ANÁLISIS COMPARATIVO DE ALGORITMOS CRIPTOGRÁFICOS PARA REDES PRIVADAS VIRTUALES

COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR VIRTUAL PRIVATE NETWORKS

Denys Ivan Capuñay Puican[1]
Ana María Guerrero Millones[2]
Juan Elias Villegas Vega[3]

Fecha de recepción: 17 de mayo 2016
Fecha de aceptación: 20 de setiembre 2016

Resumen

La necesidad de manipular la información de una manera más segura y confiable, es a través de las llamadas redes privadas virtuales (VPN), nos permitió vincularnos y tener un enlace privado, el cual se va acoplado sobre una red pública que garantiza la integridad y confidencialidad de la información gracias a los diversos procesos de autenticación, encriptación y codificación, obteniendo un enlace que garantiza la privacidad.

Es en este sentido, que la presente investigación trata de hacer un análisis comparativo de los algoritmos criptográficos usados para redes privadas virtuales, ya que el problema principal radica en asegurar la integridad y seguridad que tiene la información cuando se conecta a otro equipo de forma remota. Esto se logró seleccionando todos los algoritmos existentes para redes privadas virtuales, e implementándolos en una red donde se hizo los estudios y captura de tráfico para observar y analizar cual nos ofrece una mejor integridad y seguridad de la información.

Para el desarrollo de esta investigación se utilizó la metodología experimental, que permitió manipular las variables en función de que permita la recolección de datos, conociéndose así la encriptación que ofreció cada algoritmo.

Después que se evaluó cada algoritmo en la red implementada, se logró determinar que algoritmos es mejor en tiempos, tamaño de los paquetes, el nivel de encriptación y desencriptación, grado de encapsulación, etc. Obteniendo que el algoritmo AES divide los datos en un mayor número de paquetes y necesita menor tiempo para enviarlos en comparación con los demás algoritmos. Sobre los paquetes encriptados algoritmo AES presenta igual número de paquetes encriptados que el algoritmo DES, pero algoritmo AES desencripta mas paquetes que el algoritmo DES utilizando menos recursos.

Entre las conclusiones se obtuvo que el algoritmo AES es el mejor protocolo en tiempo de envió, en número de paquetes de encriptación y en número de paquetes de desencriptación.

Palabras claves: *Algoritmos, Análisis, Criptografía, Integridad, Redes Privadas Virtuales, Seguridad***.**

Abstract

The need to manipulate information in a more secure and reliable way is through so-called virtual private networks (VPN), which allows us to link up and have a private link, which is coupled to a public network that ensures the integrity and confidentiality of the information through the various processes of authentication, encryption and encoding, getting a link that ensures privacy.

[1] *Escuela Profesional de Ingeniería de Sistemas. Facultad de Ingeniería, Arquitectura y Urbanismo. Egresado en Ingeniería de Sistemas. Universidad Señor de Sipán. Chiclayo. Lambayeque. Perú. cpuicand@crece.uss.edu.pe.*

[2] *Escuela Profesional de Ingeniería de Sistemas. Facultad de Ingeniería, Arquitectura y Urbanismo. Docente de Ingeniería de Sistemas. Universidad Señor de Sipán. Chiclayo. Lambayeque. Perú. aguerreromi@crece.uss.edu.pe.*

[3] *Escuela Profesional de Ingeniería de Sistemas. Facultad de Ingeniería, Arquitectura y Urbanismo. Docente de Ingeniería de Sistemas. Universidad Señor de Sipán. Chiclayo. Lambayeque. Perú. jvillegas@crece.uss.edu.pe.*

It is in this context that this thesis is a comparative analysis of cryptographic algorithms used for virtual private networks, because the main problem in ensuring the integrity and security is our information to connect to another computer remotely. This was achieved by selecting all existing algorithms for virtual private networks, and implementing them in a network where traffic capture studies and was to observe and analyze which offers better integrity and security of our information.

For the development of this experimental research methodology was used, as this allowed us to manipulate the variables in terms of enabling data collection, and knowing the encryption offered each algorithm.

After evaluating each algorithm implemented in the network, it was determined that algorithms is better at times, packet size, the level of encryption and decryption, degree of encapsulation, etc. Obtaining the AES algorithm divides the data into a larger number of packets and requires less time to send as compared to the other algorithms. About AES encrypted packet has the same number of encrypted the DES algorithm, but decrypting AES algorithm more packets DES algorithm using fewer resources packages.

Among the findings it was obtained that the AES algorithm is the best time protocol sent in number of encryption packages and the number of packages decryption.

Keywords: *Algorithms, Analysis, Cryptography, Integrity, Virtual Private Networks, Security.*

---

1. Introducción

La presente investigación se refiere al tema de seguridad informática, en la cual se hizo un análisis comparativo de algoritmos criptográficos para redes privadas virtuales. Las redes privadas virtuales o VPN son aquellas conexiones punto a punto a través de una red privada o pública, como el internet. La información de una red privada se transporta de manera segura a través de la red pública para formar una red virtual. Esta tiene beneficios como ahorro de costos, escalabilidad, compatibilidad con tecnología de banda ancha y seguridad. Siendo la seguridad uno de los elementos más importantes para asegurar la información de las organizaciones debido a los múltiples ataques por parte de hackers, el gobierno que espía nuestros datos y de algunos curiosos, esto se logra configurando algoritmos de encriptamiento; es en este sentido que esta investigación tiene como objetivo principal analizar comparativamente los algoritmos criptográficos VPNs.

La investigación, Concepción de redes privadas virtuales mediante IPSec conjunto de protocolos, análisis comparativo de consultas de bases de datos distribuidas utilizando diferentes modos de cifrado IPSec. Afronto problemas como encontrar soluciones fiables para protegerse de las actividades que desconfiadas y por la ciberdelincuencia. Logró presentar una extensión de una red privada virtual hecha a través de características adicionales como encapsular los paquetes de datos con una cabecera en ambos extremos, a lo largo de las líneas de la comunicación, así como a través de túneles de comunicación (Muhamad, 2015). Sistema Red VPN utilizando el protocolo IPSec, en esta investigación se enfrentó problemas como mecanismos de comunicación pocos seguros y poco fiables, con costos considerablemente líneas arrendadas. Lo que hizo fue Estudiar el método de construcción de túneles en el sistema de IPSec. El protocolo IPSec lo estudia y pone en práctica, y analiza la seguridad en redes VPN. Propuso usar una red VPN por las características en cuanto a su seguridad de, Construye túneles usando el sistema de IPSec. (Gang, 2011).

2. Materiales y métodos

Tipo de estudio: El estudio planteado es del tipo descriptiva-comparativa, por un lado se describe los algoritmos para redes privadas virtuales objeto de este estudio y enuncia sus características, por el otro lado se elaboró un software para encriptar datos y poder enviar estos a través de una red privada virtual. Comparando con que algoritmos aumenta el nivel de integridad de los datos.

X= (Algoritmos criptográficos) Y= (Medir la Confidencialidad)

Diseño:
Variables de la investigación
Variable dependiente o variable1: *Integridad y confidencialidad de los datos en una red privada virtual.*
Variable independiente o variable 2: *Algoritmos criptográficos*

Métodos de Investigación:
Los métodos de investigación que utilicé para recolección de datos han sido Experimental.
Se usó este método porque permite manipular las variables en función que permite la recolección de datos, conociendo el tipo de encriptación que ofrece cada algoritmo.

Técnicas de recolección de datos:
Observación: Se utilizó esta técnica para poder investigar y conocer los algoritmos para redes privadas virtuales.
Entrevistas: Entrevisté a ingenieros en redes y telecomunicaciones experto en el tema, obteniendo de manera más detalla que algoritmo se utilizan más, y cual ofrece más seguridad.

Instrumentos de recolección de datos:
a) Wireshark: Le permite ver lo que está sucediendo en su red a nivel microscópico.
b) Tcpxtract: Es una herramienta para extraer los archivos de tráfico de red basado en firmas de archivo.
c) Acrylic WIFI: Acrylic WiFi puede ver y escanear las redes WiFi que hay a tu alcance, obtener información de seguridad de la red y obtener contraseñas WiFi genéricas gracias un sistema de plugins incluido.
d) PuTTy: PuTTy es un cliente de red que soporta los protocolos SSH, Telnet y Rlogin y sirve principalmente para iniciar una sesión remota con otra máquina o servidor.

Para estudiar y evaluar los algoritmos de encriptación, se implementó varios prototipos de redes privadas virtuales en el Laboratorio de Sistemas Inteligentes y Seguridad Informática de la Universidad Señor de Sipán (LABSIS). Para ello se utilizó 3 routers Cisco Serie 2900, Switch Cisco Serie 100, 2 cables seriales, 6 cables directos y cable consola para la configuración, para la configuración se utilizó el software Putty, para conectarnos a cada equipo.

Entre las técnicas de recolección de datos se utilizó la Observación, para poder investigar a detalle cada algoritmo y la Entrevista a expertos para validar la información obtenida de la evaluación.
Entre los instrumentos de recolección de datos se usó el software Wireshark para captura el tráfico y Tcpxtract, herramienta para extraer los archivos de tráfico de red basado en firmas de archivo.
Además se utilizó una topología de red estándar, ver figura 1.

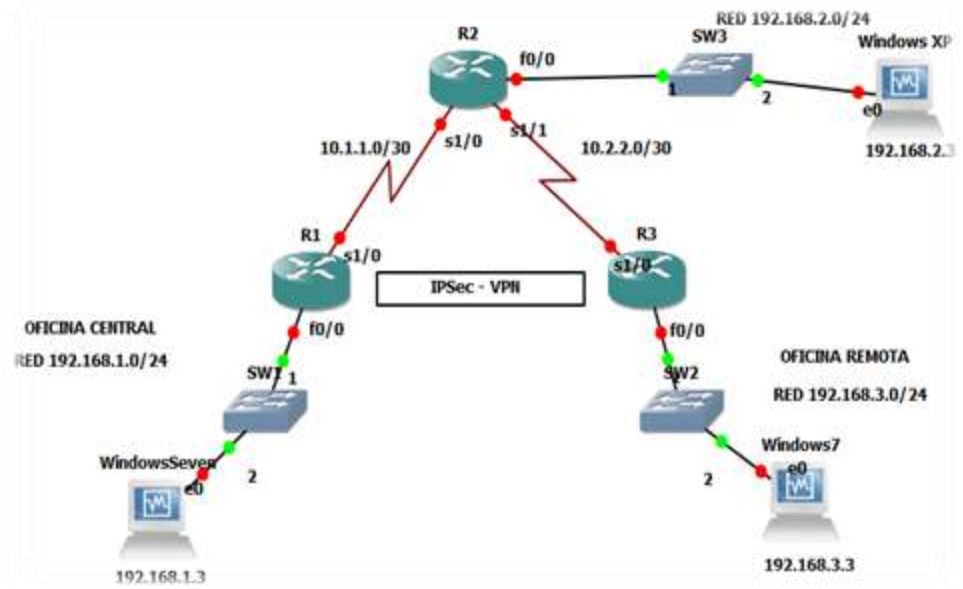

Figura 1. *Topología de red privada virtual*
Fuente: *CCNA 4 v5.2*

3. Resultados

Para la evaluación de envío de datos se utilizó un archivo de prueba: 4.53 MB**,** por el tamaño del archivo: Se utilizó el mismo archivo para hacer las pruebas con los tres algoritmos.

Tabla 1
Evaluación por el tamaño de archivo

Algoritmo	3 DES	AES	DES
Tamaño de archivo	4.53 MB	4.53 MB	4.53 MB

Por el número de paquetes generados.

Tabla 2
Evaluación por el número de paquetes

Algoritmo	3 DES	AES	DES
Número de paquetes	4995	5226	5246

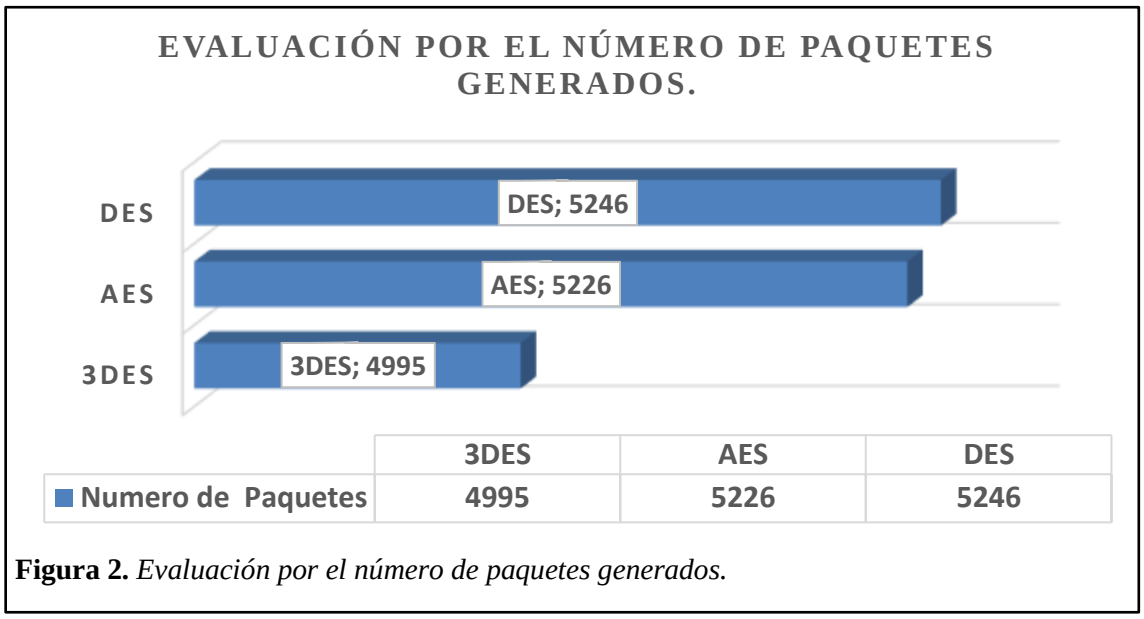

Figura 2. *Evaluación por el número de paquetes generados.*

Por el tiempo de envío.

Tabla 3
Evaluación por el tiempo de envío.

Algoritmo	3 DES	AES	DES
Tiempo de Envío.	00:04:26:59	00:04:21:42	00:04:25:07

El algoritmo AES necesita menos tiempo para enviar el mismo archivo, optimizando los recursos del computador.

Por el número de paquetes encapsulados

Tabla 4
Evaluación por el # de paquetes encapsulados

Algoritmo	3 DES	AES	DES
# Paquetes encapsulados	3271	3277	3277

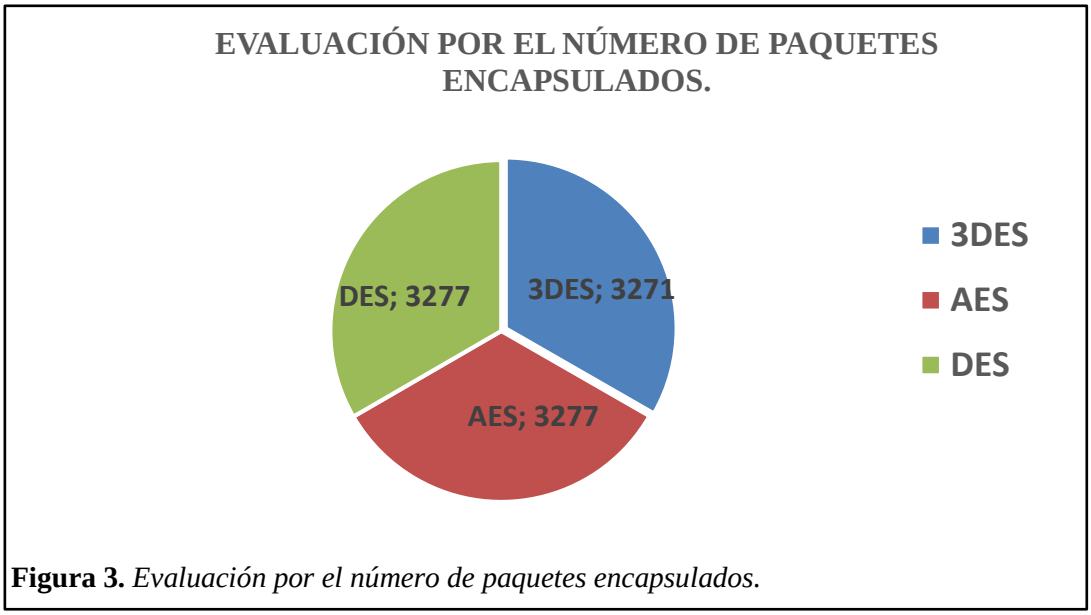

Figura 3. *Evaluación por el número de paquetes encapsulados.*

Por el número de paquetes desencapsulados.

Tabla 5
Evaluación por el # de paquetes desencapsulados

Algoritmo	3 DES	AES	DES
# Paquetes desencapsulados	1728	1702	1713

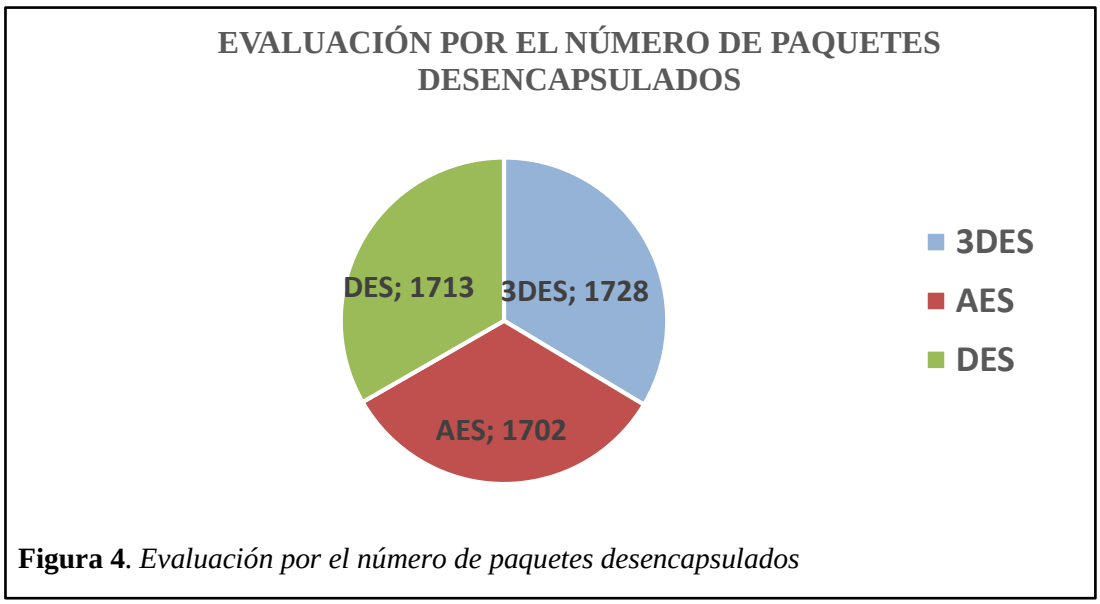

Figura 4. *Evaluación por el número de paquetes desencapsulados*

Por el número de paquetes encriptados

Tabla 6
Evaluación por el número de paquetes encriptados

Algoritmo	3 DES	AES	DES
# Paquetes encriptados	3271	3277	3277

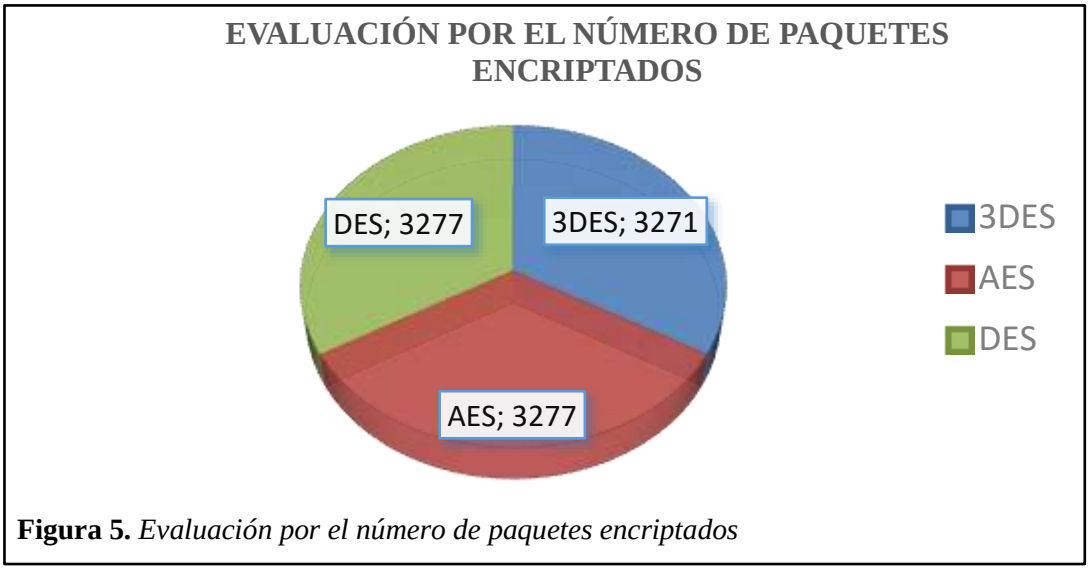

Figura 5. *Evaluación por el número de paquetes encriptados*

Por el número de paquetes desencriptados.

Tabla 7
Evaluación por el # de paquetes desencriptados

Algoritmo	3 DES	AES	DES
# Paquetes desencriptados	1728	1728	1713

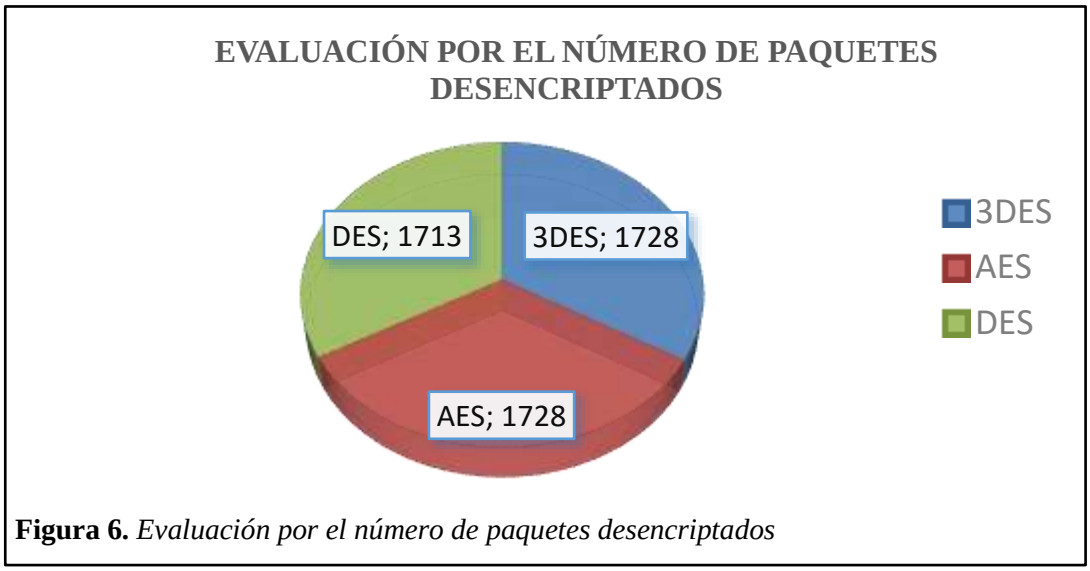

Figura 6. *Evaluación por el número de paquetes desencriptados*

Para la evaluación de envío de voz y video se utilizó una llamada de video presencia de prueba de: 6 Minutos.

Por el tiempo de Video Presencia: Se utilizó el mismo tiempo para hacer las pruebas con los tres algoritmos.

Tabla 8
Evaluación por el tamaño de archivo

Algoritmo	3 DES	AES	DES
Tiempo de Video en Minutos	6	6	6

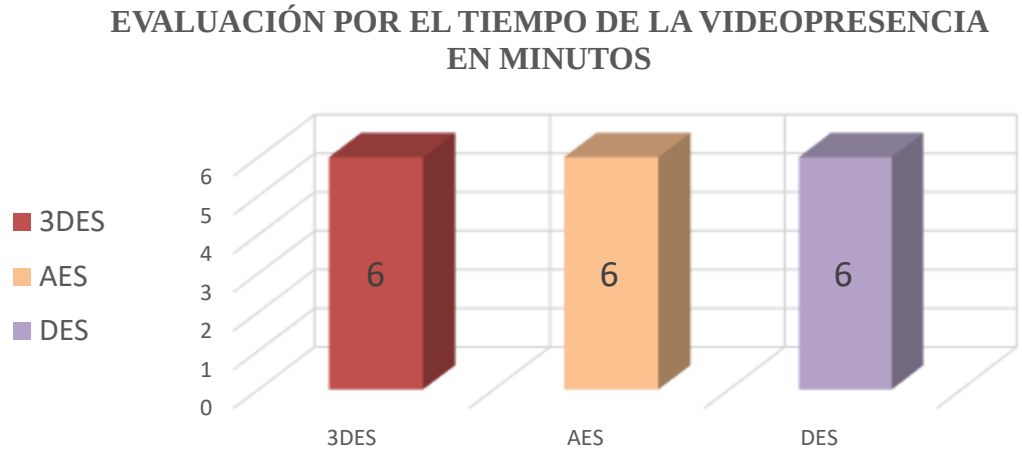

Figura 7. *Evaluación por el tiempo de la Videopresencia*

Por el número de paquetes que se generó para entablar la video presencia.

Tabla 9
Por el número de paquetes

Algoritmo	3 DES	AES	DES
Número de paquetes	40336	41071	40479

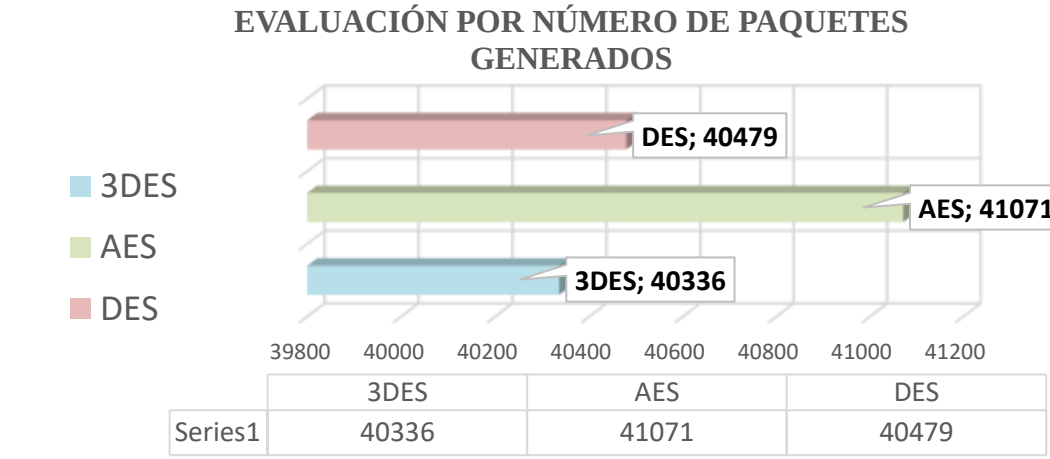

Figura 8. *Evaluación por el número de paquetes generados*

Tabla 10
Por el número de paquetes encapsulados

Algoritmo	3 DES	AES	DES
# Paquetes encapsulados	20182	20509	20235

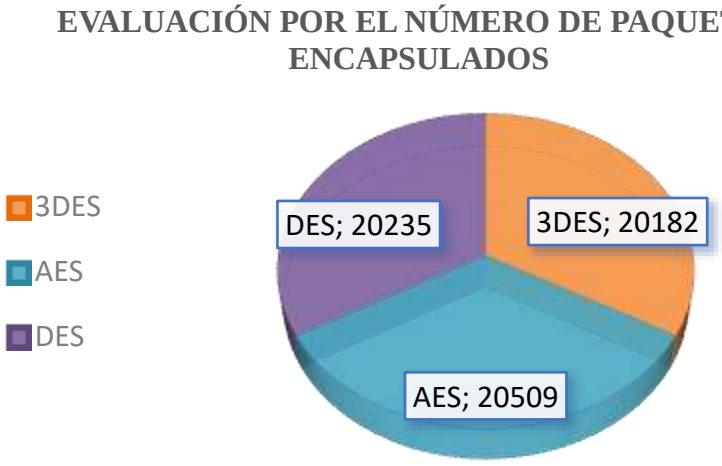

Figura 9. *Evaluación por el número de paquetes encapsulados*

Por el número de paquetes desencapsulados

Tabla 11
Por el número de paquetes desencapsulados

Algoritmo	3 DES	AES	DES
# Paquetes desencapsulados	20154	20562	20244

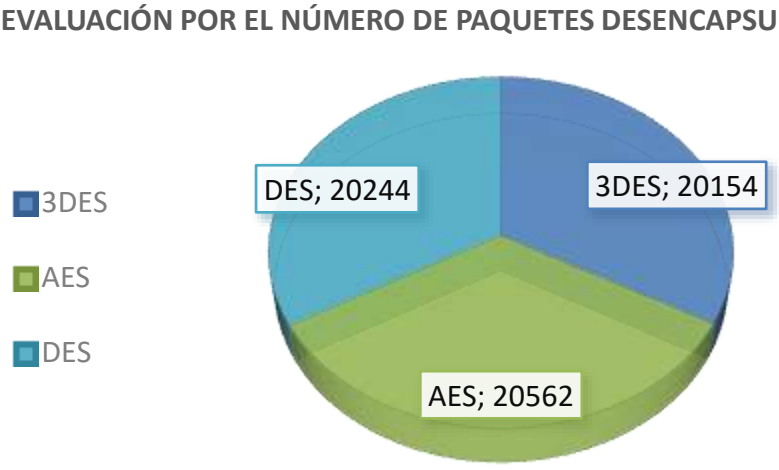

Figura 10. *Evaluación por el número de paquetes desencapsulados*

Por el número de paquetes encriptados

Tabla 12
Por el número de paquetes encriptados

Algoritmo	3 DES	AES	DES
# Paquetes encriptados	20182	20509	20235

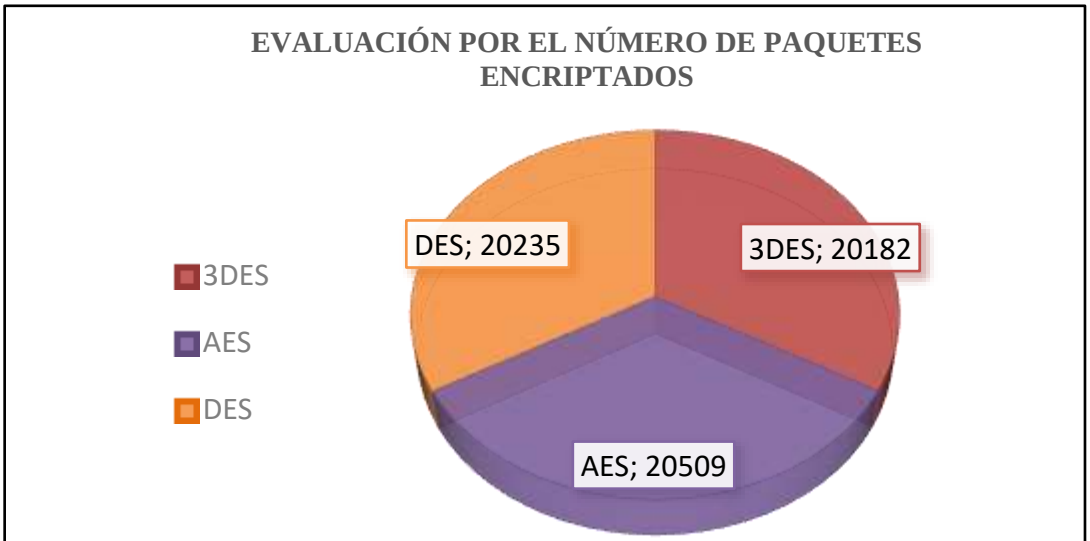

Figura 11. *Evaluación por el número de paquetes encriptados*

Por el número de paquetes desencriptados

Tabla 13
Por el número de paquetes desencriptados

Algoritmo	3 DES	AES	DES
# Paquetes desencriptados	20154	20562	20244

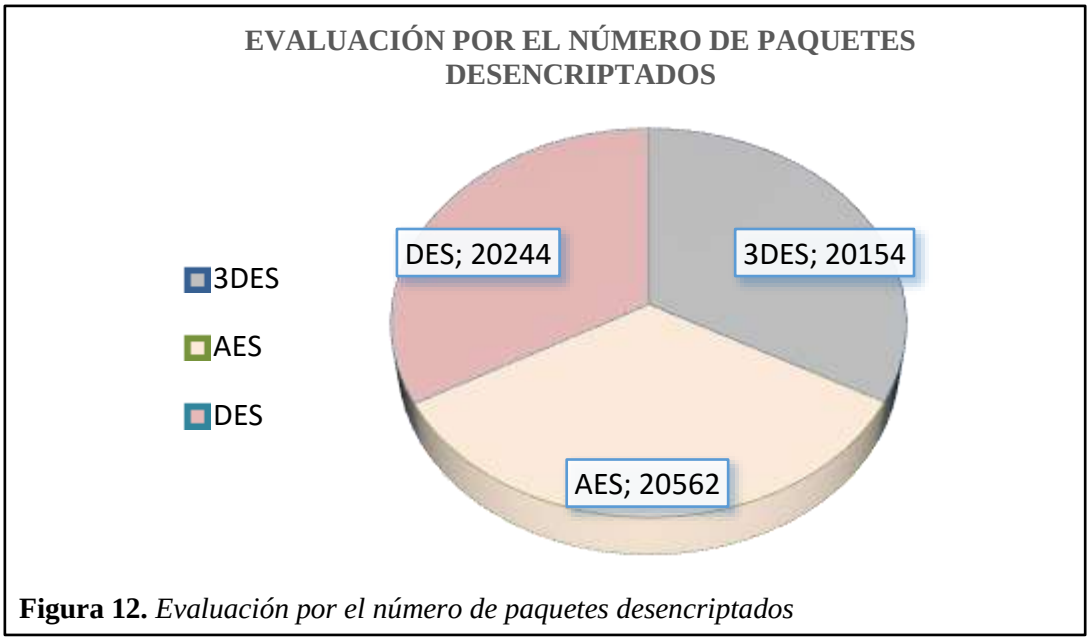

Figura 12. *Evaluación por el número de paquetes desencriptados*

Después de seleccionar e implementar los algoritmos en redes privadas virtuales, se hizo la evaluación respectiva por cada algoritmo, tanto para el envío de datos, voz y video. Obteniendo resultados respecto a número de paquetes capturados, tiempo de envío, paquetes encapsulados, paquetes desencapculados, paquetes encriptados y paquetes desencriptados.

Tabla 14
Tabla resumen de evaluación de algoritmos para Datos

Algoritmo	**3 DES**	**AES**	**DES**
Tamaño de archivo	4.53 MB	4.53 MB	4.53 MB
Número de paquetes	4995	5226	5246
Tiempo de Envió	00:04:26:59	00:04:21:42	00:04:25:07
# Paquetes encapsulados	3271	3277	3277
# Paquetes desencapsulados	1728	1702	1713
# Paquetes encriptados	3271	3277	3277
# Paquetes desencriptados	1728	1728	1713

Como resultados en la tabla 14 se obtuvo que para enviar el archivo de una pc a otra con el algoritmo AES necesita menor tiempo en comparación que los demás algoritmos. Además algoritmo AES partió el archivo en un mayor número de paquetes y lo envío en menos tiempo posible. Lo contrario del algoritmo DES que partió el archivo en más paquetes pero necesito más tiempo para enviarlo. Sobre los paquetes encriptados algoritmo AES presentó igual número de paquetes encriptados que el algoritmo DES, pero algoritmo AES desencriptó mas paquetes que el algoritmo DES utilizando menos recursos.

Tabla 15
Tabla resumen de evaluación de algoritmos para Voz y Video

Algoritmo	**3 DES**	**AES**	**DES**
Tiempo de Video en Minutos	6 min	6 min	6 min
Número de paquetes	40336	41071	40479
# Paquetes encapsulados	20182	20509	20235
# Paquetes desencapculados	20154	20562	20244
# Paquetes encriptados	20182	20509	20235
# Paquetes desencriptados	20154	20562	20244

En la tabla 15 se muestra el resumen de la evaluación de tráfico de voz y video. Como resultados se obtuvo que para enviar voz y video, el algoritmo AES partió la videopresencia en un mayor número de paquetes esto hizo que la trama fuera más pequeña. Lo contrario de los algoritmo 3DES y DES que partió la video presencia en menos paquetes haciendo más larga la trama. Sobre los paquetes encriptados algoritmo AES presentaron mayor número de paquetes encriptados y desencriptados que los algoritmo DES y 3DES, esto hizo que aumentará la seguridad de la transmisión.

4. Discusión

Para la realización de esta investigación se partió de bases teóricas a nivel internacional a fin de validar los objetivos que se plantearon, Muhammad (2015), en su investigación logró presentar una extensión de una red privada virtual hecha a través de características adicionales como encapsular los paquetes de datos con una cabecera en ambos extremos, a lo largo de las líneas de la comunicación, así como a través de túneles de comunicación. Lo hizo ofreciendo un conjunto de túneles de comunicación de datos seguras simuladas junto con una comparación de los resultados de las variables de la velocidad medidos en contra de la seguridad a través de diferentes protocolos de cifrado entre LAN remota. Sus resultados fueron la prestación de un servicio rápido, eficiente y al mismo tiempo el medio ambiente de trabajo seguro mediante la protección de sus activos de la organización además de presentar una red privada usando el protocolo IPSec.

Pandillas (2011) en su trabajo de investigación sobre el Sistema Red VPN utilizando el protocolo IPSec. Enfrentó un problema como los mecanismos de comunicación pocos seguros y poco fiables, con costos considerablemente líneas arrendadas. Lo que hizo fue estudiar el método de construcción de túneles en el sistema de IPSec. El protocolo IPSec lo estudia, pone en práctica y analiza la seguridad en redes VPN haciendo grandes avances. Propuso usar una red VPN por las características en cuanto a su seguridad de, Construye túneles usando el sistema de IPSec. Los resultados que obtuvo fueron mecanismo de comunicación segura y fiable, reduciendo considerablemente el costo de líneas arrendadas.

Quizhpe (2011) en su trabajo de investigación Soluciones de Cifrados a las Seguridades Informáticas en Procesos de Auditaje Organizacional. Tiene como objetivo principal realizar un estudio comparativo de soluciones de cifrados a las seguridades informáticas para ser utilizadas en los procesos de Auditaje Organizacional. En este estudio el autor en mención realizó el estudio comparativo de las Soluciones de Cifrados a las Seguridades Informáticas para dar a conocer de una manera clara los diferentes maneras de resguardar la información utilizando los diferentes tipos de cifrados que tenemos para encriptar la información, sobre todo las contraseñas de los usuarios lo que nos va a servir para tener protegidos nuestros equipos. Es importante recordar que es muy fácil poder encriptar nuestras contraseñas utilizado los software que los encontramos en el Internet gratuitamente, lo cual nos es una herramienta muy eficaz para poder mantener segura la Información. En este trabajo de investigación podemos apreciar que realiza un estudio comparativo de los diferentes tipos de cifrados para determinar cuál es el más conveniente para la utilización en las organizaciones, proponiendo el cifrado más confiable para asegurar la información de las organizaciones.

Moya (2015) en su trabajo de investigación desarrolló de una aplicación para encriptar información en la transmisión de datos en un aplicativo de mensajería web. Tiene como objetivo principal el desarrollo de una aplicación para encriptar datos en web. En este estudio el autor en mención aplica todas las herramientas investigadas durante el desarrollo de este trabajo, utiliza metodologías conocidas como el método de SCRUM ya que con este los entregables son pequeños y se pueden revisar periódicamente, haciendo más efectiva la identificación de errores y cambios, además de que Scrum se enfoca en la entrega de productos y no tanto en la calidad del código como Xtreme Programming. En esta investigación se hace para tener un claro ejemplo de la vulnerabilidad en la información de hoy en día. Por lo que en los últimos años ha adquirido un auge el estudio e implementación de diferentes modelos de encriptación para asegurar la confidencialidad en el intercambio de información. La investigación trata de abordar la protección desde un punto de vista que proporcione información sobre el funcionamiento de algunos algoritmos de cifrado.

De estas investigaciones se obtuvo que las redes privadas virtuales era un mecanismo que ofrecían ahorro de costos, escalabilidad, compatibilidad con tecnología de banda ancha y seguridad, necesitando saber que algoritmos eran necesarios configurar para obtener una adecuada integridad y confidencialidad a la hora de enviar datos o entablar una videoconferencia, elementos útiles en una comunicación.

5. Conclusiones

Se concluyó que el algoritmo AES es el mejor algoritmo de encriptamiento en cuanto a tiempo de envío, en número de paquetes de encriptación y en el número de paquetes de desencriptación con el protocolo IPSec.

Se seleccionaron los algoritmos criptográficos; concluyendo que los algoritmos que fueron seleccionados para este estudio fueron: AES (Advanced Encryption Standar), DES (Data Encryption Standar) y 3DES (Triple Data Encryption Standar).

Se concluyó con la implementación de tres redes privadas virtuales en el laboratorio de investigación de la escuela (LABSIS), utilizando una topología de red propietaria estándar con el protocolo IPSec.

Se hizo captura de tráfico en las tres redes implementadas con IPsec y con los algoritmos AES, DES y 3DES; obteniendo como conclusión el número de paquetes que genera cada algoritmo, el número de paquetes que encripta y desencripta, también se obtuvo el número de paquetes que encapsula y desencapsula por cada algoritmo.

En la evaluación de datos, voz y video se obtuvo el tamaño de los paquetes, número de paquetes, el grado de encriptación y desencriptación. Logrando una matriz de resultados.

Se concluyó que el algoritmo AES es el mejor protocolo de encriptamiento en cuanto a tiempo de envío, número de paquetes de encriptación y en el número de paquetes de desencriptación, número de paquetes de encapsulación y en el número de paquetes de desencapsulación.

6. Referencias

Gang, Z. (2011). *Research on VPN Network System using IPSec Protocol*. China: School of Computer Science.

Gonzales, P. (2013). *Métodos de encriptación para redes privadas virtuales.* Universidad Mayor de San Andrés. La Paz – Bolivia.

Márquez, G. (2015*). IPSec y Redes Privadas Virtuales*. España: Editorial Perfect-bound.

Medina**,** Y., Miranda, H. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Revista MundoFesc, [S.l.], v. 1, n. 9, p. 14-21, dic. 2015. ISSN 2216-0388. (Citado el 16 de mayo del 2016) Disponible en: http://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55.

Muhammad, E., Bujar, R. (2015). *Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption*. Macedonia: South East European University.

Simion, D., Ursuleanu, M., Graur, A., Potorac, A., Lavric, A. (2013). *Efficiency Consideration for Data Packets Encryption within Wireless VPN Tunneling for Video Streaming*. China: International Journal of computers communications & control.

William, S. (2004). *Fundamentos de Seguridad en Redes – Aplicaciones y Estándares*. Madrid: Editorial Pearson Educación. 2° Edición.

Xenakis, C., Laoutaris, N., Merakos, L., Stavrakakis, I. (2006). *A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms.* Iran: Iran university.