POLÍTICAS DE SEGURIDAD IPv6

UNIVERSIDAD PEDAGOGICA NACIONAL	INFORME DEL PLAN DE PRUEBAS PILOTO IPv6 UPN	UNIVERSIDAD PEDAGÓGICA Ministerio de Educación
UNIVERSIDAD PEDAGOCICA	Fecha: 25/05/2022	

REGISTRO DE CAMBIOS		
VERSIÓN	**FECHA DE CAMBIO**	**MOTIVO DEL CAMBIO**

CONTROL DEL DOCUMENTO			
VERSIÓN	**ELABORADO**	**REVISADO**	**APROBADO**
1	Daniel Beltrán		

UNIVERSIDAD PEDAGOGICA NACIONAL	INFORME DEL PLAN DE PRUEBAS PILOTO IPv6 UPN	UNIVERSIDAD PEDAGÓGICA Ministerio de Educación
UNIVERSIDAD PEDAGOCICA	Fecha: 25/05/2022	

TABLA DE CONTENIDO

Pág.

TABLA DE FIGURAS

LISTADO DE TABLAS

UNIVERSIDAD PEDAGOGICA NACIONAL	INFORME DEL PLAN DE PRUEBAS PILOTO IPv6 UPN	UNIVERSIDAD PEDAGÓGICA Ministerio de Educación
UNIVERSIDAD PEDAGOCICA	Fecha: 25/05/2022	

INTRODUCCIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) de la estrategia de Gobierno Digital, la resolución 2710 de 2017, Por la cual se establecen los lineamientos para la adopción del protocolo IPv6, la Guía para la Transición de IPv4 a IPv6 para Colombia y la Guía de Aseguramiento del Protocolo IPv6 de MinTIC, se estableció la necesidad de definir, socializar y mantener los lineamientos y políticas que se requieren tener en cuenta para la seguridad del protocolo IPv6, las cuales deberán estar contenidas en un documento de alto nivel, el cual se dé a conocer a todos los interesados por la universidad pedagógica nacional (UPN), para apoyar su implementación.

A continuación, se presentan los lineamientos técnicos de seguridad que se requieren tener en cuenta para llevar a cabo la transición del protocolo IPv4 al protocolo IPv6, en la universidad pedagógica nacional (UPN). Lo anterior, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito a nivel nacional.

1. ALCANCE

Las disposiciones de la presente política de seguridad para el protocolo IPv6 serán aplicable a toda la universidad pedagógica nacional (UPN) en el marco del proceso de adopción e implementación del Protocolo Internet Versión 6 (IPv6). De tal manera que se pueda abarcar la infraestructura tecnológica con que cuenta actualmente la entidad.

Es importante aclarar que el alcance de las políticas presentadas en el presente documento contempla su aplicación específica para el hardware, software o servicio que hace parte del inventario de activos de Información compatible con IPv6, documento STIC3-COLTEL-IFC-IR-ID000-Inventario de Activos de TI Para el Diagnostico IPv4 a IPv6 UPN y sus respectivas actualizaciones frente a la CMDB de la Entidad. Por lo tanto, no incluye los equipos que hacen parte del plan de excepciones o que no sean compatibles con el protocolo IPv6. Así mismo, se aclara que los lineamientos se documentan con el fin de proteger el protocolo IPv6. Por lo tanto, las soluciones de antivirus están fuera del alcance de este documento dado que su protección corresponde a servicio de capa de aplicación.

De igual forma se aclara que este documento corresponde a los lineamientos generales de seguridad y en ningún momento es una guía técnica para el aseguramiento del protocolo IPv6. Sin embargo, la documentación técnica se podrá encontrar dentro de los manuales propios de los fabricantes de cada plataforma y dentro del documento de configuraciones del protocolo IPv6 ().

La aplicación de los lineamientos que se establecen en este documento deberá ser realizada por el operador de servicios (actualmente Colombia Telecomunicaciones) sobre la infraestructura que tiene bajo su responsabilidad.

2. OBJETIVO

Presentar un marco de referencia sobre lineamientos de seguridad en el protocolo IPv6, que sean referentes para abordar el proceso de transición de IPv4 a IPv6 en la universidad pedagógica nacional (UPN), y así 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 la universidad pedagógica nacional (UPN).

3. DEFINICIONES

ACL: Una Lista de Control de Accesos (ACL: Access Control List) es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

AH (de IPsec): protege la mayor parte del datagrama IP

Anti DDoS: Los ataques de denegación de servicio son un arma peligrosa contra cualquier empresa. Su función principal es interrumpir la continuidad operativa para generar una crisis interna, a través de un conjunto de computadoras infectadas que hacen peticiones inútiles al servidor.

API: Interfaz de programación de aplicaciones es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones.

APT: Amenaza Avanzada Persistente. Se refiere a una especie de ciberataque muy preciso. Por otro lado, las APT pueden referirse también a grupos, a menudo apoyados o financiados de otras formas, que son responsables del lanzamiento de dichos ataques de precisión.

CSP (Cloud Service Provider): Un proveedor de servicios en la nube es una empresa de terceros que ofrece una plataforma, una infraestructura, una aplicación o servicios de almacenamiento basados en la nube. Al igual que un propietario pagaría por un servicio público como la electricidad o el gas, las empresas generalmente tienen que pagar solo por la cantidad de servicios en la nube que utilizan, según lo requieran las demandas comerciales.

DAD (de NDP): La funcionalidad de proxy del Protocolo de descubrimiento de vecinos (NDP) permite el reenvío de paquetes entre los hosts que están en la misma subred y no pueden comunicarse directamente entre sí.

Digital Rights Management (DRM); Digital Rights Management cifra el contenido, y entonces aplica una serie de derechos. Los derechos pueden ser tan simples como

copiar, o tan complejos como especificar restricciones por grupo o usuario en actividades como cortar y pegar, enviar correos, cambiar el contenido, etc. Cualquier aplicación o sistema que trabaja con datos protegidos con DRM debe ser capaz de interpretar e implementar los derechos, lo cual normalmente implica integrarse con un sistema de gestión de claves.

Dirección IP Publica: Se trata de las matrículas que se le asigna a cada usuario cuando navega por Internet, por lo que si una página o servicio la bloquea puede hacer que dejes de poder acceder a ella.

Dirección IP Privada: Una dirección de Internet creada solo para usarse en una red interna. Las direcciones privadas las emite un dispositivo de red, como un router, que las extrae de un conjunto de direcciones que le ha asignado un servidor DHCP. Para

DHCPv6: Protocolo de Configuración Dinámica de Hosts para IPv6 (DHCPv6) es un protocolo cliente-servidor, definido en la RFC 3315[1] de la IETF, que proporciona una configuración administrada de dispositivos sobre IPv6.

DNS: El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres.

DLP: Data Loss Prevention (DLP), en una traducción literal, prevención de la pérdida de datos. Las soluciones DLP se utilizan en el proceso de monitoreo de sucesos que pueden ocasionar la filtración de información. Los productos centrados en DLP posibilitan la prevención y la corrección de vulnerabilidades cuando se las diagnostican. Existen diferentes tipos de soluciones DLP, cada una orientada a un propósito específico, pero con el mismo objetivo: prevenir la pérdida de datos.

DMZ (Demilitarized Zone**):** En seguridad informática, una DMZ (en español zona desmilitarizada) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

[1] https://tools.ietf.org/html/rfc3315

acceder a Internet, las direcciones privadas se convierten en direcciones IP públicas a través de un servicio de traducción de direcciones de red (NAT).

EndPoint: Es un sistema central de seguridad que elimina los riesgos en casos de amenazas para el sistema, evitando que se transmitan a los dispositivos conectados.

ESP (de IPsec): Carga de seguridad encapsuladora, protege los datos con un algoritmo de cifrado

EUI-64: Se asignan a una tarjeta adaptadora de red o se derivan de direcciones IEEE 802

Firewall: Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

GRE: (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet. Está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar hasta 20 protocolos del nivel de red (nivel 3 del modelo OSI) distintos.

GUA: La Dirección Única Global. direcciones públicas en IPv4. El ICANN y el IANA únicamente están asignando GUAs con los tres primeros bits del primer hexteto.

HTTP: Protocolo de transferencia de hipertexto es el protocolo de comunicación que permite las transferencias de información a través de archivos en la World Wide Web

HTTPS: Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP

IaaS (Infrastructure as a Service). El proveedor del servicio se encarga de entregar una infraestructura a la entidad, normalmente mediante una plataforma de virtualización. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.

IDS: Intrusión Detection System (Sistema de Detección de Intrusos) es una aplicación de software destinado a la detección, en dispositivos o en una red, de accesos no autorizados.

ISATAP: habilita el tunneling automático tanto para direcciones IPv4 privadas como públicas en redes NBMA (Non-Broadcast Múltiple Access). De esta forma, los hosts ISATAP pueden verse entre sí usando IPv6, pero sobre una red IPv4.

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 90s con el IETF (Internet Engineering Task Force). Al día de hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en substitución de IPv4.

IPS: también conocida como panel In-Plane Switching, es un tipo de tecnología de pantalla de alta calidad que se utiliza normalmente en monitores, tablets y smartphones de alto rendimiento para computadoras y laptops.

IPSEC: Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

PaaS (Platform as a Service). El proveedor del servicio se encarga de entregar una plataforma a la entidad cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.

PKI: Infraestructura de Llave Pública. Es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.

Proxy: Se trata de unos servicios que te pueden ayudar a mejorar tu privacidad cuando navegas por la red, y que a menudo suelen confundirse con unas redes VPN con las que se pueden conseguir resultados similares, pero que son mucho más completas al no centrarse únicamente en tu navegación.

NAC: Network Access Control. Intenta unificar la tecnología de seguridad en los equipos finales, usuario o sistema de autenticación y reforzar la seguridad de acceso a la red.

NDP: El Neighbor Discovery Protocol (“protocolo de descubrimiento de vecinos”) se utiliza junto con la versión más reciente del protocolo de Internet IPv6. Su principal objetivo es resolver las direcciones IPv6 en direcciones MAC válidas, que son las direcciones de hardware propias de cada dispositivo.

NGIPS: El Sistema de Prevención de Intrusiones de última generación de Cisco (NGIPS) es una solución que ofrece una visibilidad completa e inteligencia avanzada para prevenir la red de la empresa del máximo número de amenazas posible.

MICROSOFT NAP: Network Access Protección es una tecnología de Microsoft para controlar el acceso a la red de una computadora, en función de su estado. Con NAP, los administradores de sistemas de una organización pueden definir políticas para los requisitos de salud del sistema.

MLD (de multicast): Multicast Listener Discovery es un componente del conjunto de protocolos de Internet versión 6. MLD es utilizado por los enrutadores IPv6 para descubrir oyentes de multidifusión en un enlace conectado directamente, al igual que el protocolo de administración de grupos de Internet se usa en IPv4.

RFC (Request For Comments): Solicitud de Comentarios, se compone de una serie de publicaciones de ingenieros expertos que han hecho llegar a la IETF - Engineering Task Force, sus recomendaciones para la valoración por el resto de la comunidad. 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.

SaaS (Software as a Service). El proveedor del servicio es el encargado de ofrecer al cliente o a la entidad el software como un servicio. Las aplicaciones son accesibles desde diferentes dispositivos a través de una interfaz de cliente liviano, un típico ejemplo es un servicio en un entorno Web; el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza. Las aplicaciones de ofimáticas a las que se puede acceder online son otro ejemplo.

SD-WAN: Simplifica la gestión y el funcionamiento de una WAN al desacoplar el hardware de red de su mecanismo de control. Este concepto es similar a cómo la red definida por software implementa la tecnología de virtualización para mejorar la administración y operación del centro de datos.

SIEM: Gestión de Información y Eventos de Seguridad. Un sistema de gestión de información y eventos de seguridad es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad.

Snapshot: También denominadas instantáneas de volumen o VSS (volumen snapshot Service) son un elemento de seguridad informática complementarias a las copias de seguridad o backups.

TCP: Está orientado a la conexión, es decir, los datos pueden enviarse de forma bidireccional una vez establecida la conexión.

TLS: Seguridad de la Capa de Transporte. Se trata de protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación.

Teredo: Teredo es una tecnología de transición que proporciona conectividad IPv6 a hosts que soportan IPv6 pero que se encuentran conectados a Internet mediante una red IPv4.

Túneles: Técnica que consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de equipos de cómputo.

UDP: El protocolo de datagramas de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

UPS: Sistemas de alimentación ininterrumpida, en inglés uninterruptible power supply, es un dispositivo que, gracias a sus baterías y otros elementos almacenadores de energía,

durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

ULA: Dirección Local Única es una dirección IPv6 del bloque fc00::/7, definida por el RFC 4193. ... Estas direcciones están disponibles para su uso libre en redes privadas y no deben ser enrutables en el internet IPv6 global.

VLAN: Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

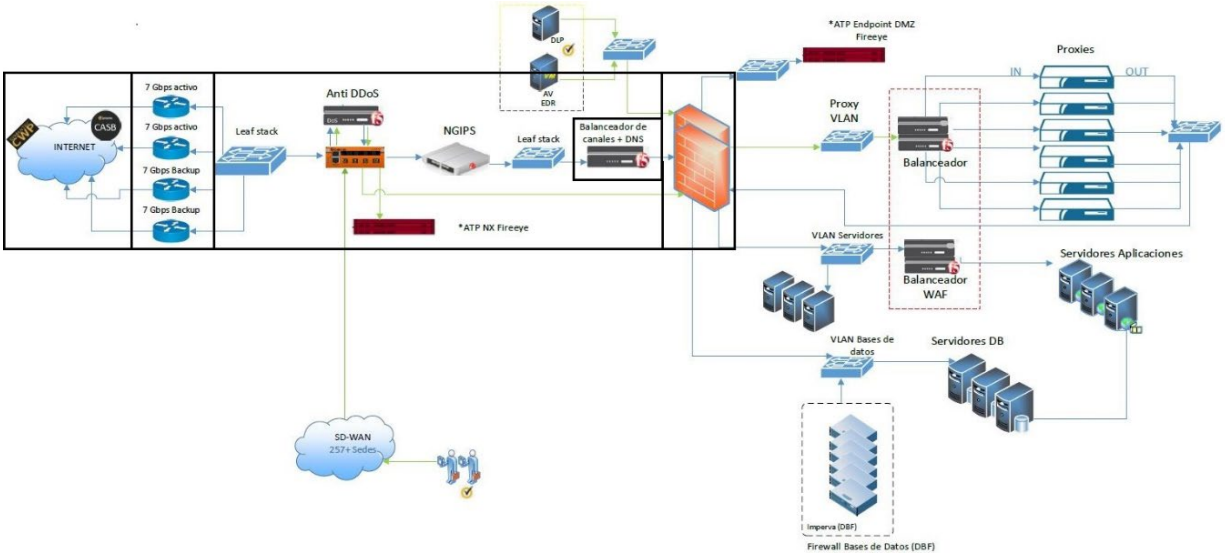
WAF: Un WAF es un tipo de firewall que protege a un servidor web de ataques cibernéticos. Las empresas necesitan un WAF eficiente y fácil de usar que les ayude.

.

4. DEFINICION DEL PERIMETRO DE SEGURIDAD EN LA ENTIDAD

A continuación, se presenta diagrama topológico de la red perimetral de la universidad pedagógica nacional (UPN), donde se evidencia la seguridad de los servicios alojados en la red. Se aclara que el perímetro que se define a continuación solamente corresponde a los equipos de seguridad y red perimetral que se encuentran de frente a internet. Por lo tanto, no incluye los equipos de usuario final o demás que están detrás de esta capa.

Figura 1 Definición del Perímetro UPN



Fuente elaboración propia

A continuación, se presenta una breve descripción de la infraestructura tecnológica que compone el servicio de seguridad perimetral de la red de la universidad pedagógica nacional (UPN).

- Se cuentan con 4 canales de internet, para poder contar con redundancia en el servicio de navegación y consultas de servicios que el cliente tiene anunciados en internet. Para esto se cuenta con 4 enrutadores perimetrales que permiten su conexión con internet.

- Se cuenta con un servicio de Anti DDoS, con lo cual se pueden contrarrestar de forma eficaz este tipo de ataques los cuales buscan saturar un servicio hasta agotar sus recursos y dejarlo inhabilitado.

- Se cuenta con una solución de monitoreo de tráfico y visibilidad de la red, con lo cual se garantiza el análisis de todo el tráfico, detectando las actividades de posibles atacantes antes de que tengan graves consecuencias reales. Esto se hace a través de los equipos de monitoreo GigaMon y Firewall que permiten recopilar diferentes datos de tráfico.

- Se cuenta con una solución de DLP, con lo cual se logra tener una protección avanzada contra amenazas, para evitar fuga de información sensible de la entidad.

- Se cuenta con una solución de NGIPS, con lo cual se tiene visibilidad completa e inteligencia avanzada para prevenir a toda la red de la entidad del máximo número de amenazas posible.

- Se cuenta con una solución de APT, con lo cual se obtiene visibilidad completa de todos los eventos de seguridad en todos los endpoints en la organización, incluyendo dispositivos móviles. De igual forma se cuentan con los servicios de Microsoft los cuales permiten complementar también la detección de este tipo de amenazas.

- Se cuenta con un servicio de Balanceadores de Carga Externos de cara a internet, que son los equipos que reciben todas las peticiones originadas desde internet, realizan las traducciones de direcciones IP públicas a privadas, para realizar luego la entrega de los paquetes a los firewalls perimetrales de la entidad, también cumplen con la función de servidores DNS Externos, desde los cuales se encuentran anunciados todos los sitios públicos de la entidad.

- Se cuenta con una solución de firewalls, estos equipos son los encargados de realizar una revisión de cada uno de los paquetes que atraviesan la red de data

center para permitir o denegar las solicitudes y/o peticiones realizadas hacia los servicios con los cuales cuenta la entidad.

- Se cuenta con una solución de WAF, firewall de capa 7 para realizar el aseguramiento de las aplicaciones web de la entidad.

- Se cuenta con una solución de proxy, con la cual se realiza el análisis del tráfico desde los equipos endpoint hacia internet, para evaluar tráfico malicioso y permitir la navegación únicamente a sitios permitidos por la entidad.

5. MODELOS DE SERVICIO EN LA NUBE

A continuación, se presentan los diferentes modelos de servicios ofrecidos por los diferentes proveedores VMware, Microsoft Azure o Amazon AWS, entre otros.

- SaaS (Software as a Service). El proveedor del servicio es el encargado de ofrecer al cliente o a la entidad el software como un servicio. Las aplicaciones son accesibles desde diferentes dispositivos a través de una interfaz de cliente liviano, un típico ejemplo es un servicio en un entorno Web; el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza. Las aplicaciones de ofimáticas a las que se puede acceder online son otro ejemplo.

- PaaS (Platform as a Service). El proveedor del servicio se encarga de entregar una plataforma a la entidad cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.

- IaaS (Infrastructure as a Service). El proveedor del servicio se encarga de entregar una infraestructura a la entidad, normalmente mediante una plataforma de virtualización. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.

5.1. RIESGOS ASOCIADOS CON LOS SERVICIOS ALOJADOS EN NUBE

A continuación, se presentan riesgos que se pueden encontrar con la implementación de este tipo de servicios:

Nota: La gestión de estos riesgos se realiza como parte del proyecto de IPv6 y se tiene documentada en el proceso de gestión de riesgos del proyecto. Por lo tanto, en este documento solo se hace mención a ellos como contextualización.

- Amenazas internas. Los empleados del proveedor de servicios en la nube tienen acceso directo al hardware y las redes, y muchos tienen acceso a los hipervisores,

los sistemas de aprovisionamiento y la infraestructura de autenticación. Por lo tanto, suponen una amenaza potencial debido a sus privilegios.

- Escape de máquinas virtuales, contenedores o sandboxes. Si un cliente puede escapar de una máquina virtual, un contenedor o un entorno aislado sin servidor, podría ganar acceso al hipervisor o sistema operativo que ejecuta las cargas de trabajo de otros clientes.

- Obtención ilícita de autenticaciones. El acceso a las cuentas utilizadas para aprovisionar las máquinas virtuales y otros servicios en la nube permite al atacante simplemente utilizar la API o la interfaz de usuario del servicio en la nube para destruir los servicios u otorgar acceso adicional según se desee.

- Vulneración de la encriptación. Una forma de obtener acceso a la nube es romper el cifrado. La mayoría de los servicios en la nube y las API están protegidos mediante el protocolo TLS, que a su vez depende de PKI para la autenticación. La forma típica de romper el cifrado es romper la PKI.

5.2. MITIGACION DE RIESGOS ASOCIADOS CON LOS SERVICIOS ALOJADOS EN NUBE

A continuación, se presentan métodos de mitigación de riesgos que se pueden implementar para este tipo de servicios:

- Localización de contenidos; es normalmente una funcionalidad de las herramientas de DLP (Data Loss Prevention;) para bases de datos, está disponible en ocasiones en los productos de monitorización de la actividad de bases de datos (DAM). DLP se define como: “Productos que, basados en políticas centralizadas, identifican, monitorizan, y protegen los datos estáticos, en movimiento, y en uso, mediante un análisis profundo de contenidos”.

- Cifrado de almacenamiento de volúmenes;
  - El cifrado de volúmenes protege de los siguientes riesgos:
  - Protege los volúmenes de su exposición a un clonado mediante snapshot.
  - Protege a los volúmenes de ser explorados por el proveedor Cloud (y los administradores de Cloud privados)

- Protege a los volúmenes de verse expuestos ante una pérdida física de discos (un problema más de cumplimiento que de seguridad real)

- Monitorización en bases de datos y archivos; Se debe realizar una monitorización en tiempo casi real de la actividad de las bases de datos y alerta en base a incumplimientos de las políticas, tales como ataques de inyección SQL o replicación de la base de datos sin autorización por el administrador. Las herramientas monitorización para entornos Cloud se basan normalmente en agentes que se conectan a un servidor recolector central (normalmente virtualizado). Se usan con instancias dedicadas a un único cliente.

- Almacenamiento con privacidad; Casi todos los sistemas de almacenamiento basados en cloud requieren de alguna autenticación de los participantes (usuario de Cloud y/o CSP) para establecer relaciones de confianza, ya sea sólo para un punto extremo de la comunicación o para ambos. Aunque los certificados criptográficos pueden ofrecer suficiente seguridad para muchos de estos fines, no suelen cubrir la privacidad, ya que están ligados a la identidad de una persona real (usuario Cloud). Cualquier uso de uno de esos certificados muestra la identidad del titular a la parte que solicita la autenticación.
  Credenciales basadas en atributos se emiten como credenciales criptográficas ordinarias (por ejemplo, las credenciales X.509) usando una clave de firma digital (secreta). Sin embargo, las credenciales (ABC) basadas en atributos permiten a su titular transformarlas en una nueva credencial que contiene sólo un subconjunto de los atributos contenidos en la credencial original. No obstante, estas credenciales transformadas pueden ser verificadas igual que las credenciales criptográficas ordinarias (utilizando la clave pública de verificación del emisor) y ofrecen el mismo nivel alto de seguridad.

- Digital Rights Management (DRM); Básicamente, Digital Rights Management cifra el contenido, y entonces aplica una serie de derechos. Los derechos pueden ser tan simples como copiar, o tan complejos como especificar restricciones por grupo o usuario en actividades como cortar y pegar, enviar correos, cambiar el contenido, etc. Cualquier aplicación o sistema que trabaja con datos protegidos con DRM debe ser capaz de interpretar e implementar los derechos, lo cual normalmente implica integrarse con un sistema de gestión de claves.

6. POLITICAS DE SEGURIDAD IPV6 EN LOS SERVICIOS DE LA ENTIDAD

La estructura de políticas que se consigna en el presente documento se resume a través de las siguientes categorías de **servicios** dentro de la entidad:

Políticas de Seguridad Servicios de Usuario Final (Host): Políticas de seguridad que deben aplicarse sobre los equipos internos de la entidad (Equipos de usuario final, Dispositivos Móviles, Equipos de Energía, Impresoras, entre otros).

Políticas de Seguridad Servicios de Conectividad: Políticas de seguridad que deben aplicarse sobre los equipos que se encuentran ubicados en la red interna de la entidad y los cuales cumplen la función de permitir la conectividad de los equipos internos de la entidad a la red y enrutar su tráfico (Switches, Routers, Access Points, entre otros).

Políticas de Seguridad Servicios de Seguridad Perimetral: Políticas de seguridad que deben aplicarse sobre los equipos que se encuentran ubicados en el perímetro de la red, y que protegen la infraestructura de la entidad de ataques externos (Firewalls, Balanceadores, WAF, entre otros).

Políticas de Seguridad Servicios de Aplicaciones: Políticas de seguridad que deben aplicarse sobre los equipos y servicios que estos alojan, los cuales son programas informáticos diseñados como una herramienta para realizar operación o funciones específicas (Aplicaciones Web, Aplicaciones de Nomina, entre otros).

Políticas de Seguridad Servicios de Monitoreo: Políticas de seguridad que deben aplicarse sobre los diferentes equipos y aplicaciones cuya función es la de realizar el monitoreo de los diferentes servicios e infraestructura tecnológica instalada en la entidad (Diferentes Herramientas de Monitoreo de Red, Aplicaciones, entre otros).

A continuación, se listan las políticas que deben adoptarse en la Entidad, de forma técnica, separadas en las categorías de servicios mencionadas anteriormente:

6.1. POLÍTICAS DE SEGURIDAD SERVICIOS DE USUARIO FINAL (HOST)

A continuación, se listan las políticas de seguridad informática recomendadas para asegurar los equipos de usuario (Host) de la universidad pedagógica nacional (UPN) frente a la implementación de IPv6.

6.1.1. Políticas Generales para todos los Equipos

- Dado que la seguridad en IPv6 depende significativamente de la protección de Host, se recomienda que se realice el aseguramiento y monitoreo a través de herramientas de seguridad distribuida (por ejemplo, Cisco NAC, Microsoft NAP, McAfee ePO entre otras). Las cuales ofrecen seguridad en endpoint como firewall de host, IPS, IDS, entre otras funcionalidades que detienen ataques a nivel de red.

- El monitoreo de los equipos debe hacerse por SNMPv3. Por lo tanto, en las herramientas de monitoreo que recopilen datos de equipos por SNMP deberán autenticarse respectivamente con usuario del dominio, así como aplicar el cifrado de paquetes en tránsito de la información monitoreada.

- Los equipos como impresoras, scanner, cámaras de video, UPSs, entre otros, que sean de uso interno y que no requieran salir a internet, deberán configurarse preferiblemente con direcciones IPv6 tipo ULA. Esto permite que dichos dispositivos cuenten con un nivel de protección adicional en cuanto al acceso no autorizado desde internet si llegasen a presentarse desbloqueos de red en los dispositivos de perímetro.

6.1.2. Para PCs y Portátiles

- Los equipos que se encuentran en las sedes NO deben ser accedidos desde internet. Por lo tanto, las configuraciones de Firewall local deben permitir únicamente la comunicación para diagnóstico desde los equipos internos, no desde redes de internet. Sin embargo, la comunicación al exterior por parte de estos equipos si debe permitirse, pero para servicios de navegación a internet únicamente. Por ejemplo, navegación a internet por HTTP y HTTPS.

- De ser posible se debe habilitar IPsec (Combinación de ESP y AH) en modo Transporte para equipos de usuario final. Esto permite que la comunicación por IPv6 entre los equipos de usuario final y los equipos de Datacenter se realice de forma cifrada y autenticada para prevenir la lectura de datos cuando se presenta la interceptación de paquetes.

- La porción de red de cada equipo y el Identificador de Interfaz deberá generarse de forma aleatoria. Por lo tanto, no se debe configurar el direccionamiento por EUI-64 por ningún motivo. Por lo tanto, la autoconfiguración de la porción de host debe utilizar extensiones de privacidad y aleatoriedad tal como ser presenta a continuación:

    - (Netsh interface ipv6 set global randomizeidentifiers=enabled).
    - (Netsh interface ipv6 set privacy state=enabled).

- El tiempo de vida de las direcciones generadas en los hosts debe ser de máximo una (1) semana. Lo anterior para poder tener un balance entre conectividad, seguridad del equipo y monitoreo de actividad de los equipos.

- Habilitar SEND en los hosts RFC3971[2]. Esto permite proteger desde los equipos de usuario final de ataques dirigidos al protocolo NDP. Esta información se puede consultar en el siguiente RFC:

    - HTTPS://DATATRACKER.IETF.ORG/DOC/RFC3971/

      En el link anterior se describen los métodos de protección desde los equipos de usuario final de ataques dirigidos al protocolo NDP.

- Se debe configurar el filtrado de paquetes en los equipos de usuario final a través de reglas de firewall de host que restrinja el tráfico indeseado. Es importante que, si los equipos quedan con algún tipo de servicio habilitado para gestión remota, como por ejemplo Terminal Services (RDP TCP 3389) o cualquier otro tipo de acceso remoto, también se deje configurado en el firewall de Windows para permitir únicamente el acceso a la red de servidores. Sin embargo, dado que aún

[2] https://tools.ietf.org/html/rfc3971

no se tiene definida esta parte, entonces lo mejor es hacerlo por IPv4 y posteriormente desplegar a través de políticas de directorio activo la regla de acceso por IPv6.

- Se debe realizar el aseguramiento en los equipos de usuario final de acuerdo con los siguientes parámetros en la guía “ERNW Guide to Configure Securely Windows Servers For IPv6.pdf”, la cual se adjunta al presente documento y contiene las configuraciones de aseguramiento para servidores sobre Sistema Operativo Microsoft Windows:

  Configuración de Interfaz IPv6:
  - Deshabilitar los mensajes "Redirect" de ICMPv6 (Sección 5.1 del documento)
  - Configurar manualmente el Limite de Saltos de red por defecto (Sección 5.2 del documento)
  - Deshabilitar configuraciones de túneles ISATAP y Teredo (Sección 5.3 del documento)

  Configuración de Firewall de Windows:
  - Tráfico entrante mensajes ICMPv6 (Sección 6.1.1 del documento)
  - Tráfico saliente, mensajes ICMPv6 (Sección 6.1.2 del documento)
  - Política de firewall por defecto (Sección 6.1.3 del documento)
  - Prevenir ataques de DoS en LAN "Smurf" (Sección 6.2 del documento)

6.1.3. Para Dispositivos Móviles

- Los dispositivos móviles que se encuentran conectados a la red Wireless deberán recibir direccionamiento IPv6 perteneciente a una VLAN totalmente aislada de los equipos portátiles que requieran acceso a la red. Esta VLAN deberá tener acceso únicamente a Internet y no a las redes internas de la Entidad.

6.1.4. Para Impresoras, Scanner o Plotters

- Los equipos de este grupo que cuenten con tarjeta de red para configurar una dirección IP deberán configurarse con direccionamiento IP estático y de tipo ULA. De igual forma, se deben conectar a una VLAN específica y diferente a los otros

dispositivos que, aunque puedan accederse desde la red de usuarios no permita ser accedidos desde internet.

- En caso de que los dispositivos de esta categoría requieran enviar correos electrónicos o tener comunicación con el exterior de la entidad, entonces se deberá configurar el relay de correo con un servidor interno y se deberán configurar políticas específicas de firewall para permitir únicamente la salida de internet de los equipos que lo requieren.

6.1.5. Para otros Equipos

- Equipos de videoconferencia periféricos, cámaras de video, UPSs, o demás equipos internos donde se deban asignar direcciones IP estáticas, deberán tener asignado preferiblemente direccionamiento estático ULA. Lo anterior dado que, aunque se cuente con filtrado a nivel de firewall, se debe asegurar que estos equipos estén protegidos del acceso externo o replicación de virus a nivel interno.

6.2. POLÍTICAS DE SEGURIDAD SERVICIOS DE CONECTIVIDAD

A continuación, se listan las políticas de seguridad informática recomendadas para asegurar los equipos de conectividad de red de la universidad pedagógica nacional (UPN) frente a la implementación de IPv6.

6.2.1. Para Equipos de Red

- A nivel de red se recomienda aplicar la funcionalidad de Port Security. Esto permite que los equipos que se conectan a la red local a través de cable físico únicamente puedan conectarse desde el punto de red que ha sido asignado.

- Para la red Wireless, se debe aplicar filtrado a través de dirección MAC y autenticación con LDAP/RADIUS/EAP o última tecnología. Lo anterior para mantener el acceso controlado y centralizado de los equipos en la red.

- Las VLANs asignadas a los hosts deben estar separadas respectivamente en VLANs diferentes y tener comunicaciones entre ellas únicamente si es requerido. Por ejemplo, diferentes VLANs de la misma sede NO deberían poder comunicarse

entre sí a menos de que se requiera comunicación para consumir servicios. De lo contrario la comunicación solo debe ser entre la VLAN de usuarios y la que dispone los servicios de red.

- Las interfaces de administración de los equipos de red deberán configurarse con direccionamiento IPv6 de tipo ULA. Lo anterior con el fin de que este tipo de direcciones no puedan ser enrutadas en internet.

- Los equipos switch de capa 2 deberán replicar las ACLs que se tienen para IPv4 acorde con el tráfico especificado para dicho protocolo. Esto con el fin de prevenir ataques a los servicios no autorizados.

- Aplicar toda la guía de aseguramiento para equipos de capa 2 con nombre: “2 Level-1 Security Hardening Policies (Mandatory).pdf”, el cual se encuentra anexo al presente documento y consigna las configuraciones técnicas para el aseguramiento de equipos de capa 2.

- Aplicar la funcionalidad de ND Snooping. Esta funcionalidad permite determinar y registrar los paquetes NS enviados por los equipos bloqueando así el tráfico malicioso que viaje sobre la red o que desee burlar los equipos con mensajes fraudulentos. Para esto se debe seguir la guía de aseguramiento “Level-2 Security Hardening Policies (Optional).pdf” en su numeral 3.2.17 IPv6 ND Security, la cual se encuentra anexa al presente documento y consigna las configuraciones técnicas para el aseguramiento de equipos de capa 2.

6.2.2. Equipos de Capa 2

a. Todos los equipos de capa 2 deben aplicar las recomendaciones generales presentadas en el presente documento.

b. Todas las VLANs que se definan en los equipos de enrutamiento y switch deben estar debidamente separadas. Debe ser posible asignar diferentes VLANs al mismo dominio si y solo si se requiere que estas VLANs se comuniquen entre ellas. De lo contrario todas las VLANs deben quedar separadas. Esto previene ataques de salto de VLANs y acceso no autorizado.

c. Los equipos switch de capa 2 deberán replicar las ACLs que se tienen para IPv4 acorde con el tráfico especificado para dicho protocolo. Esto con el fin de prevenir ataques a los servicios no autorizados.

d. Aplicar toda la guía de aseguramiento para equipos de capa 2 con nombre: “2 Level-1 Security Hardening Policies (Mandatory).pdf”, el cual se encuentra anexo al presente documento y consigna las configuraciones técnicas para el aseguramiento de equipos de capa 2.

e. Aplicar la funcionalidad de ND Snooping. Esta funcionalidad permite determinar y registrar los paquetes NS enviados por los equipos bloqueando así el tráfico malicioso que viaje sobre la red o que desee burlar los equipos con mensajes fraudulentos. Para esto se debe seguir la guía de aseguramiento “Level-2 Security Hardening Policies (Optional).pdf” en su numeral 3.2.17 IPv6 ND Security, la cual se encuentra anexa al presente documento y consigna las configuraciones técnicas para el aseguramiento de equipos de capa 2.

6.2.3. Equipos de Capa 3

a. Los equipos de red que protegen el perímetro con ACLs, que intercambian información de enrutamiento o demás parámetros deberán autenticarse entre ellos para intercambiar información. Esto requiere implementar las medidas de seguridad de autenticación entre equipos que proporcione cada fabricante. Lo anterior previene ataques de acceso no autorizado e interceptación de tráfico en texto claro.

b. Todas las VLANs que se definan en los equipos de enrutamiento y switch deben estar debidamente separadas. Debe ser posible asignar diferentes VLANs al mismo dominio si y solo si se requiere que estas VLANs se comuniquen entre ellas. De lo contrario todas las VLANs deben quedar separadas. Esto previene ataques de salto de VLANs y acceso no autorizado.

f. En caso de que se configuren túneles entre dispositivos switch, router u otros, deberá habilitarse IPsec (Combinación de ESP y AH) en modo Túnel. Esto aplica para la red MPLs todos equipos de borde WAN. Lo anterior previene ataques de alteración, modificación o reenvío de paquetes IP.

g. Los equipos de enrutamiento o equipos que actúen como router (Por ejemplo, Switch de Capa 3) deberán implementar la funcionalidad RA-Guard (Router Advertisement Guard), la cual se describe en el RFC6105[3]. Esto permite prevenir ataques de suplantación de paquetes RAs que podrían generarse para enviar información fraudulenta a los equipos de la red.

h. Los equipos de enrutamiento o equipos que actúen como router (Por ejemplo, Switch de Capa 3) deberán implementar la funcionalidad RPO (Router Preference Options) la cual se describe en el RFC4191[4]. Esta funcionalidad permite asegurar el intercambio de rutas que entregan estos equipos a los diferentes clientes o servidores.

6.3. POLÍTICAS DE SEGURIDAD SERVICIOS DE SEGURIDAD PERIMETRAL

A continuación, se listan las políticas de seguridad informática recomendadas para asegurar el perímetro de la universidad pedagógica nacional (UPN) frente a la implementación de IPv6.

6.3.1. Políticas Generales para todos los Equipos del Perímetro

a. El modelo de seguridad en IPv6 para el perímetro depende de los dispositivos de control de acceso perimetral. En este caso los dispositivos de Firewall, enrutadores, balanceadores de cargas, entre otros. Estos deben tener un control periódico que permita identificar la creación, modificación y eliminación de reglas basado en el presente documento de políticas. Por lo tanto, todo cambio en el set de reglas deberá quedar documentado. Su revisión deberá realizarse por lo menos 2 veces al año.

b. La aplicación de seguridad en el perímetro contempla el aseguramiento de las siguientes capas:

    a. Red: Paquetes transmitidos a través del protocolo IPv6 y sus subprotocolos (NDP, DAD, entre otros)

[3] https://tools.ietf.org/html/rfc6105
[4] https://tools.ietf.org/html/rfc4191

b. Transporte: Paquetes transmitidos por TCP/UDP para prevenir ataques de denegación de servicio o descubrimiento de equipos por modificación de banderas, entre otros. (SYN Flood, Xmas)
c. Aplicación: Restricción de paquetes de capa de aplicación a través del filtrado de tráfico en diferentes tipos de protocolos de capa 7. (FTP, SSH, SMB, SNMP, entre otros)

c. La asignación de direcciones IPv6 que se realice en los equipos de protección perimetral deben ser del rango ULA y no deben tener una secuencia. Esto previene tanto ataques frente al descubrimiento iterativo de los equipos como la alcanzabilidad de los mismos desde internet.

d. Se debe documentar toda la configuración de reglas, ACLs, agrupamiento de VLANs, permisos y restricciones de DMZ entre otras configuraciones de seguridad implementadas para IPv6.

e. El monitoreo de los equipos de perímetro hacia los equipos internos de monitoreo debe realizarse por SNMPv3. Esta versión permite efectuar una autenticación entre el origen y el destino antes de enviar los datos. Esto previene fuga de información en ataques de interceptación de tráfico.

f. Para realizar el monitoreo de los equipos se debe asignar direccionamiento ULA o bien utilizar las direcciones link local que tienen los equipos. El objetivo es restringir la circulación de tráfico SNMP a través de direcciones globales GUA. Esto previene ataques de descubrimiento y alcanzabilidad de los equipos fuera del perímetro.

g. Debe realizarse la actualización de firmware de todos los equipos en el área perimetral a su última versión. Esto permite que con nuevas actualizaciones propuestas por los fabricantes se mantengan cerradas las vulnerabilidades de seguridad más recientes que podrían afectar a la capa de red IPv6.

h. El direccionamiento para todas las conexiones Punto a Punto se debe configurar con direcciones Estáticas ULA no enrutables en internet. De igual forma se debe asignar un /64 para cada conexión punto a punto, pero la configuración de las interfaces debe realizarse con direcciones entre /127 y /124. El objetivo de esta

política previene los ataques de descubrimiento de la red en los enlaces punto a punto.

i. En caso de definirse la aplicación de Multicast a través del protocolo MLD. Entonces se deberán aplicar las recomendaciones de MLD snooping del RFC4541[5]. Estas permiten configurar el protocolo MLD para protegerlo frente a su uso indebido, interceptación, notificación o recepción no autorizada de mensajes. De igual forma se deben adoptar las medidas descritas para el aseguramiento de Multicast descritas en la siguiente referencia o la que se encuentre más actualizada. Esta política previene ataques al control de acceso, ataques de inundación de tráfico y otros dirigidos a IPv6 en lo llamado broadcast de IPv4.

   - HTTPS://TOOLS.IETF.ORG/ID/DRAFT-VYNCKE-PIM-MLD-SECURITY-00.HTML

     Nota: En el link anterior se identifican los parámetros de Aseguramiento de Multicast.

j. Las interfaces de administración de los dispositivos deben realizarse a través de la conexión a las direcciones IPv6 ULA o IPv6 link local. Esto permite que no se cuente con direccionamiento global GUA que pueda ser objetivo de ataque desde el exterior.

6.3.2. Equipos de Seguridad

a. Los equipos host internos no necesitan ser accedidos desde “fuera” de la entidad. Por lo tanto, las políticas de dispositivos de protección de seguridad perimetral Firewall, switches con ACLs o enrutadores deberán restringir el acceso desde el exterior, por cualquier servicio y a todos los equipos internos de usuario final que pertenezcan a cualquiera de las sedes. Todo lo anterior replicando las reglas de IPv4 al protocolo IPv6.

b. En caso de que se requiera que un equipo interno sea accedido desde internet. Por ejemplo, cuando este equipo preste algún servicio que deba publicarse, el

[5] https://tools.ietf.org/html/rfc4541

equipo interno deberá estar respectivamente aislado en una red de servicios públicos desmilitarizada (DMZ).

c. Dentro del set de reglas, se deben filtrar los Túneles IPv6. Esto a través del filtrado de tráfico IPv4 con los siguientes protocolos:
   - IP Protocolo 41: Filtrado de Túneles ISATAP, 6to4, 6in4
   - IP Protocolo 47: Filtrado de Túneles GRE
   - UDP puerto 3544: Encapsulado de túneles Teredo.

d. Los equipos de filtrado perimetral Firewalls deben configurarse para inspeccionar el tráfico encapsulado. Esto permite detectar en cualquier tipo de paquete entrante o saliente pueda transmitirse ataques de malware o denegación de servicio. Lo anterior para el caso de tráfico que viene encapsulado con IPsec.

e. Se debe implementar el siguiente filtrado de paquetes en los dispositivos de Firewall tanto para NDP como para túneles:

Figura 2 Recomendaciones para filtrado de paquetes de NDP

ICMPv6 Filtering recommendations RFC4890 (https://tools.ietf.org/html/rfc4890)

Type - Code	Description	Action
Type 1 - all	Destination unreachable	ALLOW
Type 2 - all	Packet Too Big	ALLOW
Type 3 - Code 0 & 1	Time Exceeded	ALLOW
Type 4 - Code 0, 1 & 2	Parameter Problem	ALLOW
Type 128	Echo Reply	ALLOW for connectivity check and some services. Rate limit
Type 129	Echo Request	ALLOW for connectivity check and some services. Rate limit
Type 130,131, 132, 143	MLD	ALLOW if Multicast or MLD goes through FW
Type 133	Router Solicitation	ALLOW if NDP goes through FW
Type 134	Router Advertisement	ALLOW if NDP goes through FW
Type 135	Neighbor Solicitation	ALLOW if NDP goes through FW
Type 136	Neighbor Advertisement	ALLOW if NDP goes through FW
Type 137	Redirect	NOT ALLOW
Type 138	Router Renumbering	NOT ALLOW
Type 139 & 140	Node Information Query & Reply	NOT ALLOW

Fuente Elaboración propia

Figura 3 Reglas de filtrado para túneles

Tecnología	Regla de Filtrado
IPv6 Nativo	EtherType 0x86DD
6in4	IP proto 41
6in4 (GRE)	IP proto 47
6in4 (6-UDP-4)	IP proto 17 + IPv6
6to4	IP proto 41
6RD	IP proto 41
ISATAP	IP proto 41
Teredo	UDP dest port 3544
Tunnel Broker con TSP	(IP proto 41)||(UDP dst port 3653 || TCP dst port 3653)
AYIYA	UDP dest port 5072 || TCP dest port 5072

Fuente Elaboración propia

f. Como reglas generales de filtrado, la estructura debe contemplar la regla principal de “Deny All”, y posterior a esto permitir únicamente el tráfico autorizado. De acuerdo con lo anterior, una vez se cuente con la regla “Deny All” se deberán configurar como mínimo las siguientes reglas:

- Permitir la salida a internet desde los equipos que se encuentran en las sedes. Origen: Equipos de las Sedes, Destino: Internet, Puertos/Servicios: HTTP (TCP80, 8080) y HTTPS (TCP443, 8443).
- Permitir la salida a internet de los equipos servidores especificados en control de cambios y que requieren salida a internet. Esto puede incluir navegación a:
  - Sitios web para la descarga de actualizaciones.
  - Interoperabilidad con sistemas de información externos.
- Permitir la salida a internet como respuesta a peticiones de servicios de resolución de nombres DNS.
- Permitir tráfico de ingreso por puertos específicos a los equipos que hacen parte de la DMZ. Por ejemplo, página web, portales que disponen servicios entre otros.

Ejemplo1:

Figura 4 Política IPv6

IPv6 Policy

Rule	Source	Destination	Protocol	Action
1	Any-IPv6	V6-web-1	HTTP & HTTPS	Permit
2	Any-IPv6	Any-IPv6	Any	Deny

Fuente Elaboración propia

Ejemplo 2:

Figura 5 Reglas IPv6

Rule	Source	Destination	Protocol	Action
1	Any-IPv4 Any-IPv6	V4-Web-1 V6-Web-1	HTTP & HTTPS	Permit
2	Any-IPv4 Any-IPv6	DNS	TCP 53 UDP 53	Permit
4	Any-IPv4 Any-IPv6	V4-Mail-1 V6-Mail-1	SMTP	Permit
5	Any-IPv4 Any-IPv6	Any-IPv4 Any-IPv6	ICMPv6	Permit
6	Any	Any	Any	Deny

Fuente Elaboración propia

- Reglas de filtrado Para Multicast:

Figura 6 Reglas multicast

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
deny	3ffe::/16	host/net	any	service
deny	any	any		

Fuente Elaboración propia

g. Se debe realizar el filtrado de los prefijos no asignados o reservados. Esto incluye prefijos de documentación, ULA, MLD, entre otros que son para funcionalidades específicas y no debe permitirse que se accedan desde internet.

Figura 7 Prefijos a filtrar

Rutas	Prefijos	Comentario
Default	**::/0**	
Unspecified Address	**::/128**	**Se pueden agrupar en el prefijo 0000::/8 o mayor**
Loopback Address	**::1/128**	
IPv4-mapped Addresses	**::ffff:0.0.0.0/96**	
IPv4-compatible Addresses (deprecated)	**::/96**	
Link-local Addresses	**fe80::/10 o mayor**	
Site-local Addresses (deprecated)	**fec0::/10 o mayor**	
Unique-local addresses	**fc00::/7 o mayor**	
Multicast Addresses	**FF00::/8 o mayor**	**Si no se usa multicast**
Documentation addresses	**2001:db8::/32 o mayor**	
6Bone Addresses (deprecated)	**3ffe::/16, 5f00::/8**	**RFCs 1897,2471,3701**
ORCHID	**2001:10::/28**	**RFC 4843**

Fuente Elaboración propia

h. Para equipos de seguridad como Firewall de aplicación, IPSs, IDSs, SIEM, entre otros que permiten proteger la entidad desde el perímetro, se deben replicar las

políticas establecidas para IPv4 en IPv6. Esto incluye la relación de objetos, reglas, políticas entre otras. Lo anterior es importante dado que, aunque se tienen políticas de IPv4 configuradas, se recomienda que la configuración de las reglas de IPv6 se haga de forma separada. Todo acorde con la configuración específica de cada fabricante, la cual es aplicada por los administradores de plataformas con base en sus manuales técnicos y experiencia.
Nota: se aclara que la configuración de estas políticas podría variar dependiendo del tipo de equipo para algunos podría realizarse por aparte, pero en otros podría ser solo modificar los objetos existentes.

i. Para los equipos balanceadores de carga, se deben aplicar como mínimo las políticas generales mencionadas en el presente documento. Sin embargo, en estos equipos las configuraciones que se encuentran en IPv4 deberán replicarse respectivamente en IPv6.

6.4. POLÍTICAS DE SEGURIDAD SERVICIOS DE APLICACION

A continuación, se listan las políticas de seguridad informática recomendadas para asegurar los servidores de aplicaciones de la universidad pedagógica nacional (UPN) frente a la implementación de IPv6.

6.4.1. Para servicio de Aplicaciones

- Los equipos servidores NO deben ser accedidos desde internet. Por lo tanto, las configuraciones de Firewall local deben permitir únicamente la comunicación para diagnóstico y comunicación desde los equipos internos, no desde redes de internet. Sin embargo, la comunicación del exterior hacia estos equipos si debe permitirse, pero para únicamente servicios de aplicaciones web por los protocolos HTTP y HTTPS.

- Para todos los servidores se debe aplicar la guía completa: “IPv6 Hardening Guide for Windows Servers” y “IPv6 Hardening Guide for Linux Servers” las cuales se entregan como anexo al presente documento. Esta guía consigna las configuraciones técnicas que deben aplicarse a equipos servidores que tienen configuraciones específicas, como direccionamiento estático, aseguramiento de firewall interno, y configuración del protocolo ICMPv6, entre otras.

- En caso de que se requiera que un equipo interno sea accedido desde internet. Por ejemplo, cuando este equipo preste algún servicio que deba publicarse, el equipo interno deberá estar respectivamente aislado en una red de servicios públicos desmilitarizada (DMZ).

- Permitir tráfico de ingreso por puertos específicos a los equipos que hacen parte de la DMZ. Por ejemplo, página web, portales que disponen servicios entre otros.

- Algo a tener en cuenta en las aplicaciones, y los programas en general, son las buenas prácticas de programación segura.

- Igual para IPv6 que para IPv4, pero:

    - En IPv6 puede ser código nuevo.
    - En IPv6 se manejan cadenas y datos “más grandes”, cuidado con “overflows”.

Nota:

6.4.2. Para servicio de DNS

- En un entorno DNS se identifican varios puntos donde posibles ataques pueden desarrollarse. Estos puntos o “vectores de ataque” se sitúan tanto localmente en el propio servidor DNS y red local, como en las comunicaciones entre servidores y clientes.

- Para proteger el servicio DNS se recomienda:

- El sistema operativo del servidor debe ser actualizado y parcheado, es importante una política de mantenimiento de parches y seguimiento de posibles vulnerabilidades que pudiesen comprometer el sistema.
- Desactivar servicios innecesarios. Destinar el servidor exclusivamente al servicio DNS, desactivando todos los servicios innecesarios adicionales al software de DNS y a la administración del sistema. Aplicar las reglas de firewall estrictamente necesarias para permitir el funcionamiento de DNS.

- Una buena implementación de DNS debe separar siempre los servidores según su rol. Servidores autoritativos y cache recursivos serán dos componentes funcionales claramente diferenciados que requieren ser tratados de forma independiente en el diseño de la arquitectura de red.

6.4.3. Para servicio de DHCP

- El servicio DHCP requiere autorización dentro de una infraestructura de Active Directory. Si un servidor que forma parte de un dominio de Microsoft instala el rol de DHCP, necesitará autorización de una cuenta con privilegios en el Directorio Activo para iniciar el servicio DHCP.

- Windows Server 2016 permite configurar un clúster de servidores DHCP. Al utilizar dos o más servidores se evita la pérdida del servicio por la “caída” de uno de los equipos. Gracias al clúster se mantiene la totalidad del Pool de direcciones disponibles; además, la característica DHCP Clúster permite optimizar las cargas de trabajo entre los servidores que componen el clúster.

- El servicio de DHCP permite asociar identificadores del servidor DHCP a los registros DNS que se crean en las actualizaciones de los registros de equipo, que reciben la configuración del adaptador de red con DHCP. Utilizando este identificador se puede proteger la suplantación de nombres en las zonas DNS por parte de un equipo que no disponga de este identificador de DHCP y trate de suplantar el registro del nombre de equipo en el DNS.

- El uso de credenciales para las actualizaciones dinámicas de los registros DNS desde el Servidor de DHCP es otra medida de seguridad que es interesante configurar.

- En los entornos virtualizados se puede habilitar DHCP Guard; esta medida evita que las máquinas virtuales suplanten servidores DHCP. El servidor descartará todo el tráfico DHCP de servidores no autorizados.

6.4.4. Para servicio Web

- Deshabilitar Headers del servidor: Las cabeceras HTTP pueden contener información muy útil para un atacante. Cuando se realiza una petición hacia un servidor web, éste en las distintas respuestas HTTP que ofrece, incluye la cabecera Server que generalmente contiene información sobre el software que ejecuta el servidor web.

- Deshabilitar los módulos que no se utilizan: El deshabilitar los módulos que no se vayan a utilizar, va a ofrecer dos ventajas principales. Por un lado, no solo se evitarán ataques sobre estos módulos (a mayor número de módulos, mayor número de posibilidades de ataque); y por otro, también consumirá menos recursos.

- Usuarios y grupos de ejecución: Un aspecto que debe tener en cuenta en la ejecución de servicios, pasa por controlar qué usuario lo ejecuta. La idea consiste en que un servicio sea ejecutado por un usuario dedicado a él, con los mínimos privilegios posibles, de modo que ante un fallo en la aplicación el impacto sea menor.

- Disminuir el valor máximo de tiempo de espera: Disminuir el tiempo de espera para mejorar la resistencia a ataques de denegación de servicio.

- Limitar el tamaño de peticiones: Limitar el tamaño de una petición, lo que puede ser muy útil para asegurarlo contra ataques por desbordamiento.

- Poder contar con un firewall de aplicaciones el cual permitirá mitigar ataques a los servidores web. realizando un análisis de vulnerabilidades encontrado en el servidor.

6.5. POLÍTICAS DE SEGURIDAD SERVICIOS DE MONITOREO

A continuación, se listan las políticas de seguridad informática recomendadas para asegurar los servidores de monitoreo de la universidad pedagógica nacional (UPN) frente a la implementación de IPv6.

6.5.1. Para servicio de Monitoreo

- El monitoreo de los equipos debe hacerse por SNMPv3. Por lo tanto, en las herramientas de monitoreo que recopilen datos de equipos por SNMP deberán autenticarse respectivamente con usuario del dominio, así como aplicar el cifrado de paquetes en tránsito de la información monitoreada.

- Para realizar el monitoreo de los equipos se debe asignar direccionamiento ULA o bien utilizar las direcciones link local que tienen los equipos. El objetivo es restringir la circulación de tráfico SNMP a través de direcciones globales GUA. Esto previene ataques de descubrimiento y alcanzabilidad de los equipos fuera del perímetro.

- Las interfaces de administración de los dispositivos deben realizarse a través de la conexión a las direcciones IPv6 ULA o IPv6 link local. Esto permite que no se cuente con direccionamiento global GUA que pueda ser objetivo de ataque desde el exterior.

7. POLITICAS DE SEGURIDAD DE LA INFORMACION VS AFECTACION DE IPV6

7.1. AFECTACION DE LA ADOPCION DEL PROTOCOLO IPV6 FRENTE A LAS POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA UPN

En el anexo 9.1, se relacionan las políticas de seguridad de la información que se encuentran actualmente aprobadas por el UPN, frente a la afectación que podría llegar a tener con la adopción del protocolo IPv6 en la Entidad. Se lista una a una las políticas y se especifica si aplica o no para la adopción de IPv6, así como la descripción de la aplicación o afectación que podría tener frente a dicha adopción.

NOTA: Las políticas se revisaron de la siguiente publicación del UPN a la fecha del mes de octubre de 2020, en el siguiente documento:

- Manual de Políticas de Seguridad de la Información y protección de datos personales UPN.

7.2. ANALISIS DE LOS RESULTADOS

De acuerdo con la revisión realizada sobre las 123 políticas de seguridad de la información, se identificó que 30 políticas pueden ser afectadas de forma positiva o negativa dependiendo de la forma como se realice el despliegue de IPv6. Por lo tanto, se deberá considerar durante la adopción y la operación del protocolo IPv6 las medidas de control respectivas para prevenir la contravención de dichas políticas. A continuación, se presenta la distribución de la afectación de las políticas a partir de la adopción de IPv6.

Figura 8 Cantidad de Políticas de Seguridad que Afectan IPv6

Fuente Elaboración Propia

Como recomendaciones para reducir el impacto frente a dichas políticas por causa de la adopción de IPv6, se hacen las siguientes:

Recomendaciones:

- Definir un responsable de la transición a IPv6, así como de su gestión y monitoreo durante la operación. Esto permite que se garantice un control transversal sobre el uso de direccionamiento IPv6, así como su cumplimiento frente a lo requerido por MinTIC. De igual forma, es importante que el responsable se encargue de la renovación del direccionamiento IPv6 de la entidad
- Garantizar que cada activo que sea configurado con IPv6 se actualice dentro de la CMDB. Esto permite que se cuente con control y documentación de los activos y su correspondiente IPv6.
- El grupo de seguridad debería realizar verificaciones periódicas de reglas de firewall que permitan identificar accesos no autorizados, así como realizar pruebas de hacking ético para validar dichos accesos.
- Se recomienda validar la configuración de la comunicación que se realice con terceros con el fin de implementar el protocolo IPSEC en caso de que sea necesario.

- Para los cambios que se realicen sobre la infraestructura y sistemas de información se debe aplicar el correspondiente RFC.
- Realizar la vinculación de los dispositivos que tengan IPv6 en las herramientas de monitoreo. Lo anterior con el fin de poder contar con estadísticas de monitoreo que permitan verificar el comportamiento del despliegue.
- Realizar un escaneo de vulnerabilidades sobre los dispositivos que actualmente tienen IPv6. Lo anterior con el fin de identificar si se debe asegurar el protocolo IPv6 en servicios que ya cuenten con este protocolo.
- Luego de terminar el despliegue de IPv6. el grupo de operación debería mantener constantemente la revisión de asignación del direccionamiento IPv6 en todos sus segmentos, así como asignar los nuevos segmentos de manera uniforme tal como se realice en la fase de despliegue.
- La operación deberá mantener de forma confidencial la información de direccionamiento y enrutamiento de la Entidad.
- Los RFCs que incluyan modificaciones en el servicio de navegación a internet por parte de los usuarios, deberían incluir pruebas de verificación de navegación a internet o el consumo de los servicios afectados por IPv6.
- Socializar la política de adopción de IPv6 a toda la entidad, así como a los proveedores actuales. Lo anterior permite que todos los funcionarios y contratistas conozcan los servicios permitidos y los requisitos de adopción de este protocolo. De igual forma se debe socializar el documento técnico de políticas de seguridad de IPv6 para que se adopten con cada instalación o configuración que incluya este protocolo.
- Cada RFC que incluya modificación o adopción de IPv6 en los sistemas de información deberá incluir las pruebas respectivas de funcionamiento sobre el protocolo IPv6.
- Realizar la adopción de IPv6 en los sistemas de información en los ambientes de preproducción antes de modificar los ambientes de producción. Esto permite que se controle el riesgo de indisponibilidad de las aplicaciones. Todo lo anterior a través del proceso de gestión de cambio de la Entidad.
- El grupo de operación, dentro de su categoría de incidentes de conectividad deberá incluir la categoría de Incidentes de conectividad sobre IPv6, lo anterior con el fin de contar con una métrica de la cantidad de incidentes de Ipv6 que puedan ocurrir a causa del uso de este protocolo.
- Socializar el documento de plan de contingencias con el grupo de operación una vez se entregue el despliegue de IPv6 para su correspondiente operación. Esto

permite que la operación conozca los posibles eventos de riesgo que pueden llegar a presentarse con el uso de este protocolo.

- Los documentos deberán ser entregados a la operación y relacionados a MinTIC en las plataformas dispuestas para ello. Esto permite dar el cumplimiento respectivo de adopción del protocolo.

Nota: En el Capítulo 9. Anexos en el Subcapítulo 9.1 Políticas de Seguridad de la Información Frente a la Afectación con la adopción del Protocolo IPv6 en la Entidad, se encuentra el detalle de cada una de las políticas de seguridad y la afectación frente al protocolo de red IPv6.

8. GESTION DE VULNERABILIDADES IPv6

8.1. COMPORTAMIENTO DE VULNERABILIDADES IPV4 – IPV6

8.1.1. Vulnerabilidades IPv4 con Comportamiento Similar con IPv6

A continuación, se presentan las vulnerabilidades que se encuentran en el protocolo de red IPv4 y los cuales se pueden encontrar en el protocolo de red IPv6 y los cuales tienen un comportamiento similar:

- Sniffing: Técnica utilizada para escuchar todo lo que ocurre dentro de una red. IPSec puede ayudar a mitigar esta amenaza.

- Ataques a Nivel de Aplicación: IPSec puede usarse para evitarlo, aunque introduce problemas para los IDS. También puede usarse protección en el nivel de Aplicación.

- Dispositivos no Autorizados: Se hacen pasar por conmutadores, encaminadores, puntos de acceso o recursos como servidores DNS, DHCP o AAA.

- Ataques de 'Hombre-en-el-medio' (man-in-the-middle): Es un tercer host que reenvía de forma transparente la información digital como una pasarela entre dos o más socios de comunicación y espías simultáneamente. El remitente y el destinatario no saben que hay un tercer host entre los dos y que en realidad no se están comunicando directamente. IPSec puede ayudar.

- Ataques por Inundación (flooding). Comportamiento abusivo de la red de comunicaciones, normalmente por la repetición desmesurada de algún mensaje en un corto espacio de tiempo.

8.1.2. Vulnerabilidades IPv4 con Diferente Comportamiento con IPv6

A continuación, se presentan las vulnerabilidades que se encuentran en el protocolo de red IPv4 y los cuales se pueden encontrar en el protocolo de red IPv6 y los cuales tienen un comportamiento similar:

- Escaneo de Red: Escaneo de una red típica (/64) en la práctica es más difícil. También los ataques automatizados, por ejemplo, gusanos que seleccionan direcciones aleatorias para propagarse, se ven dificultados => cambio métodos escaneo

- Ataques de Amplificación Broadcast (Smurf): Ataque DoS. Se envía echo ICMP a dirección de broadcast de una red con la dirección de origen falseada a la del host víctima. Todos los nodos del prefijo destino envían una echo Reply a la víctima. En IPv6, no existe el concepto de broadcast-> Multicast => no respuesta ICMP

- Ataques relacionados con Mecanismos de Transición: No se utilizan nuevas tecnologías, el mismo tipo de vulnerabilidades que con IPv4:
  - Redes doble-pila pueden ser atacadas usando ambos protocolos.
  - Los túneles IPv6 necesitan nuevos puertos abiertos en los firewalls.

- Recomendaciones:
  - En redes/hosts de doble-pila usar medidas de seguridad similares para IPv4 e IPv6.
  - Controlar el uso de túneles cuando sea posible.
  - Habilitar que los firewalls inspeccionen el tráfico encapsulado.

8.1.3. Nuevas Vulnerabilidades con IPv6

A continuación, se presentan las nuevas vulnerabilidades que se pueden encontrar con el protocolo de red IPv6:

- Amenazas a NDP -> First-Hop Security: Funcionalidad RA-Guard y otros. Es vulnerable a diversos ataques (RFC3756).
- Routing HeaderType0 [RFC5095]: Puede explotarse para lograr la amplificación del tráfico en una ruta remota con el fin de generar tráfico de denegación de servicio.
- Mecanismos de Transición: En el sentido de que funcionan encapsulando tráfico y los firewalls y otros dispositivos/software de seguridad deben ser capaces de procesarlos.
- IPSec: Envío de datos cifrados que los firewalls no pueden inspeccionar, especialmente firewalls 'full-state'
- Autoconfiguración: En IPv6 se definen varias herramientas para la autoconfiguración
  - NDP tiene varias amenazas (como ARP en IPv4), e IPSec y SEND se pueden usar para añadir seguridad
  - DHCP tiene las mismas consideraciones en IPv4 e IPv6
- Dependiendo del nivel de control y seguimiento que se requiera se deben usar distintos métodos de configuración de direcciones.
  - De más a menos:
    - Direcciones estáticas
    - Autoconfiguración 'Statefull': DHCPv6
    - Autoconfiguración 'Stateless': Identificador de interfaz a partir de la dirección MAC
    - Autoconfiguración 'Stateless': Identificador de interfaz utilizando las extensiones de privacidad o aleatorios

8.2. RECOMENDACIONES PARA PREVENCION DE ATAQUES ESPECIFICOS

Las siguientes políticas se incluyen con el fin de poder identificar las acciones que deben tomarse para prevenir diferentes tipos de ataques.

8.2.1. Recomendaciones para Contener Ataques de Red

a. Para mitigar ataques de Suplantación: Estos ataques se pueden prevenir mediante la aplicación de RA-Guard del RFC4191[6], filtrado de direcciones IPv6 origen y el aseguramiento plasmado en la guía "Level-2 Security Hardening Policies (Optional).pdf " en su numeral 3.2.15 Defense Against IP Address Spoofing Attacks. Lo anterior aplicado al protocolo IPv6.

b. Para mitigar ataques de Reconocimiento de Red: Este tipo de ataques se puede prevenir mediante la asignación aleatoria de direccionamiento IPv6. Lo anterior con el fin forzar al atacante a que inicie un escaneo en un rango totalmente amplio que podría requerir de tiempo significativo, así como ser detectable. De igual forma, para los enlaces punto a punto, como se menciona en las recomendaciones generales, la asignación del /64 a los enlaces punto a punto es necesaria, aunque se configuran /127 a /124 en cada interfaz.

   Por otro lado, el aseguramiento de cara a internet en dispositivos de firewall, debe realizarse acorde para filtrar el tráfico desde el exterior a los equipos internos.

c. Para mitigar ataques al DHCPv6**:** Para prevenir este tipo ataques se debe realizar el filtrado respectivo de Servidores DHCP, configurando las opciones de routing adecuadamente para entregar las direcciones a nivel de red. Lo anterior acorde con la guía "Level-2 Security Hardening Policies (Optional).pdf" en su numeral 3.2.2 DHCP Security, aplicado a IPv6.

d. Para mitigar ataques a Multicast**:** Para prevenir este tipo de ataques se deben aplicar políticas de MLD Guard mencionadas en la siguiente guía, la cual brinda los lineamientos específicos de como configurar adecuadamente el protocolo Multicast y qué consideraciones de seguridad deben aplicarse para filtrar grupos, direccionamiento de multicast definido entre otras.

   - https://tools.ietf.org/id/draft-vyncke-pim-mld-security-00.html

En el link anterior se presentan los lineamientos específicos de como configurar adecuadamente el protocolo Multicast

[6] https://tools.ietf.org/html/rfc4191

e. Para mitigar ataques a ICMPv6**:** Los ataques a ICMPv6 son los más comunes. Lo anterior dado que este protocolo realiza la gestión de comunicación total para IPv6. Por lo tanto, para mitigar estos ataques se debe realizar el aseguramiento en equipos de red aplicando el filtrado respectivo de paquetes ICMPv6 Echo Reply, Host Unreachable, y Port Unreachable de acuerdo con la guía "Level-2 Security Hardening Policies (Optional).pdf" en su numeral 3.2.13 Defense Against ICMPv6 Attacks.

f. Para mitigar ataques al Protocolo ND**:** Para prevenir este tipo de ataque se deben asegurar los equipos de red a partir de la implementación de la funcionalidad ND Snooping, la cual permite determinar y registrar los paquetes NS enviados por los equipos bloqueando así el tráfico malicioso que viaje sobre la red o que desee burlar los equipos con mensajes fraudulentos. Para esto se debe seguir la guía de aseguramiento "Level-2 Security Hardening Policies (Optional).pdf" en su numeral 3.2.17 IPv6 ND Security.

8.2.2. Recomendaciones para Contener otro tipo de Ataques

a. Para mitigar ataques de DoS/DDoS**:** Los ataques de denegación de servicio normalmente se pueden detectar a través de herramientas de monitoreo en los equipos de borde, donde se puede medir el volumen de tráfico para las interfaces respectivas. Para esto se deben implementar reglas de filtrado y monitoreo por dirección IP origen, así como notificaciones automáticas frente a la identificación de alarmas de este tipo.

b. Para mitigar ataques a Capas Superiores: Ataques de autenticación, registro de logs, control de acceso a equipos, enrutamiento y protocolos de enrutamiento, seguridad de contraseñas, entre otros. Para mitigar estos ataques se debe seguir la guía de aseguramiento "Aseguramiento para contener ataques de red Security Hardening Guide.pdf" que se entrega como anexo al presente documento.

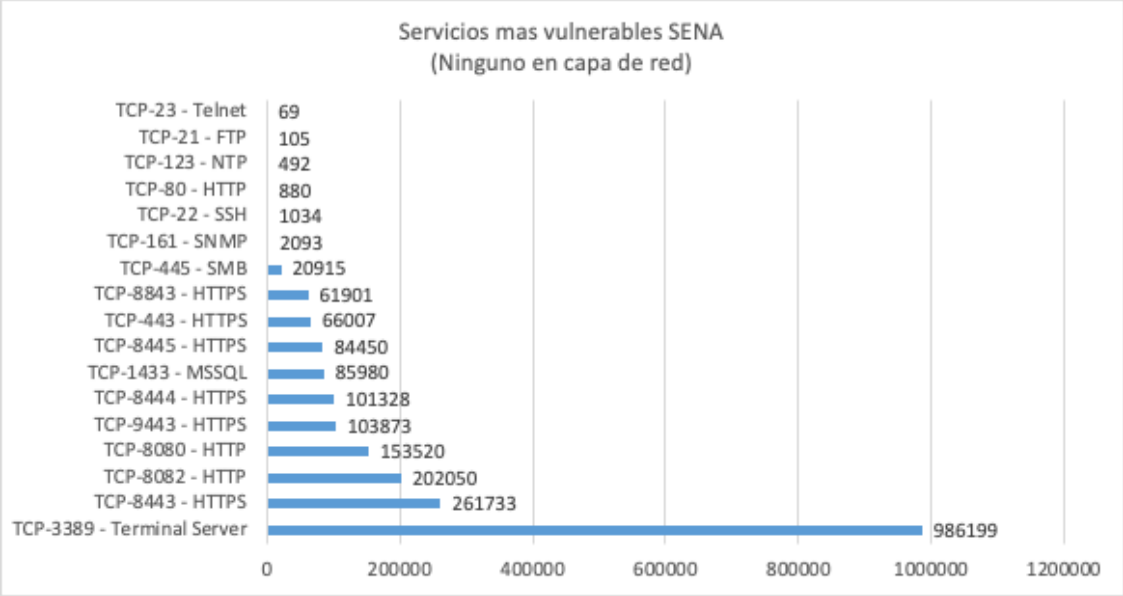
8.3. ESCANEO DE VULNERABILIDADES IPV4 – IPV6

Dentro de la entidad se deberá realizar el escaneo de vulnerabilidades sobre IPv6. Por lo tanto, se deberán tener en cuenta las siguientes recomendaciones:

- Realizar el escaneo de vulnerabilidades sobre IPv6 al menos 1 vez al año con el fin de detectar vulnerabilidades sobre este protocolo y que puedan afectar la confidencialidad, integridad y disponibilidad de la información o de los servicios.
- Con los resultados de los escaneos, se deben revisar las vulnerabilidades que aplican al protocolo IPv6 y reportarlas al grupo encargado para que se realicen las remediaciones correspondientes.
- Se debe tener en cuenta que cuando se realicen los escaneos se apliquen los Plug-Ins respectivos (si existen) que permitan detectar vulnerabilidades en IPv6.

A la fecha, los servicios vulnerables que tiene la UPN son los siguientes:

Figura 9 Cantidad de vulnerabilidades vs Servicios de la entidad



Fuente Elaboración Propia

De acuerdo con lo anterior, el servicio que tiene mayor número de vulnerabilidades es el servicio de Terminal Server. Sin embargo, para el contexto de IPv6, no aplica ninguno de los servicios dado que son de capas superiores (aplicación) y no es afectado por el despliegue de IPv6 en la Entidad. De todas formas, se debe seguir evaluando el nivel de vulnerabilidad de la infraestructura y sistemas de información para poder detectar otro

tipo de vulnerabilidades y servicios que si apliquen a la capa de red y por tanto al protocolo IPv6.

9. NORMOGRAMA

- Resolución 2710 del 2017. Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Modelo de Seguridad y Privacidad de la Información. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en HTTPS://WWW.MINTIC.GOV.CO/GESTIONTI/615/ARTICLES-5482_MODELO_DE_SEGURIDAD_PRIVACIDAD.PDF

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Transición de IPv4 a IPv6 para Colombia. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en

- HTTPS://WWW.MINTIC.GOV.CO/GESTIONTI/615/ARTICLES-5482_G20_TRANSICION_IPV4_IPV6.PDF

- Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Aseguramiento del Protocolo IPv6. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en HTTPS://WWW.MINTIC.GOV.CO/GESTIONTI/615/ARTICLES-5482_G19_ASEGURAMIENTO_PROTOCOLO.PDF