FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Evaluación del nivel de seguridad que ofrecen algoritmos criptográficos en una Red Privada Virtual

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor (es)

Bach. Tocto Lopez Christian Alexis

ORCID: https://orcid.org/0000-0002-3882-5919

Asesor(a)

Mg. Bravo Ruiz Jaime Arturo

ORCID: https://orcid.org/0000-0003-1929-3969

Línea de Investigación

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2023

EVALUACIÓN DEL NIVEL DE SEGURIDAD QUE OFRECEN ALGORITMOS CRIPTOGRÁFICOS EN UNA RED PRIVADA VIRTUAL

Aprobación del jurado

Mg. Bravo Ruiz Jaime Arturo

Presidente de Jurado

Mg. Arcila Diaz Juan Carlos

Secretario de Jurado

Dr. Tuesta Monteza Victor Alexci

Vocal de Jurado

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy egresado del Programa de Estudios de Ingeniería de Sistemas de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

EVALUACIÓN DEL NIVEL DE SEGURIDAD QUE OFRECEN ALGORITMOS CRIPTOGRÁFICOS EN UNA RED PRIVADA VIRTUAL

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Tocto Lopez Christian Alexis DNI: 73476702

Tocto Lopez Christian Alexis	DNI: 73476702	

Pimentel, 30 de Julio de 2024.

Dedicatoria

Este trabajo de investigación está dedicado especialmente a Dios por ser mi guiador y redentor en cada instante de mi vida.

Mis abuelos Lindaura y Alberto por ser los responsables de mi educación, mi formación, creyendo siempre en mí y en mis fortalezas.

A mi mamá Nancy por todo el esfuerzo que me brindan día a día por llegar a verme cumpliendo mis metas y objetivos.

Mi esposa Tatiana y mis bellos hijos Piero y Derek que con una sonrisa me motivan para que día a día salga adelante

Christian Alexis Tocto Lopez

Agradecimientos

A mis padres por ser mis facultativos principales a lo largo de mi vida.

A mi madre Nancy por estar en cada momento conmigo, entusiasmándome y animándome para no decaer.

A esposa e hijos Gabriel y Gael por ser los motores de culminar con éxito mi formación, presentándoles un orgullo para toda la familia.

A la Universidad Señor de Sipán por abrirme sus puertas para poder seguir mis estudios universitarios llenándome de conocimiento, gracias al acompañamiento y apoyo de los docentes de esta casa de estudios, en especial a mi asesor Mg. Mejía Cabrera Hever Iván por su paciencia y perseverancia.

Índice

Índice de tablas

Índice de figuras

Resumen

A lo largo de los años se ha empleado las claves secretas para evitar su divulgación, protegiendo la confiabilidad de esta. La criptografía es un lenguaje secreto, siendo el cifrado una forma que se puede presentar la criptografía empleando algoritmos para codificar texto plano de una manera que denote eficiencia y complejidad. El estudio presenta la finalidad de determinar el nivel de seguridad que ofrecen los algoritmos criptográficos en una red privada virtual. La investigación esta abordado desde un enfoque cuantitativo, bajo un diseño experimental, de tipo descriptivo correlacional porque no presento alguna manipulación de las variables directamente, describió y analizó tal cual se presentó en la realidad, las muestras de los algoritmos seleccionados fueron el AES, DES, 3DES, exponiéndolos a los instrumentos de ficha técnica del algoritmo criptográfico, matrices de comparación entre algoritmos criptográficos, matriz de resultados de la confidencialidad, matriz de resultados de la integridad, matriz de resultados de la disponibilidad. Se empleó como herramienta el programa GNS3 para la recolección de información. Los resultados que obtuvo se analizaron, utilizó la matriz de resultados para medir los valores de la variable seguridad de la información. El resultado obtenido fue que el algoritmo AES presenta mayor nivel de seguridad en términos de confidencialidad, integridad y disponibilidad. Concluyendo que el algoritmo criptográfico AES es el más adecuado para las empresas ya que es más seguro, y emplea menos cantidad de recursos.

Palabras Clave: Algoritmo, seguridad de los datos, código.

Abstract

Over the years, secret keys have been used to prevent their disclosure, protecting its reliability. Cryptography is a secret language, encryption being a way in which cryptography can be presented using algorithms to encode plain text in a way that denotes efficiency and complexity. The study presents the purpose of determining the level of security offered by cryptographic algorithms in a virtual private network. The research is approached from a quantitative approach, under an experimental design, of a correlational descriptive type because it does not present any manipulation of the variables directly, described and analyzed as it was presented in reality, the samples of the selected algorithms were AES, DES . , 3DES, exposing them to the instruments of the cryptographic algorithm technical sheet, comparison matrices between cryptographic algorithms, confidentiality results matrix, integrity results matrix, availability results matrix. The Wireshark program was used as a tool to collect information. The results obtained were analyzed, the results matrix was used to measure the values of the information security variable. The result obtained was that the AES algorithm presents a higher level of security in terms of confidentiality, integrity and availability. Concluding that the AES cryptographic algorithm is the most suitable for companies since it is more secure, and uses less resources.

Keywords: Algorithm, data security, code.

INTRODUCCIÓN

1.1. Realidad problemática.

En pleno siglo XXI estamos viviendo una revolución de la tecnología, por el mismo hecho que la virtualidad y las herramientas tecnológicas son básicas para el desarrollo de la sociedad [35]. Ya se veía previstos ciclos anteriores, sin embargo, el uso de las herramientas tecnológicas y la virtualidad se intensificó y obligó a las empresas públicas y privadas emplearlas para poder ejercer sus actividades como una medida preventiva del COVID-19 [36]. Cabe recalcar que a lo largo de los años se ha empleado las claves secretas para evitar su divulgación de información valiosa de las empresas, teniendo en cuenta criterios evaluativos de la confiabilidad [37]. La criptografía es un lenguaje secreto, se emplea el cifrado como una forma de presentar la criptografía empleando algoritmos para codificar texto plano de una manera que denote eficiencia y complejidad [1]. Los algoritmos cifrados utilizan claves criptográficas para darle una apariencia de sinsentido a los datos aparentemente aleatorios, los actuales descomponen los datos de texto plano en grupos llamados bloques y luego cifran cada bloque como una unidad [2].

La red virtual privada (VPN) emplea el cifrado como una de las funciones más básicas [38]. Nos explican que las VPN buscan hacerte invisible en internet, por ello cifran sus datos. El emplear un tipo de cifrado debe ser de mucho cuidado ya que debe garantizar seguridad (indescifrable y privado) de la información que se intercambie. Además, la ciberseguridad es amenazada constantemente por fugas de información debido a la escasa implementación de cifrado, presentando un riesgo para la empresa en la divulgación de sus datos [3]. En la realidad que nos encontramos ya no solo se considera una opción, sino que es obligatorio que las empresas contemplen el cifrado de sus datos para evitar la pérdida de información valiosa ante los ciberdelincuentes. Para generar mayor protección de la información de los clientes se presentaron nuevos reglamentos como el GDPR en la Unión Europea o la CCPA en USA [4]. Los ciberdelincuentes el PII (información de identificación personal) muchas veces lo toman como rehén, posteriormente amenazan con reportar la brecha de seguridad a las autoridades del cumplimiento del

reglamento del GDPR. Teniendo en cuenta que mientras más seguro es algoritmo menos rendimiento presentará ya que, que la seguridad se ve reflejada en el largo de su clave. Mientras más largo es la clave genera mayor tiempo, costo, productividad de descifrado disminuyendo su rendimiento.

Ante todo, lo expuesto se propone realizar esta presente investigación para identificar qué algoritmo criptográfico ofrece el mejor nivel de seguridad en una red privada virtual en la provincia de Chiclayo, 2023.

1.2. Formulación del problema

¿Qué algoritmo criptográfico ofrece el mejor nivel de seguridad en una red privada virtual en la provincia de Chiclayo, 2023?

1.3. Hipótesis

El algoritmo criptográfico AES presenta un alto nivel de seguridad en la red privada virtual, 2021.

Justificación e importancia del estudio.

Justificación Tecnológica

Esta investigación se justifica tecnológicamente porque empleamos tecnología, y más aún la seguridad de la información en el año 2023 es un tema muy controversial y de hincapié para las empresas, por lo que las empresas optan la implementación de VPN.

Justificación Social

La sociedad es muy cambiante, más aún con la presente pandemia que estamos atravesando del COVID-19, las empresas y entidades optaron por el trabajo remoto, masificando su demanda en la conectividad empleando redes inalámbricas. Por ende, es necesario determinar el nivel de seguridad de algoritmos criptográficos más conocidos para que las empresas puedan escoger la implementación de alguna de estas y así mantener seguro su información garantizando la integridad privacidad y disponibilidad.

Justificación Económica

Económicamente este proyecto pretende contribuir en la reducción del uso de recursos computacionales, optimizar el tiempo de cifrado y descifrado de paquetes, entre otros. Además de reducir los riesgos de pérdidas económicas

que pueden sufrir las empresas si un tercero con malas intenciones robara la información.

1.4. Objetivos

Objetivo general.

Determinar el nivel de seguridad que ofrecen los algoritmos criptográficos en una red privada virtual.

Objetivos específicos.

- Identificar los algoritmos criptográficos de la red privada virtual.
- Configurar accesos, interfaces y enrutamiento.
- Valorar a los tres algoritmos criptográficos según sus tres dimensiones.

1.5. Teorías relacionadas al tema

En la investigación *“An Examination of Encryption Methods",* en Egipto. Para la tecnología y la electrónica, la seguridad de datos, viene siendo uno de los principales desafíos que presenta, para estar conectados de forma eficiente en términos de tiempo y seguridad a través de la web, esta información debe estar en condición de encriptados. Para una empresa es esencial determinar la opción más idónea del algoritmo criptográfico que va ser responsable de su información reflejando protección y seguridad. Se realizó un estudio comparativo de los algoritmos más conocidos como son AES, DES, TDES, DSA, RSA, ECC, EEE y CR4, en condiciones de seguridad de información, tamaño de clave, complejidad y tiempo, entre otros. Como resultado obtuvo que los algoritmos criptográficos AES, Blowfish, RC4, E-DES y TDES son los más eficientes en tiempo de cifrado, velocidad y flexibilidad. Además, que el AES es más seguro flexible y resistente. Concluyendo que el AES es más confiable en condiciones de cifrado de velocidad, decodificación, complejidad, longitud de la clave, estructura y flexibilidad [5].

Para el investigador, está investigación le contribuye para el diseño del proyecto.

En la investigación: "Analysis and Comparison of Cryptographic Algorithms Applied to IoT in Coimbra, Portugal" El Internet de las cosas (IoT), ofrece muchas ventajas a los usuarios como integrar múltiples servicios, facilidad de

acceso y políticas de seguridad, aunque también presentan desventajas como fallas de seguridad, dejando como en consecuencia daños sociales y económicos. Para solucionar esta problemática se propone desarrollar métodos de seguridad que sean eficientes y eficaz para mantener integra la información de las empresas y usuarios. Compararon cinco algoritmos criptográficos clásicos simétricos AES (128 con longitud de clave 128), Simon (32/64), Speck (32/64), Curupira1 (96/96) y Curupira (96/96). La evaluación métrica se determinó por la velocidad de cifrado y descifrado de claves, la caracterización fue empleando el tiempo de ejecución de algoritmos, consumo de memoria RAM empleado en la ejecución, el rendimiento del algoritmo, consumo de memoria RAM utilizado durante la ejecución de los métodos medidos en bytes; rendimiento del algoritmo y el gasto energético para las simulaciones en el ESP826 microcontrolador. Obteniendo como resultado que el algoritmo AES presento el mayor rendimiento porque tenía mayor capacidad de cifrar información, mayor estabilidad en tiempo de ejecución, memoria empleada y gastada, mejor seguridad en el cifrado. La determinación de la eficiencia estuvo basada métricamente, además empleo algoritmos de diferente clasificación [6].

Por otro lado desarrollaron la investigación: Performance evaluationof INDECT security architecture, Bogotá. INDECT es un Proyecto que ayuda a la policía europea en su labor, presenta una mixtura de aplicaciones y servicios TIC, sin embargo, debe ser evaluado su desempeño en la dimensión de seguridad para comprobar su eficiencia de la información. En este artículo se evaluó el rendimiento de la arquitectura del INDECET. Se emplearon tres mecanismos para detectar errores, entre ellos, comprobación de pariedad, códigos Berger y verificación por redundancia clínica, del algoritmo cifrado de bloque INDECT implementado en el software y harware. Seguidamente se analizó el rendimiento en servidores web al momento de activación del TLS/SSL. Finalmente se evaluó el rendimiento y el tiempo de demora del tráfico en una VPN utilizando el software VPN comparándolo con los algoritmos IDEA, RC2, AES, DES, BF, CAST, INDECTO, INDECT. El resultado obtenido evidencia la viabilidad y eficiencia del algoritmo cifrado

INDECT en seguridad de la información y comunicación. Concluyendo que la arquitectura de seguridad de INDECT presenta un riesgo en el desempeño de comunicación, está es mínima a comparación de las ventajas que brinda para el uso de sistemas LEA y redes. La seguridad es una variable de constante actualización, porque la ciberdelincuencia se alinea rápidamente a los patrones empleados para la protección de la información [7].

En otra investigación: A Survey of Lightweight Cryptography Methods, en Rumanía. Optimizar los algoritmos cifrados en dispositivos es bastante difícil, por ello radica la importancia de la seguridad de nodos finales, debido a que no se cuenta los suficientes recursos. Este artículo empleó una encuesta sobre los métodos criptográficos, además empleó un método analítico crítico y actuaciones específicas. Obteniendo como resultado que para crear métodos efectivos de criptografía se tebe tener en cuenta en utilizar algoritmos clásicos, modificación y adaptación de estos en las características del hardware, finalmente el desarrollo de nuevas soluciones algorítmicas y software en términos de hardware. Concluyendo que el tamaño de la clave del cifrado de bloque es el determinante de la confiabilidad con respecto al costo, el número de rondas de cifrado con respecto a la fiabilidad y rendimiento, y, por último, las características del diseño de hardware con respecto al precio y rendimiento. Mientras más pequeña es la clave menor uso de recursos se emplearán [8].

Además en la investigación: Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time, localizado en Malasia. Centrando como problema la seguridad de los datos digitales, ya que es uno de atributos más resaltantes de la comunicación. Esta investigación realiza una propuesta de modificación del algoritmo estándar cifrado AES, presentando una reducción de rondas de cifrado a 14 con el fin de optimizar el tiempo de cifrado y descifrado, garantizando seguridad de la información digital. Como resultado obtuvo que la modificación presenta mayor eficiencia en condiciones de tiempo de cifrado y descifrado en comparación a los otros algoritmos criptográficos (DES, 3DES). Concluyendo que la modificación del

algoritmo AES genera seguridad a la información [9].

En la investigación: Symmetric Encryption Algorithms: Review and Evaluation study, en Kuwai. La problemática presentada fue conocer la descripción general de los algoritmos cifrados más conocidos explicando su funcionalidad. La metodología consistió en seleccionar 10 algoritmos criptográficos de cifrado simétrico AES,BlowFish, RC2, RC4, RC6, DES, DESede, SEED, XTEA yIDEA, realizando simulaciones en JAVA para determinar el desempeño, enviando paquetes de 1MB hasta 1 GB. Como resultado se obtuvo que los algoritmos RC4, RC6 y AES con mejores en términos de tiempo de cifrado, rendimiento y tasa de utilización de la CPU. Concluyendo que el algoritmo AES es la mejor opción de desempeño en nivel de seguridad [10].

Por otro lado investigación: Privacy Preserving of Data Files & Audio / Video Encryption –Decryption Using AES Algorithm, en Nagpur. Presentaron como problemática la seguridad de sus datos de videos y grabación de voz en redes sociales. Metodológicamente proponen la opción de cifrado y descifrado de archivos que se puedan cargar en las redes sociales, empleando el cifrado avanzado especial Rijndael. Obteniendo como resultado que el AES 256 es mejor File Size, AES 128, AES 192 y DES, por ello es que tomaron el cifrado AES Rijndael. Concluyeron que es importante la seguridad de los datos en las diferentes áreas y empresas, enfatizándolo especialmente en la minería y fraudes del mercado de valores [11].

También en la investigación sobre el Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3, el análisis de potencia se emplea como un modelo matemático para descifrar la clave oculta del dispositivo criptográfico. Diseño cuasi experimental, tipo descriptivo. Metodológicamente implementaron el ataque de análisis de potencia a tres algoritmos criptográficos simétricos: DES, AES y BC3. Como resultado obtuvieron que el algoritmo simétrico AES recuperó en un 100% la clave oculta, utilizando 500 trazas y el algoritmo DES lo recuperó en un 75%

utilizando 320 trazas. Concluyendo que el algoritmo BC3 es el más seguro frente al DES y AES [12].

Además en la investigación: Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor. Tienen como objetivo optimizar los algoritmos AES y DES en un procesador heterogéneo en el sistema Sunway TaihuLight. Conversión del DES y AES en serie a la plataforma experimental. Aplicaron la optimización de la comunicación maestro-esclavo, la tubería paralela de tres etapas y la vectorización. Concluyendo que los algoritmos convertidos son 70 veces más eficientes que los originales [13].

En la investigación: Encryption of accounting data using DES algorithm in computing environment, el objetivo fue la utilidad del algoritmo DES para cifrar información de un estudio contable. La propuesta es un algoritmo genético cuántico con modificaciones para su mejoría, orientándose en el diseño de la caja S del algoritmo simétrico DES, la no linealidad del S-box presenta cambios, disminuye la homogeneidad diferencial. El DES mejorado disminuye la cantidad de interacciones mientras se hace más grande la longitud de la clave, proporcionando mayor seguridad del algoritmo y mayor rapidez en la velocidad en el cifrado del texto. Los 64 textos cifrados está entre los 32 bits, por tal motivo se presenta las consecuencias posibles al emplear este algoritmo DES. Concluyendo que el algoritmo DES mejorado, es más seguro y eficiente en calidad de que emplea menos tiempo para el cifrado y descifrado [14].

En la investigación: Impact encryption algorithm used in three pass protocol for securing WiMAX link, tiene como objetivo examinar el empleo del protocolo que se da en tres pasos (TPP), para pasar las claves del texto cifrado. Se comparó los algoritmos criptográficos BF, AES, 3DES y DES según el Protocolo de almohadilla. Como resultado se obtuvo mejor seguridad, gracias al cifrado el tiempo de retardo fue más largo, obteniéndose valores inferiores a 150 ms. Concluyendo que BF es mejor porque presenta menor retraso, a comparación de los otros algoritmos criptográficos [15].

Así también en la investigación: Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications, presentaron como objetivo el análisis de los algoritmos AES, DES, 3DES, RSA y Blowfish basado en tiempo de envío y cifrado, el tamaño, rendimiento de cifrado y descifrado. Estudiaron las variables empleando simuladores de ataques de adivinanzas en IoT complejo de aprendizaje profundo en tiempo real. Los resultados muestran que RSA es más lento en comparación con los otros algoritmos. Concluyendo que el Blowfish ofrece un mejor rendimiento y el AES presenta deficiencia en su rendimiento porque para su funcionamiento requiere un proceso de alta resistencia [16].

En la investigación: Image steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and blowfish. Buscan mejorar la seguridad de los datos empleando algoritmos de la criptografía (AES, RSA, DES, 3 DES y el Blrowfish) y la esteganografía el LSB, empleando una imagen de portada para ocultar el mensaje. Los resultados muestran que los 6 algoritmos empleados obtienen una buena calidad de la imagen stego. El que implicó mayor tiempo de ejecución fue el RSA. Concluyendo que el algoritmo DES y pez globo llevan el menor tiempo de encriptación y descifrado, seguidamente el AES [17].

En la investigación: Time Evaluation of Different Cryptography Algorithms Using Labview, ejecutó el simulador de LabVIEW, comparándolo el programa paquete de cifrado avanzado. Se emplearon los algoritmos AES, DES, 3 DES y RSA. Como resultados se muestra que el LabVIEW fue mejor, en tiempo de cifrado y descifrado son inferiores al cifrado avanzando (en velocidad y rendimiento). Finalmente concluye que el algoritmo más eficiente en velocidad y rendimiento es el AES [18].

Finalmente en la investigación: Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. Busca describir la eficiencia del algoritmo criptografico AES. Pone a prueba este algoritmo teóricamente, y practico aplicando un diseño basado en este algoritmo para

verificar la seguridad. Como resultados se obtiene que el AES es más eficiente que el algoritmo DES, concluyendo que el AES muestra mucha sensibilidad a los cambios en el inicio de las claves. Puesto que, un cambio de clave implica modificación en los datos cuando se pretende restaurar el original [19].

Criptografía es la rama encargada de estudiar la transformación de un mensaje o también llamado texto plano, en un texto o mensaje no descifrable o reconocible para otra persona (también llamado como texto cifrado), empleando la clave secreta. El conjunto de pasos secuencial de cifrado y descifrado en la creación de claves se le considera como criptosistema [20].

Criptografía simétrica está compuesta por los criptosistemas que emplean una misma contraseña para el cifrado del mensaje y descifrado de este [20].

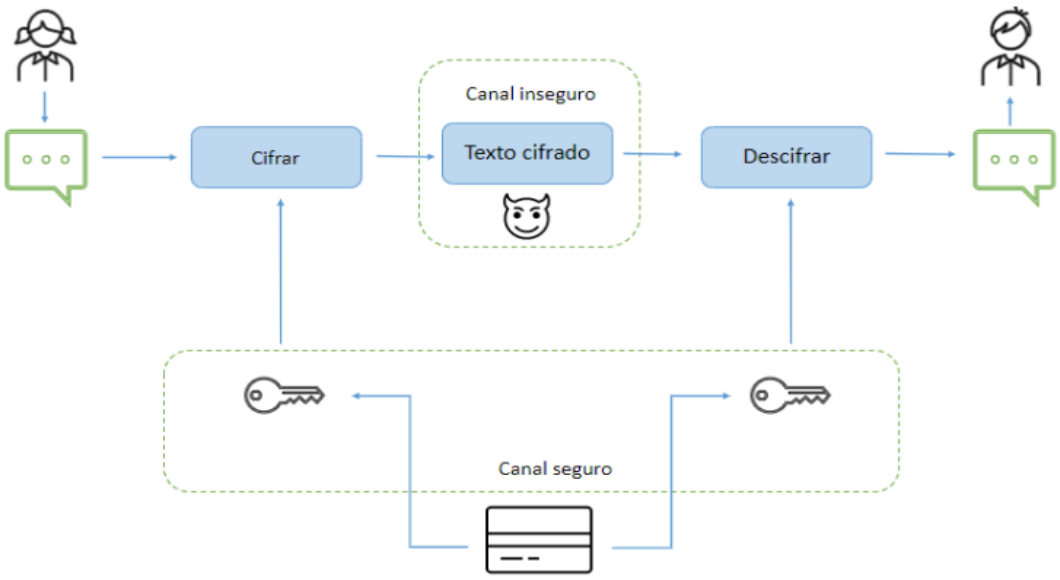


Fig. 1 Criptografía simétrica *[20]*

Criptografía asimétrica también llamada clave pública, son aquellas que el emplean dos contraseñas, una para el cifrado del mensaje y la otra para el descifrado, siendo la pública para el cifrado y la secreta para el descifrado [20].

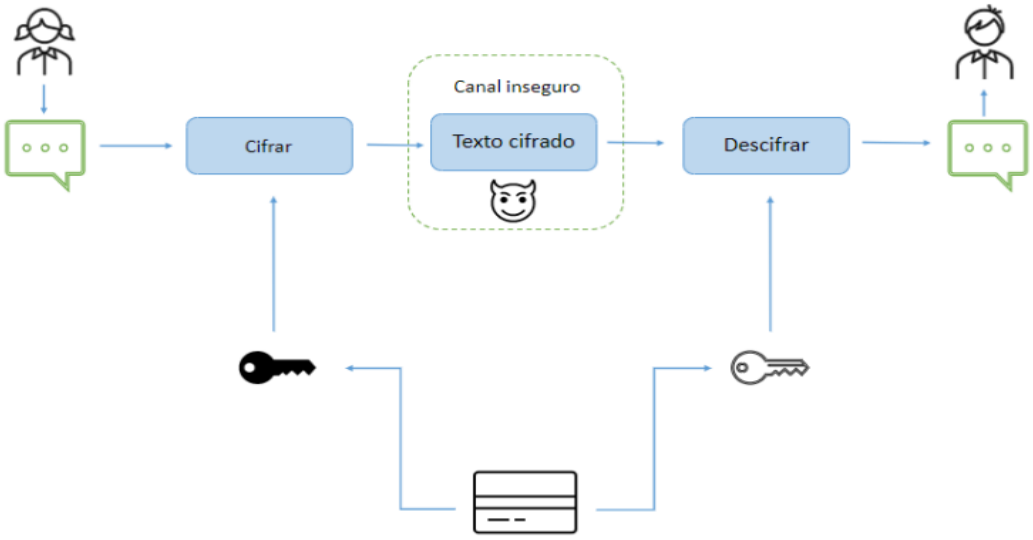


Fig. 2 Criptografía asimétrica [20]

Las VPN también son llamadas Redes Privadas, por medio de ellas se transportan información cifrada, por consiguiente, solo podrán ser descifradas por el destinatario. La implementación de la VPN ofrece la conexión a una red local desde un ambiente geográfico remoto a través de otro tipo red [21].
Para que se consideré seguro el tráfico de la información, este debe cumplir algunos principios.

- Autentificación y autorización: Permite la identificación del usuario que realiza las operaciones.
- No repudio: Garantiza que las operaciones realizadas han sido hechas por la persona que se autentificó.
- Integridad: Es el principio que garantiza la información de forma pulcra sin ser modificada ni manipulada en el trayecto, por algún tercero o fallas en la red.

- Confidencialidad: Consiste en el cifrado de los datos evitando su facilidad de adivinación.

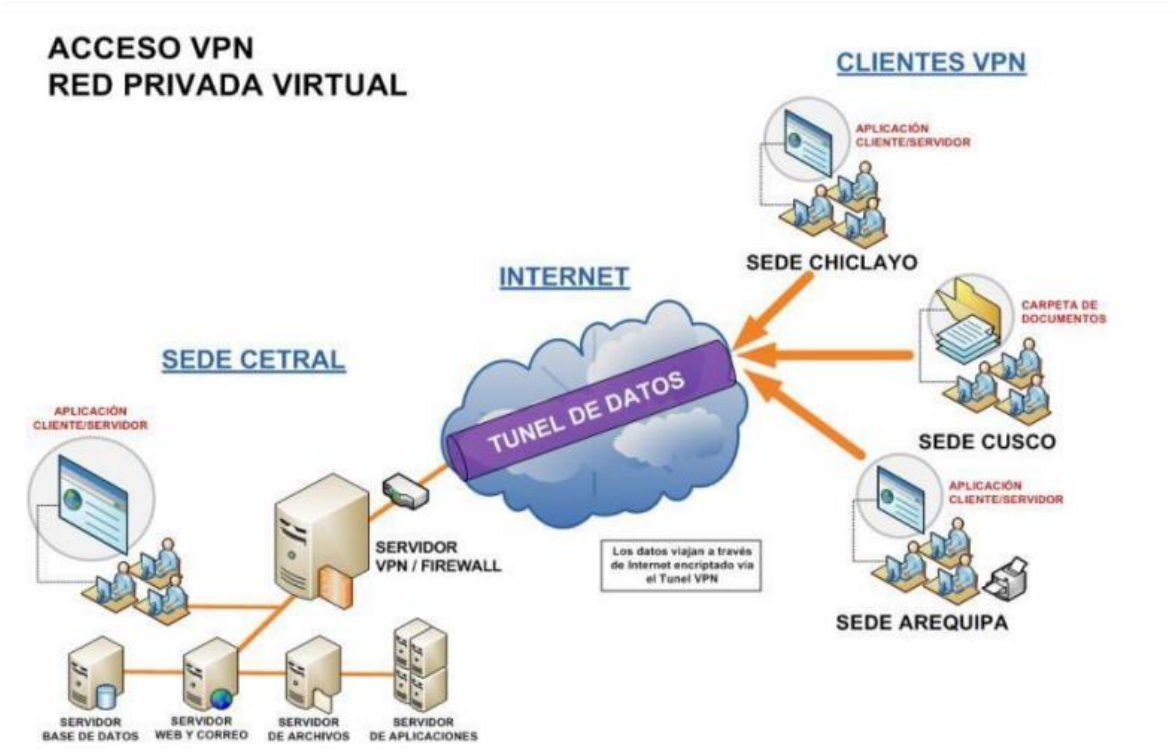


Fig. 3 Funcionamiento de una VPN. [21]

La seguridad de la información ISO/TEC 27001 [22] es la agrupación de disposiciones técnicas, organizativas y legal que permiten a las empresas garantizar los principios de integridad, disponibilidad e integridad, tal y como lo anuncia las ISO/IEC 27001, además añade que pueden integrarse otros principios como autenticidad, responsabilidad, confiabilidad y el no repudio.

La seguridad continua por lo que los riesgos siempre están latentes, pero se pueden mitigar. Presentándose los problemas de seguridad que tienen muchos factores entre ellos la naturaleza tecnológica.

Dimensiones de la seguridad de la información:

- La confidencialidad: Es un competente indispensable de la privacidad, pues representa a la capacidad de proteger nuestra información de aquellas personas que no están autorizados [23].
- La integridad: Se refiere en la conservación intacta de la información, sin

presentar modificaciones [23].

- La disponibilidad: Se orienta a la capacidad de acceder a nuestra información cuándo se requiera hacerlo. La disponibilidad dependerá de la energía, del sistema operativo, los ataques de la red de energía el impedimento de usuarios para acceder a tu información [23].

Por otro lado, los algoritmos cifrados es el algoritmo matemático que asegura la seguridad de la información. Entre ellos se tienen los algoritmos cifrados que más se utilizan y son de bloque:

- AES: El algoritmo estándar de tipo de cifrado, por sus siglas en inglés (Advanced Encryption Standard). En su estructura y arquitectura presenta operaciones a nivel de byte, las cifras por bloques de 128 bits el largo de la clave, además trabaja con longitudes de clave de 128, 192 y 256 bits. Este algoritmo fue creado por primera vez en 1988 por Joan Daemen e incent Rijmen [32].
- DES: También llamado Data Encryption Standard, Creado en IBM por WL Tuchman durante el año 1972. Algoritmo cifrado simetrico de bloque de 64 bits, clave de 56 bits. Capacidad de encriptación de 64 bits en texto plano en texto de cifrado de 64 bits con claves interno de 56 bits clave externa de 64 bits. de una clave externa (clave externa) que tiene una longitud de 64 bits [30].
- 3 DES: Triple Data Encryption Standard, es la modificación del algoritmo DES. El agoritmo 3DES presenta 3 teclas de tamaño 168 bits (el triple de la clave del DES) [30].

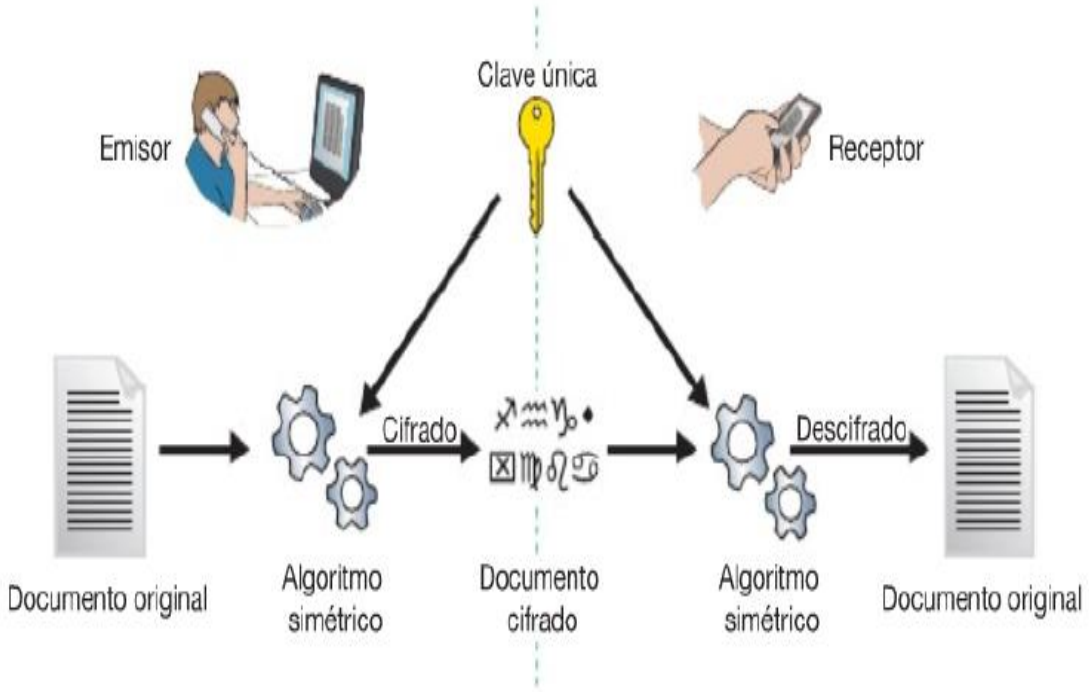


Fig. 4 Representación del uso de algoritmos cifrados [40]

II. MATERIALES Y MÉTODO

2.1. Tipo y Diseño de Investigación

Tipo

Este proyecto fue de enfoque cuantitativo, tipo básico. La investigación pura o también llamada básica o sustantiva, es dicha de esa manera porque el indicio es la curiosidad de seguir destapando nuevos conocimientos [24], es básica porque es la estructura de soporte para la investigación aplicada o tecnológica.

Diseño

Sigue un diseño cuasi experimental, por el tiempo de aplicación del instrumento de corte transversal, descriptivo y correlacional. Cuasi experimental porque el investigador manipula o tiene control de la variable independiente con la finalidad de observar su efecto y relación con la otra variable dependiente.

Para esta investigación se ha pronosticado trabajar con el corte transversal porque es aquella que sirve para recolectar datos en un solo momento y en un tiempo único.

Descriptiva porque solo va a describir lo percibido.

M O

M: muestra.

O: Información (Observación)

2.2. Variables, Operacionalización

Variable independiente: Algoritmo criptográfico.

Definición conceptual.

Un algoritmo criptográfico, es aquel que se encarga de camuflar la información de un texto o documento, con la finalidad de presentar grados de seguridad reflejados en la autenticación, esquema e integridad y confidencialidad. Se dice también que la Seguridad de la Información, es la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización [22].

Definición operacional

La seguridad de la información se determinará tomando en cuenta las tres

dimensiones la seguridad, esquema y rendimiento en los 4 algoritmos criptográficos de una red privada virtual.

Variable dependiente: Seguridad en la comunicación y almacenamiento de la información.

Definición conceptual.

Es la agrupación de disposiciones técnicas, organizativas y legal que permiten a las empresas garantizar los principios de integridad, disponibilidad e integridad, además añade que pueden integrarse otros principios como autenticidad, responsabilidad, confiabilidad y el no repudio [22].

Definición operacional.

La seguridad de la información se determinará tomando en cuenta las tres dimensiones la seguridad, esquema y rendimiento en los 4 algoritmos criptográficos de una red privada virtual.

Tabla 1: Operacionalización de la variable

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
Seguridad en la comunicación y almacenamiento de la información.	Confiabilidad	Capacidad de Almacenamiento	Tiempo de traspaso de datos.	Técnica: Técnica de la observación. Instrumentos: Ficha técnica del AES, DES, 3DES. Matrices de relación entre algoritmos criptográficos Matriz de la confiabilidad. Matriz de resultados de la integridad. Matriz de la disponibilidad. Matriz de Resultados
			Dimensión del archivo.	
			Cantidad de paquetes encriptados.	
	Integridad		Cantidad de paquetes desencriptados.	
		Fortaleza clave	Longitud de la clave.	
	Disponibilidad	Accesibilidad	Configuración. Tráfico de datos con IPSec en Router.	
			Conectividad entre Host.	
			Configuración de IPSec con los algoritmos.	
Algoritmos criptográficos	Grado de seguridad	Disponibilidad	Accesibilidad	
	Rendimiento	Integridad	Fortaleza de la clave	

Nota: La dimensiones e indicadores fueron organizadas por las bases teóricas. Fuente: Elaboración propia (2023)

2.3. Población de estudio, muestra, muestreo y criterios de selección

Población

Los Algoritmos criptográficos de una red privada virtual.

- DES
- 3DES
- RC2
- RC4
- RC5
- IDEA
- AES
- Blowfish

Criterio de inclusión

- Algoritmos simétricos.
- Utilizan claves para el proceso de cifrado y descifrado. La seguridad del sistema depende en gran medida de la longitud y la fortaleza de la clave utilizada.
- Algoritmos diseñados para cifrar datos, lo que significa convertir la información legible en un formato ilegible para protegerla contra accesos no autorizados.
- Algoritmos de bloque que cifran datos en bloques fijos.
- Estándares de Seguridad.

Criterio de exclusión

- Algoritmos de flujo que cifran datos continuamente.
- Algoritmos sin reconocimiento de seguridad de la información.

Muestra

Se determinó empleando el método no probabilístico, a criterio del investigador. Los tres algoritmos criptográficos: AES, DES, 3 DES.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnica

La técnica empleada fue de la observación, para que se pueda describir los datos

percibidos de la muestra.

Instrumentos

Los instrumentos empleados fueron:

- La ficha técnica del AES, DES, 3DES.
- Matrices de relación entre las muestras.
- Matriz de Resultados.

Las herramientas que se utilizaron fueron:

- Wireshark: es un programa que permite observar lo que está pasando en su red a nivel imperceptible.

Materiales

- USB to Serial Converter TU-S9
- Tarjeta Hwic
- Cable consola

Equipos

- Router Cisco C1111-8P (Router CPE02)
- Router Cisco 1921 (Router PE)
- Router Cisco C1111-8P (Router CPE01)
- 3 Laptop Lenovo 5I

2.5. Procedimiento de análisis de datos

La información se analizó empleando cuadros de relación entre los algoritmos criptográficos, además estos cuadros se plasmaron en gráficos para la facilidad de su interpretación.

2.6. Criterios éticos

La ética es una mixtura de reglas morales que orientan la forma de actuar y comportarse de un ser humano [24].

Toda investigación debe regirse a los principios éticos de integridad de su información y la protección de los participantes que serán objeto de estudio. Incluyen dentro de estos principios el respeto a las personas, la beneficencia y la justicia [33].

Respeto. Libre elección de participación en la investigación, incluyendo un trato

digno, seguridad y autonomía.

Beneficencia. Hace referencia al provecho que se obtendrá de la investigación priorizando los beneficios y disminuyendo los posibles daños o secuelas que pueda dejar la investigación.

Justicia. Es la distribución más asertiva de los posibles riesgos y ventajas para el objeto de estudio.

Criterios de Rigor Científico.

El rigor científico es el proceso donde se evidencia la socialización de los resultados en fuentes de reconocidas o de confiabilidad, bajo un sistema imparcial, representando el cumplimiento de las normas editoriales, éticas y de comunicación científica [29].

Según los criterios racionalistas estos son la validez y la confiabilidad [26].

La fiabilidad. Técnica que se aplica en reiteradas ocasiones al mismo objeto de estudio, para obtener el mismo resultado.

La validez. Significancia real de la evaluación empírica.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

Se muestran los resultados obtenidos después de su evaluación de cada algoritmo criptográfico.

a) **Identificar los algoritmos criptográficos de la red privada virtual.**

En este objetivo se seleccionó algoritmos para Redes Privadas Virtuales utilizando el protocolo IPSec. Las fichas técnicas se encuentran en el Anexo 2.

- DES (Data Encryption Standar).
- AES (Advanced Encryption Standar).
- 3DES (Triple Data Encryption Standard).

b) **Configurar accesos, interfaces y enrutamiento.**

Para ello se rigió al siguiente procedimiento:

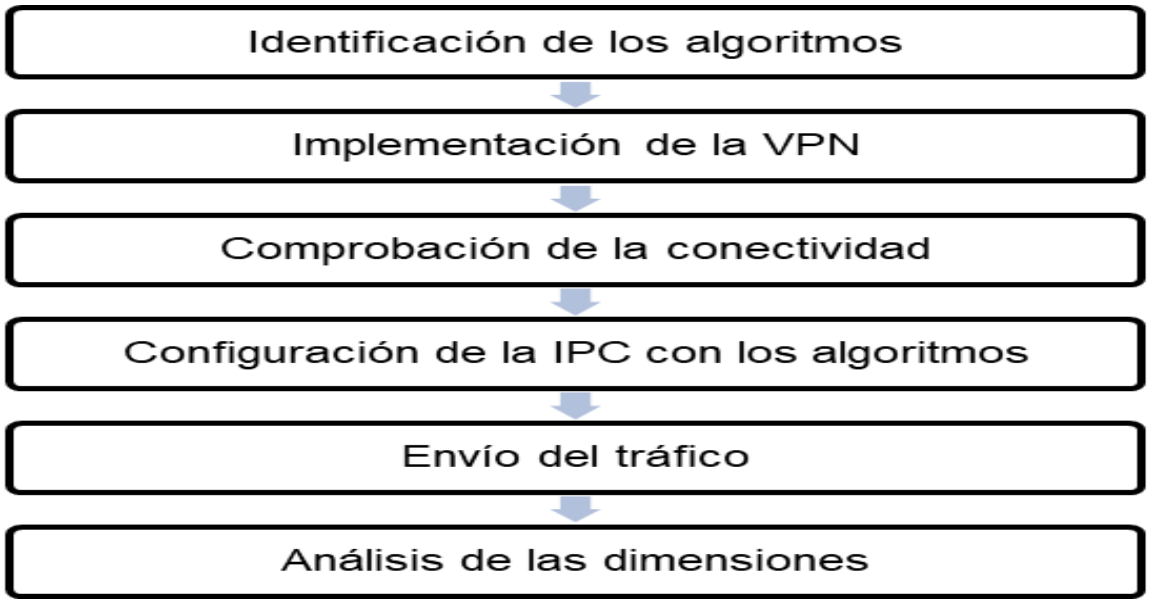


Fig. 5 Procedimiento de la comparación de los algoritmos criptográficos. Nota. Elaboración propia.

c) **Valorar a los tres algoritmos criptográficos según sus tres dimensiones.**

Para la evaluación de envío de datos se utilizó un Archivo de Prueba:

Tamaño del archivo: 64 MB

a) **Por el tamaño del archivo:** Se utilizó el mismo archivo para hacer las pruebas con los tres algoritmos**.**

Tabla 2: Matriz comparativa de los algoritmos criptográficos

Factores	**AES**	**DES**	**3DES**
Longitud de la clave	128,192,256 bits	K1,K2,K3 112-162 bits	56 bits
Tipo	Simétrico	Simétrico	Simétrico
Tamaño de bloque	128, 192, 256 bits	64 bits	64 bits
Creación	2000	1978	1977
Rondas	10,12 o 14	48	16
Fundamento	Transformaciones lineales	Criptoanálisis diferencial	Diferencial y lineal.
Aplicación			

Nota: Matriz comparativa de los algoritmos. Fuente: Elaboración propia

Tabla 3: Matriz de resultados de la confiabilidad

Algoritmos	**AES**	**DES**	**3 DES**
Tiempo de envío	00:02:10:50	00:02:15:02	00:02:13:35
Tamaño del archivo de envío	64 MB	64 MB	64 MB
Número de paquetes encapsulados	20925	147933	168986
Número de paquetes desencapsulados	164444	175001	38107

Nota: Matriz comparativa de la confiabilidad de los algoritmos. Fuente: Elaboración propia

Tabla 4: Matriz comparativa de la integridad de los algoritmos

Sub dimensión	AES	DES	3 DES
Longitud de la clave.	256 bits	112 bits	56 bits

Nota: Matriz comparativa de la integridad de los algoritmos. Fuente: Elaboración propia.

Tabla 5: Evaluación por el tamaño de archivo

Algoritmo	3 DES	AES	DES
Tamaño de archivo	64 MB	64 MB	64 MB

Nota. Se envió el mismo tamaño de paquete a los tres algoritmos.

b) **Por el número de paquetes**

Tabla 6: Evaluación del número de paquetes.

Algoritmo	AES	3 DES	DES
Número de paquetes	185,369	322,934	207,093

Nota. Se generó diferentes números de paquetes en base al mismo archivo.

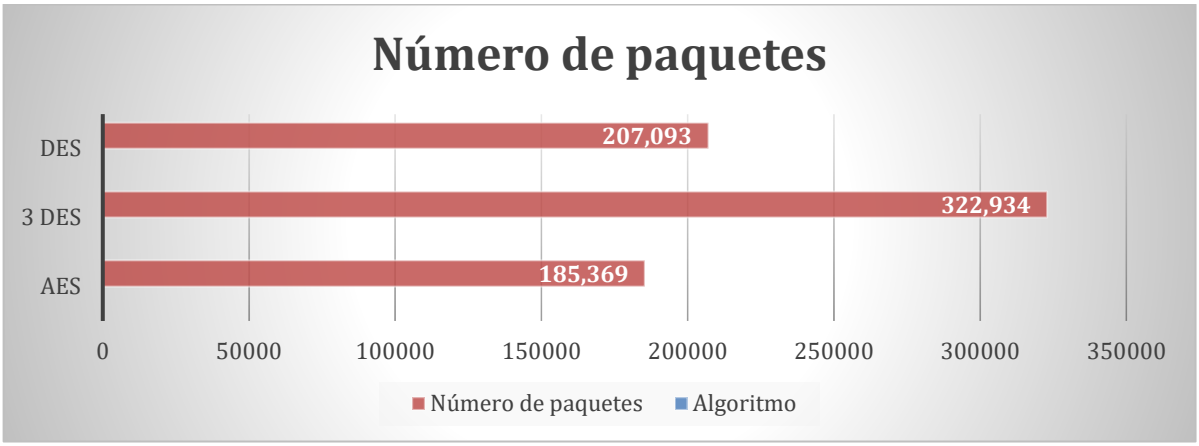


Fig. 6 Comparación de los números de paquetes en cada algoritmo. Nota. Elaboración propia.

En la figura 6 se observa que el algoritmo DES generó el mayor número de paquetes.

c) **Por el tiempo de envío.**

Tabla 7: Evaluación del tiempo de envío

Algoritmo	**3 DES**	**AES**	**DES**
Tiempo de Envío.	00:02:10:50	00:02:15:02	00:02:13:35

Nota. Tiempo que tardó el archivo de 64 MB en enviarse cada algoritmo.

En la tabla 7 se observa que el algoritmo AES necesita menos tiempo para enviar el mismo archivo, optimizando los recursos del computador.

d) **Por el número de paquetes encapsulados.**

Tabla 8: Evaluación del número de paquetes encapsulados

Algoritmo	**AES**	**3 DES**	**DES**
# **Paquetes encapsulados**	20,925	147,933	168,986

Nota. El número de paquetes encapsulados que se generó en cada algoritmo por el archivo de 64 MB.

En la tabla 8 se observa que el algoritmo DES generó mayor número de paquetes encapsulados y el menor fue el algoritmo AES.

e) **Por el número de paquetes desencapsulados.**

Tabla 9: Evaluación del número de paquetes desencapsulados

Algoritmo	**AES**	**3 DES**	**DES**
# **Paquetes desencapsulados**	164,444	175,001	38,107

Nota. El número de paquetes desencapsulados que se generó en cada algoritmo por el archivo de 64 MB.

f) **Por el número de paquetes encriptados.**

Tabla 10: Evaluación del número de paquetes encriptados.

Algoritmo	**AES**	**3 DES**	**DES**
# **Paquetes encriptados**	20,925	147,933	**168,986**

Nota. El número de paquetes encriptados que se generó en cada algoritmo por el

archivo de 64 MB.

g) **Paquetes desencriptados**

Tabla 11: Evaluación del número de paquetes desencriptados

Algoritmo	**AES**	**3 DES**	**DES**
# Paquetes desencriptados	164,444	175,001	38,107

Nota. El número de paquetes desencriptados que se generó en cada algoritmo por el archivo de 64 MB.

En la tabla 11 se observa que el algoritmo DES presenta menor número de paquetes desencriptados a comparación con los otros dos.

h) **Resumen de la evaluación cuantitativa de los algoritmos.**

Tabla 12: Matriz comparativa de la disponibilidad de los algoritmos.

	AES	**DES**	**3 DES**
Configuración en router 1	**x**	**x**	**x**
Configuración en router 2	**X**	**x**	**x**
Tráfico de datos con IPSec en router	**x**	**x**	**x**
Conectividad entre Hots.	**x**	**x**	**x**
Configuración de IPSec con los algoritmos	**x**	**x**	**x**

Nota: Matriz comparativa de la disponibilidad de los algoritmos. Fuente: Elaboración propia.

Tabla 13: Matriz comparativa de la disponibilidad de los algoritmos.

Sub dimensión	**Indicador**	**AES**	**DES**	**3 DES**
Confiabilidad	Tiempo	00:02:10:50	00:02:15:02	00:02:13:35
	Paquetes encapsulados	20925	147933	168986
	Paquetes desencapsulados	164444	175001	38107
Integridad	Longitud de la clave	256 bits	112 bits	56 bits

Nota: Matriz comparativa de los resultados de los algoritmos. Fuente: Elaboración propia

Tabla 14: Matriz resumen de los algoritmos 3des, aes y des.

Algoritmo	**AES**	**3 DES**	**DES**
Tamaño de archivo	64 MB	64 MB	64 MB
Número de paquetes	185,369	322,934	207,093
Longitud de la clave	256 bits	112 bits	56 bits
Tiempo de Envió	00:02:10:50	00:02:15:02	00:02:13:35
# Paquetes encapsulados	20,925	147,933	168,986
# Paquetes desencapsulados	164,444	175,001	38,107
# Paquetes encriptados	20,925	147,933	168,986
# Paquetes desencritados	164,444	175,001	38,107

Nota. Resumen de la evaluación cuantitativa de cada algoritmo por el archivo de 64 MB.

En la tabla 14 se puede observar que el algoritmo AES muestra mayor eficiencia en cuanto al rendimiento puesto que al mismo tamaño de archivo generó menor número de paquetes a un menor tiempo, así mismo generó el menor número de paquetes encriptados y número de paquetes desencriptados, desencapsulados en menor número.

Tabla 15. Valoración De Los Algoritmos Criptográficos

	Valor obtenido	**porcentaje**
AES	21	84.00%
DES	18	72.00%
3DES	14	56.00%

*Nota. En anexo 5 se encuentra las escalas y las tablas valorativas

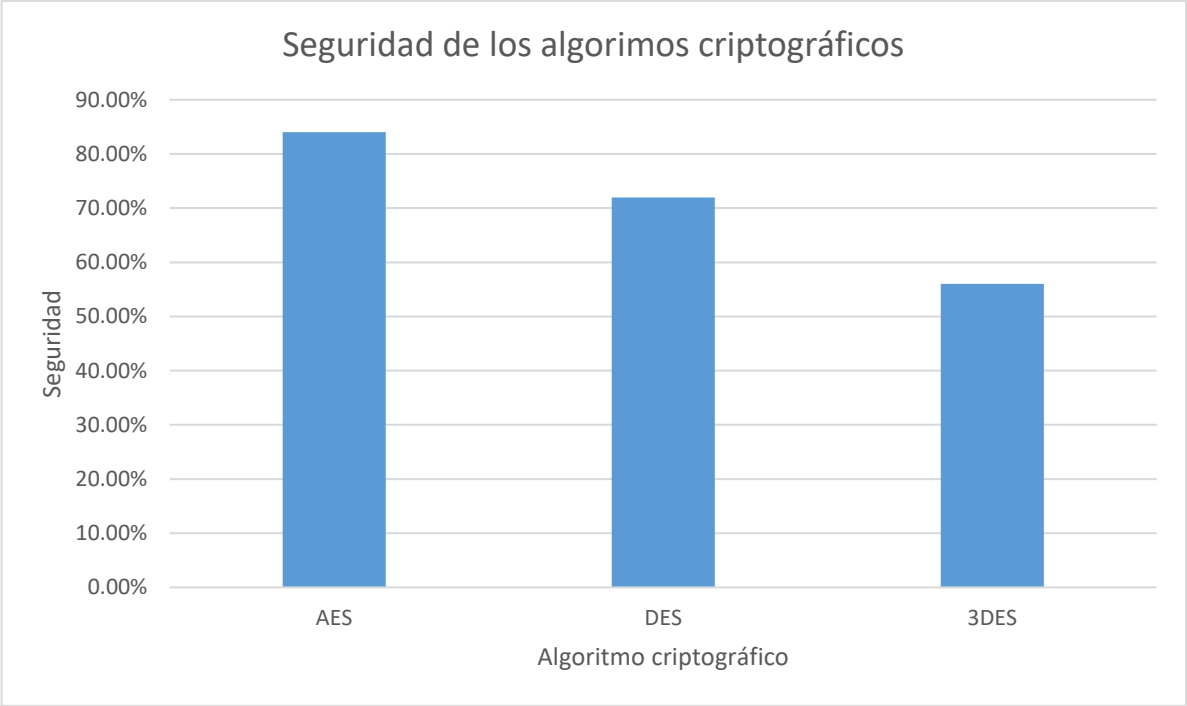


Fig. 7 Seguridad de los algoritmos criptográficos.

En la figura 7 se evidencia que el algoritmo AES es más seguro que el algoritmo DES y el 3 DES en un 84%. También se puede notar que los tres algoritmos brindan seguridad a la red virtual.

3.2. Discusión

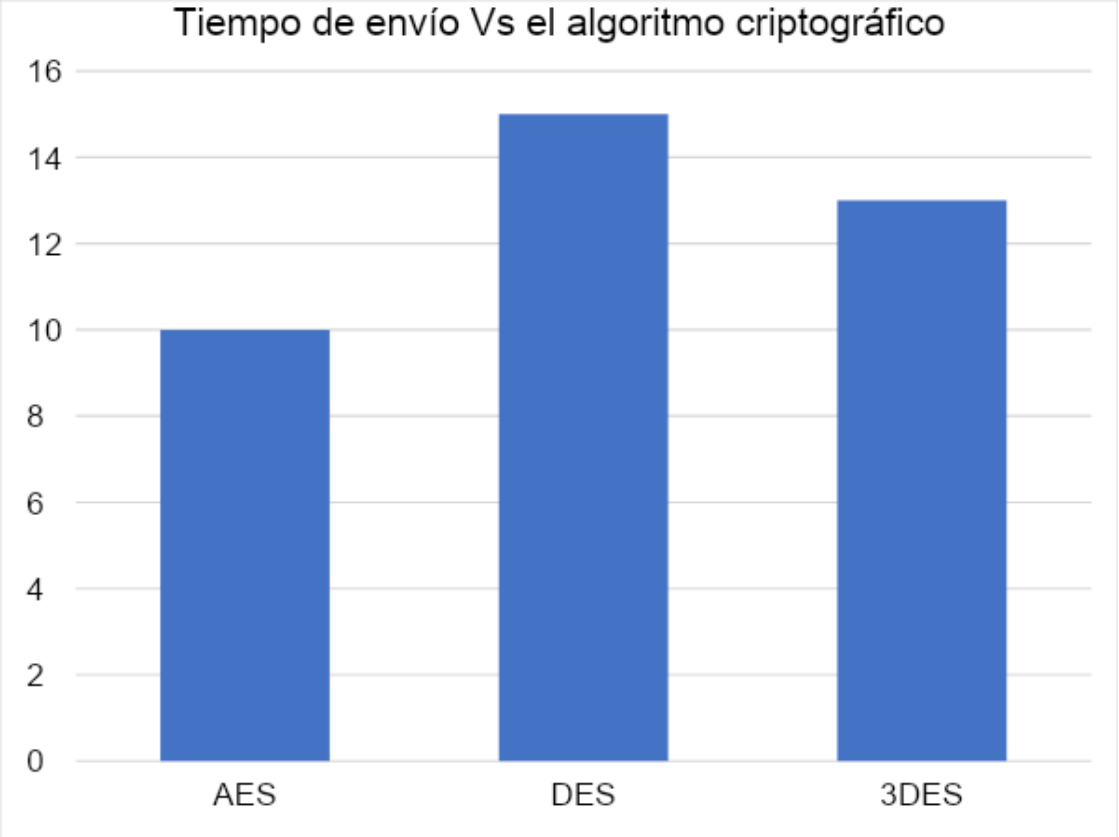


Fig. 7 Tiempo de envío del paquete frente al algoritmo criptográfico aplicado. Nota. Tiempo pasando los cuatro minutos. Elaboración propia.

En esta figura podemos observar que AES es el algoritmo criptográfico más adecuado en cuestión de tiempo de envío de paquetes acumulados a 64 MB para los tres algoritmos ya que emplea menos a comparación de los otros, mostrando reducción de recursos y optimización de estos, siendo favorable para las empresas. Además, refuerza los resultados en comparación a otros estudios realizados, por la autora Samaniego Zanabria, Ana Liz en su proyecto de investigación sobre la evaluación de los Algoritmos Criptográficos con la finalidad de potenciar la Seguridad en la Comunicación y Almacenamiento de la Información, dónde también resalta el rendimiento óptimo del algoritmo AES en

el tiempo de envío.

De acuerdo a los resultados obtenidos, se concuerda con los resultados obtenidos [5] [6], dónde afirman que AES es más confiable en condiciones de cifrado de velocidad, decodificación, complejidad, longitud de la clave, estructura y flexibilidad.

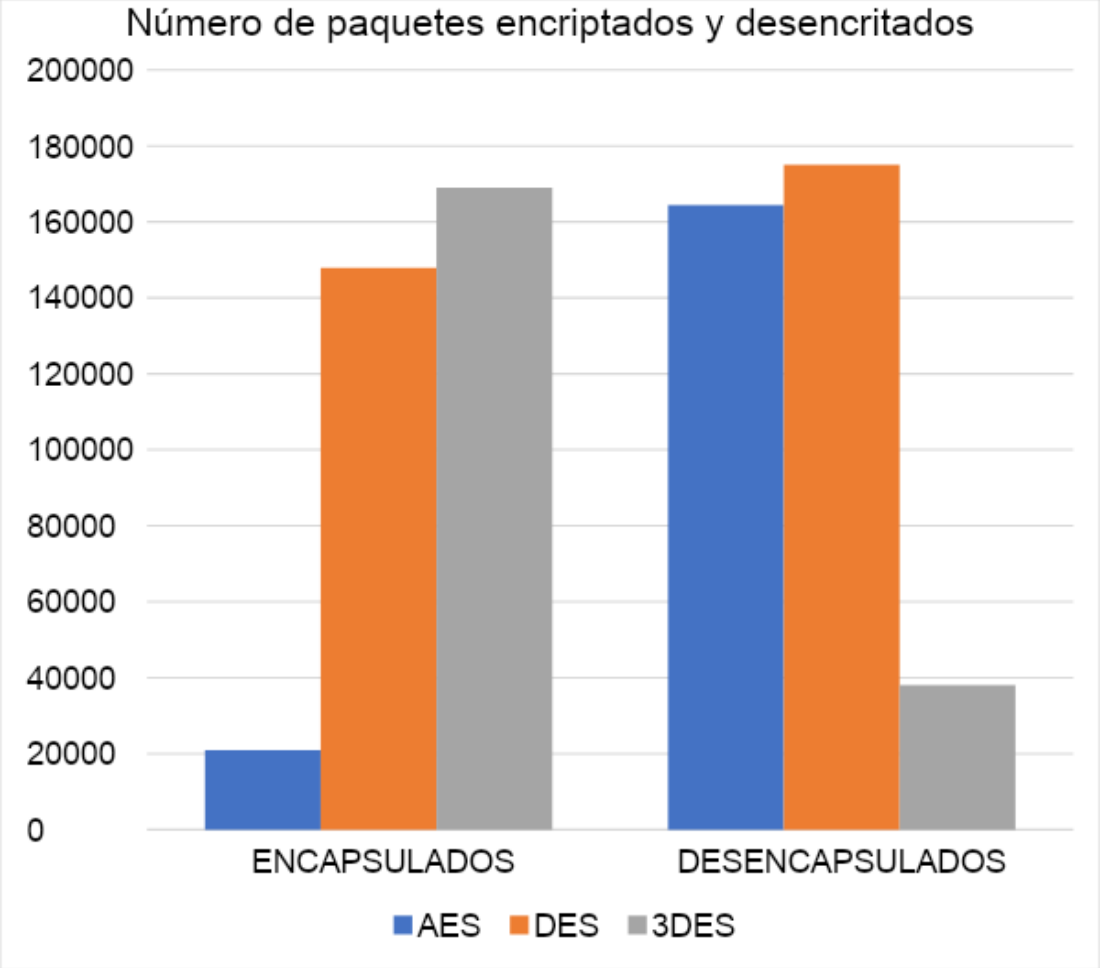


Fig. 8 Número de paquetes encapsulados. Nota. Elaboración propia.

En la figura 8 se visualiza la comparación de la cantidad de paquetes encapsulados por cada algoritmo criptográfico, siendo el DES el algoritmo que encapsula y desencapsula el mayor número de paquetes y el menor el 3 DES.

Esto refleja que el nivel de seguridad en la dimensión de confiabilidad aumentara, siendo el AES la mejor opción en esta dimensión.

La longitud de la clave del algoritmo AES el que se encuentra en el óptimo a comparación del DES y 3 DES, mostrando seguridad en la clave, ya que refleja un criterio de dificultad de adivinación empleando claves alfanuméricas. Además, en optimización de recursos presenta ventaja ante estos resultados

De acuerdo con Cangea [8] el tamaño de la clave del cifrado de bloque es el determinante de la confiabilidad con respecto al costo, el número de rondas de cifrado con respecto a la fiabilidad y rendimiento, y, por último, las características del diseño de hardware con respecto al precio y rendimiento. Mientras más pequeña es la clave menor uso de recursos se emplearán.

En la dimensión de disponibilidad los resultados no intervinieron para decidir cuál es el mejor en seguridad, sin embargo, fueron la base para determinar las otras dimensiones ya que se trata de la configuración de cada algoritmo, el indicador de conectividad los tres presentaron conectividad.

Finalmente se concuerda con las diversas investigaciones de Alenezi et al. [10] y Murlidhar y Raut [11], donde afirman según sus resultados obtenidos, que el algoritmo AES es el de mejor nivel de seguridad. Siendo importante la seguridad de los datos en las diferentes áreas y empresas, enfatizándolo especialmente en la minería y fraudes del mercado de valores.

Discrepando con la investigación de Damrudi y Aval [17], donde afirman que el algoritmo DES y pez globo llevan el menor tiempo de encriptación y descifrado que el AES.

3.3. Aporte de la investigación (opcional)

Se inició desarrollando el primer objetivo específico:

A. **Identificación de los algoritmos criptográficos de la red privada virtual.**

Para poder lograr con este objetivo específico, se realizaron las fichas técnicas para cada algoritmo simétrico y por bloque: AES, DES, 3DES. Destacando la estructura y arquitectura de cada uno de ellos, facilitándonos información y características. Ubicados en el Anexo 2. Fichas técnicas.

Una vez identificados los algoritmos criptográficos se procedió con el segundo objetivo específico:

B. **Valoración de los tres algoritmos criptográficos según sus tres dimensiones.**

Se tomó en cuenta las dimensiones de integridad, confiabilidad y disponibilidad de las variables para su valoración de cada algoritmo.

1. Se inició con dimensión de la disponibilidad, siendo necesario implementar la configuración en los tres Router: Router CPE01 modelo cisco isr c1111, Router CPE02 modelo cisco isr c1111 y el Router PE modelo Cisco isr 1921. La configuración el Router 1 se muestra en el Anexo 4, del Router 2 en el Anexo 5, del Router 3 en el anexo 6.

VPN Implementada.

El modelo de la VPN fue realizado en el programa GNS3 v2.2.41 y se implementó en equipos reales en el Laboratorio.

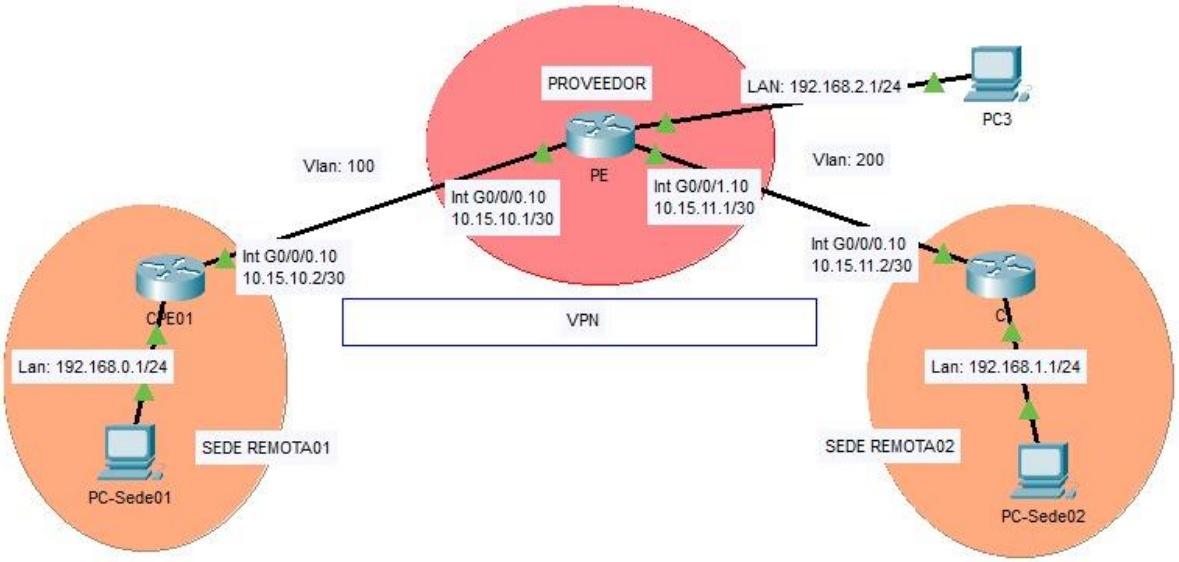


Fig. 9 Red VPN. Nota. Elaboración propia.

Posteriormente se realizó las pruebas de envío de paquetes por medio de los túneles, empleando archivo de 64 MB para los tres algoritmos.

Seguido se determinó el tráfico de datos con los comandos de mando IPSec en el DES, 3 DES y AES. Se empleó el programa del WIRESHARKS para poder capturar el tráfico.

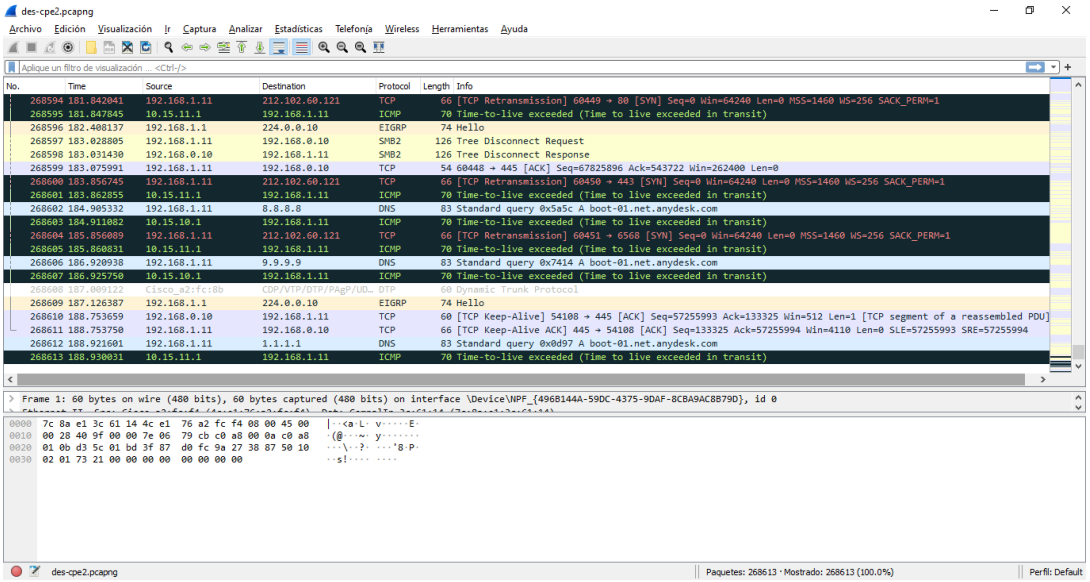


Fig. 10 Tráfico con WIRESHARK del algoritmo DES. Nota. Elaboración propia

En la figura 10, se muestra el tráfico del algoritmo DES, observándose el número de paquetes, el tiempo de transito ejecutado y los paquetes capturados.

Se capturo la estructura del paquete 268590 de 146 bytes.

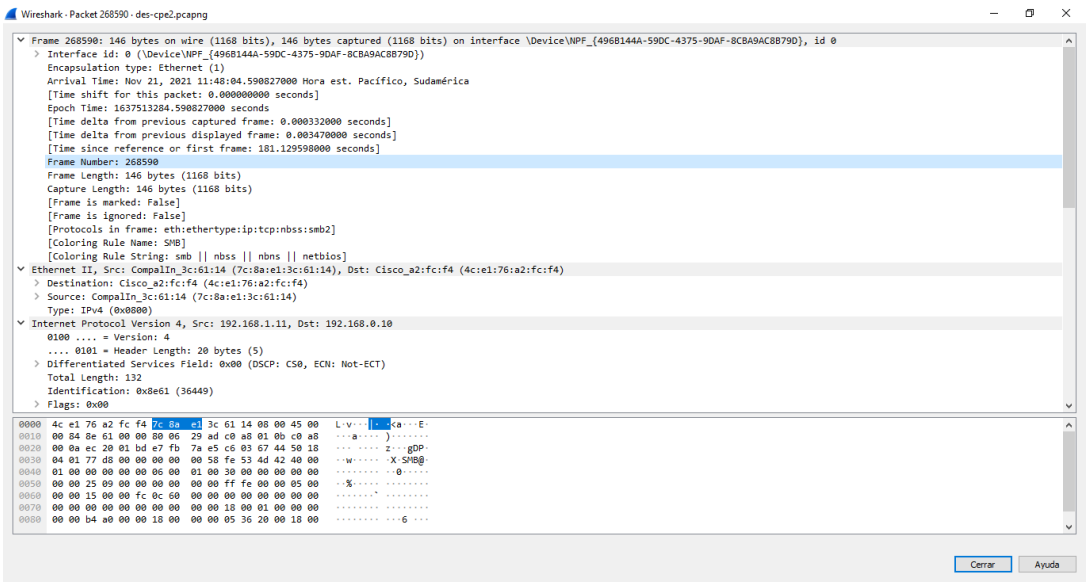


Fig. 11 Estructura de un paquete capturado 268590 con 147 bytes. Fuente: Elaboración propia

En la figura 11 se muestra la estructura del paquete capturado del algoritmo DES.

Finalmente, para el primer algoritmo se capturó los paquetes depurados por IP de origen 192 168 111, con la finalidad de determinar la capacidad del DES. Siendo

de 146 bytes.

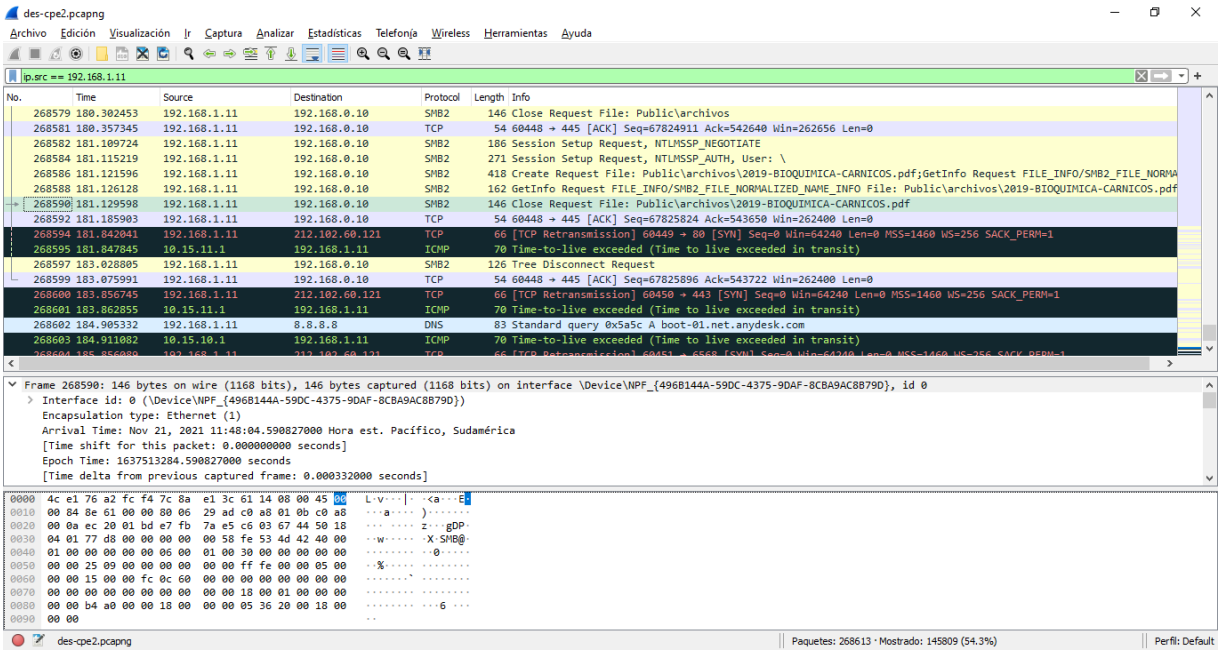


Fig. 12 Paquetes depurados por el IP de inicio 192.168.1.11. Fuente: Elaboración propia

Por último, se determinó los paquetes depurados por IP llegada 192 168 010, con 462 bytes capturados.

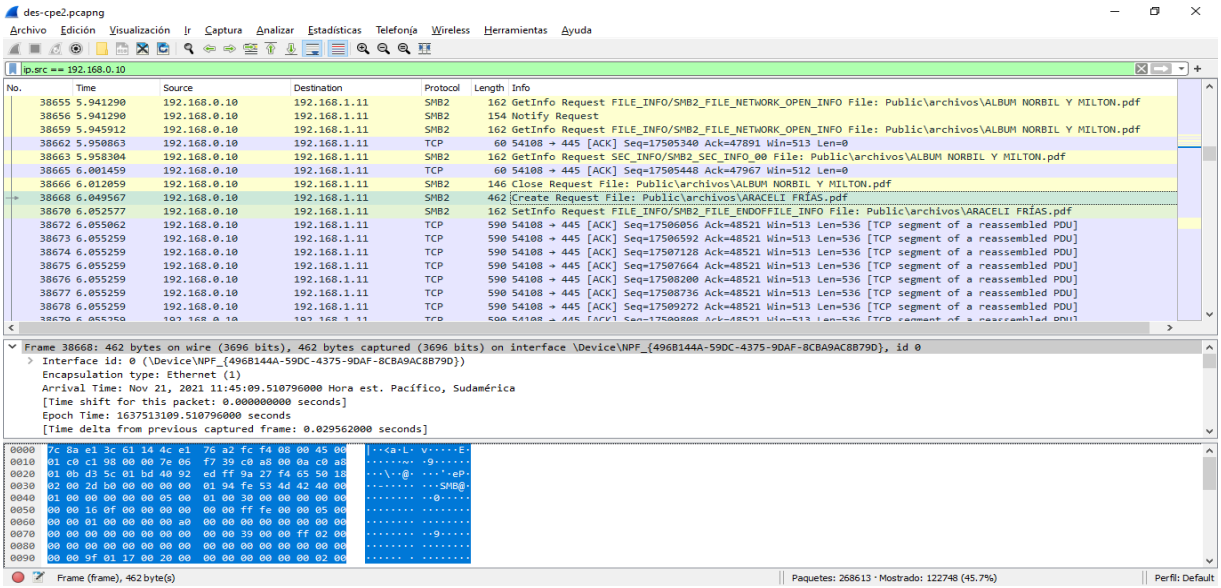


Fig. 13 Paquetes depurados por el IP de llegada 192.168.0.10. Fuente: Elaboración propia.

Para el algoritmo DES el tiempo que se emplea para duplicar el archivo de 00:02:15:02. y el tamaño es de 64.4 MB.

De la misma secuencia se realizó para el algoritmo 3 DES y AES. El tráfico de datos con IPSec en el algoritmo 3 DES.

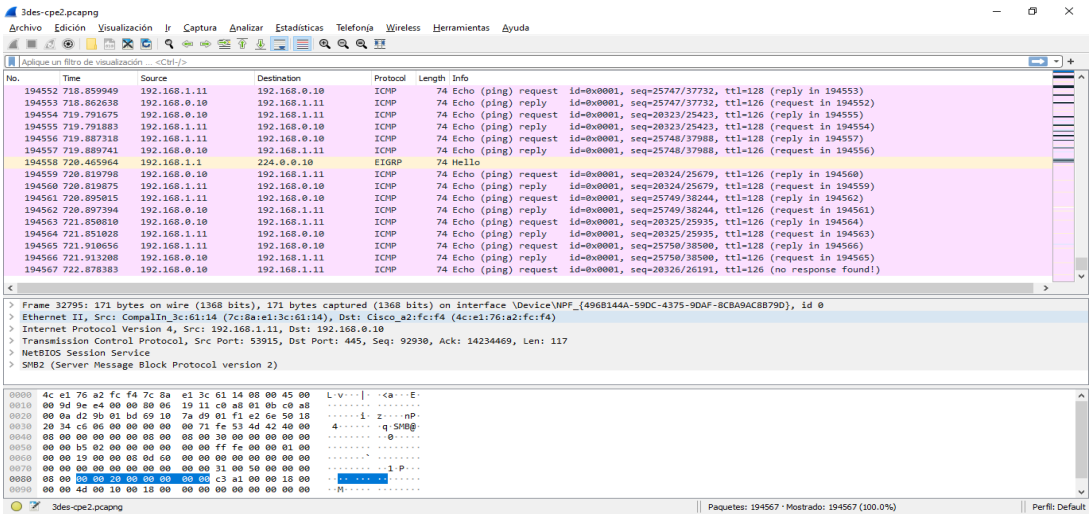


Fig. 14 Tráfico con WIRESHARK del algoritmo 3DES. Fuente: Elaboración propia.

Mostrándose la captura de 194567 paquetes en el 3DES de 171 bytes.

Seguidamente se muestra el esqueleto de paquete capturado (del paquete capturado 97259 171 bytes).

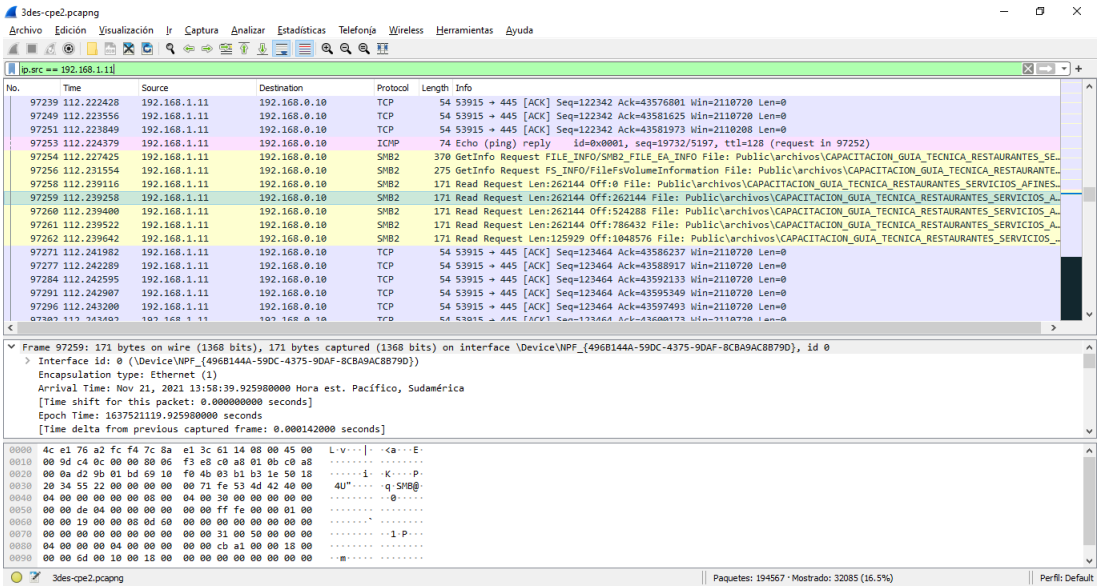


Fig. 15. Esqueleto de un paquete en proceso de captura 97259 de 171 bytes.

Fuente: Elaboración propia

En la figura 15 se muestra la estructura del paquete 972559 de 1368 bits.

Paquetes depurados por el IP de inicio 192.168.1.11 según el 3 DES.

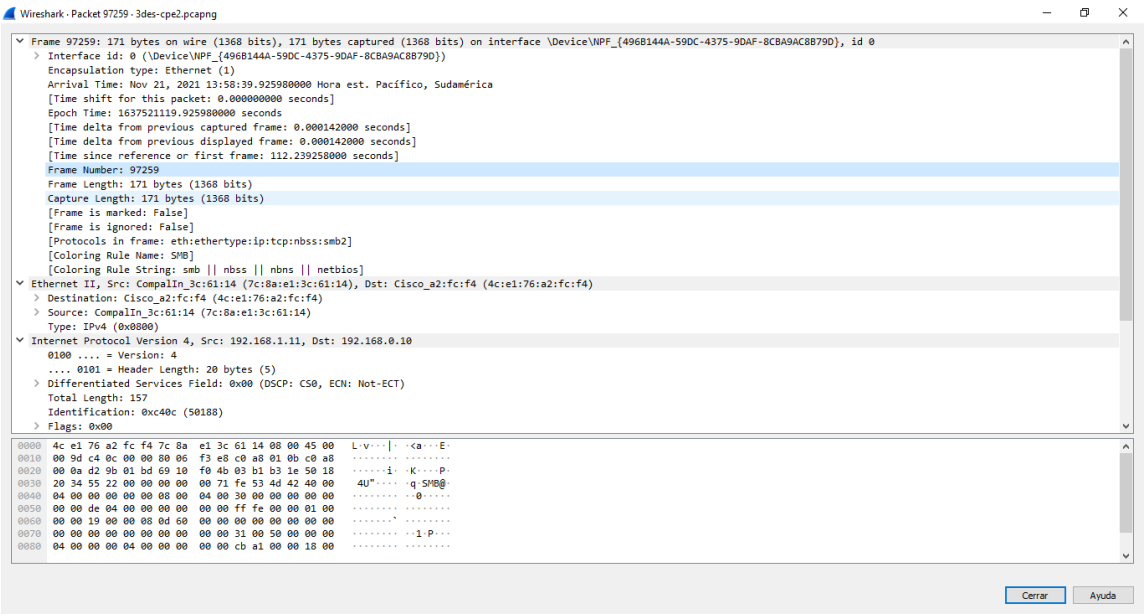


Fig. 16 Paquetes depurados por el IP de inicio 192.168.1.11. Fuente: Elaboración propia

Se capturo la cantidad de paquetes depurados en el IP de origen siendo un total de 97259. Se determinó el número de paquetes depurados por el IP de llegada.

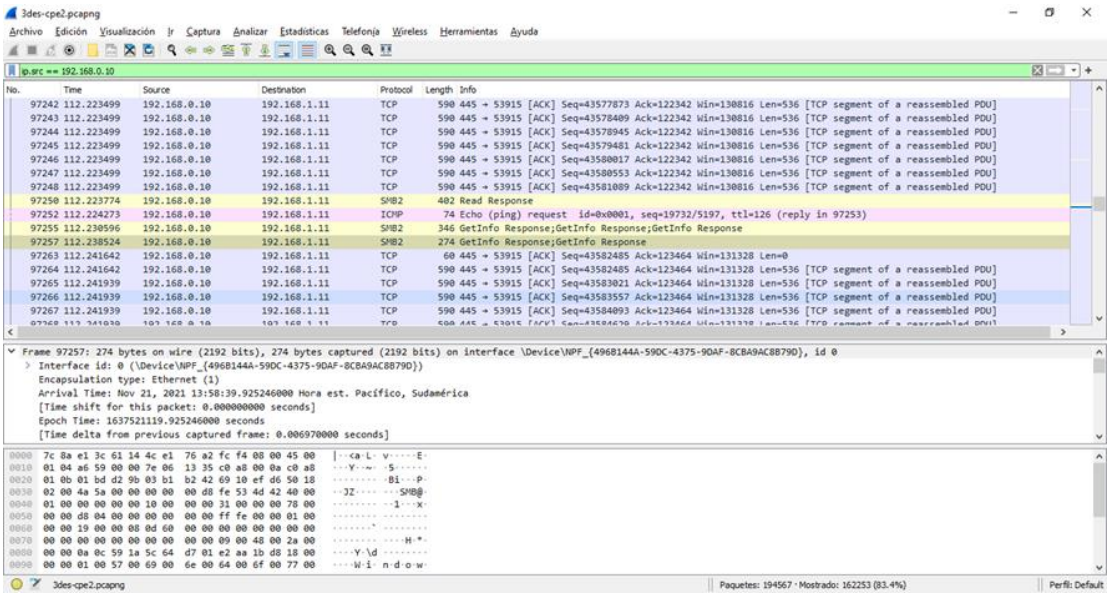


Fig. 17 Paquetes depurados por el IP de llegada 192.168.0.10. Fuente: Elaboración

propia

El número de paquetes depurados en el IP de llegada fueron 194567.

El tiempo de duplicación del archivo: 00:02:13:35 y el tamaño: 64.4 MB

Finalmente se hizo lo mismo para el algoritmo AES. El Tráfico de datos con IPSec empleando el WIRESHARK.

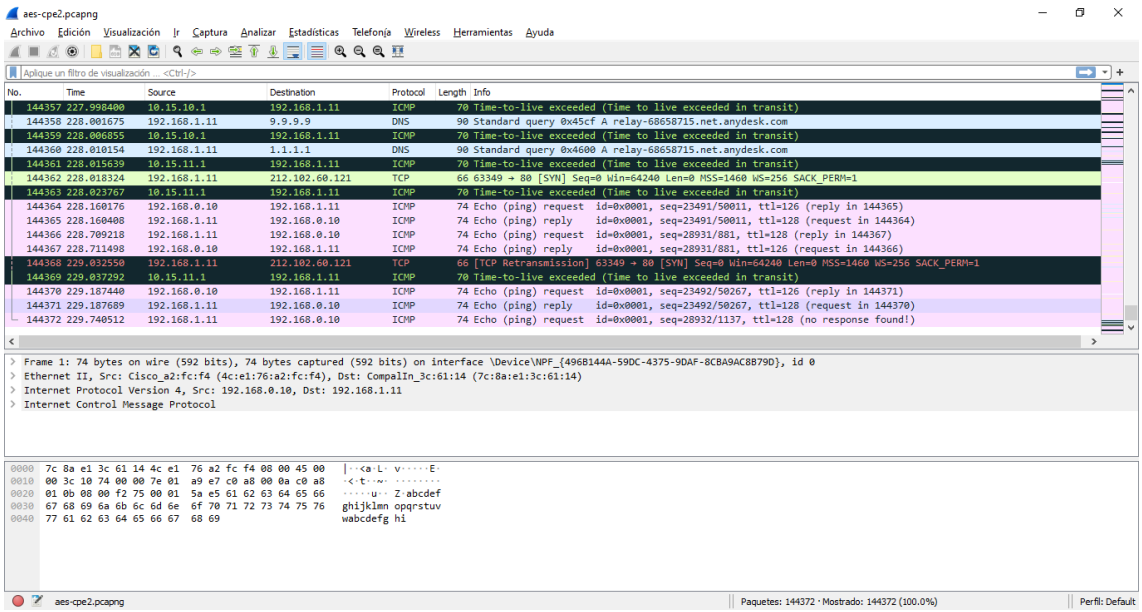


Fig. 18 Tráfico con WIRESHARK del algoritmo AES. Fuente: Elaboración propia

Mostrando en la figura 18 el número de paquetes capturados con una totalidad de 144372 de 74 bytes. Se capturó el esqueleto del paquete capturado (del paquete capturado 126390 de 130 bytes)

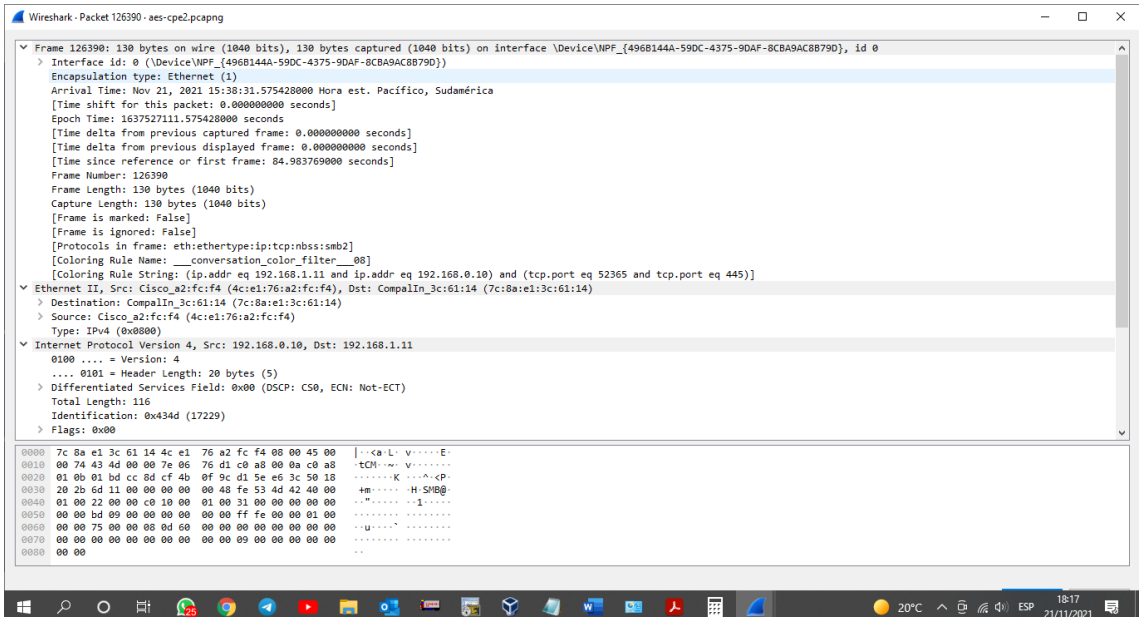


Fig. 19 Esqueleto de un paquete capturado. Fuente: Elaboración propia.

En la figura 19 se muestra la captura del paquete 126390 de 130 bytes y 1040 bits.

Se capturó los paquetes depurados por el IP de inicio - 192.168.1.11

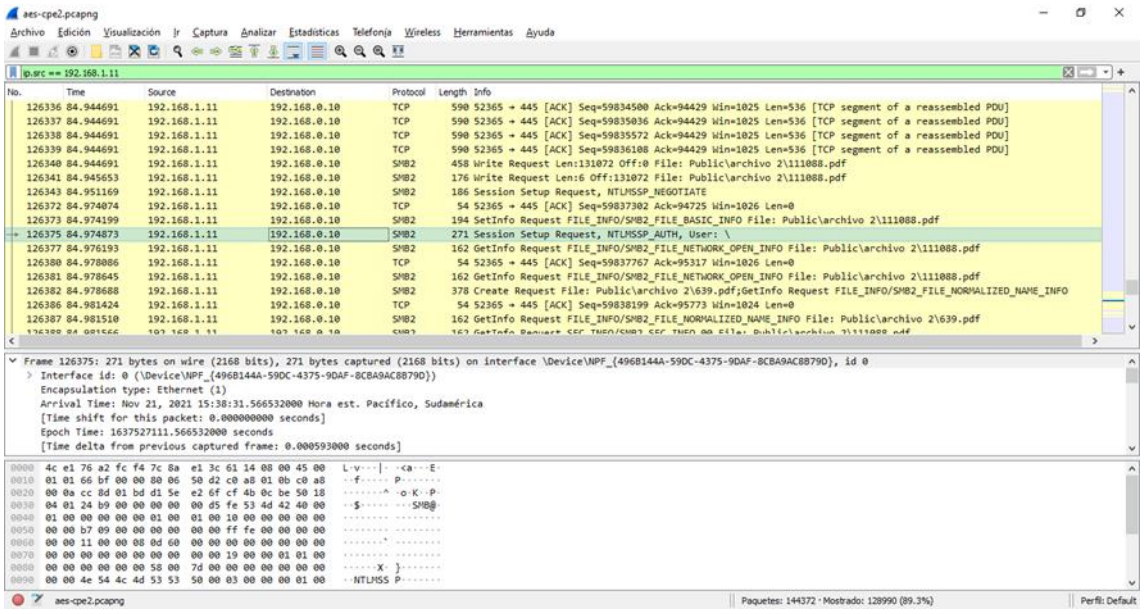


Fig. 20 Estructura de un paquete depurados por el IP de inicio 192.168.1.11. Fuente: Elaboración propia

En la figura 20 se muestra el número de paquetes depurados por el IP de origen siendo un total de 126375.

Finalmente se determinó el número de paquetes depurados por el IP de llegada -

192.168.0.10.

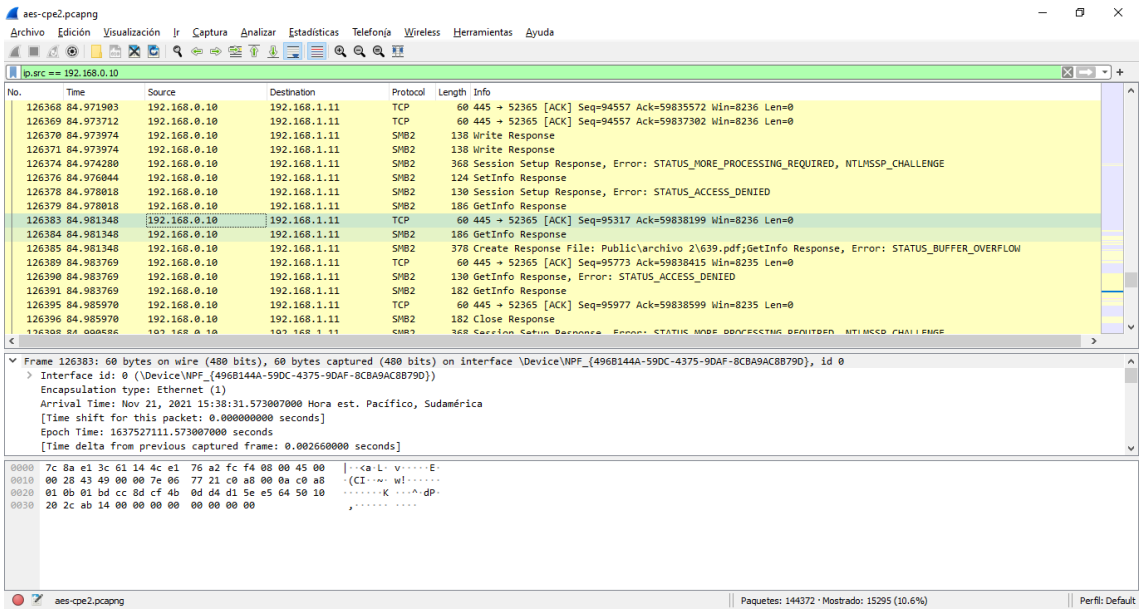


Fig. 21. Paquetes depurados por el IP de llegada 192.168.0.10. Fuente: Elaboración propia

El tiempo de duplicación del documento: 00:02:10:50 y tamaño: 64.4 MB en el algoritmo AES.

Después se realizaron las comprobaciones de conectividad entre HOST.

Para ello se realizó la configuración del IPC01 y el IPC02.

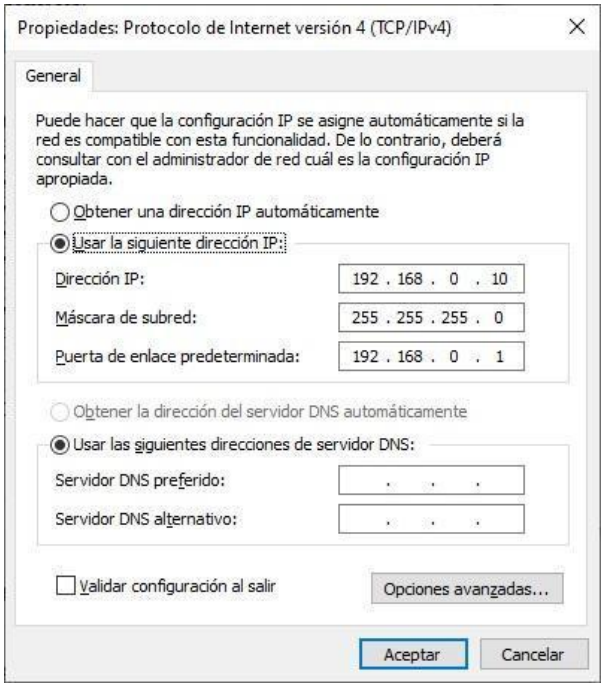


Fig. 22 Configuración de IP CP 01. Fuente: Elaboración propia

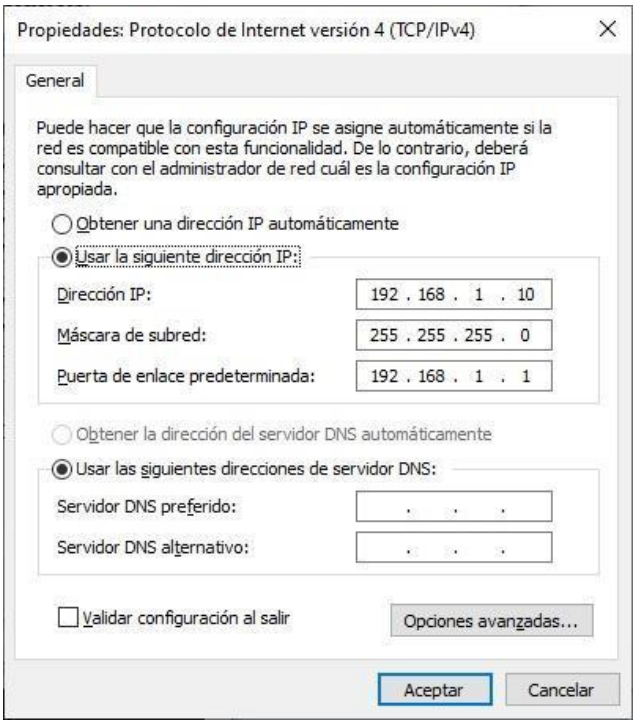


Fig. 23 Configuración de IP CP 02. Fuente: Elaboración propia

Se capturó la comprobación IP en CP 1 y el CP 2, para determinar la accesibilidad.

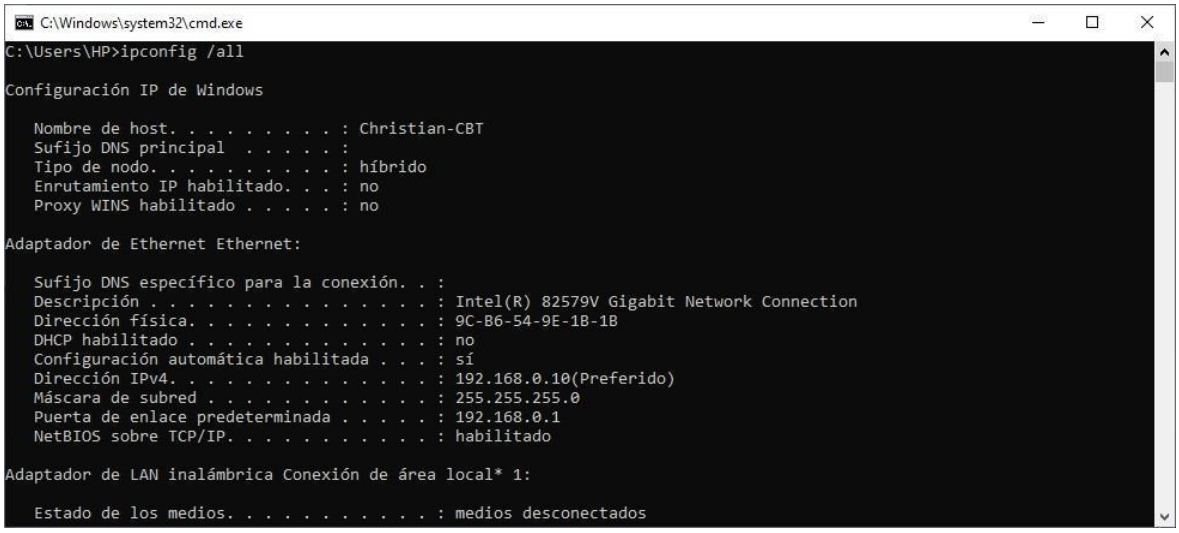


Fig. 24 Comprobación IP en CP 1. Fuente: Elaboración propia

En la figura 24 se muestra la habilitación del IP en la CP 1.

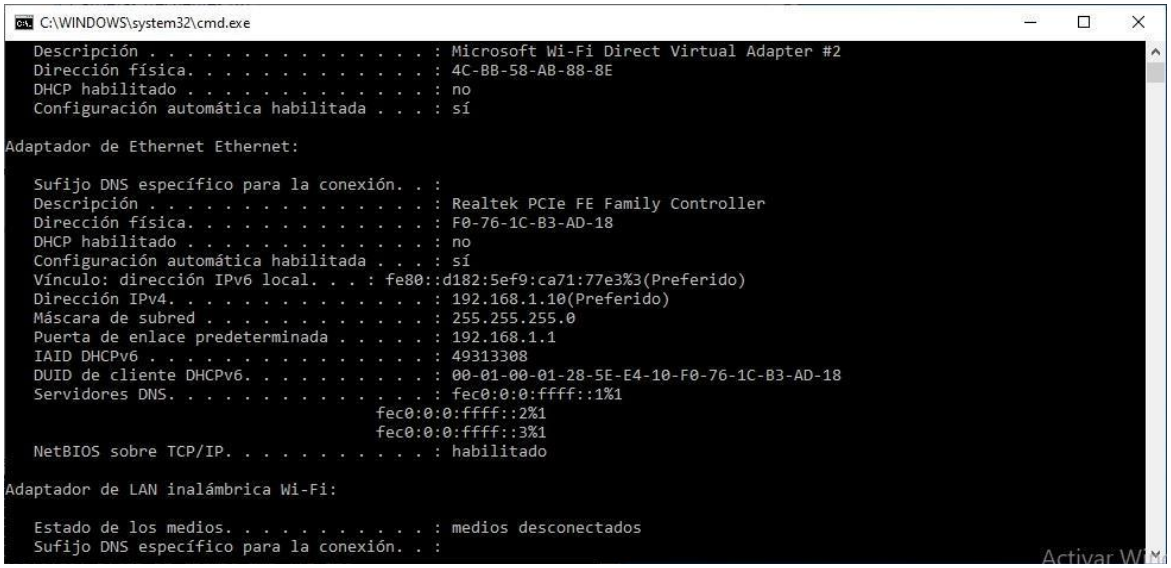


Fig. 25 Comprobación IP en CP 2. Fuente: Elaboración propia

En la figura 25 se muestra la habilitación del IP en el CP 2.

Después se verificó la conectividad de PC 01-02 y PC 01-02.

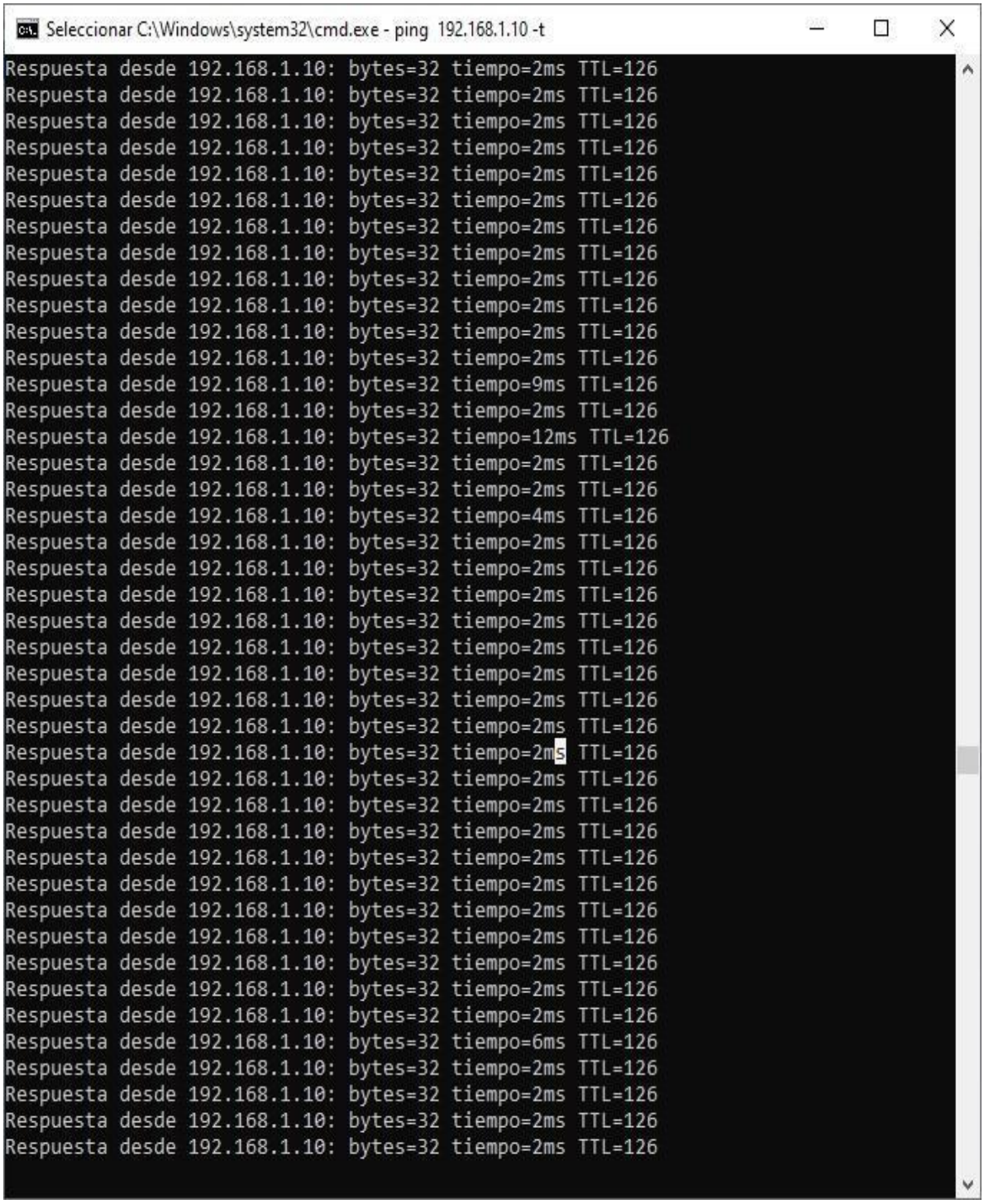


Fig. 26 Conectividad PC 01 a 02. Fuente: Elaboración propia

Se verificó la Conectividad de PC 01-02.

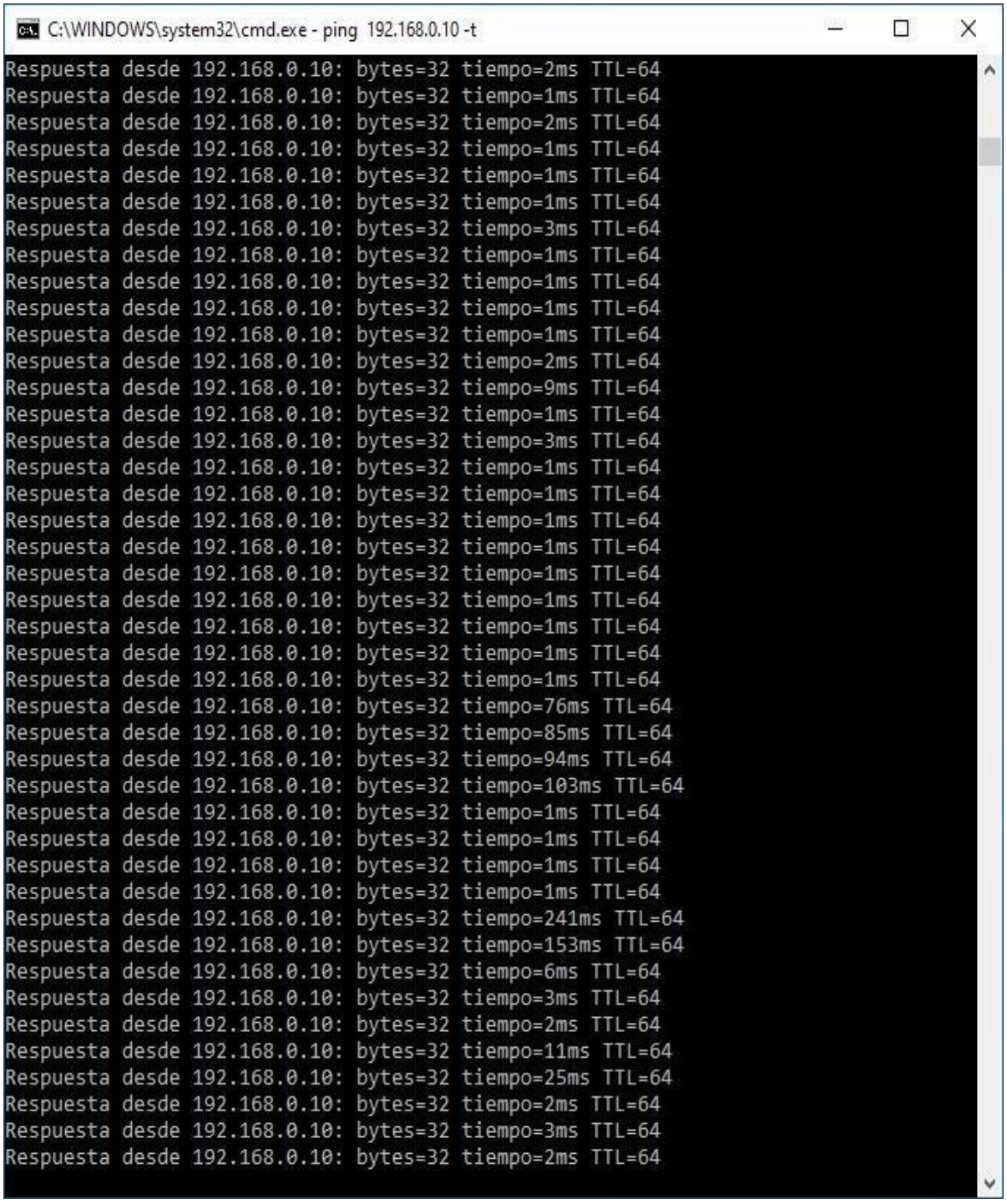


Fig. 27 Conectividad PC 02 a 01. Fuente: Elaboración propia

Se verificó la Conectividad de PC 02-01.

Luego se configuraron las IPSec en cada algoritmo. Iniciando con la configuración de IPSec con el algoritmo DES en router 1.

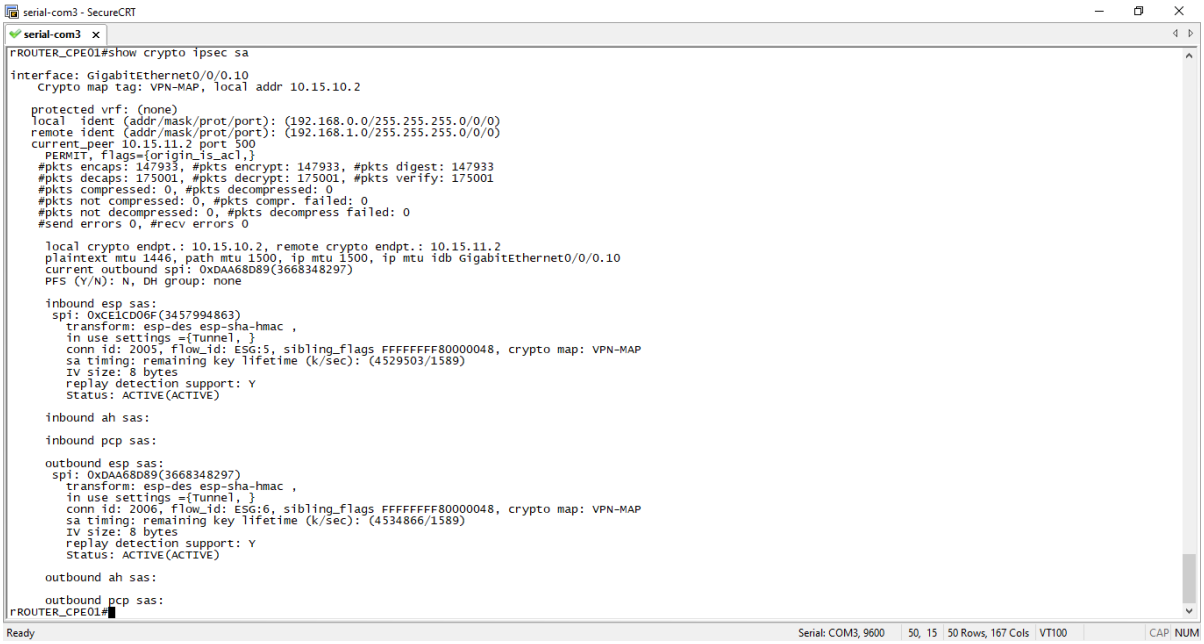


Fig. 28 Configuración del IPSec con el algoritmo DES en router 01. Fuente: Elaboración propia

En la figura 28 se muestra la configuración del primer algoritmo en el Router 1, seguidamente se realizó en el router 2.

Fig. 29 Configuración del IPSec con el algoritmo DES en router 02. Fuente: Elaboración propia

Después se hizo la configuración del IPSec del algoritmo 3 DES en el Router 1 y 2.

Fig. 30 Configuración del IPSec con el algoritmo 3DES en router 01. Fuente: Elaboración propia

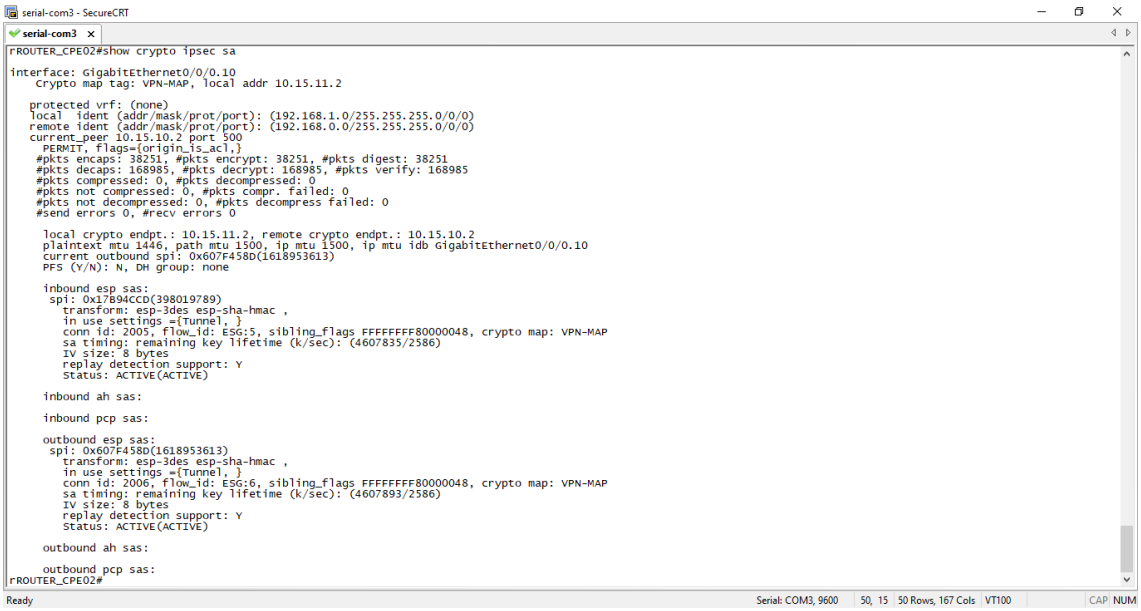


Fig. 31 Configuración del IPSec con el algoritmo 3DES en router 02. Fuente: Elaboración propia

Finalmente se hizo la configuración del IPSec del algoritmo AES en el Router 1 y

2.

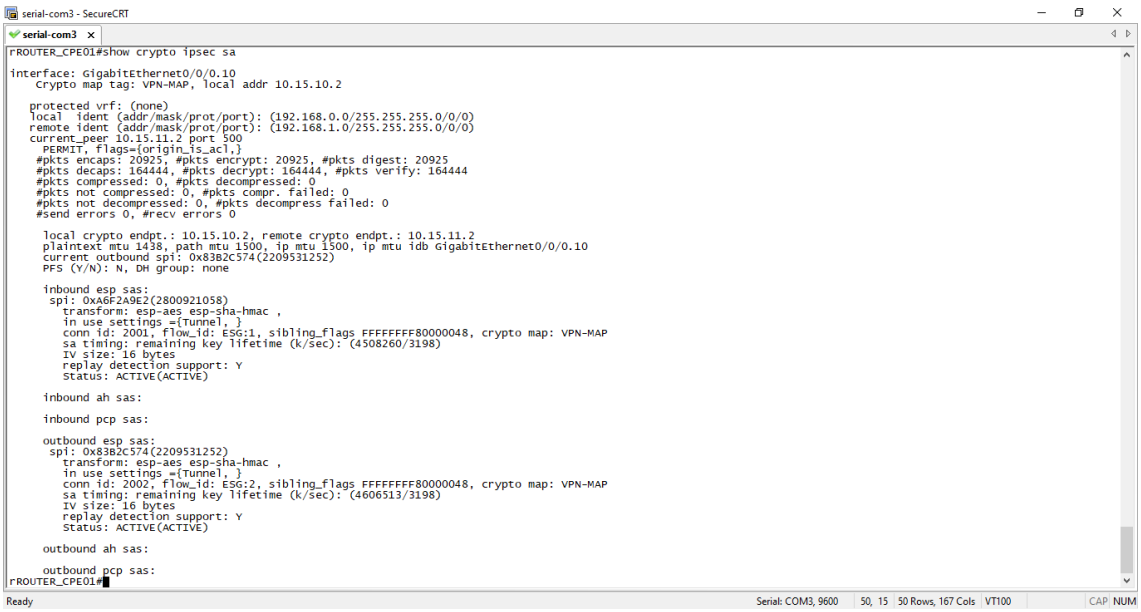


Fig. 32 Configuración del IPSec con el algoritmo AES en router 01. Fuente: Elaboración propia

Los algoritmos AES, DES. 3 DES.

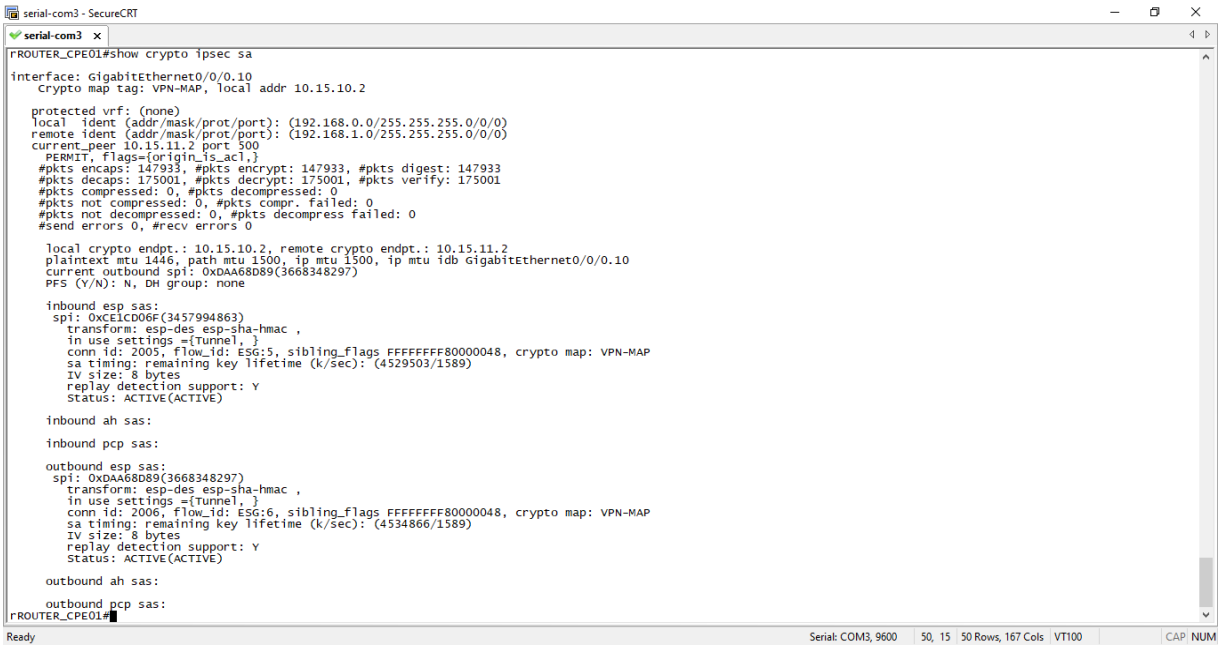


Fig. 33 Número de paquetes encapsulados y desencapsulados algoritmos DES CPE 01. Fuente: Elaboración propia

Fig. 34 Número de paquetes encapsulados y desencapsulados algoritmos 3 DES CPE 01. Fuente: Elaboración propia

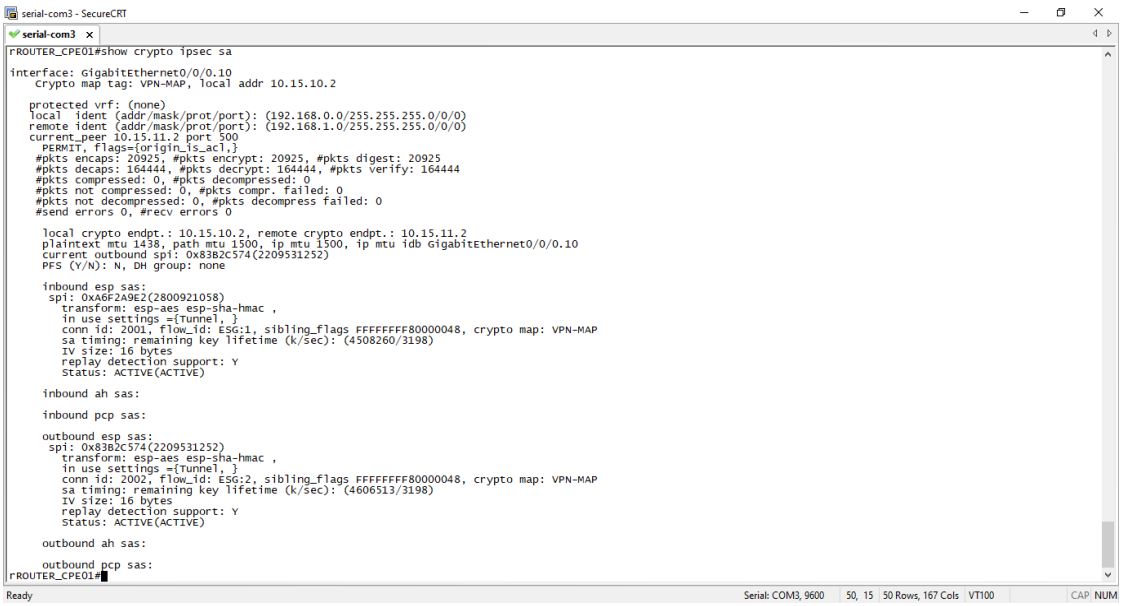


Fig. 35 Número de paquetes encapsulados y desencapsulados algoritmos AES CPE 01. Fuente: Elaboración propia

Por último, en la dimensión de la integridad, se determinó por la fortaleza de la clave, están basados en la longitud de la clave.

Fig. 36 Configuración del IPSec con el algoritmo AES en router 02. Fuente: Elaboración propia

La dimensión de la confiabilidad se determinó hallando primero la capacidad de almacenamiento de cada algoritmo. Para ello se capturo la ubicación y el tamaño del archivo a compartir.

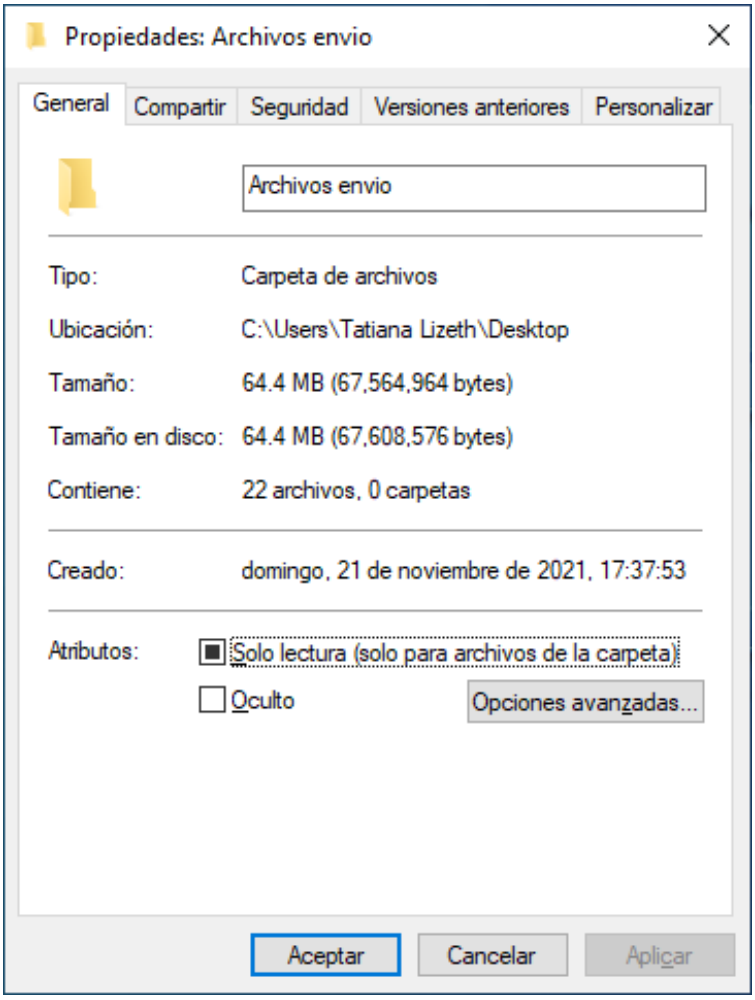


Fig. 37 Ubicación del archivo y tamaño a compartir en PC02-CP02. Fuente: Elaboración propia

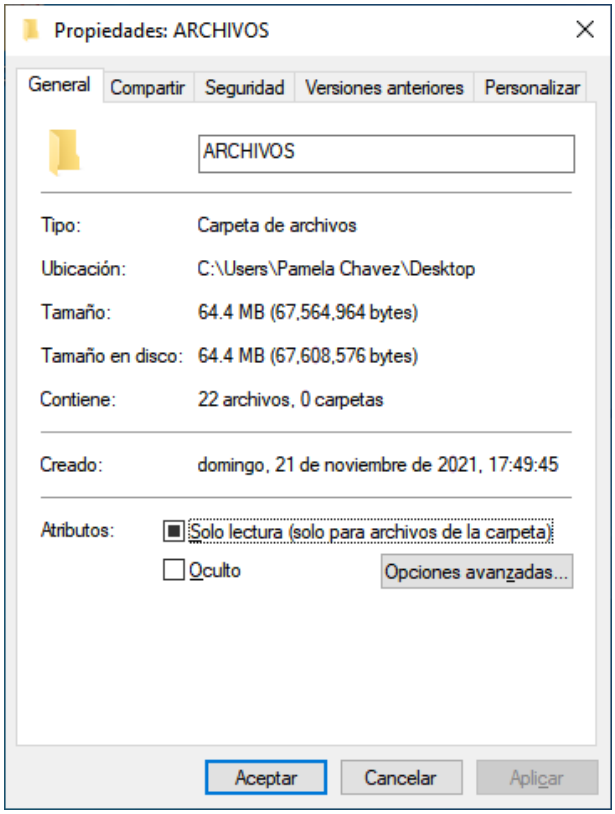


Fig. 38 Ubicación de archivo y tamaño a compartir en PC01-CP01. Fuente: Elaboración propia

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. Se logró determinar el nivel de seguridad que ofrecen los algoritmos criptográficos AES, DES y 3DES en una red privada virtual, empleando una red virtual de tres Router por medio del programa GNS3, sobresaliendo el algoritmo AES en rendimiento.

2. Se identificaron los algoritmos criptográficos, reconociendo sus características, diseño y arquitectura de cada uno, siendo los más usados el AES, DES y 3DES.

3. Se realizó la configuración de los accesos, interfaces y enrutamiento de una red virtual, lo que permitió la interconexión entre los tres Routers.

4. Se valoró los tres algoritmos criptográficos según sus tres dimensiones, determinándose que el algoritmo AES presenta ventaja en el tiempo de envío de un archivo según el protocolo de encriptamiento, de encapsulamiento y desencapsulamiento. El algoritmo aes es más seguro en un 84% a comparación de los otros dos.

4.2. Recomendaciones

a) Principalmente se recomienda realizar la configuración en redes virtuales y evaluar la conectividad.
b) Emplear el algoritmo AES para las empresas ya que representa un mayor nivel de seguridad, reflejados en las tres dimensiones evaluadas confiabilidad, integridad y disponibilidad.
c) Se recomienda emplear otras metodologías para analizar algoritmos híbridos, respondiendo a sus particularidades.
d) También se recomienda realizar el análisis de la seguridad que brinda cada algoritmo en redes inalámbricas para reconocer el comportamiento de estos algoritmos.

REFERENCIAS

[1] M. Tarzan, «Ciberseguretat i vulnerabilitat en les telecomunicacions,» Arxius, nº 4 Compàs d'amalgama, 2021.

[2] Avast, «Cifrado de datos: ¿en qué consiste?,» 22 abril 2021. [En línea]. Available:https://www.avast.com/es-es/c-what-is-an-ssl-certificate#:~:text=Avast%20SecureLine%20VPN%20le%20ofrece,otra%20persona%20que%20intente%20espiarle.. [Último acceso: 03 noviembre 2021].

[3] Eset, «Cifrado simple y potente para empresas de todos los tamaños.,» 2018. [En línea]. Available: https://www.eset.com/pe/empresas/cifrado/. [Último acceso: 12 octubre 2021].

[4] Security Panda, «La primera línea de defensa para proteger datos.,» 23 julio 2019. [En línea]. Available: https://www.pandasecurity.com/es/mediacenter/noticias/panda-full-encryption-proteger-datos/. [Último acceso: 02 octubre 2021].

[5] O. Abood y S. Guirguis, «A Survey on Cryptography Algorithms,» International Journal of Scientific and Research Publications, vol. 8, nº 7, pp. 1-22, 1 Julio 2018.

[6] L. Valtensir, J. Gabriel y C. Miranda, «Análise e Comparação de Algoritmos Criptográficos aplicados à IoT,» Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-8, 19 junio 2019.

[7] P. Machník, M. Urueña, N. Stoianov y M. Niemiec, «Performance evaluation of INDECT security architecture,» Universidad Santo Tomas, vol. 15, nº 1, pp. 34-42, 15 Junio 2018.

[8] O. Cangea, «A Survey of Lightweight Cryptography Methods,» Petroleum

Gas University of Ploiesti, Blvd., vol. 71, nº 2, pp. 29-40, 2019.

[9] N. Mohd y A. Ahmed, «Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time,» de Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time, Malaysia, 2020.

[10] M. Alenezi, H. Alabdulrazzaq y N. Mohammad, «Symmetric Encryption Algorithms: Review and Evaluation study,» International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, nº 2, pp. 256-272, Agosto 2020.

[11] A. Murlidhar y V. Raut, «Privacy Preserving of Data Files & Audio / Video Encryption –Decryption Using AES Algorithm,» International Journal on Recent and Innovation Trends in Computing and Communication, vol. 6, nº 5, pp. 238 - 242, Mayo 2018.

[12] S. Dwi Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan y A. Suwandi Ahmad, «Power analysis attack against encryption devices:a comprehensive analysis of AES, DES, and BC3,» TELKOMNIKA, vol. 17, nº 3, pp. 1282-1289, 2019.

[13] B. Xing, D. Wang, Y. Yang, Z. Wei, J. Wu y C. He, «Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor.,» International Journal of Parallel Programming, vol. 49, nº 3, pp. 463-486. 24p., 2021.

[14] Y. Wu y X. Dai, «Encryption of accounting data using DES algorithm in computing environment,» Journal of Intelligent & Fuzzy Systems, vol. 39, nº 4, p. 5085–5095, 2020.

[15] S. Suherman, «Impact encryption algorithm used in three pass protocol for securing WiMAX link,» Journal of Physics: Conference Series, vol. 1783, pp. 1-3, 2021.

[16] M. Kamrul, M. Shafiq, S. Islam, B. Pandey, Y. Baker, N. Shaker, R. Ciro y D.

Esenarro, «Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications,» Complexity, vol. 2021, pp. 1-13, 2021.

[17] M. Damrudi y K. Aval, «Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish,» International Journal of Engineering and Advanced Technology, vol. 8, nº 6, pp. 204-108, 2019.

[18] I. Latif, «Time Evaluation of Different Cryptography Algorithms Using Labview,» IOP Conference Series: Materials Science and Engineering, vol. 745, pp. 1-10, 2019.

[19] K. Muttaqin y J. Rahmadoni, «Analisis and desing of file security system AES (Advanced Encryption Standard) Cryptography Based,» Journal of Applied Engineering and Technological Science, vol. 1, nº 2, pp. 113-123, 2020.

[20] D. Rambaut, Introducción a la Criptografía post-cuántica basada en teoría de códigos, Bogotá: Universidad del Rosario, 2021, pp. 1-102.

[21] P. Aguilera, «Seguridad informática,» de Ciclos formativos, Editex, Ed., España, Editex, 2010, p. 240.

[22] ISO/TEC 27001, «Seguridad informática y seguridad de la información,» 12 Enero 2021. [En línea]. [Último acceso: 11 octubre 2021].

[23] E. Vega, 3 ciencias, Primera ed., Alzamora: Editorial Área de Innovación y Desarrollo,S.L., 2021.

[24] F. León, «Investigación en salud. Dimensión ética,» Acta bioethica, vol. 12, nº 2, pp. 257-258, 2006.

[25] J. Pillou, «Introducción al cifrado mediante DES,» 12 enero 2008. [En línea]. Available: https://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des.

[26] E. Babbie, «Manual para la práctica de la investigación social.,» Bilbao: Desclée de Brower, pp. 165-6., 1995.

[27] O. Alsmari y H. Mat, Introducing an Encryption Algorithm based on IDEA., Universiti Tenaga Nasional., 2013.

[28] R. Alvarez, «Seguridad en redes,» mayo 2017. [En línea].

[29] Y. Cano, «El rigor científico: Una necesidad de las investigaciones en Ciencias de la Educación.,» Revista Científica Multidisciplinaria, pp. 41-50, 29 agosto 2017.

[30] S. Diajukan y G. Untuk, Analisis perbandingan unjuk kerja algoritma DES, 3DES, AES, blowfish dan twofish pada dokumen, Indonesia: UNIVERSITAS SANATA DHARMA DEKAN, 2019.

[31] A. Mantaut y M. Ruizba, «FIUBA: herramientas de aprendizaje criptográfico,» 26 marzo 2015. [En línea].

[32] F. Martinez, Criptosistemas de cifrado en flujo basados en matrices triangulares con múltiples bloques., 2016.

[33] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, «Informe Belmont. Principios y guías éticas para la protección de los sujetos humanos de investigación.,» 30 mayo 2017.

[34] F. Velasquez, «IMPLEMENTACIONES CRIPTOGRÁFICAS EN FPGA CRYPTOGRAPHIC IMPLEMENTATIONS FOR FPGA,» 12 octubre 2021. [En línea].

[35] E. Fajardo y L. Cervante, «Modernización de la educación virtual y su incidencia en el contexto de las Tecnologías de la Información y la Comunicación (TIC),» Academia y Virtualidad, vol. 13, nº 2, p. 103–116, 2020.

[36] N. Sosa, N. Acosta y N. Balbuena, «Uso de herramientas digitales en tiempos de COVID-19, en la Facultad Politécnica de la UNA,» Revista Paraguaya de Educación a Distancia, FACEN-UNA, vol. 4, nº 1, pp. 60-72, 2023.

[37] L. Cárdenas, H. Martínez y L. Becerra, «Gestión de seguridad de la información: revisión bibliográfica.,» Profesional De La información, vol. 25, nº 6, p. 931–948, 2016.

[38] J. Marín, A. Patiño y J. Acevedo, «Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS,» Revista Universidad Católica de Oriente, vol. 31, nº 45, pp. 84-99, 2020.

[39] P. Castro y L. Moreira, Desarrollo de un prototipo de un sistema de análisis y monitoreo de una red utilizando la herramienta open source SNORT para identificar las vulnerabilidades de la red y brindar seguridad a las conexiones de los diferentes dispositivos finales con servido, Guayaquil: Universidad de Guayaquil, 2021, pp. 1-148.

[40] V. Fernandez y A. Roca, Criptografía simétrica avanzada: diseño y análisis de eficiencia en mejoras avanzadas del estándar de cifrado simétrico DES, Sevilla: Universidad de Sevilla, 2020.

ANEXOS

Anexo 1. Resolución de aprobación del trabajo de investigación

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°2320-2020/FIAU-USS

Pimentel, 17 de noviembre de 2020

VISTOS:

El Acta de reunión N°2610-2020 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida el 12 de noviembre de 2020 mediante oficio N°0237-2020/FIAU-IS-USS de la Dirección de Escuela de INGENIERÍA DE SISTEMAS, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar los temas de las Tesis a cargo de los estudiantes y/o egresados que se detallan en el anexo de la presente Resolución.

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°2320-2020/FIAU-USS

Pimentel, 17 de noviembre de 2020

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes y/o egresados del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción del Tema de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Mario Fernando Ramos Mescol
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

MBA. María Noelia Sialer Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°2320-2020/FIAU-USS

Pimentel, 17 de noviembre de 2020

ANEXO

N°	APELLIDOS Y NOMBRES	TEMA DE TESIS
1	ROJAS GUILLEN REYNALDO FRANCISCO	ANÁLISIS, DISEÑO, IMPLEMENTACIÓN Y MEJORA DE UN SISTEMA INTEGRADO DE TRANSPORTES BAJO LA PLATAFORMA WEB Y ESCRITORIO PARA MEJORAR LA TOMA DE DECISIONES EN LOS PROCESOS DE LA EMPRESA DE TRANSPORTES EL PICAFLOR TOURS S.A.C.
2	CALLIRGOS GUIMAREY BRYAN ALFREDO	MEJORAMIENTO DE IMÁGENES DIGITALES APLICANDO REDES GENERATIVAS ADVERSARIAS PARA FACILITAR LA IDENTIFICACIÓN DE ROSTROS
3	CRUZ MEJIA PERCY JHIN SAMUELITO	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN DE CALIDAD DE GRANO DE CAFÉ UTILIZANDO PROCESAMIENTO DE DIGITAL DE IMÁGENES Y APRENDIZAJE DE MÁQUINA
4	AGUILERA ALVARADO YEISSER FROILAN	EVALUACIÓN DE ARQUITECTURAS TECNOLÓGICAS OPEN SOURCE PARA MEJORAR LA CALIDAD DE SERVICIOS WEB. CASO DE ESTUDIO GRUPO COTLEAR
5	GUZMAN LOPEZ RICARDO ARTURO	EVALUACIÓN DE LA USABILIDAD DE UNA APLICACIÓN MÓVIL DE SOPORTE TÉCNICO UTILIZANDO LA NORMA ISO/IEC 25010
6	CISNEROS ZAPATA CHRISTIAN ANDERSON	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN DE MUSA PARADISIACA PARA EXPORTACIÓN UTILIZANDO PROCESAMIENTO DIGITAL DE IMÁGENES
7	TAPIA LLATAS MANUEL AURELIO	COMPARACIÓN DE TÉCNICAS DE SISTEMAS INMUNES ARTIFICIALES EN LA IDENTIFICACIÓN DE MALWARE
8	TOCTO LOPEZ CHRISTIAN ALEXIS	EVALUACIÓN DEL NIVEL DE SEGURIDAD QUE OFRECEN ALGORITMOS CRIPTOGRÁFICOS EN UNA RED PRIVADA VIRTUAL

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Anexo 2. Fichas técnicas

Se tendrá las fichas técnicas de los tres algoritmos criptográficos seleccionados como

muestra.

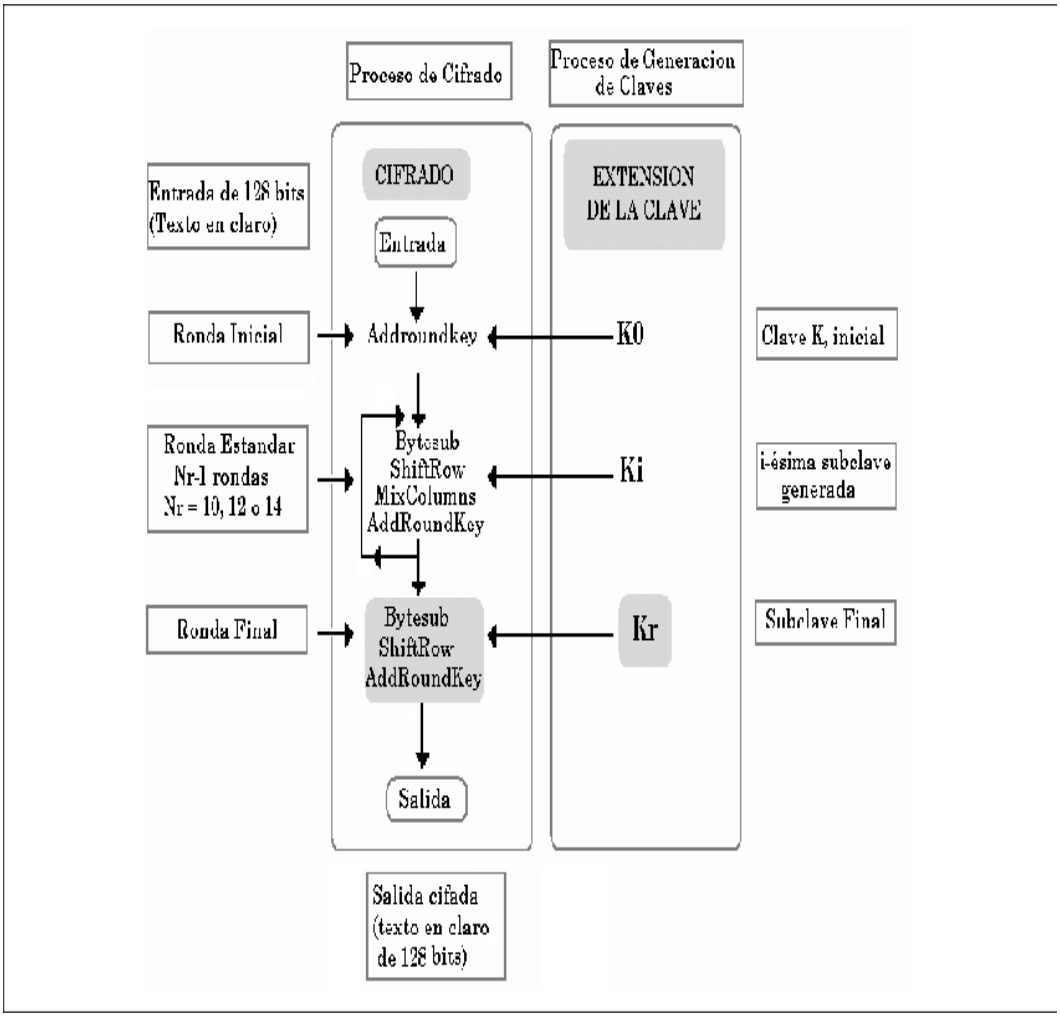
- AES
- DES
- 3DES

A) **Algoritmo AES.**

Ficha técnica del algoritmo AES.

Característica	***Especificaciones básicas***
Arquitectura	El algoritmo AES es un sistema de cifrado simétrico, es decir, utiliza la misma clave tanto para el cifrado como para el descifrado. Además, es un algoritmo de cifrado en bloque que trabaja con bloques de cifrado de 128 bits. La clave puede ser de distintas longitudes, de 128, 192 o 256 bits, y en función de ella el algoritmo realizará un determinado número de rondas correspondiente en orden a las longitudes 10,12,14. AES es un cifrador de bloque iterativo, que realiza varias rondas de cifrado sobre un bloque o matriz de 4x4 bytes llamada estado o state.
Estructura	Etapas: ● SubBytes. Aporta confusión al proceso al realizar una sustitución byte a byte con propiedades óptimas de no linealidad. ● ShiftRows. Introduce difusión de información a la ronda mediante la rotación de las filas del estado. ● MixColumns. Permite un alto nivel de difusión mezclando las columnas entre sí. ● AddRoundKey. Introduce un grado de confusión que depende de la subclave de ronda.

Nota: Ficha técnica del algoritmo AES. Fuente: Elaboración propia.



Esquema del algoritmo AES. Fuente: (Velasquez, 2021)

Apreciación: El proceso de cifrado del algoritmo AES se aplicará cuatro funciones matemáticas invertibles en el texto inicial. Será repetitivo el proceso en Nr-1 veces, conocido también como Ronda Estándar. El resultado final es el texto cifrado.

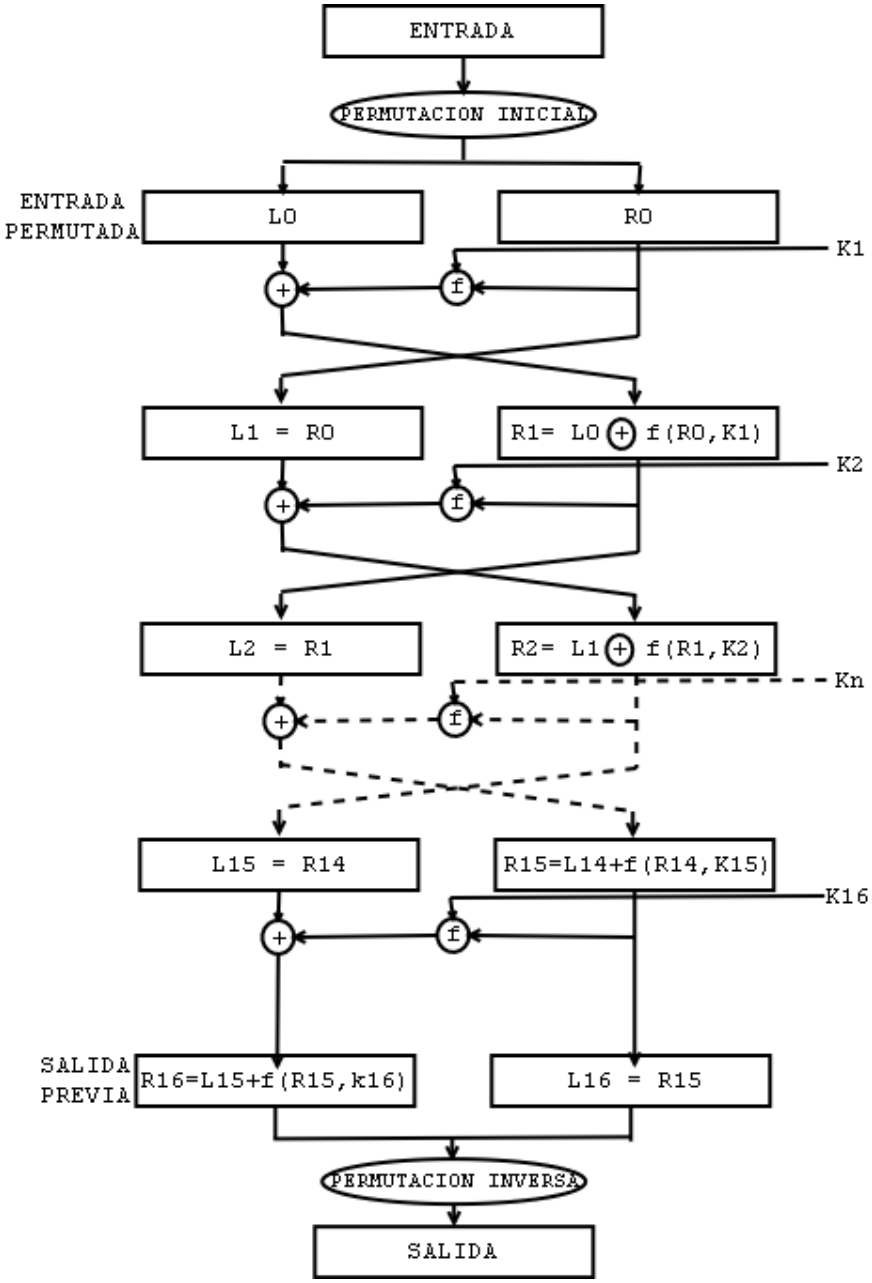
B) **Algoritmo DES**

Ficha técnica del algoritmo DES.

Característica	***Especificaciones básicas***
Arquitectura	DES (Data Encryption Standard) es un esquema de encriptación simétrico. Se basa en un sistema monoalfabético, con un algoritmo de

	cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.
Estructura	PI y PF no son criptográficamente significativas, pero se incluyeron presuntamente para facilitar la carga y descarga de bloques sobre el hardware de mediados de los 70. Antes de las rondas, el bloque es dividido en dos mitades de 32 bits y procesadas alternativamente. Este entrecruzamiento se conoce como esquema Feistel. En la estructura de Feistel las subclaves se aplican en orden inverso cuando desciframos. El resto del algoritmo es idéntico. El símbolo rojo "⊕" representa la operación OR exclusivo (XOR). La función-F mezcla la mitad del bloque con parte de la clave. La salida de la función-F se combina entonces con la otra mitad del bloque, y los bloques son intercambiados antes de la siguiente ronda. Tras la última ronda, las mitades no se intercambian; ésta es una característica de la estructura de Feistel que hace que el cifrado y el descifrado sean procesos parecidos.

Nota: Ficha técnica del algoritmo AES. Fuente: Elaboración propia.



Esquema del algoritmo DES. Fuente: [25]

Apreciación: El algoritmo DES tiene un bloque de entrada de 64 bits, ejecutándolo en permutaciones inicial, como resultado se obtendrá una entrada permutada, esta se divide en dos partes que va de izquierda a derecha con 32 bits, individualmente estas son de 32 bits, a cada parte se le ejecutará un conjunto de transformaciones en 16 rondas. Posteriormente obtendremos una salida que se aplicará una permutación inversa, obteniendo un bloque de cifrado de 64 bits.

C) **3 DES**

Ficha técnica del algoritmo 3 DES.

Característica	***Especificaciones básicas***
Arquitectura	El algoritmo 3DES (Triple Data Encryption Standard), se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES; se basa en aplicarlo tres veces, con tres claves distintas, por lo que resulta mucho más seguro.
Estructura	Realiza principalmente un cifrado en tres pasos bajo lo que se conoces con DES, que sus siglas corresponden al Data Encryption Standard. Se trata en aplicar el cifrado en tres elementos diferentes, con claves completamente distintas para ubicar el sistema de manera permanente. La seguridad de repetir el proceso se debe a que uno de los objetivos bien claros es proporcionar un nivel de seguridad a grandes escalas y medidas. Su velocidad es mucho más elevada en comparación con otros sistemas, siendo hasta cinco o seis veces más ágil en todos los sentidos del desarrollo.

Nota: Ficha técnica del algoritmo 3 DES. Fuente: Elaboración propia.

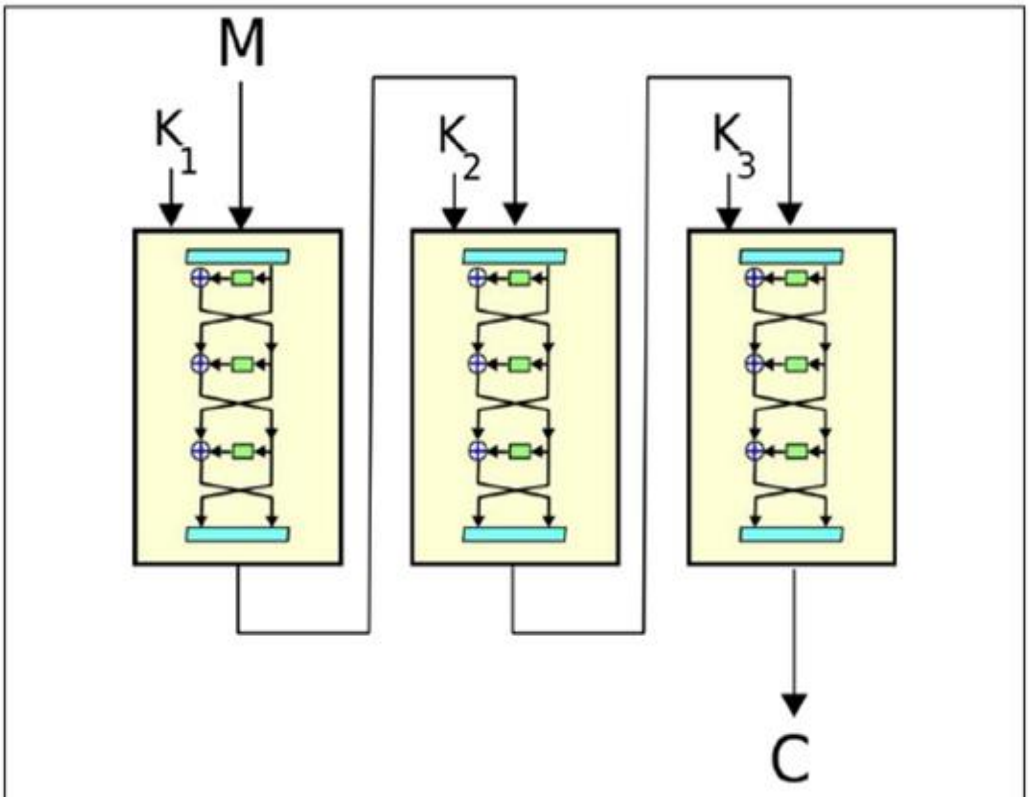


Figura 1 Diagrama del Cifrado por TDES

Esquema del algoritmo 3DES. Fuente: (Álvarez y Montoya, 2020)

Apreciación: El 3 DES no presenta grupos, por tal motivo se puede aplicar reiteradas veces el algoritmo con diferentes claves. Se cifra primero la clave K1, posteriormente la K2 y finalmente se vuelve a cifrar la clave K1. Obteniendo una clave total de longitud de 112 bits.

Anexo 3. Panel Fotográfico

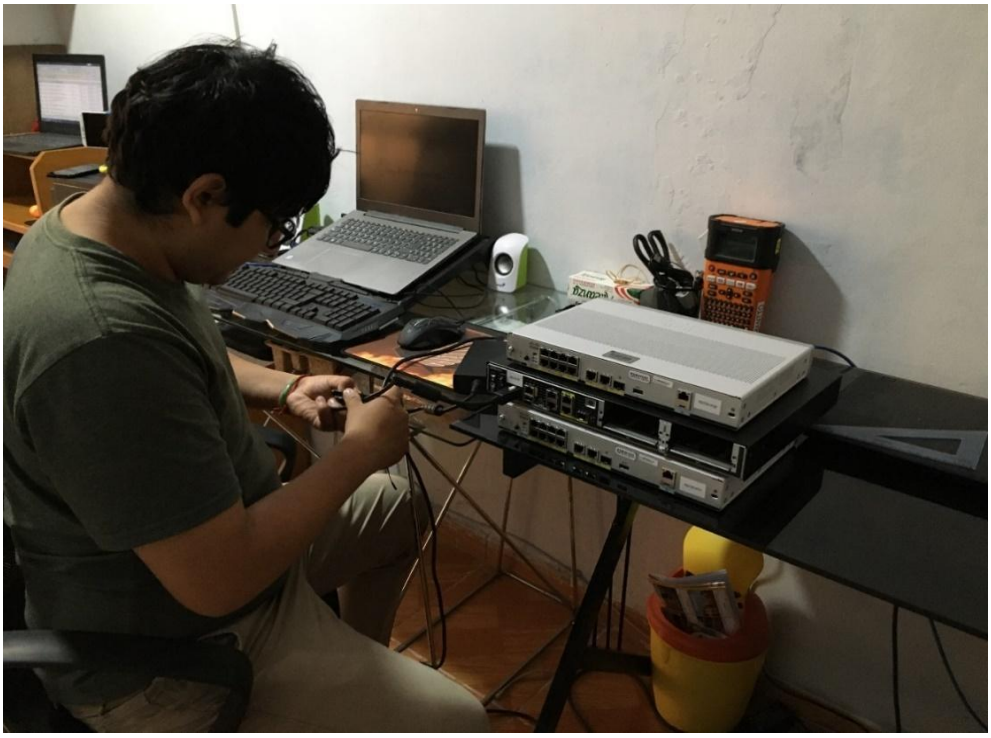


Imagen 1. Organización y conexión de equipos para configuración. Fuente: Elaboración propia (2023).

Imagen 2. Fotografía de Router Cisco C1111-8P (Router CPE01), simulador de Sede01. Fuente: Elaboración propia (2023).

Imagen 3. Fotografía de Router Cisco 1921 (Router PE), simulador de red de un Operador de servicio. Fuente: Elaboración propia (2023).

Imagen 4. Fotografía de tarjeta Hwic, para conexión de servicios de diferentes redes WAN para Router Cisco1921. Fuente: Elaboración propia (2023).

Imagen 5. Fotografía de Router Cisco C1111-8P (Router CPE02), simulador de Sede02.

Fuente: Elaboración propia (2023).

Imagen 6. Fotografía de equipos Simulando Sedes de Conexión de Una Red Privada Virtual y un Proveedor. Fuente: Elaboración propia (2023).

Imagen 7. Fotografía frontal de equipos utilizados para conexión de una Red Privada Virtual.

Fuente: Elaboración propia (2023).

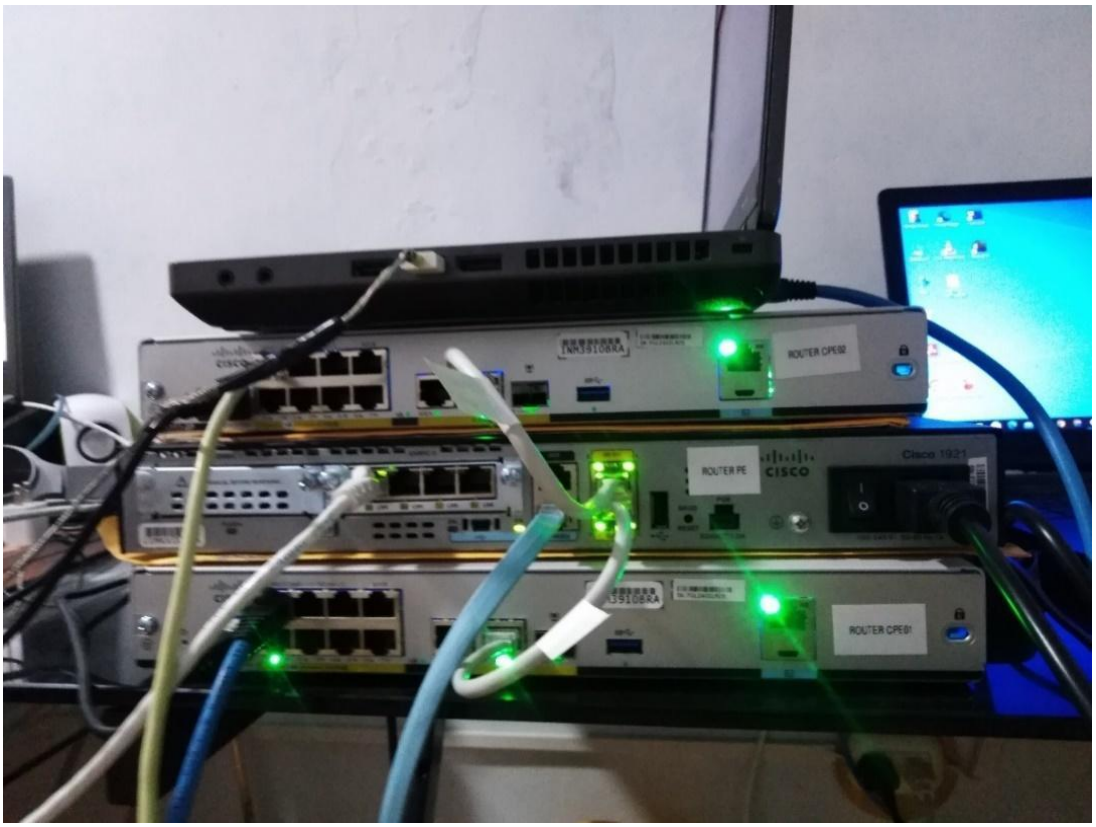


Imagen 8. Fotografía de conexión de equipos utilizados para conexión de una Red Privada Virtual. Fuente: Elaboración propia (2023).

Imagen 9. Fotografía USB to Serial Converter TU-S9. Fuente: Elaboración propia (2023).

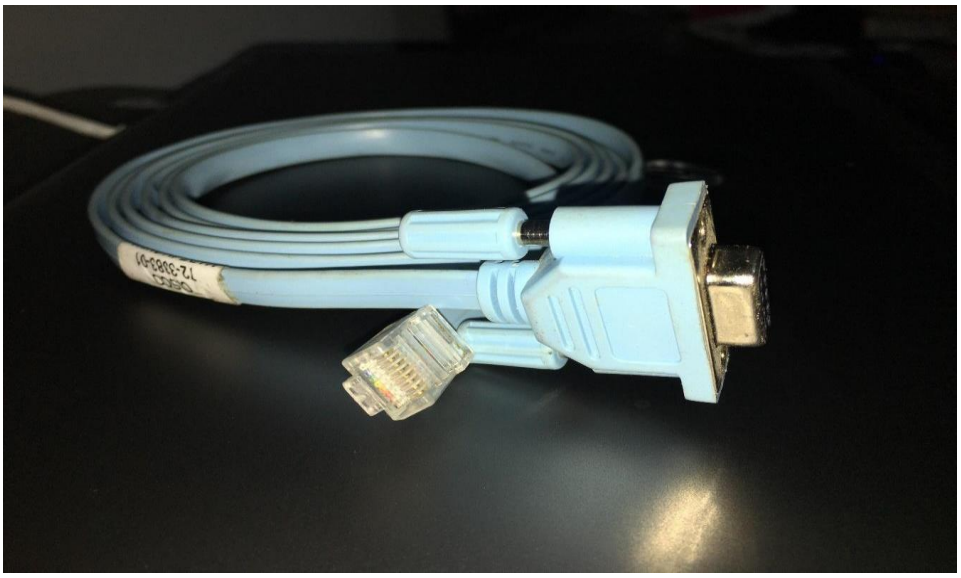


Imagen 10. Fotografía cable consola. Fuente: Elaboración propia (2023).

Anexo 4

Configuración de IPSec en Router.

a) Configuración de acceso router CPE01

```
enable secret cisco
service password-encryption
!
line console 0
session-timeout 10 output
password cisco
logging synchronous
!
line vty 0 4
session-timeout 10 output
logging synchronous
transport input all
access-class 25 in
password cisco
!
service timestamps log datetime localtime
service timestamps debug datetime msec
service timestamps log datetime msec
logging buffered 9000 debugging
service datetime localtime
service timestamps debug
clock timezone GMT –5
!
```

```
no service tcp-small-servers
no service udp-small-servers
no ip source-route
no ip bootp server
no service finger
no ip http server
no ip finger
!
```

b) Configuración interface y VLAN router CPE01

```
interface GigabitEthernet0/0/0
description Interface WAN ROUTER_CPE01
no ip address
no ip directed-broadcast
load-interval 30
no ip unreachables
no ip redirects
no ip proxy-arp
no negotiation auto
duplex full
speed 1000
media-type rj45
no shutdown
!
interface GigabitEthernet0/0/0.10
description Interface WAN | Conexion ROUTER_PE
encapsulation dot1Q 100
ip address 10.15.10.2 255.255.255.252
```

```
no ip directed-broadcast
no ip unreachables
no ip redirects
no ip proxy-arp
!
interface Vlan1
description Interface LAN ROUTER_CPE01
ip address 192.168.0.1 255.255.255.0
no ip directed-broadcast
load-interval 30
no ip unreachables
no ip redirects
no ip proxy-arp
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 10.15.10.1 name Gateway_PE
!
access-list 25 permit 10.15.10.1
```

c) Enrutamiento con EIGRP CPE01

```
router eigrp 100
network 10.15.10.0 0.0.0.3
network 192.168.0.0
network 192.168.1.0
exit
```

d) Configuración de IPSEC-3DES router CPE01

```
!
license boot level securityk9
!
exit
!
wr
!
reload
!
access-list 110 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
!
crypto isakmp policy 10
encryption 3des
authentication pre-share
group 2
exit
!
crypto isakmp key cisco address 10.15.11.2
!
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to ROUTER_CPE02
set peer 10.15.11.2
set transform-set VPN-SET
match address 110
exit
!
interface GigabitEthernet0/0/0.10
```

crypto map VPN-MAP

!

- Configuración en router 2

a) Configuración de acceso router CPE02

enable secret cisco

service password-encryption

!

line console 0

session-timeout 10 output

password cisco

logging synchronous

!

line vty 0 4

session-timeout 10 output

logging synchronous

transport input all

access-class 25 in

password cisco

!

service timestamps log datetime localtime

service timestamps debug datetime msec

service timestamps log datetime msec

logging buffered 9000 debugging

service datetime localtime

service timestamps debug

clock timezone GMT –5

!

no service tcp-small-servers

no service udp-small-servers

no ip source-route

no ip bootp server

no service finger

no ip http server

no ip finger

!

Exit

b) Configuración interface y VLAN router CPE02

interface GigabitEthernet0/0/0

description Interface WAN ROUTER_CPE02

no ip address

no ip directed-broadcast

load-interval 30

no ip unreachables

no ip redirects

no ip proxy-arp

no negotiation auto

duplex full

```
speed 1000
media-type rj45
no shutdown
!
interface GigabitEthernet0/0/0.10
description Interface WAN | Conexion ROUTER_PE
encapsulation dot1Q 200
ip address 10.15.11.2 255.255.255.252
no ip directed-broadcast
no ip unreachables
no ip redirects
no ip proxy-arp
!
interface Vlan1
description Interface LAN ROUTER_CPE02
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
load-interval 30
no ip unreachables
no ip redirects
no ip proxy-arp
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 10.15.11.1 name Gateway_PE
!
access-list 25 permit 10.15.11.1
```

c) Enrutamiento con EIGRP

```
router eigrp 100
network 10.15.10.0 0.0.0.3
!
network 10.15.11.0 0.0.0.3
network 192.168.0.0
network 192.168.1.0
exit
```

d) Configuración de IPSEC-3DES router CPE02

```
!
license boot level securityk9
!
wr
!
exit
!
reload
!
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
!
crypto isakmp policy 10
encryption 3des
authentication pre-share
group 2
exit
```

!

crypto isakmp key cisco address 10.15.10.2

!

crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to ROUTER_CPE02

set peer 10.15.10.2

set transform-set VPN-SET

match address 110

exit

!

interface GigabitEthernet0/0/0

crypto map VPN-MAP

!

- Configuración en router 3

a) Configuración de acceso router PE

enable secret cisco

service password-encryption

!

line console 0

session-timeout 10 output

password cisco

logging synchronous

!

line vty 0 4

session-timeout 10 output

logging synchronous

transport input all

access-class 25 in

password cisco

!

service timestamps log datetime localtime

service timestamps debug datetime msec

service timestamps log datetime msec

logging buffered 9000 debugging

service datetime localtime

service timestamps debug

clock timezone GMT –5

!

no service tcp-small-servers

no service udp-small-servers

no ip source-route

no ip bootp server

no service finger

no ip http server

no ip finger

!

exit

b) Configuración interface y VLAN ROUTER PE

interface GigabitEthernet0/0/0

description Interface WAN ROUTER_CPE01

no ip address

no ip directed-broadcast

load-interval 30

no ip unreachables

no ip redirects

no ip proxy-arp

no negotiation auto

duplex full

speed 1000

media-type rj45

no shutdown

!

interface GigabitEthernet0/0/0.10

description Interface WAN | Conexion ROUTER_CPE01

encapsulation dot1Q 100

ip address 10.15.10.1 255.255.255.252

no ip directed-broadcast

no ip unreachables

no ip redirects

no ip proxy-arp

!

interface GigabitEthernet0/0/1

description Interface WAN ROUTER_CPE02

no ip address

no ip directed-broadcast

load-interval 30

no ip unreachables

no ip redirects

no ip proxy-arp

no negotiation auto

```
duplex full
speed 1000
no shutdown
!
interface GigabitEthernet0/0/1.10
description Interface WAN | Conexion ROUTER_CPE02
encapsulation dot1Q 200
ip address 10.15.11.1 255.255.255.252
no ip directed-broadcast
no ip unreachables
no ip redirects
no ip proxy-arp
!
interface Vlan1
description Interface LAN ROUTER_PE
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
load-interval 30
no ip unreachables
no ip redirects
no ip proxy-arp
no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.15.10.2 name Gateway_CPE01
ip route 0.0.0.0 0.0.0.0 10.15.11.2 name Gateway_CPE02
!
access-list 25 permit 10.15.10.1
access-list 25 permit 10.15.11.1
```

c) Enrutamiento con EIGRP ROUTER PE

router eigrp 100

network 10.15.10.0 0.0.0.3g

network 10.15.11.0 0.0.0.3

network 192.168.0.0

network 192.168.1.0

exit

Anexo 5. Valoración de los algortimos

Escala de valoración						
Descripción	Valor	Longitud de la onda	Tiempo de envío	Paquetes encapsulados	Paquetes desencapsulados	# Paquetes generados
Muy bueno	5	128-256 bits	5- 9 segundos	89,00>	89,00>	196,00-146,00
Bueno	4	112-127 bits	10-14 segundos	119,00-90,00	119,00-90,00	247,00-197,00
Ni bueno ni malo	3	30-56 bits	15-18 segundos	149,00-120,00	149,00-120,00	298,00-248,00
Malo	2	10-29 bits	19-24 segundos	179,00-150,00	179,00-150,00	349,00-299,00
Muy malo	1	0-9 bits	25 segundos <	200,00-180,00	200,00-180,00	400,00-350,00

BASE DE DATOS						
	Longitud de onda	Tiempo de envío	Paquetes encapsulados	Paquetes desencapsulados	#Paquetes generados	Total
AES	5	4	5	2	5	21
DES	3	4	2	5	4	18
3DES	4	3	3	2	2	14

NOMBRE DEL TRABAJO

TOCTO LOPEZ CHRISTIAN ALEXIS- turnitin.docx

AUTOR

Christian Tocto

RECUENTO DE PALABRAS

7184 Words

RECUENTO DE CARACTERES

38962 Characters

RECUENTO DE PÁGINAS

49 Pages

TAMAÑO DEL ARCHIVO

3.1MB

FECHA DE ENTREGA

Aug 13, 2024 5:37 PM GMT-5

FECHA DEL INFORME

Aug 13, 2024 5:38 PM GMT-5

13% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 12% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 9% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)