la toma de decisiones.

10.1 Valoración del Activo de Información

- La valoración para cada uno de los activos de información de la entidad permite calificar el nivel de criticidad, si es "Alto", "Medio" o "Bajo"; el impacto del uso de IPv6 de acuerdo al grado de confidencialidad, integridad y disponibilidad, de los equipos de comunicaciones, equipos de cómputo/almacenamiento y aplicaciones de cada una las entidades.

Activo de Información	Confidencialidad de IPv6	Integridad de IPv6	Disponibilidad de IPv6
Equipos de Comunicaciones			
Equipos de Cómputo y de Almacenamiento			
Aplicaciones (Bases de datos)			

Tabla 1. Valoración de Activos de Información

10.2 Gestión del Riesgo para el proceso de transición de IPv4 a IPv6

La tabla de gestión de riesgos para la transición de IPv4 a IPv6 debe caracterizar lo que es necesario tener en cuenta para cada una de las fases del proceso de transición frente a los riesgos de iniciar la transición

Fases de transición IPv4 a IPv6	Características de la fase	Actividades de Gestión de Riesgo
Planeación		
Implementación		
Pruebas de funcionalidad		

Tabla 2. Gestión del Riesgo para el Proceso de Transición

10.3 Hacking Etico

La siguiente tabla corresponde a un modelo de referencia para tomar los test de vulnerabilidades de direcciones IP, producto de una valoración de servicios críticos en cada una de las Entidades al momento de aplicar el protocolo IPv6.

Direcciones IPv6 de acuerdo a:	Servicios	Direccionamiento Web
Servidores y Aplicaciones		
Portales Web		
Equipos de Comunicaciones		
Equipos de Almacenamiento y otros		

Tabla 3. Hacking Ético

Un ejemplo sería el siguiente:

Direcciones IPv6 de acuerdo a:	Servicios	Direccionamiento Web/Puerto
Servidores y Aplicaciones		
2001:db8:6800:102::/48	Backup	http://backup:1598/
Portales Web		
2001:db8:6800:103::/48	DNS	DNS – TCP/UDP 389
Equipos de Comunicaciones		
2001:db8:6800:104::/48	Firewall	
Otros Equipos		
2001:db8:6800:105::/48	Telefonía	telefonía.empresa.gov.co

Tabla 4. Ejemplo Hacking Ético

10.3 Pruebas de penetración en redes

IPv4/IPv6

Las siguientes consideraciones se requieren tener en cuenta al iniciar un proceso de pruebas de penetración sobre redes IPv6:

- ✓ Obtención de información: Direccionamiento IP, dominios de red, cuentas del directorio activo, nombres de personas, infraestructura de TI, establecimiento del alcance de las actividades de reconocimiento, obtención de información de la intranet y sitios web, información corporativa, grupos de noticias, redes sociales, webs personales, metadatos, entre otros.
- ✓ Reconocimiento de la red corporativa: Manejo de DNS, Whois, búsquedas de reversa, obtención de información pública descuidada a través de herramientas de búsqueda disponibles.
- ✓ Recopilación pasiva: Hacer uso legítimo de obtención de información a través de los medios disponibles en Internet.
- ✓ Obtención de información pública disponible: Portal web de la organización, ubicación física, personas de contacto, sucesos, políticas de seguridad, archivos con información legendaria, exfuncionarios descontentos, foros, ofertas de empleo.
- ✓ Reconocimiento de los nombres de dominio en Internet: Direccionamiento IPv6, parámetros de protocolos y números de puertos.
- ✓ Recopilación activa: Ataques de enumeración, fuerza bruta, hacer búsquedas de dominio y subdominios, transferencia de zonas DNS, consulta de servidores DNS existentes, búsquedas inversas de DNS, ingeniería social.
- ✓ Reconocimiento de la red: Que permite localizar las rutas de acceso y la topología de la red.
- ✓ Hacer el mapeo de la red a través de: Descubrimiento de vecinos, direcciones MAC, topología de red, rastreo de puertos (TCP, UDP, ICMP), descubrimiento de direcciones IP, determinación de rutas que siguen los paquetes apoyado en herramientas como por ejemplo *traceroute*, entre otras.
- ✓ Establecimiento de los servicios activos: Búsqueda de puertos abiertos de determinados sistemas, búsqueda de puertos en estado de "escucha".

- ✓ Escaneo de puertos: Se requiere hacer exploración de TCP ACK, de TCP FIN, de TCP XMAS, TCP Null, de TCP RPC, de protocolo IP, de UDP. El scanner verifica conectividad y funcionamiento del equipo, verifica servicios, comprueba reglas de firewalls, analiza estructura de la red.
- ✓ Identificación de los sistemas operativos.
- ✓ Verificación de vulnerabilidades: Software actualizado, verificación de puertos, puertas traseras, y modo de comunicación de túneles.
- ✓ El resultado de las pruebas de penetración debe mantenerse en forma confidencial.
- ✓ Definición sobre el alcance de las pruebas indicando recursos a utilizar.

11. Lineamientos de seguridad en la nube bajo IPv6

La seguridad en la nube en entornos tanto de IPv4 como de IPv6 deben responder a una estrategia de análisis para ambientes tanto físicos como lógicos que permitan a las entidades construir políticas adecuadas para su correcta administración e implementación en las infraestructuras de TI; en cumplimiento de estas premisas es preciso conformar un equipo de trabajo de las Oficinas de TI, encargado de dictar lineamientos para el tratamiento de la información en ambientes de comunicación, computación y almacenamiento en la nube, esto con la ayuda o el apoyo de las empresas proveedoras del servicio en la nube.

Es necesario presentar los lineamientos de seguridad en la nube a los distintos proveedores de este servicio, considerando los siguientes aspectos:

- ✓ Confección de un mapa de riesgos y sus implicaciones (Con el apoyo de los proveedores de servicios).
- ✓ Establecimiento de control de identidad de usuarios.
- ✓ Adopción de normas de protección de información.
- ✓ Revisión de esquemas de virtualización (si existen).
- ✓ Revisión de la infraestructura del tipo de nube que se requiere implementar para adecuarla a IPv6 (nube híbrida, federada, privada, pública, entre otras).
- ✓ Adopción de retención de datos.
- ✓ Acuerdos de Nivel de Servicio (ANS) con el proveedor del servicio.
- ✓ Conexión a través de Redes Privadas Virtuales - VPN.

- ✓ Uso de claves complejas.
- ✓ Almacenamiento de cifrado de la información.
- ✓ Evaluación de los estándares de servicio.
- ✓ Verificación de pruebas del servicio, es decir garantía de que los canales y servicios en la nube estén funcionando correctamente.
- ✓ El proveedor de servicio contratado debe ofrecer gran reputación, esto debido a que la información en la nube puede estar en muchas partes del mundo.
- ✓ Establecer acuerdos de confidencialidad de la información.
- Recomendaciones antes de subir a la nube:
 - ✓ Hacer un análisis de la criticidad de la información (Activos de información, directorio activo, cuentas de correo, bases de datos importantes, entre otros).
 - ✓ Validar la calidad y las condiciones del servicio que ofrezca el proveedor de la nube.
 - ✓ Definir con claridad qué tipo de información debe ser publicada en la nube.
 - ✓ Verificar la información que requiere ser almacenada en una estructura convencional.
 - ✓ Garantizar a los usuarios que la contratación de servicios con un proveedor en la nube sea de alta calidad y experiencia que apoye a la seguridad de la información.
 - ✓ La seguridad en la nube debe estar presente en cada una de las capas de funcionamiento en esta, es decir:
 - Capa de infraestructura
 - Capa de almacenamiento
 - Capa de gestión de infraestructura
 - Capa de aplicación y
 - Capa de servicios.¹⁹

¹⁹ Capas propuestas por Gartner Group

12. Recomendaciones para mitigar riesgos en IPv6

Debido a que el proceso de transición de IPv4 a IPv6 en las Entidades, debe abordarse por fases de conformidad con lo establecido en la Guía de transición de IPv4 a IPv6 para Colombia, que son: Planeación, Implementación y Pruebas de Funcionalidad; es importante identificar dentro de estas fases y en especial en la fase de implementación, los riesgos de seguridad al momento de implementar el nuevo protocolo IPv6, por lo tanto, se requiere tener en cuenta las recomendaciones citadas.²⁰

A este respecto cabe mencionar que dentro de las actividades establecidas para la Fase de Planeación, no solo está el plan de diagnóstico, sino también es recomendable elaborar un plan de contingencias para IPv6, con el fin de tener todo preparado en caso de que al momento de implementar un servicio con IPv6, este pueda tener la posibilidad de que en caso de falla, pueda establecerse un plan de marcha atrás a fin de revisar que inconvenientes se ha presentado, poderlos resolver y volver intentar aplicar IPv6 nuevamente, esto garantiza la seguridad de las operaciones.

12.1 Reconocimiento de los riesgos de las configuraciones de Doble-Pila

En una configuración de doble-pila, un dispositivo admite simultáneamente IPv4 e IPv6. Las reglas de los firewalls y otros controles de seguridad que detienen el tráfico no deseado en IPv4, es improbable que sean eficaces para detener tráfico IPv6, por lo que las organizaciones suelen necesitar tecnologías de seguridad paralelas para afrontar esta nueva situación.

Sin la posibilidad de mantener ambientes de seguridad en la doble-pila, IPv6 está en alto riesgo de ser utilizado para comprometer o abusar de un dispositivo, creando posibles riesgos de seguridad que podrían no ser detenidos o detectados.

²⁰ <http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/338-comp-proteger-el-cambio-a-redes-ipv6>

12.2 Des-habilitación y bloqueo de IPv6

Una práctica de seguridad general es desactivar todos los protocolos de red innecesarios, sin embargo, incluso si una agencia tiene una política contra el uso de IPv6, encontrará que muchos dispositivos están habilitados para el uso de IPv6 por defecto. El nuevo hardware a menudo viene con IPv6 habilitado automáticamente por omisión, y dada la creciente popularidad de traer su propio dispositivo al trabajo, es probable que algunos de éstos tendrán IPv6 habilitado.

- Se recomienda deshabilitar temporalmente IPv6 en dispositivos cuando se detecten problemas de bajo desempeño en el Core de la red de comunicaciones que afecten las operaciones y servicios de la empresa, es por ello por lo que es altamente recomendable tener ambientes piloto de prueba con VLAN.

De otro lado, como política de seguridad, se recomienda deshabilitar los equipos y sistemas de comunicaciones, cuando se detecte la existencia de equipos con capacidad para bloquear tráfico bajo IPv4 y/o no deseado, en especial sobre las redes inalámbricas de la Entidad; en todo caso todo esto debe ser previamente estudiado y documentado con el establecimiento de reglas de firewall y políticas de seguridad de TI.

12.3 Traducción de direcciones de red

La traducción de direcciones de red (NAT), es una práctica de las redes IPv4 que se mal-interpreta que tiene como efecto secundario, proporcionar una capa de protección frente a los dispositivos habilitados para IPv4 mediante la ocultación de ellos del contacto directo con las redes externas. Sin embargo, es una falacia, ya que es muy fácil atravesar NAT, si no va acompañado de un firewall. Curiosamente, debido a que no hay contrapartida de NAT en dispositivos IPv6 y a que no es la esencia del nuevo protocolo, siempre es importante tener definida las reglas de doble-pila para evitar que los dispositivos puedan estar directamente expuestos a los ataques desde IPv4.

Esto es particularmente probable en las redes domésticas (residenciales), donde no hay otros controles de seguridad perimetral en el lugar. Para mitigar esto, se recomienda que cualquier dispositivo que ejecuta IPv6 esté protegido por un software de firewall en el equipo de la red misma, que bloquee el tráfico entrante no deseado de las direcciones IPv6 Globales Unicast (GUA).

12.4 Ataques en ambientes IPv6

Como se ha mencionado en este documento anteriormente, la implementación del IPv6 puede generar riesgos que pueden desencadenar en vulnerabilidades tales como:

- ✓ Fallas en la implementación del protocolo, debido a un desarrollo deficiente de un software que permite usar el protocolo para fines maliciosos.
- ✓ Falla en la especificación del protocolo que genera vulnerabilidades para ser explotado por los Hackers. La utilización de mecanismos del propio protocolo para realizar ataques permite que se deba realizar una revisión del protocolo y su estándar a fin de eliminar los posibles fallos y proponer un nuevo estándar.
- ✓ La utilización por parte de los operadores (proveedores del servicio de Internet) del esquema CGN (Carrier Grade NAT), ofrecen la sensación de una falsa seguridad incluso en los clientes, ofreciendo complicaciones en la red al desarrollar técnicas de NAT, por el hecho de utilizar los dos protocolos simultáneamente sin las debidas políticas de tráfico dentro de los Firewalls.

12.5 Riesgos de utilización de túneles de IPv6 en IPv4

Dado que IPv6 utiliza IPsec como protocolo de protección, de no existir este, se pueden presentar varios riesgos potenciales:

Una de las técnicas de transición hacia IPv6, aunque ya no es recomendada por la escasez de direcciones IPv4, es la utilización de túneles de tráfico de IPv6 en IPv4 que permite el encapsulamiento de un protocolo en otro, sin embargo, la técnica puede generar una pérdida de control de tráfico en la red, producto de una desactivación en las configuraciones de seguridad de IPv6 de los paquetes, generando que el protocolo se convierta en una "puerta trasera", que podría ser aprovechada por personas maliciosas.

Si bien es cierto el mecanismo de transmisión extremo a extremo usado por IPv6 puede generar ventajas de desempeño y mejores tiempos de respuesta en los sistemas de comunicaciones y de Información, también es cierto que al no tener procesos NAT, las vulnerabilidades en las terminales finales quedan expuestas desde cualquier punto de la red. A fin de mitigar este aspecto se recomienda la utilización de firewalls de protección.²¹

²¹ Consultar en: Análisis de Seguridad en Redes IPv6, Ingeniería de Telecomunicación, Universidad Carlos III de Madrid, Carlos García Martín, julio 2012.

A este respecto, cabe aclarar que un proceso NAT no es para brindar seguridad y el hecho de “esconder” direcciones IPv4 tampoco es sinónimo de seguridad, este aspecto nació en virtud de remediar la falta de direcciones IPv4 y poder optimizarlas en el acceso a Internet.

De otro lado, frente a IPv6 que maneja direcciones globales y estas se enrutan directamente a Internet, entonces con el fin de mitigar los riesgos de seguridad posibles, es necesario la aplicación de reglas de firewall precisas con el fin de desplegar tráfico IPv6 nativo de manera segura.

12.6 Escaneo en redes IPv6

Es común que muchos de los ataques a las redes de comunicaciones se realicen por medio de técnicas de escaneo, en donde los atacantes utilizan nodos con puertos activos, servidores DHCP con identificación de la estructura de la red; en el caso de IPv4 el ataque es más simple por la utilización de una máscara de subred de 24 bits que generaría un grupo de no más de 254 nodos por red, lo que facilita un escaneo para identificar redes TCP o UDP. Un ataque bajo estas condiciones no sería probable en IPv6, por cuanto el espacio de direccionamiento en IPv6 llevaría muchísimo más tiempo sobre la red por ser el paquete más grande (128 bits) y el proceso de ataque podría quedar desestimado; sin embargo, no es recomendable tener confianza frente a los ataques por escaneo y se reitera el establecimiento de reglas de firewall en los elementos activos del “Core” de la red y la distribución no secuencial de redes y direcciones en todos los segmentos.

13. RFCs de seguridad en IPv6

Lista de RFC que aplican a la seguridad en IPv6:²²

- RFC 5619: Software Security Considerations, Agosto 2009
- RFC 5269: FMIP Security Distributing a Symmetric Fast Mobile IPv6 (FMIPv6)
- RFC 4942: IPv6 Transition/Coexistence Security Considerations
- RFC 4218: Threats Relating To IPv6 Multihoming Solutions
- RFC 4891: Using IPsec To Secure IPv6 Tunnels
- RFC 4890: Recommendations For Filtering ICMPv6 Messages in Firewalls
- RFC 4864: Local Network Protection For IPv6
- RFC 4843: An IPv6 Prefix For Overlay Routable Cryptographic hash Identifiers (ORCHID)
- RFC 5213: Proxy Mobile IPv6
- RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4487: Mobile IPv6 And Firewalls: Problem Statement
- RFC 4449: Securing Mobile IPv6 Route Optimization Using a Static Shared Key
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models Threats
- RFC 4301: Asociaciones de seguridad (SA). Security Architecture for the Internet Protocol. Soporte para IPsec-V2. (Hace obsoleto el RFC 2401)
- RFC 2401: Security Architecture for the Internet Protocol (Actualizado por RFC 3168), Soporte para IPsec-V2.
- RFC 4302: IP Authentication Header (Hace obsoleto RFC 2402)
- RFC 4303: IP Encapsulation Security Payload
- RFC 5282: Using Authenticated Encryption Algorithms with the encrypted payload of the Internet key Exchange Versión 2 (IKEv2) Protocol.
- RFC 5996: Internet Key Exchange (IKEv2) Protocol
- RFC 4877: Mobile IPv6 Operation with IKEv2 and the revised IPSec Architecture
- RFC 4581: Cryptographically Generated Addresses (CGA) extension field format (Actualiza el RFC 3972)
- RFC 4982: Support For Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA). (Actualiza el RFC 3972 errata)

²² Para mayor información consultar en <http://www.mintic.gov.co/porta/604/w3-article-5938.html>

RFC 3414: User – Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)

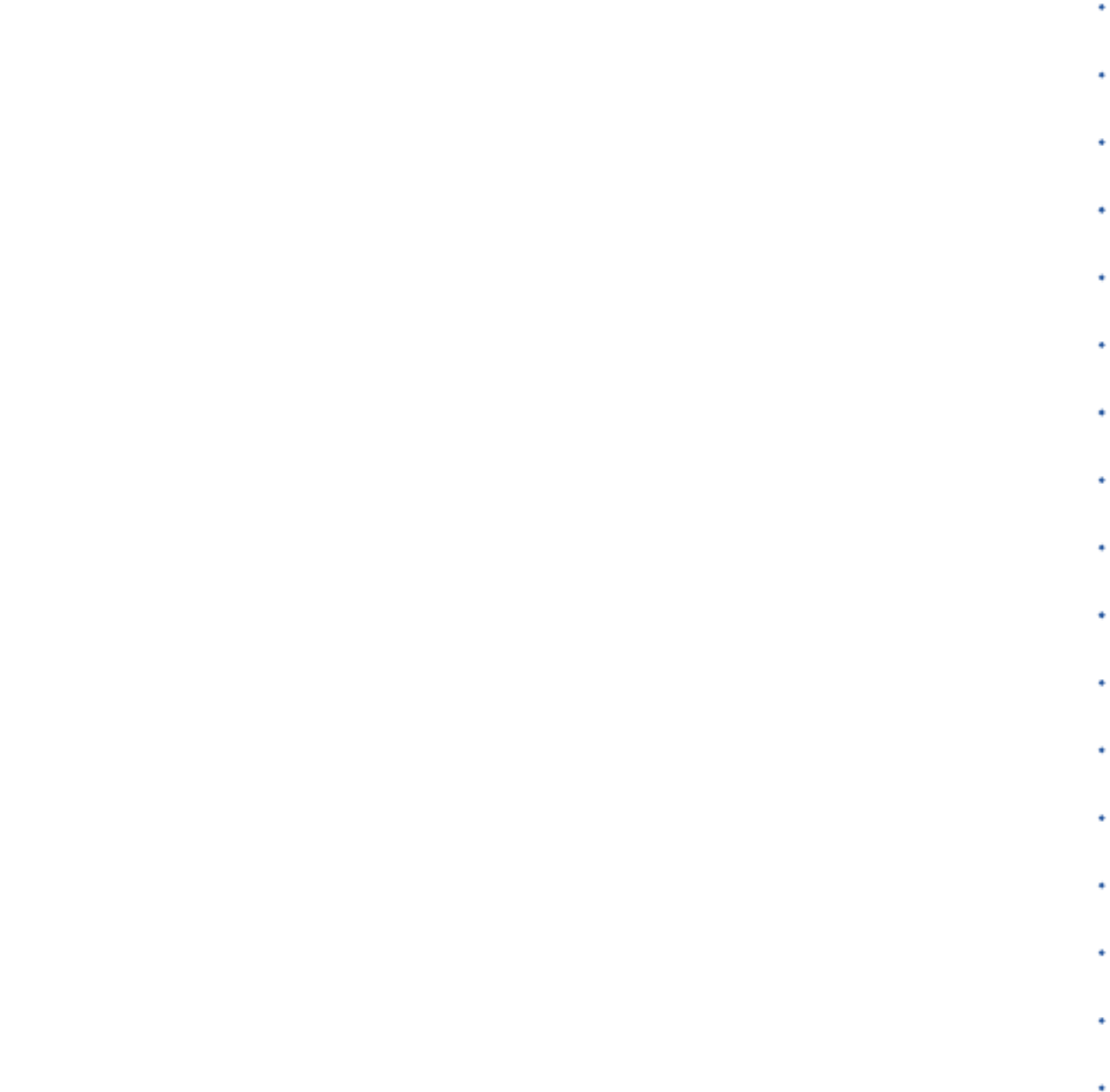
RFC 4807: IPsec Security Policy Database Configuration – MIB.

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 4718: IKEv2 Clarifications and implementation Guidelines

RFC 7721: Security and Privacy Considerations for IPv6 Address Generation Mechanisms 2016.

draft-ietf-opsec-v6



14. Conclusiones

• Como se ha observado a lo largo del documento, en IPv6, los esquemas de seguridad deben ser la máxima prioridad bajo criterios de fiabilidad y autenticidad a fin de garantizar el tránsito seguro de la información a través de la red; con ello la puesta en marcha del protocolo con ayuda de IPSec siempre será una regla importante a tener presente en el tránsito de los servicios para las entidades del estado y también para la industria en general, ya que con ello no solo se ofrece conectividad bajo IPv6 sino también la posibilidad de garantizar transmisiones seguras a nivel de todas las capas de las redes de comunicaciones, que ayudan a mitigar los nuevos riesgos y mantener controlados los ataques que actualmente existen sobre IPv4 y sobre IPv6.

• Desde el punto de vista técnico, IPv6 presenta nuevos mecanismos de trabajo basados en DHCPv6 e ICMPv6, en razón al nuevo tamaño de las direcciones del paquete de información que permiten introducir nuevos dispositivos a la red de IPv6 y un concepto nuevo a nivel de introducción de cabeceras de extensión. Adicionalmente IPv6 realiza un proceso de cifrado con la utilización del protocolo IP Security – IPSec, que ofrece una buena comunicación confiable entre nodos con infraestructuras de IPv6; esto con el fin de tener en forma nativa un tráfico altamente seguro.

• De otro lado, el escenario que se prevé es el uso simultáneo y coexistente entre los protocolos IPv4 e IPv6, con el objetivo de IPv6-only e IPv4 como servicio, lo que puede generar el surgimiento de nuevos riesgos, como por ejemplo, problemas de mecanismos de control por la eliminación de procedimientos NAT, activación de IPv6 en sistemas operativos de manera innecesaria dentro de la red y aumento significativo del número de dispositivos conectados que elevan los riesgos de nuevos ataques en una red IPv6; por ello es importante hacer los planes de diagnóstico en la entidades que permitan mostrar cuales son los dispositivos que aun soportando IPv6 puedan presentar riesgos de seguridad al momento de la implementación y comenzar a tomar los correctivos necesarios.

• Las entidades al momento de empezar la fase de planeación, con ayuda del plan de diagnóstico mencionado antes, deben revisar que elementos activos de TI son compatibles con IPv6 y hacer también un análisis de la seguridad ya que la implementación del nuevo protocolo por sí mismo no es compleja, pero si genera un alto impacto en la seguridad de las redes, las aplicaciones y los servicios de las Entidades.

• Finalmente, diseñar una red sobre IPv6 con seguridad puede ser una tarea muy dispendiosa, ya que puede traer consigo, vulnerabilidades en los diferentes sistemas, que pueden ser aprovechadas por los atacantes para iniciar un evento malicioso; por ello resulta clave que las entidades se concienticen a través de la alta dirección, sus administradores de redes y administradores de sistemas de información, que el protocolo IPv6 cuenta con mecanismos de cifrado importantes a

nivel de IPSec, lo que implica que este servicio debe permanecer activo en todo momento, así mismo, independiente de este protocolo es necesario la implementación de nuevas políticas de seguridad de TI que garanticen la mitigación de nuevos riesgos sobre los sistemas de información, sobre los sistemas de comunicaciones y en general sobre las aplicaciones y servicios de las entidades del estado.

15. Anexo 1

15.1 Sistema RPKI para Recursos Numéricos Asignados en la Región (LACNIC)

15.1.1 Actividades de Estandarización

- El proyecto de certificación de recursos RPKI (Resource Public Key Infrastructure), establece una infraestructura de clave pública (o PKI) comúnmente llamada RPKI. Esta infraestructura combina la jerarquía del modelo de asignación de recursos de Internet a través de Registros Regionales (RIRs) o Registros Nacionales, con el uso de certificados digitales basados en la norma X509.²³

Los trabajos de estandarización de la infraestructura RPKI se llevan adelante en el IETF (Internet Engineering Task Force). El grupo de trabajo RPSEC (Routing Protocol Security Requirements) analizó en su documento RFC 4593, las amenazas de seguridad de los protocolos de enrutamiento IP, en particular dicho documento menciona la falsificación de información dentro de un mensaje de enrutamiento.

En el año 2007 IETF creó el grupo de trabajo SIDR (Secure Inter-Domain Routing) para la elaboración de la arquitectura que permita eliminar las amenazas identificadas en el RFC 4593 para el enrutamiento entre dominios (o externo). La tecnología a desarrollar deberá permitir su implementación de forma incremental.

- Particularmente, el grupo SIDR está documentando el uso de certificados para la delegación del derecho de uso de un recurso en Internet. El trabajo abarca la especificación de la arquitectura del RPKI, de las políticas de certificación, de los perfiles de los certificados a emitir y de diferentes materiales criptográficos de utilidad, entre otros. Antes de poder emitir certificados RPKI, fue necesario definir extensiones de los certificados X509 para representar direcciones IPv4 e IPv6 y ASNs; estas extensiones se definen en el documento RFC3779.²⁴

15.1.2 Función de Certificación de Recursos (RPKI)

En general las funciones realizadas por las entidades certificadoras permiten: Gestionar listas de revocación de certificados, realizar el registro de entidades, gestionar y generar certificados, generar

²³ <http://www.lacnic.net/web/lacnic/informacion-general-rpki>

²⁴ Tomado de <http://www.lacnic.net/web/lacnic/informacion-general-rpki>

y distribuir claves, establecer políticas de certificación y almacenar certificados; en ese orden de ideas, por medio de la existencia de una PKI de recursos de Internet, es posible validar el derecho a uso de un recurso por parte de una organización.

El principal objetivo de esta infraestructura es el de proporcionar las bases para el mejoramiento de la seguridad en el encaminamiento (o "routing") de paquetes IP. Algunas de las aplicaciones propuestas para esta infraestructura son:

- ✓ Construcción de filtros para anuncios utilizando protocolos BGP (Border Gateway Protocol).
- ✓ Construcción de reglas de enrutamiento basadas en la validez criptográfica de los prefijos anunciados.
- ✓ Extensiones de seguridad para protocolo BGP, a través de las propuestas SBGP o BGP.
- ✓ Extensiones de seguridad para protocolos de enrutamiento interno, como ser OSPF o ISIS.
- ✓ Autenticación de enrutadores en las redes de área local (o LANs) para el protocolo de Descubrimiento de Vecinos Seguro o SEND.
- ✓ Firma de información en servicios de Whois o en objetos RPSL (Routing Policy Specification Language).²⁵

15.1.3 Especificaciones de la RFC 4593 – *Generic threats to routing protocols*

El documento de la RFC 4593 contiene los lineamientos de buenas prácticas sobre los siguientes aspectos:

- ✓ Generalidades de las funciones de enrutamiento IP
- ✓ Modelo de amenazas de protocolos de enrutamiento genéricos
- ✓ Fuentes de amenazas
- ✓ Consecuencias de las amenazas
- ✓ Sniffing, (Robo de información en la red), Spoofing (Suplantación de identidad)
- ✓ Análisis de tráfico
- ✓ Falsificación por originadores y por tramitadores
- ✓ Consideraciones de seguridad

El documento RFC enuncia que los protocolos de enrutamiento son objeto de amenazas y ataques que pueden afectar tanto a los usuarios individuales como a las operaciones de la red en su

²⁵ Tomado de <http://www.lacnic.net/web/lacnic/informacion-general-rpki>

conjunto, por lo tanto, este documento proporciona un resumen de las amenazas genéricas que afectan los protocolos de enrutamiento.

El trabajo desarrollado, es el primero de un conjunto de requisitos de seguridad para los protocolos de enrutamiento, como resultado de un análisis que permitió observar las deficiencias en la implementación de protocolos, que conllevaron a fallos que pueden aumentar el riesgo de ataques en las redes de manera contundente.

Sin embargo, el documento solo contempla ataques contra infraestructuras robustas de protocolos de enrutamiento tales como el Open Shortest Path First (OSPF), Sistema Intermedio a Sistema Intermedio (IS-IS), el RIP (Routing Information Protocol); el BGP (Boundary Gateway Protocol), no están definidos los análisis que permiten detectar ataques contra las debilidades específicas fuera del alcance de los protocolos de enrutamiento.

En el marco de las consideraciones de seguridad de enrutamiento IP, la RFC 4593 dice que "En un contexto más amplio, el trabajo basado en el reconocimiento de la comunidad IETF, que la señalización y los planes de control/gestión de los dispositivos de red se deben fortalecer. Los protocolos de enrutamiento se pueden considerar como parte de la señalización y los planes de control". Sin embargo, hasta la fecha los protocolos de enrutamiento tienen en gran parte ataques maliciosos abiertos sin protección. Este documento discute las amenazas intra-dominio de enrutamiento actualmente conocidos y sienta las bases para que otros documentos discutan requisitos de seguridad para protocolos de enrutamiento. Este documento es independiente del protocolo.²⁶

²⁶ <http://tools.ietf.org/html/rfc4593>

16. Anexo 2

Requerimientos de IPv6 para equipos de TIC (LACNOG BCOP 20160127-01)²⁷

Best Current Operational Practice (BCOP)

16.1 Resumen del BCOP

Para asegurar la inserción suave y rentable de IPv6 en sus redes, es importante que los gobiernos y las grandes corporaciones especifiquen requerimientos de compatibilidad de IPv6 en la búsqueda de ofertas de equipamiento y soporte de TIC (Tecnologías de Información y Comunicaciones). Este documento tiene como objeto proporcionar una "Mejor Práctica Actual" Best Current Practice (BCP) y no especifica ninguna norma ni política por sí mismo.

16.2 Transfondo del BCOP / Historia

Los certificados IPv6 Ready Logo, pueden ser requeridos para cualquier dispositivo. Esta es la forma más fácil para que los proveedores que ofrecen equipos pueden demostrar que cumplen con los requisitos básicos de IPv6. El iniciador de la licitación también proporcionará la lista de RFCs obligatorios y opcionales requeridos, con el fin de no excluir a los proveedores que aún no exponen sus equipos a la prueba de certificación del programa IPv6 Ready Logo. De esta forma los licitadores públicos no pueden ser acusados de preferir cualquier tipo de proveedor de equipamiento.

Cuando especificamos la lista de RFCs requeridos, debemos enumerar todos los requisitos obligatorios, con excepción de las entradas que comienzan con: "Si [funcionalidad] Se solicita ...". Estas entradas son obligatorias sólo si el iniciador de la licitación requiere cierta funcionalidad. Tenga en cuenta que el iniciador de licitación debe decidir qué funcionalidad se requiere, no el proveedor de equipos.

²⁷ Extracción parcial del documento LACNOG BCOP 20160127-01, Requerimientos de IPv6 para equipos TIC, Jan Zorz, Documentos de referencia: RIPE-554, Traducción de Azael Fernández Alcántara, Ernesto Pérez Estévez, Ariel Weher, otros, 27/01/2016. http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2016.pdf

Algunas de las funciones que se encuentran en la sección "opcional" en este documento pueden ser importantes para su caso y / u organización específica. En tales casos, el iniciador de licitación debe mover el requisito hacia la sección "necesaria" en su solicitud de licitación.

16.3 Texto del BCOP

16.3.1 Requisitos para "equipamiento de seguridad en la red"

El equipamiento en esta sección se divide en tres subgrupos:

- Cortafuegos o Firewalls (FW)
- Sistema de prevención de intrusos (IPS)
- Firewalls de aplicación (APFW)

Para cada norma obligatoria los subgrupos aplicables se especifican entre paréntesis al final de la línea.

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
Inspecting IPv6-in-IPv4 protocol-41 traffic, que está especificado en:
"Basic Transition Mechanisms for IPv6 Hosts y Routers" [RFC4213] (IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (FW, IPS, APFW) *
- Neighbor Discovery [RFC4861] (FW, IPS, APFW) *
- Si la petición es para el protocolo BGP4, el equipo debe cumplir con RFC4271, RFC1772, RFC4760 y RFC2545 (FW, IPS, APFW)
- Si la petición es para "dynamic internal gateway protocol (IGP)", entonces se deben soportar RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308]. La entidad de contratación especificará el protocolo requerido. (FW, IPS, APFW)
- Si se requiere OSPF-v3, el dispositivo debe soportar "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- Soporte para QoS [RFC2474, RFC3140] (FW, APFW)

- Si se requiere encapsulamiento, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts and Routers” [RFC4213] (FW)

• Un dispositivo de seguridad de red a menudo se coloca donde lo haría un switch de capa 2/capa 3. En función de su colocación, esos requisitos deberían ser incluidos.

• La funcionalidad y características que se soportan para IPv4 deben ser comparables con la funcionalidad soportada para IPv6. Por ejemplo, si un sistema de prevención de intrusiones es capaz de operar en IPv4 en modos de capa 2 y capa 3, entonces también debe ofrecer esta funcionalidad en IPv6. O si un Firewall se está ejecutando en un clúster capaz de sincronizar sesiones IPv4 entre todos los miembros del cluster, entonces esto también debe ser posible con sesiones IPv6.

• Soporte opcional:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for Multipart Messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- BGP Communities Attribute [RFC1997]
- BGP Capabilities Advertisement WITH-4 [RFC3392]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPF-v3 [RFC5340]
- Authentication/Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling y IPv6 [RFC2473]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891]
- Multicast Listener Discovery version 2 [RFC3810] *

- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode) *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

17. Referencia

- Acosta, A., Aggio, S., et al. (2014). IPv6 para Operadores de Red, ISOC-AR.
- Bermejo, J., (2013), Hacking Ético, Fases pruebas de Penetración, Edita y Maqueta, Fundación IN-Nova, Catilla de la Mancha.
- Cicileo, G., Gagliano, R., et al. (2009). IPv6 para todos, 1a ed. - Buenos Aires: Asociación Civil Argentinos en Internet.
- Ciprian, P., (2006). Deploying IPv6 Networks, Cisco Systems.
- Lobo, J., Rico, D., (2012), Implementación de la Seguridad del Protocolo de Internet Versión 6, UFPSO.
- Mur, P., (2000). Seguridad a nivel de IP: IPSec, Estudiante de la ETSETB, UPC. Ramas de estudiantes del IEEE, recuperado del sitio web de la Universidad Politécnica de Cataluña - Barcelona:<https://upcommons.upc.edu/revistes/bitstream/2099/9944/1/Article005.pdf>
- Rekhter, Y., Li, T., and S. Hares. (2006), A Border Gateway Protocol 4 (BGP-4), RFC 4271.
- Rosen, E., (1981). Vulnerabilities of network control protocols: An example, RFC 789.
- Shirey, R., (2000). Internet Security Glossary, RFC 2828.