Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	28/05/2020
Programa:	Seguridad Informática
Línea de Investigación:	Infraestructura Tecnológica y Seguridad en Redes
Título:	Transición al Protocolo IPV6, Aspectos de Seguridad Informática para Tener Presente
Autor(es):	Ricardo Andrés Chica Mora
Palabras Claves:	Protocolo, IPV6, IPV4, Redes
Descripción:	El siguiente trabajo investigativo plantea los pasos necesarios para llevar a cabo una transición del protocolo IPV4 al protocolo IPV6, mencionando las herramientas necesarias a implementar para lograr un buen proceso de migración, evitando complicaciones en los servicios de la entidad que desea realizar la actualización; Esto con el fin de dar solución a las múltiples problemáticas que se han evidenciado en el protocolo Ipv4, como el agotamiento de direcciones IP. Problemáticas que generan un atraso e impiden el uso de nuevas aplicaciones que son fundamentales para la evolución de los procesos de comunicación. El nuevo protocolo se presenta como solución y forma de subsanar las falencias que su antecesor ha dejado en evidencia. Comprendiendo que este proceso de migración es bastante complejo, y requiere de una rigurosa investigación y conceptualización, se presenta la siguiente monografía con el fin de guiar de forma correcta en el curso de la transición

Fuentes bibliográficas destacadas:

[1] AHUATZIN SANCHEZ, Gerardo. Capitulo I. Panorama actual del cambio de IPV4 a IPV6. [En Línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo1.pdf

[2] ALONSO, Juan. Agotamiento del espacio Ipv4. [En Línea]. Disponible en: http://www.eslared.org.ve/walc2012/material/track2/03-Agotamiento.pdf

[3] BEJARANO RAMIREZ, Ana. MIRANDA CASTILLA, Diego. HENRIQUEZ CELEDON, Javier. [En Línea]. Venezuela. Disponible en: https://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Redes%20Informaticas/IPv4%20Vs%20IPv6.pdf

[4] CASTILLO, Yarisol. Agotamiento de IPv4 en la región latinoamericana. [En Línea]. Panamá. Disponible en: http://www.utp.ac.pa/documentos/2015/pdf/07-ACTUALIDAD_TECNOL._AGOTAMIENTO_26-28_0.pdf

[5] CCOYLLO, Ingrid. Enrutamiento IPv6 - con el software Packet Tracer. [En Línea]. Disponible en: https://informatica.ucm.es/data/cont/media/www/pag-66886/Presentacion%20Enrutamiento%20IPv6.pdf

Contenido del documento:	La monografía de estudio inicia con una introducción sobre las incidencias que ha presentado el protocolo de internet IPV4, allí se evidencia las necesidades y la importación de la transición hacia su versión más actualizada. El desarrollo de este trabajo consta de lo siguiente: **Formulación del Problemas** Después de analizar la problemática que presenta IPV4,y tras evidencias sus fallas en la seguridad se plantea la siguiente interrogante: ¿Cómo realizar una transición al protocolo IPV6 en una empresa que aun labora con las limitaciones del protocolo IPV4, sin alterar las funciones de las aplicaciones que dependen del protocolo IP en su cuarta versión para su funcionamiento? **Objetivo General** Presentar un documento que permita determinar el debido proceso de la migración de protocolo IPV4 a IPV6 teniendo presente aspectos relevantes en el tratamiento de la información y la seguridad informática. **Objetivos Específicos** • Realizar un estudio sobre los mecanismos y procesos implementados en el protocolo IPV6. • Establecer recomendaciones para mejorar la seguridad aplicando las nuevas tecnologías que soportan IPV6.

	• Generar un documento que contribuya y brinde orientación en el proceso de transición de IPV4 a IPV6. **Marco Conceptual:** Aquí se definen conceptos importantes sobre procesos y herramientas que intervienen en la operación de las versiones más recientes del protocolo de internet. **Marco Teórico:** Observamos el estado de IPV6 en el mundo, cuales han sido los países pioneros en la implementación de este protocolo y las diferentes novedades presentadas. Se observa el porcentaje de implementación en Colombia, y el propósito de Mintic de guiar a mas empresas en este proceso, con el fin de una actualización nacional, apoyando un despliegue masivo para aprovechar los beneficios de IPV6. **Razones para realizar la migración a IPV6:** Se especifican las razones mas importantes y que mas destacan para la transición, aquí observamos las diferencias principales entre ambos protocolos y se evidencia las mejores de IPV6 sobre IPV4. **Seguridad IPV6:** Observamos la estructura y el comportamiento de IPSEC en IPV6, también como es el comportamiento de IPV6 en temas como la seguridad en los centros de datos, las VPNs y seguridad en la nube. Se describen los pilares de la seguridad con IPV6 **Fases para el proceso de transición:** Observamos las tres fases que intervienen en este proceso (planeación, implementación, pruebas de funcionalidad) con sus respectivas actividades a desarrollas, estas actividades son planteadas con el fin de que la transición sea transparente para el usuario final, que no afecte el desarrollo normal de los aplicativos y servicios que estén operando con IPV4. Cada fase finaliza con unos productos entregables que serán el aval para continuar con la siguiente, finalizar la

	implementación y garantizar la funcionalidad de IPV6 en la infraestructura TI. **Requerimientos para el proceso de transición:** Se lista lo necesario para que el proceso de transición se logre con la mayor transparencia posible, evitando que sea un cambio traumático y no se presenten brechas en la seguridad que pueden afectar la información manejada por la entidad.
Marco Metodológico:	La metodología usada para la ejecución de esta monografía fue una metodología documental, la cual se baso en la construcción de conocimiento por medio de fuentes bibliográficas, seleccionando la información y compilando lo necesario por medio de lecturas y análisis de documentos que aportaran a la solución de la problemática planteada.
Conceptos adquiridos :	Las ventajas y mejoras que tiene el protocolo IPV6 sobre su antecesor, comprender los beneficios que obtendría una infraestructura TI cuando el trafico de red se realice por medio de este nuevo protocolo.
Conclusiones:	En el presente escrito, se plantearon las fases (Planeación, Implementación, Pruebas de funcionalidad), en donde se mencionan las actividades que permiten orientar a las empresas en el proceso de transición hacia IPV6. En la fase de implementación el proceso de migración debe ser estructurado tomando como fuente las políticas de seguridad que establezca la entidad que busca la migración. Estas políticas forman la base, para que IPV6 contemple la confidencialidad, integridad y disponibilidad de la información. La disposición de la infraestructura TI de las áreas de la entidad configuradas o administradas por Firewall y sus respectivos servicios segmentados afianzan la capacidad de IPV6 en los temas de conexión y seguridad en la que se inicie el tráfico por medio de este protocolo, que ofrece la garantía de una mayor posibilidad

	de conexiones gracias al incremento a 128 bits, esto apoyado mediante vías de direccionamiento disponibles en IPV6 (Anycast, Multicast, Unicast).En el estudio realizado, se identifica en IPV6 un notable mejoramiento en comparación a su antecesor en cuestión de la capacidad de autentificación y privacidad de los paquetes enviados y recibidos. Es importante que los nombres de los servicios que operan con IPV4 se mantengan iguales al momento de realizar la transición y el tráfico de red se enrute por IPV6. Esta recomendación tiene como fin la transparencia en la resolución de nombres de dominio para ambos protocolos y al igual que en el protocolo IPV. En IPV6 es aconsejable no usar direcciones literales, esto en el caso de librerías y en el desarrollo de aplicaciones. Otra recomendación importante para preservar la seguridad de la información es la verificación de las segmentaciones de los bloques IPV6, cuando estos se han configurado por zonas DMZ (Zonas desmilitarizadas), la base es lo requerido por cada entidad, quienes establecen sus respectivos niveles y/o criterios de seguridad. Dentro del análisis expuesto, se ha evidenciado que en el proceso de migración se pueden generar riesgos que afectan la seguridad de los datos, por tal motivo en cada fase planteada es necesario análisis las variantes que lleguen a desencadenar vulnerabilidades ya que IPV6 no es un protocolo que opere de forma independiente, por el contrario, es apoyado por otros servicios como Ipsec, SIP, TCP, UDP, entre otros. Desarrollar un plan de contingencia permite garantizar disponibilidad a todos los usuarios si en algún momento se presentan inconvenientes que atenten contra la seguridad de la información.

	Finalmente se ha generado un documento, donde se relacionan los parámetros necesarios para que IPV6 opere con normalidad en una infraestructura TI que cuenta con IPV4 para esto es importante la revisión del nivel de impacto de aplicativos en funcionamiento o servicios tale como DNS, el sistema de correo electrónico, el servicio DHCP, directorio activo, el sistema Proxy, Sistemas de monitoreo y sistemas de gestión