UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIEROS EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

APLICACIÓN DE LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN, PARA EL MANEJO DE LA INFORMACIÓN EN REDES DE DATOS, AÑO 2023.

AUTORES:

ERIK ADRIAN CHELA HINOJOZA
JHORDAN PABLO UTITIAJA KATAN

DIRECTOR:

ING. RODRIGO DEL POZO DURANGO.

GUARANDA – ECUADOR
2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

APLICACIÓN DE LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN, PARA EL MANEJO DE LA INFORMACIÓN EN REDES DE DATOS, AÑO 2023.

AGRADECIMIENTO

Con gratitud eterna a Dios, mi creador, por permitirme culminar esta etapa significativa en mi vida. También deseo expresar mi agradecimiento a mis padres, hermanas y demás miembros de mi familia, cuyo apoyo invaluable y contribución han sido esenciales para hacer realidad este sueño.

Quiero extender mi reconocimiento a la Universidad Estatal de Bolívar ya la Escuela de Sistemas, así como a todos los profesores que la integran. Han compartido generosamente su sabiduría y experiencias conmigo. Mi director, el Ing. Rodrigo Humberto Del Pozo Durango, y mis pares académicos, el Ing. Danilo Barreno y Ing. Henry Albán, mi agradecimiento total por brindarme la orientación necesaria en este trabajo de titulación.

Asimismo, agradezco a todos mis amigos por los momentos y experiencias inolvidables que hemos compartido; Estos recuerdos siempre estarán presentes en mi corazón.

Jhordan Utitiaja

En primer lugar, quiero expresar mi profundo agradecimiento a Dios, fuente de fortaleza y guía constante en mi vida. A mis padres por su apoyo inquebrantable y sacrificio incansable han forjado el camino hacia este logro académico. A mi adorada esposa por su apoyo constante, a mi querido hijo, mi mayor inspiración, por ser mi razón para superar obstáculos y perseverar. Les agradezco desde lo más profundo de mi corazón por hacer de este logro una realidad

También agradezco a mi director de tesis Ing. Rodrigo Humberto Del Pozo Durango y a nuestros pares académicos Ing. Henri Alban y al Ing. Danilo Barreno por su guía y orientación durante todo el proceso, por su paciencia y dedicación en cada fase del proyecto, y por su valiosa contribución en la elaboración de este documento.

Adrian Chela

DEDICATORIA

Dedico este proyecto en primer lugar a Dios, quien ha sido la fuerza motriz de mi vida y me ha proporcionado la determinación necesaria para seguir avanzando a pesar de los desafíos que se enfrenta en mi camino. También, quiero expresar mi gratitud hacia mis padres, Pablo Utitiaja y Margarita Katan, por su confianza inquebrantable, apoyo incondicional y por haber sido un pilar fundamental a lo largo de todos estos años.

A mis queridas hermanas y hermanos, quienes siempre han estado a mi lado y han demostrado que el amor y la importancia que sentimos por las personas que amamos no se ven afectados por la distancia. Del mismo modo, a mis sobrinos, a mi hijo y a mi mujer quienes han sido una constante fuente de inspiración y felicidad en mi vida.

Jhordan Utitiaja

Con un corazón lleno de emoción, dedico este logro significativo primeramente a Dios por guiarme y a toda mi familia a mis padres y hermanos que han estado a mi lado en cada paso de este arduo camino, brindándome aliento, acompañamiento y sus valiosos consejos que me han impulsado a avanzar día tras día. A mi hijo Nayri y mi esposa, mi apoyo inquebrantable, les agradezco desde lo más profundo de mi ser, ustedes han sido mi motor fundamental, mi razón para perseverar. A mis apreciados docentes, este logro es el fruto de sus enseñanzas y orientación, y se lo dedico con gratitud.

Finalmente, quiero dedicar este hito a mí mismo como un recordatorio de que en la vida, los obstáculos y fracasos son inevitables, pero solo uno mismo tiene el poder de decidir si seguir adelante. Este logro representa la prueba de que todo es posible y nada es inalcanzable en esta vida.

Adrian Chela

CERTIFICADO DE VALIDACIÓN

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Rodrigo Del Pozo, Ing. Danilo Barreno e Ing. Henry Albán, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "APLICACIÓN DE LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN, PARA EL MANEJO DE LA INFORMACIÓN EN REDES DE DATOS, AÑO 2023" desarrollado por los señores Utitiaja Katan Jhordan Pablo y Chela Hinojoza Erik Adrian.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamossu presentación y defensa.

Guaranda, 5 de febrero del 2024

Firmado electrónicamente por: RODRIGO HUMBERTO DEL POZO DURANGO

Ing. Rodrigo Del Pozo
Director

DANILO GEOVANNY BARRENO NARANJO
Firmado digitalmente por DANILO GEOVANNY BARRENO NARANJO
Fecha: 2024.02.05 17:18:10 -05'00'

Ing. Danilo Barreno
Par Académico

Firmado electrónicamente por: EDGAR HENRY ALBAN YANEZ

Ing. Henry Albán
Par Académico

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

DERECHOS DE AUTOR

DERECHOS DE AUTOR

Nosotros, **Jhordan Pablo Utitiaja Katan y Erik Adrian Chela Hinojoza** portadores de las cédulas de identidad **N° 1401164346** y **0202486312** respectivamente**,** en calidad de autores y titulares de los derechos morales y patrimoniales del Trabajo de Titulación: **APLICACIÓN DE LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN, PARA EL MANEJO DE LA INFORMACIÓN EN REDES DE DATOS, AÑO 2023,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Los autores declaran que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Nombre: JHORDAN PABLO UTITIAJA KATAN
Emitido por: UANATACA CA2 2016
Lugar: Guaranda, Ecuador
Fecha: 6/2/24

Jhordan Pablo Utitiaja Katan
CI. 1401164346

Nombre: ERIK ADRIAN CHELA HINOJOZA
Emitido por: UANATACA CA2 2016
Lugar: Guaranda, Ecuador
Fecha: 6/2/2024

Erik Adrian Chela Hinojoza
CI. 0202486312

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El presente proyecto de investigación, titulado " Aplicación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos, año 2023", surge en respuesta al cambiante panorama tecnológico de este año. En este contexto, la gestión segura de la información en redes de datos se ha convertido en un imperativo tanto para empresas como para instituciones y usuarios en general, cada vez es mayor la interconexión de dispositivos y la expansión de la digitalización han dado origen a un vasto ecosistema de datos que fluye constantemente a través de las redes y que posee un valor crítico y altamente sensible, en consecuencia, la seguridad de la información se sitúa en el centro de las preocupaciones. El proyecto se desarrolló utilizando diferentes metodologías tales como: investigación documental, que se caracteriza por la búsqueda, procesamiento y almacenamiento de la información contenida en los documentos; investigación descriptiva, que se caracteriza por la observación y recopilación datos sobre un tema determinado sin intentar inferir relaciones de causa y efecto; y la investigación experimental, se caracteriza por la manipulación deliberada de una o más variables independientes para evaluar su efecto sobre una o más variables dependientes, mientras se controlan cuidadosamente las variables extrañas y se utilizan métodos de asignación aleatoria para garantizar la validez interna.

En este escenario, la encriptación emerge como una herramienta fundamental para garantizar la seguridad de los datos, ya sea en tránsito o en reposo. La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información se presenta como un requisito esencial. Por tanto, el propósito primordial de este proyecto consiste en investigar y elaborar un manual de las mejores prácticas de encriptación para el manejo de la información en redes de datos.

El presente proyecto de investigación está estructurado por los siguientes capítulos:

Capítulo I: Se enfoca en la formulación general del proyecto, donde se presenta la problemática actual a tratar en relación a la aplicación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos. Además, se expone

la justificación, detallando los motivos, aportes y beneficios que se esperan obtener a partir del desarrollo del proyecto. Otro punto abordado son los objetivos específicos, conjuntamente con el objetivo general.

Capítulo II: Corresponde al marco teórico, el cual incluye los antecedentes de trabajos previos al desarrollo del proyecto investigativo, así como las bases científicas, conceptuales y legales sobre las que se fundamenta el proyecto, que nos permiten conocer ampliamente esta problemática.

Capítulo III: Presenta la metodología, donde se especifica y se describen las técnicas e instrumentos de recopilación de datos empleados para llevar a cabo el proyecto, el cual consta de cuatro etapas documentación teórica, simulación, aplicación ficha de observación y la obtención de resultados.

Capítulo IV: Corresponde a los resultados y discusión, se formaliza mediante el análisis, interpretación y discusión de los resultados recopilados mediante la ficha de observación.

Capítulo V: Se enfoca a la propuesta, se elabora un manual con las mejores prácticas de encriptación, que permitirá a las empresas, organizaciones, instituciones y persona contar con una guía para seleccionar las mejores prácticas de encriptación apropiadas y garantizar la protección de la información.

Finalmente, se presentan las conclusiones, recomendaciones y anexos, en los cuales se describen los resultados obtenidos tras el desarrollo del proyecto.

RESUMEN

El presente trabajo de titulación se planteó como objetivo principal, la implantación las mejores prácticas de encriptación en redes de datos. Para ello, se empleó la técnica de la observación con el fin de identificar las fortalezas y debilidades de diversas técnicas de encriptación, lo que resultó en la elaboración de un manual de mejores prácticas. Este manual brindará orientación a empresas, organizaciones, instituciones y personas para la elección adecuada de técnicas de encriptación y así garantizar la protección de la información. La metodología empleada se basó en un enfoque cualitativo y en técnicas de recopilación de datos, como la ficha de observación. Se realizaron simulaciones de ataques a técnicas de encriptación como AES, DES y 3DES, lo que reveló diferencias significativas en términos de seguridad, velocidad, gestión de claves y cumplimiento normativo. En resumen, se destacó que AES es uno de los algoritmos más seguros y ampliamente utilizado para la protección de la privacidad y la seguridad de los datos, en contraste con DES, que es menos seguro, pero ofrece una velocidad moderada. Como resultado, se concluyó que el algoritmo más adecuado es AES, debido a su mayor seguridad y eficiencia en comparación con otros algoritmos. La elección adecuada de algoritmos de criptografía desempeña un papel esencial en la mejora de la selección de la seguridad de un sistema, previniendo posibles vulnerabilidades en los datos. Este enfoque contribuye de manera efectiva a fortalecer la seguridad de la información y salvar la privacidad de manera integral.

Palabras clave: AES, Encriptación, Seguridad informática, Ataque informático.

ABSTRACT

The main objective of this degree work was to implement the best encryption practices in data networks. To this end, the observation technique was used to identify the strengths and weaknesses of various encryption techniques, which resulted in the development of a manual of best practices. This manual will provide guidance to companies, organizations, institutions and individuals for the appropriate choice of encryption techniques and thus ensure the protection of information. The methodology used was based on a qualitative approach and data collection techniques, such as the observation sheet. Simulations of attacks on encryption techniques such as AES, DES and 3DES were carried out, revealing significant differences in terms of security, speed, key management and regulatory compliance. In summary, it was highlighted that AES is one of the most secure and widely used algorithms for privacy protection and data security, in contrast to DES, which is less secure, but offers moderate speed. As a result, it was concluded that the most suitable algorithm is AES, due to its higher security and efficiency compared to other algorithms. The proper choice of cryptographic algorithms plays an essential role in improving the security screening of a system, preventing potential data vulnerabilities. This approach effectively contributes to strengthening information security and saving privacy in a comprehensive manner.

Palabras clave: AES, Encryption, Computer security, Computer attack.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

El presente proyecto se desarrolló como un caso de investigación que se enfoca en la aplicación de las mejores prácticas de encriptación para el manejo de la información en redes de datos, esto se justifica por el aumento de amenazas cibernéticas que comprometen la privacidad y la integridad de los datos que circulan en la red, exponiéndolos a diferentes tipos de ataques informáticos, como la suplantación de identidad, la falsificación de documentos y la destrucción de la información.

Se cree que el problema radica en que muchas organizaciones, empresas e instituciones no aplican correctamente las mejores prácticas de encriptación en la gestión de la información en redes de datos, lo que las vuelve vulnerables a los ataques cibernéticos y al robo de información sensible. Además, se estima que existe una falta de conciencia acerca de la importancia de la encriptación de datos y una comprensión limitada de las diferentes técnicas de encriptación y su aplicación en distintos entornos. Por lo tanto, es fundamental que las organizaciones, empresas e instituciones apliquen las mejores prácticas de encriptación, para el manejo de la información en redes de datos y tomen medidas preventivas, adecuadas para proteger los datos.

En la actualidad, las brechas de seguridad de datos representan un costo significativo para las empresas en todo el mundo. Según el informe de (Ponemon Institute, 2020), el costo promedio global de una brecha de seguridad de datos fue de $3.86 millones de dólares. Además, el 95% de los ataques cibernéticos se debe a errores humanos, como la falta de capacitación en seguridad y la introducción de contraseñas débiles.

Por otro lado, los ataques de phishing también son una amenaza constante para las empresas. En el año 2020, el 46% de las empresas experimentaron algún tipo de ataque de phishing. (Proofpoint, 2020)

Los impactos derivados de una brecha de seguridad de datos pueden resultar devastadoras para las organizaciones. Según un informe de (IBM,2019), el 60% de las organizaciones que experimentaron una violación de datos no pudieron recuperarse y cerraron dentro de los seis meses posteriores al incidente.

Ante esta situación, cada vez más organizaciones están implementando medidas de seguridad para proteger sus datos. De acuerdo con un informe del (Ponemon Institute, 2020), el 67% de las organizaciones encuestadas informaron que estaban implementando la encriptación de datos para cumplir con las regulaciones gubernamentales y de la industria.

En la actualidad, la mayoría de las empresas, organizaciones, instituciones y personas confían en las redes de comunicación para transmitir información crítica y sensible, como datos financieros, de salud y personales, por lo tanto, la protección de esta información se ha vuelto más crítica que nunca.

1.2. Formulación del Problema

¿Cuál es la eficacia de la implementación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos, y cómo contribuyen a garantizar la seguridad y la privacidad de los datos transmitidos?

1.3. Preguntas de Investigación

- ¿Cuáles son las mejores prácticas efectivas para la encriptación de información en redes de comunicación?
- ¿Cuáles son los algoritmos de encriptación más utilizados en el año 2023 para proteger la información en las redes de datos?
- ¿Cómo se puede demostrar el uso de las mejores prácticas de encriptación (algoritmo y protocolos) en una simulación dentro de una institución de Educación Superior?

1.4. Justificación

Este proyecto surge por la necesidad de que las empresas, organizaciones e instituciones y personas conozcan sobre la importancia de la aplicación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos. A medida que la tecnología avanza, la cantidad de información que se transmite a través de las redes se incrementa exponencialmente y con ello aumenta también la vulnerabilidad de los datos a ataques cibernéticos y robos de información confidencial, por lo tanto la seguridad de la información es una de las principales preocupaciones en la actualidad debido a la gran cantidad de ataques cibernéticos que se presentan constantemente, ya que las empresas e instituciones manejan información confidencial, lo que las hace vulnerables a estos ataques y a la exposición de información privada.

En este sentido, el uso de mejores prácticas de encriptación es una de las principales medidas para garantizar la seguridad de la información en redes de comunicaciones. La encriptación permite proteger la información confidencial a través del uso de algoritmos matemáticos que codifican los datos, de manera que sólo puedan ser leídos por los destinatarios autorizados.

Se enfocará en conocer las diferentes técnicas de encriptación empleadas en la actualidad y determinar su eficacia en términos de seguridad y protección de la información, de esta forma, se busca identificar las fortalezas y debilidades de cada uno de estos mecanismos y proponer mejoras o alternativas que permitan garantizar una mayor seguridad en la transmisión de información.

El resultado de esta investigación permitirá a las empresas e instituciones contar con una guía para seleccionar las mejores prácticas de encriptación apropiadas y garantizar la protección de la información que manejan. Además, contribuirá a la generación de conocimiento en el campo de la seguridad de la información en redes de comunicaciones y a la identificación de nuevas tendencias y herramientas que permitan mejorar la protección de la información, la presente investigación es relevante para la seguridad de la información en el entorno

empresarial e institucional y contribuirá a mejorar la protección de la información y la privacidad.

Finalmente, el proyecto de investigación planeado aporta a las líneas de investigación de la carrera Ingeniería de Software, Redes y Telecomunicaciones y a la sub línea Pruebas y aseguramiento de la calidad del software, redes y telecomunicaciones.

1.5. Objetivos

General

Aplicar las mejores prácticas de encriptación, para el manejo de la información en redes de datos, año 2023.

Específicos

- Analizar las diferent**es** técnicas de encriptación (algoritmos y protocolos) para redes de datos.
- Demostrar con una simulación el uso de las mejores prácticas de encriptación (algoritmos y protocolos) dentro de una institución de educación superior.
- Elaborar el manual con las mejores prácticas de encriptación.

1.6. Idea a Defender

La aplicación de las mejores prácticas de encriptación para el manejo de la información mejorará la confidencialidad, disponibilidad, seguridad y privacidad de los datos transmitidos, generando confianza en las redes y cumpliendo con las regulaciones y estándares relacionados con la protección de datos**.**

1.7. Variables

Variable independiente: Aplicación de las mejores prácticas de encriptación (algoritmos y protocolos).

Variable dependiente: Confidencialidad, integridad y disponibilidad de la información en redes de datos.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

A continuación, se exponen los aspectos teóricos relacionados con la autoría, especialmente sobre la aplicación de mejores prácticas de encriptación para el manejo la información en redes de datos, permitiendo establecer los conocimientos fundamentales para el desarrollo de la investigación.

Un primer trabajo corresponde a (Gutiérres, 2020), quien realizó una publicación académica acerca de la Encriptación de Datos: Una Guía Para Buenas Prácticas de Seguridad. Esta publicación fue realizada con el propósito de resaltar la importancia de mantener actualizado en el ámbito de la seguridad digital, dado que este campo está en constante evolución. Mantenerse al día en esta materia resulta esencial para prevenir posibles ataques maliciosos que puedan afectar tanto a usted como a su negocio. A medida que los ciberataques y las infracciones se vuelven comunes, es más importante que nunca proteger tanto la computadora de su empresa como la suya propia. La encriptación de datos moderna es el último modo de protección de datos en una larga línea de prácticas. Es una forma de criptografía, una técnica antigua de ofuscación de información donde se sustituye una letra por otra.

Un segundo trabajo de (Ahn et al, 2022), menciona que proporciona una revisión exhaustiva de las vulnerabilidades causadas por los ataques de computación cuántica, las posibles estrategias de defensa y los desafíos restantes para las redes DER. Primero, se exploran nuevas vulnerabilidades de seguridad y modelos de ataque de los sistemas DER ciberfísicos causados por ataques de computación cuántica. Además, este documento presenta posibles estrategias de defensa contra ataques cuánticos, incluida la distribución de claves cuánticas (QKD) y la criptografía poscuántica (PQC), que se pueden aplicar a las redes DER y evalúa las estrategias de defensa.

Un tercer trabajo corresponde a (Pacheco, 2022), en donde se destaca que la seguridad en las redes de datos permite la interconexión entre diferentes sistemas finales. Esto implica no solo a equipos de comunicaciones, sino también a los medios físicos por donde se transporta la información digital. Además, se resalta que las técnicas de protección utilizadas en la actualidad no se limitan únicamente a mecanismos defensivos. Por lo tanto, esta editorial no se enfocará únicamente en una perspectiva de seguridad de la información o ciberseguridad, sino que buscará una sinergia entre ambas. Independientemente de los métodos en el área de las Tecnologías de la Información (TI), el objetivo es mantener la confidencialidad, disponibilidad e integridad de los datos.

Un cuarto trabajo corresponde a (Carrillo, 2022), en donde menciona que el incremento del uso del servicio de internet y conectividad entre agencias mediante una red de datos ha ocasionado que la disponibilidad de los servicios se mantenga en un porcentaje alto, perder conectividad o presentar intermitencias, llevará consigo una pérdida económica de los clientes corporativos, quienes al tener bajos recursos o no aplicar de manera adecuada las políticas y técnicas de seguridad no logran proteger sus redes internas de manera adecuada frente a ciberataques. Esto ocasiona inconvenientes a los ISP (Proveedores del Servicio de Internet) que se ven obligados a tomar acciones para mitigar la afectación en sus enlaces. Por lo que, resulta importante, que se apliquen un conjunto de buenas prácticas de seguridad tanto en clientes como en el ISP para mantener la comunicación activa.

2.2. Científico

ISO / IEC 27000: Es una guía que ayuda a las organizaciones a gestionar los riesgos de seguridad de la información desde su identificación hasta su monitoreo y mantenimiento, para garantizar que los datos sensibles de la organización, como información financiera, intelectual, personal y de comportamiento, estén protegidos adecuadamente, tanto si son datos de la propia organización como si son datos de terceros. La norma ISO 27000 ayuda a las organizaciones a establecer y mantener prácticas efectivas de seguridad de

la información para proteger sus activos críticos y reducir los riesgos de seguridad. (Blandonnet, 2018)

ISO 27001: es una norma internacional emitida por la Organización Internacional de Normalización (ISO). Esta se basa en la teoría de gestión de calidad, o por sus siglas en inglés PDCA (Plan, Do, Check, Act. Planificar, Hacer, Verificar, Actuar en español) y describe cómo gestionar la seguridad de la información en una empresa para la mejora continua de los sistemas de información y garantizar la ciberseguridad de los activos de información. La filosofía que rige a esta norma es la investigación de los riesgos para la futura creación de un plan de tratamiento adecuado.

Es una norma que especifica los controles necesarios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, o ISMS por sus siglas en inglés (Information Security Management System), dentro del contexto de la organización. Los requisitos de la norma son de carácter genérico y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

La ISO 27001 es una forma de seguridad de información. Entendiendo esto último como las medidas preventivas de resguardo de información de sistemas. Esto quiere decir que busca mantener la confidencialidad e integridad de los datos, independientemente de su formato.

Las buenas prácticas de gestión de seguridad de la información y cumplimiento de los controles establecidos por la ISO 27001 produce ventajas esenciales para una empresa. Los mismos los veremos a continuación:

Minimización de riesgos: Se disminuye la posibilidad de sufrir un incidente que comprometa la información de la organización. Esto mediante la evaluación de riesgos que permite conocer las vulnerabilidades y a partir de allí, tomar las acciones correctivas para dar paso a la continuidad del negocio.

Algunos riesgos que se evitan o minimizan con la ISO 27001 son: obtención de datos privados del usuario o la organización, hackeo a sistemas y ataques financieros. Dicho de otra forma, promueve la ciberseguridad.

Aumento de confianza: El contar con esta certificación genera mayor confianza en clientes, proveedores y otras entidades. Además de proteger a la organización de ciberataques, al seguir los pasos de certificación, se demuestra que la misma es confiable, responsable y capaz.

Incremento de reputación: El cumplimiento de esta norma proyecta una imagen de profesionalidad que genera cada vez mayor y mejor reputación.

Reducción de costos: El cumplimiento de esta norma evita multas muy costosas de incumplimiento de leyes de protección de información personal y datos personales. De esta misma forma reduce la necesidad de realizar auditorías constantes, generando una única auditoría de certificación.

Facilitación de la continuidad de negocio: Mediante el correcto tratamiento de riesgos, la norma ISO 27001 permite una mejor gestión de continuidad del negocio al dar paso a la mitigación de amenazas que comprometan la seguridad de información o den paso a disponibilidad de la información a ciber atacantes. (Martinez, 2022)

Encriptación

De acuerdo el autor (Urrutia, 2020), la encriptación o cifrado de archivos es lo que se conoce como el proceso que toma cierta información que tenga sentido y la codifica de forma que no pueda ser interceptada mientras se encuentra a través de la web.

Según el autor (Encriptación, 2019), la encriptación es un procedimiento de seguridad que consiste en la alteración, mediante algoritmos, de los datos que componen un archivo. El objetivo es hacer que dichos datos se vuelvan ilegibles en caso de que un tercero los intercepte.

La encriptación es un recurso muy utilizado hoy en día para garantizar una transferencia segura de datos y documentos. Si bien no se puede garantizar que

no se sustraiga información sensible, sí puede evitar que se utilice para el perjuicio de sus dueños legítimos.

ISO/IEC 27002: Proporciona pautas para la gestión de riesgos de seguridad de la información, la selección y aplicación de controles de seguridad, y la implementación de un proceso de mejora continua para la seguridad de la información en la organización.

La norma ISO 27002 se utiliza comúnmente en conjunto con la norma ISO 27001, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), y juntas proporcionan un marco sólido para la gestión de la seguridad de la información en una organización. (Mkinsi, 2022)

Tipos de encriptación

Debido a los múltiples tipos de datos y varios casos de uso de seguridad, existen muchos métodos diferentes de encriptación. Podemos agrupar ampliamente los métodos de cifrado de datos en dos categorías: cifrado de datos simétrico y asimétrico.

Encriptación simétrica

Cuando se usan métodos de encriptación simétrica, se usa una única clave secreta para encriptar el texto plano y desencriptar el texto cifrado. Tanto el remitente como el receptor tienen acceso privado a la clave, que solo pueden utilizar los destinatarios autorizados. El cifrado simétrico también se conoce como criptografía de clave privada.

Algunos algoritmos de cifrado simétrico comunes incluyen:

- Estándar de cifrado avanzado (AES)
- Estándar de cifrado de datos (DES)
- Triple DES (TDES)

AES: Uno de los tipos de cifrado más seguros, el Estándar de cifrado avanzado (AES), lo utilizan los gobiernos y las organizaciones de seguridad, así como las empresas cotidianas, para las comunicaciones clasificadas. AES utiliza

encriptación de clave "simétrica". Alguien en el extremo receptor de los datos necesitará una clave para decodificarlos. (Knerl, 2019)

AES-128 encripta bloques de un tamaño de 128 bits.

AES-192 encripta bloques de un tamaño de 192 bits.

AES-256 encripta bloques de un tamaño de 256 bits.

AES se diferencia de otros tipos de cifrado en que cifra los datos en un solo bloque, en lugar de bits de datos individuales. Los tamaños de bloque determinan el nombre de cada tipo de datos cifrados con AES:

DES: Aceptado como estándar de cifrado en la década de 1970, el cifrado DES ya no se considera seguro por sí solo. Cifra solo 56 bits de datos a la vez y se descubrió que era fácil de piratear poco después de su introducción. Sin embargo, ha servido como el estándar en el que se basaron futuras herramientas de encriptación más seguras. (Knerl, 2019)

TDES: El estándar de cifrado de datos triple , a veces abreviado como Triple DES o 3DES, es un método de cifrado simétrico que utiliza una clave de 56 bits para cifrar bloques de datos. Es una versión más avanzada y segura del algoritmo del Estándar de cifrado de datos (DES). Como su nombre lo indica, TDES aplica DES a cada bloque de datos tres veces.

Hoy, algunos líderes de la industria indican que TDES se está eliminando de ciertas herramientas y productos. La seguridad general de AES sigue siendo superior a la de TDES, según NIST . (Kidd, 2022)

Encriptación asimétrica

Este método de cifrado se conoce como criptografía de clave pública. En el cifrado asimétrico, se utilizan dos claves: una clave pública y una clave privada. Se utilizan claves separadas para los procesos de cifrado y descifrado: La clave pública, como sugiere el nombre, está disponible públicamente o se comparte con destinatarios autorizados.

Se requiere la clave privada correspondiente para acceder a los datos cifrados por la clave pública. La misma clave pública no funcionará para descifrar los datos en esta técnica.

El cifrado asimétrico ofrece otro nivel de seguridad a los datos que hace que las transferencias en línea sean más seguras. Los métodos de cifrado asimétrico comunes incluyen Rivest Shamir Adleman (RSA) y Criptografía de curva elíptica (ECC). (Kidd, 2022)

2.3. Conceptual

Encriptar: Es una manera de codificar la información para protegerla frente a terceros. Por lo tanto, la encriptación informática es la codificación de la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red. Es por medio de la encriptación informática como se codifican los datos. Solamente a través de un software de descodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información.

Por lo que la encriptación informática es simplemente la codificación de la información que vamos a enviar a través de la red. La encriptación de la informática se hace cada vez más necesaria debido al aumento de los robos de claves de tarjetas de crédito, número de cuentas corrientes, y en general toda la información que viaja por la red. Todo esto ha fomentado que se quiera conseguir una mayor seguridad en la transmisión de la información sobre todo a través de Internet. (La Revista Informática, 2018)

Seguridad informática: La seguridad informática como se mencionó con anterioridad consiste en asegurar la ausencia de riesgos en cualquiera de los componentes de un sistema (hardware, software, personal informático, redes, usuarios, datos y procedimientos), impidiendo que cualquier persona sin autorización pueda tener acceso a la información contenida en el sistema y por lo tanto no pueda modificarla, dañarla, alterarla, eliminarla o darle cualquier tratamiento que no esté autorizado. (CARVAJAL, 2018)

Amenazas a la seguridad de la información.

Una amenaza a la seguridad de las TIC puede definirse como “cualquier circunstancia o evento capaz de explotar, intencionalmente o no, una

vulnerabilidad específica en un sistema de TIC, lo que resulta en una pérdida de confidencialidad, integridad y disponibilidad de la información manipulada. (Domingues, 2017)

- Amenazas lógicas. Hay todo tipo de programas que pueden dañar nuestro sistema de una forma u otra y se crean intencionalmente como malware; llamado malware o simplemente errores, que pueden ser errores o agujeros.
- Software malicioso. las amenazas al sistema más comunes son causadas por errores inadvertidos por parte de los desarrolladores del sistema o de la aplicación.
- Herramientas de seguridad. Todas las herramientas de seguridad son un arma de doble filo: así como un administrador las usa para identificar y reparar sus sistemas o una subred completa, un futuro intruso puede usarlas para descubrir y explotar las mismas fallas. equipos ofensivos.
- Puertas traseras. durante el desarrollo de grandes aplicaciones o sistemas operativos, es común que los desarrolladores agreguen "atajos".
- Virus. Es una secuencia de código que se agrega a un archivo ejecutable para que cuando se ejecute el archivo, el virus haga lo mismo y se inserte en otros programas.
- Gusanos. Este es un programa que puede iniciarse y propagarse a través de las redes, a veces transportando virus o explotando errores en los sistemas conectados para dañarlos. •Caballos de Troya. Son instrucciones ocultas en un programa que parecen realizar tareas que el usuario espera que realice. pero en realidad realiza funciones ocultas sin el conocimiento del usuario.
- Usuarios. En su mayoría, las miradas indiscretas y los crackers realizan ataques pasivos que se pueden cambiar a activos; mientras que terroristas y exempleados llevan a cabo ataques puramente activos. (Chávez, 2016)

Aspectos de seguridad que compromete un ataque

La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.

Confidencialidad: La información llegue solamente a las personas autorizadas, por lo cual al no ser confidencial puede haber filtraciones de cierta información, como también de accesos no autorizados.

Integridad: La información al ser manipulada está violando la seguridad, afectando a las empresas u organizaciones. Lo que se debe garantizar que los datos e información deben estar seguros para no sufrir pérdidas o alteraciones.

Disponibilidad: Garantiza el paso a quienes cuenten con las credenciales requeridas para tener acceso a los servicios para ser usados cuando sea necesario. La falta de disponibilidad afecta a los servicios, interrumpiendo en la productividad de las empresas. (Lisboa Díaz, 2020)

Ataque informático

Un ataque informático implica explotar software, hardware o incluso debilidades o fallas humanas en un entorno informático; para obtener beneficios, a menudo de naturaleza financiera, que afectan adversamente la seguridad del sistema y luego afectan directamente los activos de la organización. (Berhanu Aebissa, 2023)

Para minimizar el impacto negativo de un ataque, existen procedimientos y mejores prácticas que pueden facilitar la lucha contra la actividad delictiva y reducir significativamente el alcance de un ataque. Comprender las diferentes etapas que componen un ataque cibernético le brinda la ventaja de aprender a pensar como un atacante y nunca subestimar su propio estado de ánimo. (Chávez, 2016)

- Reconocimiento. Esta etapa recopila información sobre las posibles víctimas, que pueden ser personas u organizaciones. Por lo general, en esta etapa, los datos objetivo se recopilan a través de varias fuentes de Internet como Google, entre otros.

- Investigación. En la segunda fase, la información obtenida en la primera fase se utiliza para sondear el objetivo e intentar obtener información sobre el sistema de la víctima, como dirección IP, nombre de host, datos de autenticación, entre otros.
- Obtener acceso. Algunos de los métodos que un atacante puede usar son ataques de desbordamiento de búfer, denegación de servicio (DoS), denegación de servicio distribuida (DDos), filtrado de contraseñas y secuestro de sesión.
- Generar acceso. El ataque comienza explotando las vulnerabilidades y los errores del sistema descubiertos durante la fase de reconocimiento e investigación. Algunos de los métodos que un atacante puede usar son ataques de desbordamiento de búfer, denegación de servicio (DoS), denegación de servicio distribuida (DDos), filtrado de contraseñas y secuestro de sesión.
- Mantener el acceso. Una vez que los atacantes obtienen acceso al sistema, intentarán implementar herramientas que les permitan acceder nuevamente en el futuro, independientemente de dónde puedan acceder a Internet.
- Eliminar los registros. Una vez que un atacante logra obtener y mantener el acceso a un sistema, intentará eliminar todo rastro de la intrusión para evitar que lo detecten los profesionales de seguridad o los administradores de red. (Félix, 2018)

2.4. Legal

Que, la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, señala: "Art. 6.- Accesibilidad y confidencialidad. - Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo

uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.

La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos (..)". (De, n.d.)

Que, el artículo 66 numeral 19 de la Constitución de la República, reconoce y garantiza a las personas: "(…)19. El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley (…)" (Antonio et al., 2021)

Que, el artículo 13 del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, determina que "La Dirección Nacional de Registro de Datos Públicos, de conformidad con la ley, expedirá las normas técnicas que contengan los estándares, mecanismos y herramientas para precautelar la seguridad, custodia y conservación de la información accesible y confidencial. La integridad y protección de los registros de datos públicos es responsabilidad de las instituciones del sector público y privado, a través de sus representantes legales y las personas naturales que directamente los administren.". (Antonio et al., 2021)

2.5. Georreferencial

No aplica

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

Investigación documental.

Esta investigación es de tipo documental, según el autor (Tancara Q, 1993) expone que, la investigación documental, es una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en el presente estudio se recopiló información documentada y de origen formal actualizada, mediate el uso de libros, internet, estudios científicos, investigaciones nacionales e internacionales relacionadas con la aplicación de las mejores prácticas de encriptación para el manejo de la información en redes de datos, con la finalidad de exponer las características más relevantes para la elaboración del manual de buenas prácticas.

Investigación descriptiva: Según el autor (Sirisilla, 2023)**,** el diseño de investigación descriptivo implica observar y recopilar datos sobre un tema determinado sin intentar inferir relaciones de causa y efecto. En esta investigación se utilizó para describir el análisis de diferentes técnicas de encriptación para redes, lo que implicó recopilar información sobre diferentes técnicas de encriptación existentes, describir cómo funcionan y comparar sus fortalezas y debilidades.

Investigación experimental: Según el autor Sekaran y Bougie (2016), "La investigación experimental implica la manipulación deliberada de una o más variables independientes para evaluar su efecto sobre una o más variables dependientes, mientras se controlan cuidadosamente las variables extrañas y se utilizan métodos de asignación aleatoria para garantizar la validez interna".

Se realizó el manual de las mejores prácticas de encriptación, para el manejo de la información en redes de datos, se dio a conocer los métodos más conocidos y relevantes utilizados hoy en día, en las cuales se desarrolló una investigación experimental con la técnica de la observación y con el instrumento de ficha de observación, como resultado de esta nos permitió evaluar y comparar objetivamente las diferentes técnicas de encriptación (algoritmos y protocolos) de esa manera identificando sus fortalezas y debilidades en cuanto a seguridad, rendimiento y facilidad de implementación. A través de la recopilación de datos con el instrumento de ficha de observación, se logró extraer conclusiones sólidas y fundamentadas sobre la eficacia y aplicabilidad de cada método en el contexto de las redes de comunicaciones.

3.2. Enfoque de la investigación

Investigación cualitativa.

El enfoque que se tomó en esta investigación es cualitativo, ya que se realizó una revisión documental exhaustiva (cualitativa), para la recopilación de información teórica y antecedentes sobre el tema de la aplicación de las mejores prácticas de encriptación para el manejo de la información en redes de datos y conocer el manejo actual y disposición final, por consiguiente, se planteó una solución que permitirá minimizar los riegos de las consecuencias.

3.3. Métodos de Investigación

Método comparativo: En el desarrollo de esta investigación, se empleó el enfoque metodológico comparativo, lo cual consistió en la comparación de diferentes técnicas de encriptación utilizadas hoy en día en redes de datos, el principal objetivo será analizar, evaluar las ventajas y desventajas, de igual manera el nivel de seguridad que ofrece por cada uno de las técnicas.

La presente investigación, se realizó una comparación exhaustiva de los procesos, documentación y conjuntos de datos relacionados con la encriptación de información en redes de datos. A través de este análisis comparativo se buscó identificar las mejores prácticas en términos de seguridad y eficacia de encriptación para la información en redes de datos.

3.4. Técnicas e Instrumentos de Recopilación de Datos

Técnica: Observación.

Instrumento: Ficha de observación**.**

Según el objetivo uno: Para alcanzar el primer objetivo se utilizó la técnica de revisión bibliográfica como: trabajó de tesis, estudios científicos, así como la norma ISO 27001.

Según el objetivo dos y tres:

Para alcanzar el objetivo dos se demostró mediante una simulación las fortalezas, debilidades y la seguridad que tiene cada uno de las encriptaciones (algoritmos y protocolos), el instrumento utilizado para la recopilación de la información fue las fichas de observación que nos permitió sintetizar y resumir la información de manera más detallada, para alcanzar el objetivo tres se diseñó un manual de las mejores prácticas de encriptación en base a los resultados de las ficha de observación que se realizó en el objetivo dos.

3.5. Universo, Población y Muestra

En la presente investigación no se aplicó el universo, población y muestra porque el enfoque de la investigación es cualitativo.

3.6. Procesamiento de la Información

Una vez recopilada la información mediante el instrumento de la ficha de observación se procedió a realizar en análisis y discusión de resultados, en donde se dio a conocer las técnicas de encriptación más relevantes que existe hoy en la actualidad de la misma manera se conoció las debilidades y las ventajas de cada técnica de encriptación de la información en redes de datos.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

Analizar las diferentes técnicas de encriptación (algoritmos y protocolos) para redes.

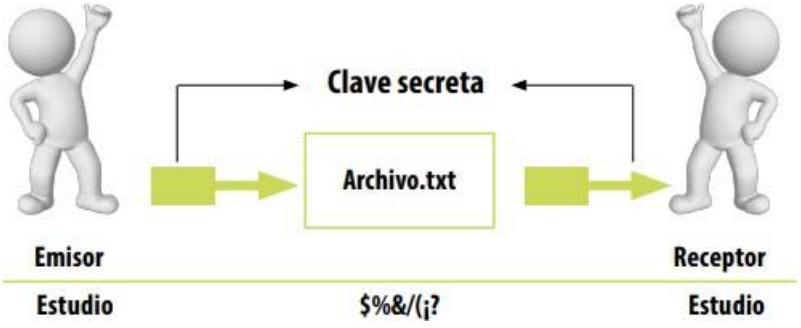
Para el análisis de las diferentes técnicas de encriptación (algoritmos y protocolos) para redes se recopiló información de forma actualizada mediante el uso de libros, internet, estudios científicos, investigaciones nacionales e internacionales relacionadas con la aplicación de las mejores prácticas de encriptación para el manejo de información de redes de datos.

Existen 3 formas básicas para encriptar los datos: la encriptación simétrica, la asimétrica y la híbrida. En cada una de estas formas se incluyen un grupo de algoritmo de cifrado diferentes.

4.2. Encriptación simétrica

Figura 1

Cifrado y Descifrado de información con clave Simétrica.



Fuente: (Noemy, 2017)

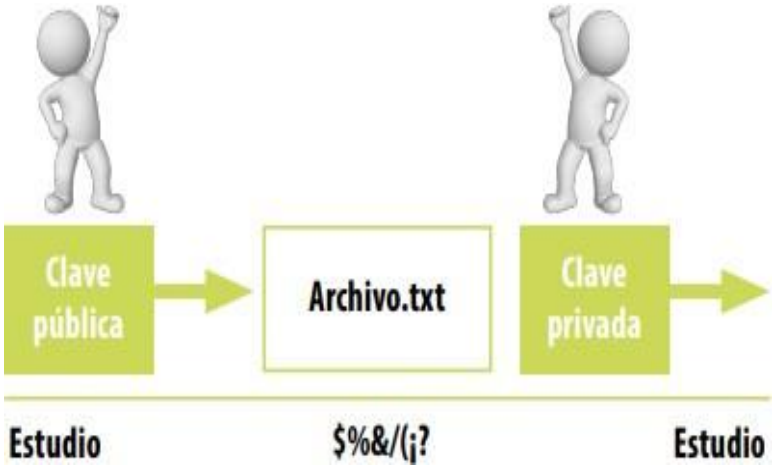
El cifrado simétrico es un método criptográfico en el cual se utiliza una única clave tanto para encriptar como para desencriptar el mensaje. Es crucial que esta clave sea mantenida en secreto, con el fin de garantizar que no sea posible descifrar el mensaje de manera sencilla.

En la película basada en hechos reales que hemos comentado en la sección anterior podemos ver como Enigma utilizaba un sistema criptográfico simétrico para la codificación de los mensajes de los alemanes. (Canadas, 2022)

4.3. Encriptación Asimétrica

Figura 2

Cifrado con clave Asimétrica



Fuente: (Noemy, 2017)

La criptografía asimétrica, también conocida como criptografía de dos claves o de clave pública y clave privada, es un tipo de encriptación que a diferencia de la criptografía simétrica utiliza dos claves: la clave pública y la clave privada.

La llave pública la puede saber todo el mundo. En cambio, la privada es solo para nosotros y nadie más puede conocerla.

Cuando queremos mandar un mensaje encriptado a alguien lo ciframos usando la clave pública del receptor ya que solo el receptor con su clave privada podrá descifrar el mensaje encriptado con su clave pública.

Esto permite que podamos enviar el mensaje por un canal inseguro ya que por mucho que alguien lo intercepte no podrán leer el contenido de su interior ya que no poseen la clave privada del receptor. Esto nos permite tener confidencialidad.

Otra propiedad importante de la criptografía es la autenticidad. Para asegurarnos que el emisor que envía el mensaje es realmente quien dice ser, el mensaje se firma digitalmente usando la clave privada del emisor.

La criptografía asimétrica es más lenta que la simétrica. No obstante, es más segura y es la que se utiliza para el envío de correos electrónicos o para intercambiar mensajes en plataformas como WhatsApp o Telegram. (Canadas, 2022)

4.4. Encriptación Híbrida

La criptografía híbrida mezcla las dos anteriores para unir las ventajas de ambos métodos y eliminar las desventajas. Con esta mezcla se consigue un procedimiento de cifrado más seguro que la encriptación simétrica y un cifrado más rápido que la criptografía asimétrica (Canadas, 2022)

4.5. Algoritmos de encriptación simétricos.

Las empresas, los productos de encriptación y las agencias gubernamentales utilizan varios algoritmos de encriptación diferentes en la actualidad. Éstas incluyen:

4.5.1. Estándar de cifrado avanzado (AES)

Un algoritmo de clave simétrica ampliamente utilizado que se ha convertido en el estándar para proteger datos confidenciales. Basado en el cifrado de bloques Rijandael, AES ofrece un alto nivel de seguridad y eficiencia. Opera en bloques de datos de tamaño fijo, normalmente de 128 bits, y admite tamaños de clave de 128, 192 y 256 bits. Además, utiliza operaciones de sustitución, permutación y mezcla para un cifrado sólido. Se utiliza en el gobierno federal de los EE. UU. y en tecnologías de consumo como la computadora Apple Macintosh. (Alvaro, 2021)

Cantidad de rondas del AES

En función del tamaño de clave que se esté utilizando en el algoritmo es la cantidad de rondas que ejecuta. Cuando se escoge AES 256 quiere decir que se está usando el algoritmo AES con una clave de 256 bits. A mayor tamaño de clave es más seguro el cifrado, pero también requiere más procesamiento y toma más tiempo realizarlo. (Alvaro, 2021)

El AES por ser un estándar permite varias longitudes de claves para que el usuario lo adapte a sus necesidades.

- 16 bytes (128 bits) = 10 rondas.
- 24 bytes (192 bits) = 12 rondas
- 32 byte (256 bits) = 16 rondas

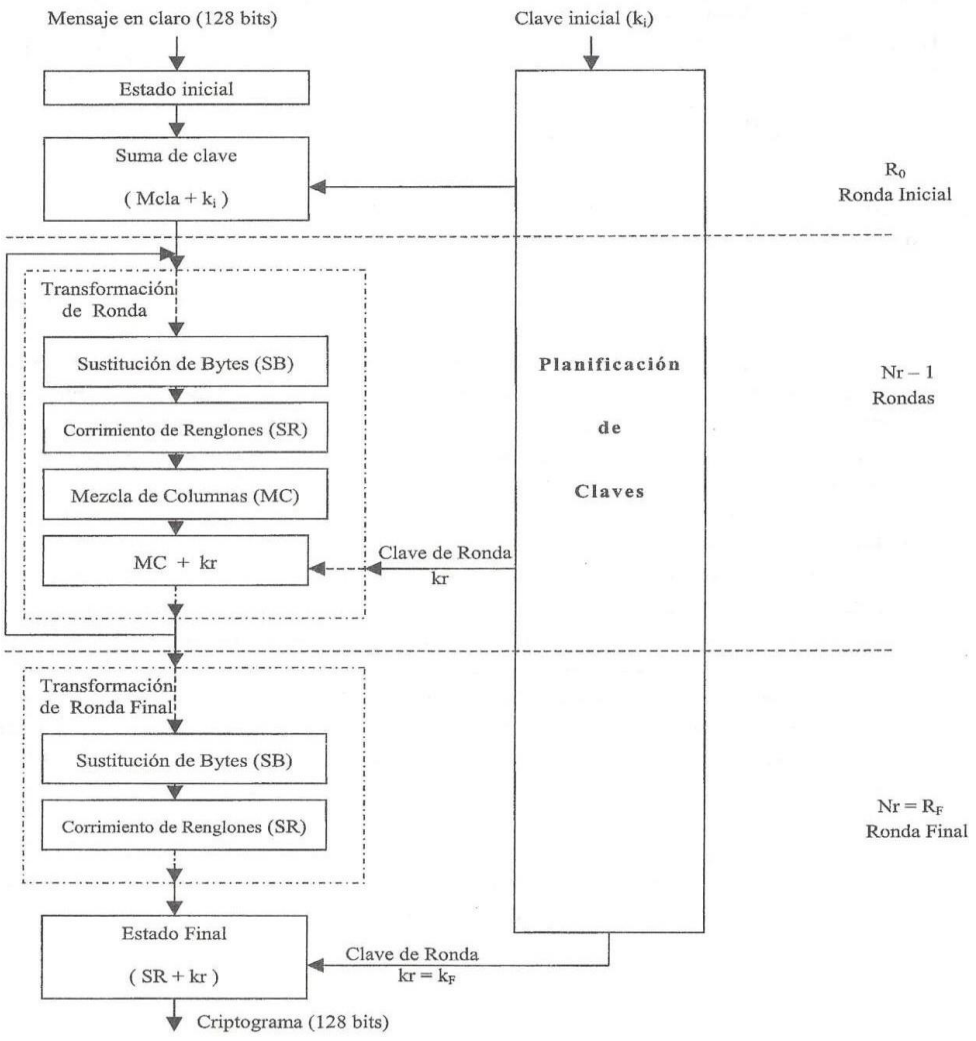
Características del AES

1. Tamaño de clave variable 128, 192, 256 bits (estándar). Múltiplos de 4 bytes.
2. Tamaño de bloques de texto de 4 bytes (128 bits).
3. Emplea cajas S similares al DES.
4. Numero de rondas variable en dependencia de la longitud de clave que esté utilizando. (Alvaro, 2021)

Secuencia de ejecución del AES para cifrar un bloque de datos

Figura 3

Funcionamiento de AES.



Fuente: (Alvaro, 2021)

Pasos realizados durante la ejecución del AES

1. A partir de la clave introducida por el usuario se ejecuta una función de expansión de clave donde se calculan las subclaves (Ki) que se van a utilizar en cada ronda de cifrado donde “i” es el número de subclaves.
2. La ronda 0 comienza con la función AddRounKey entre la subclave K0 y el bloque a cifrar.
3. Luego se ejecuta desde la ronda 1 hasta la penúltima ronda un ciclo donde se ejecutan las transformaciones sobre el bloque a cifrar en el

siguiente orden: ByteSub, ShiftRow, MixColumns y nuevamente AddRounKey con la próxima subclave.

4. La ronda final de algoritmo ejecuta ByteSub, ShiftRow, AddRounKey.
5. Al concluir la última ronda se obtiene un bloque cifrado.
6. El proceso se repite para cada bloque de bytes hasta cifrar el mensaje completo. (Alvaro, 2021).

Cómo se utiliza el AES en 2022.

VPNs: Las VPNs suelen utilizar AES. El propósito principal de una VPN es proporcionar una conexión a Internet segura y privada, que puede ser apoyada por AES. Esto hace que sea casi imposible que alguien sepa quién eres o dónde te encuentras. Las mejores VPN, como ExpressVPN y NordVPN, utilizan el cifrado AES-256 (que es el más alto disponible). Sin embargo, no todas las VPN lo utilizan, así que consulta nuestras reseñas antes de elegir una VPN. (Alvaro, 2021)

Herramientas de compresión: Seguro que todos os habéis encontrado alguna vez con un archivo comprimido. A menudo, si descargas un archivo de Internet, estará en un formato comprimido. El archivo se comprimirá en un tamaño más pequeño para que pueda descargarse más rápidamente y ocupe menos espacio en su dispositivo. Herramientas como 7Zip y WinZip pueden utilizarse para comprimir (y descomprimir) archivos cifrados con AES. (Alvaro, 2021)

Compartir archivos: Cuando utilices un software para compartir archivos como FileZilla, es de esperar que utilices una conexión HTTPS (segura). En la mayoría de los casos, AES mantendrá sus datos y archivos a salvo durante el proceso de transferencia. Esto evita que los atacantes intercepten sus archivos y puedan acceder a ellos. (Alvaro, 2021)

4.5.2. AES-256

El cifrado AES-256 utiliza una longitud de clave de 256 bits para cifrar y descifrar un bloque de mensajes. Hay 14 rondas de claves de 256 bits, y cada

ronda consiste en pasos de procesamiento que implican sustitución, transposición y mezcla de texto plano para transformarlo en texto cifrado.

El cifrado AES-256 es extremadamente seguro. Es el algoritmo de cifrado más seguro disponible en la actualidad y se utiliza ampliamente en aplicaciones gubernamentales y militares, así como en empresas que operan en sectores regulados El cifrado tiene un tamaño de clave de 256 bits, que se considera prácticamente infranqueable, incluso con la potencia de cálculo y los algoritmos más avanzados. Es el mismo nivel de seguridad que utilizan los bancos y otras instituciones financieras para proteger la información confidencial de sus clientes (MC Lee, 2022).

Características de cifrado de AES

AES consta de varias características principales:

Red de sustitución-permutación (SP)

El cifrado AES-256 se basa en una red de sustitución-permutación, también conocida como red SP. El cifrado funciona sobre una estructura de red SP en lugar de una estructura de cifrado Feistel que utiliza el mismo algoritmo básico tanto para el cifrado como para el descifrado.

Expansión de claves

El algoritmo utiliza una única clave durante la primera etapa. Posteriormente se amplía a múltiples claves utilizadas en cada ronda.

Datos en bytes

El algoritmo de cifrado AES funciona con bytes en lugar de bits. Esto significa que trata el tamaño de bloque de 128 bits como 16 bytes durante el proceso de cifrado.

Longitud de la clave

El número de rondas de encriptación a realizar depende de la longitud de la clave que se utilice para encriptar los datos. El tamaño de clave de 256 bits tiene 14 rondas. (MC Lee, 2022).

Proceso de descifrado de AES-256

Los textos cifrados AES pueden restaurarse a su estado inicial con ayuda del cifrado inverso. Como hemos visto anteriormente, el AES utiliza cifrado simétrico, lo que significa que la clave secreta utilizada para el cifrado es la misma que se utiliza para el descifrado.

En el caso del descifrado AES-256, el proceso comienza con la clave inversa de la ronda. A continuación, el algoritmo invierte todas las acciones, a saber: desplazamiento de filas, sustitución de bytes y mezcla de columnas, hasta descifrar el mensaje original. (MC Lee, 2022).

Usos de AES-256 en la actualidad

Es algo que no se puede conocer con exactitud con todo el flujo de datos constante que hay en el mundo, pero podemos recurrir a algunos ejemplos reales, por ejemplo, aplicaciones y sistemas ampliamente usados en los que se vea cómo confían en AES.

Partamos de los diversos sistemas de encriptación de ficheros que se usan en la actualidad. Podríamos hablar de BitLocker de Windows, que emplea AES para el cifrado seguro de datos en un disco, o la alternativa de código abierto VeraCrypt. También lo encontramos en el cifrado de ficheros comprimidos con WinRAR o 7Zip, o en documentos de las últimas versiones de Microsoft Word, Oracle e IBM también utilizan el estándar de cifrado AES-256

En software que usamos en el día a día, es uno de los tipos de clave del cifrado de extremo a extremo en WhatsApp, o los chats secretos de Telegram. El protocolo de Signal, el sistema de comunicación segura por excelencia también tiene como una de sus primitivas al AES-256. Gestores de contraseñas como el freemium LastPass o el de código abierto KeePass también lo emplean. (Gómez, 2021)

4.5.3. Data Encryption Standard (DES)

Es un algoritmo de clave simétrica que jugó un papel muy relevante en la historia del cifrado de datos. I fue desarrollado en la década de 1970 y se adoptó

ampliamente como un estándar criptográfico para proteger la información. Opera en bloques de datos de 64 bits y emplea un tamaño de clave de 56 bits, que se consideró robusto en el momento de su creación. Sin embargo, debido a los avances en el poder de cómputo y la aparición de ataques más sofisticados, el algoritmo DES ahora se considera relativamente débil en términos de seguridad. (Taylor, 2023)

El dominio de DES llegó a su fin en 2002, cuando el Estándar de cifrado avanzado (AES) reemplazó el algoritmo de cifrado DES como el estándar aceptado, luego de una competencia pública para encontrar un reemplazo. El NIST retiró oficialmente FIPS 46-3 (la reafirmación de 1999) en mayo de 2005, aunque Triple DES (3DES) sigue aprobado para información gubernamental confidencial hasta 2030 (Simplilearn, 2020).

Las ventajas del algoritmo DES:

- Está establecido como un estándar por el gobierno de los Estados Unidos.
- En comparación con el software, funciona más rápido en el hardware.
- Triple DES, utilizó una clave de 168 bits que es muy difícil de descifrar.

Las desventajas del algoritmo DES:

- Algoritmo débilmente seguro.
- Hay una amenaza de ataques de fuerza bruta.
- Una máquina de galletas DES conocida como Deep Crack está disponible en el mercado.

4.5.4. Triple DES (3DES)

Un algoritmo de cifrado que proporciona seguridad mejorada al aplicar el algoritmo Estándar de cifrado de datos (DES) varias veces en forma de cascada. Cada ronda consta de una operación de cifrado, descifrado y otra de cifrado. Este enfoque de tres capas aumenta significativamente la longitud de la clave a 112 o 168 bits, lo que la hace más resistente a los ataques y otras vulnerabilidades criptográficas. A pesar de sus mejoras, 3DES se está

eliminando gradualmente a favor de algoritmos de cifrado más avanzados. (Taylor, 2023).

Características generales

- Las características clave de 3DES incluyen:
- Cifrado simétrico: Utiliza la misma clave para cifrar y descifrar los datos.
- Triple aplicación del algoritmo DES: Los datos se cifran tres veces antes de ser transmitidos, aumentando significativamente la seguridad.
- Claves diferentes: Cada una de las tres aplicaciones del algoritmo utiliza una clave diferente.
- Compatibilidad y facilidad de implementación: 3DES es compatible con muchos sistemas y aplicaciones existentes y es fácil de implementar en nuevas soluciones.
- Velocidad: 3DES es un algoritmo relativamente lento en comparación con algunos de los métodos de cifrado más nuevos.

En general, 3DES es un algoritmo de cifrado que proporciona una mayor seguridad en la transmisión de información en comparación con el algoritmo DES original, pero ya no es considerado el método más seguro disponible en la actualidad (García, 2023).

Cómo se usa

3DES se usa para cifrar y descifrar información en la transmisión. Para utilizarlo, se requiere una clave secreta compartida entre el remitente y el destinatario. La siguiente es una descripción general de los pasos para utilizar 3DES:

- Generación de clave: El remitente y el destinatario acuerdan una clave secreta que se utilizará para cifrar y descifrar los datos.
- Cifrado de los datos: Antes de ser transmitidos, los datos se cifran tres veces utilizando 3DES y la clave compartida.
- Transmisión de los datos cifrados: Los datos cifrados se transmiten a través de la red.

- Descifrado de los datos: El destinatario descifra los datos utilizando 3DES y la clave compartida.

Es importante tener en cuenta que la clave secreta debe mantenerse segura y protegida para garantizar la seguridad de los datos cifrados. Cualquier acceso no autorizado a la clave puede permitir a los atacantes descifrar la información y acceder a los datos confidenciales. (García, 2023)

Donde podemos encontrar implementado el algoritmo 3DES

Queda a destacar estas bibliotecas de criptografía que admiten 3DES:

- Botan: Proporciona una amplia variedad de algoritmos, formatos y protocolos criptográficos, por ejemplo, SSL y TLS. Es de código abierto y está disponible bajo la licencia BSD de 2 cláusulas. También utilizado para el desarrollo de software seguro y aplicaciones de red.
- Cryptlib: es una biblioteca de herramientas de seguridad que permite a los programadores incorporar servicios de cifrado y autenticación al software. Proporciona una interfaz de alto nivel para que se puedan agregar sólidas capacidades de seguridad a una aplicación sin necesidad de conocer muchos de los detalles de bajo nivel de los algoritmos de encriptación o autenticación. Es de código abierto y está disponible bajo la licencia Sleepycat. (García, 2023)

4.5.5. Pes globo (Blowfish)

Blowfish es un algoritmo de cifrado de cifrado de bloque de clave simétrica diseñado por Bruce Schneier en 1993, y ha ganado popularidad por su eficiente proceso de cifrado y descifrado. (Nagaraj, 2023)

Características clave de Blowfish

Cifrado de bloques: Blowfish es un algoritmo de cifrado de bloques que opera en bloques de texto sin formato de 64 bits a la vez.

Cifrado de clave simétrica: Blowfish utiliza un sistema de cifrado de clave simétrica, lo que significa que se utiliza la misma clave tanto para el cifrado como para el descifrado.

Tamaño de clave variable: Blowfish permite tamaños de clave variables de hasta 448 bits, lo que lo hace más seguro en comparación con otros algoritmos de cifrado.

Cifrado de Feistel: Blowfish utiliza la estructura de cifrado de Feistel, que divide el texto sin formato en dos mitades y luego cifra iterativamente cada mitad mediante una serie de operaciones matemáticas.

Proceso de cifrado

El proceso de cifrado de Blowfish implica los siguientes pasos:

1. Generación de claves: la clave de cifrado se genera aplicando el algoritmo de expansión de claves a la clave original, que genera una serie de subclaves.
2. Permutación inicial: el texto sin formato de 64 bits está sujeto a una permutación inicial.
3. División: el bloque de 64 bits se divide en dos mitades, cada una con 32 bits.
4. Rondas: Blowfish consta de 16 rondas, y cada ronda implica una secuencia compleja de sustituciones y permutaciones en ambas mitades del bloque.
5. Permutación final: después de las 16 rondas, se aplica una permutación final a la salida para producir el texto cifrado. (Nagaraj, 2023)

Proceso de descifrado para Blowfish

El proceso de descifrado de Blowfish es esencialmente el reverso del proceso de cifrado.

El texto cifrado primero se divide en bloques de 64 bits, al igual que en el proceso de cifrado. Las subclaves se generan de la misma manera que en el proceso de encriptación, utilizando el mismo programa de claves.

- Para descifrar un bloque de texto cifrado, primero se pasa el bloque a través de la función F un total de 16 veces, utilizando las 16 subclaves en orden inverso.

- Luego, la salida final de la función F se somete a XOR con los 32 bits anteriores del bloque de texto cifrado. Esto se repite para cada bloque de 64 bits del texto cifrado hasta que se hayan descifrado todos los bloques. (Nagaraj, 2023)

Ventajas del pez globo

1. Blowfish es un algoritmo de cifrado ampliamente utilizado que es rápido, eficiente y seguro.
2. El tamaño variable de la clave de Blowfish lo hace más seguro en comparación con otros algoritmos de encriptación.
3. Blowfish es fácil de implementar y es compatible con varios lenguajes y plataformas de programación. (Nagaraj, 2023)

4.5.6. Twofish (DOS PECES)

Twofish es un algoritmo de cifrado simétrico que fue diseñado por Bruce Schneier y Niels Ferguson en 1998. Cuando se publicó en 1998, Twofish estaba entre los finalistas de una competencia para determinar el mejor algoritmo de cifrado de bloques para reemplazar DES. La competencia fue organizada por el Instituto Nacional de Estándares y Tecnología. Sin embargo, Twofish perdió ante el algoritmo de Rijndael como la mejor alternativa posible a DES, principalmente porque, aunque Twofish es seguro, es más lento que Rijndael. Es un cifrado de bloque de clave simétrico altamente seguro. Es conocido por su fuerte resistencia contra varios ataques criptográficos. Twofish es un algoritmo de cifrado de código abierto (sin licencia) que no está patentado y está disponible gratuitamente para su uso, opera en bloques de datos de 128 bits y admite tamaños de clave que van desde 128 a 256 bits, lo que lo hace flexible y adaptable a diferentes requisitos de seguridad. Además, emplea un cronograma de claves complejo, múltiples rondas de operaciones de sustitución y permutación, y una estructura de red Feistel cuidadosamente diseñada, todo lo cual contribuye a su solidez y resiliencia contra los ataques (Taylor, 2023).

Características:

- El cifrado TwoFish es un cifrado de bloque de clave simétrica, lo que significa que se utiliza la misma clave tanto para el cifrado como para el descifrado.
- Utiliza un programa de claves para generar claves redondas, que se utilizan en el proceso de cifrado y descifrado.
- El cifrado TwoFish utiliza una estructura de red Feistel, que es un tipo de diseño criptográfico que utiliza múltiples rondas de sustitución y permutación para brindar seguridad.
- El tamaño de la clave del cifrado TwoFish puede variar de 128 a 256 bits. (Nagaraj, TwoFish Encryption: A comprehensive guide, 2023).

Puntos fuertes de TwoFish Encryption:

- El cifrado TwoFish es muy seguro y resistente a los ataques conocidos, lo que lo hace adecuado para su uso en aplicaciones de alta seguridad.
- Tiene un gran espacio de claves, lo que significa que hay una gran cantidad de claves posibles, lo que hace que los ataques de fuerza bruta sean prácticamente imposibles.
- El cifrado TwoFish es rápido y eficiente, lo que lo hace adecuado para aplicaciones que requieren cifrado y descifrado de datos de alta velocidad.
- El cifrado TwoFish se ha estudiado exhaustivamente y se ha descubierto que es muy resistente a varios ataques, incluidos los ataques diferenciales y lineales (Nagaraj, TwoFish Encryption: A comprehensive guide, 2023).

Debilidades de TwoFish Encryption:

- El cifrado TwoFish es vulnerable a los ataques de canal lateral, como los ataques de análisis de tiempo y potencia.

- Puede ser un desafío implementar el cifrado TwoFish correctamente, y los errores en la implementación pueden generar vulnerabilidades que los atacantes pueden aprovechar.
- El cifrado TwoFish puede no ser adecuado para dispositivos de bajo consumo o aplicaciones con recursos informáticos limitados debido a su complejidad computacional. (Nagaraj, TwoFish Encryption: A comprehensive guide, 2023).

Proceso de cifrado:

1. Expansión de clave: la clave de entrada se expande en un conjunto de claves redondas utilizando el algoritmo de programación de claves.
2. Ronda inicial: el texto sin formato de entrada se divide en bloques y se aplica XOR con la tecla de la primera ronda.
3. Transformación de rondas: se realizan múltiples rondas de sustitución y permutación en los datos para brindar seguridad. En cada ronda, los datos primero se dividen en cuatro partes, y cada parte se transforma mediante una combinación de operaciones de sustitución y permutación.
4. Ronda final: la salida de la última ronda se XOR con la clave de la ronda final para producir el texto cifrado. (Nagaraj, TwoFish Encryption: A comprehensive guide, 2023).

Proceso de descifrado:

1. Expansión de clave: la clave de entrada se expande en un conjunto de claves redondas utilizando el algoritmo de programación de claves.
2. Ronda inicial: el texto cifrado de entrada se divide en bloques y se aplica XOR con la clave de ronda final.
3. Transformación de ronda inversa: se realizan múltiples rondas de sustitución inversa y permutación en los datos para recuperar el texto sin formato. En cada ronda, los datos primero se dividen en cuatro partes, y cada parte se transforma mediante una combinación de operaciones de permutación y sustitución inversa.

4. Ronda final: la salida de la última ronda se XOR con la tecla de la primera ronda para recuperar el texto sin formato. (Nagaraj, TwoFish Encryption: A comprehensive guide, 2023).

4.5.7. IDEA

- Los algoritmos de cifrado como IDEA (Algoritmo de cifrado de datos internacional) proporcionan un método seguro para proteger los datos.
- IDEA fue desarrollado inicialmente como un cifrado patentado por los criptógrafos suizos Xuejia Lai y James L. Massey en 1991.
- Luego fue estandarizado por la Organización Internacional de Normalización (ISO) en 1992. (Nagaraj, 2023)

¿Qué es el cifrado IDEA?

- El cifrado IDEA es un cifrado de bloque de clave simétrica que opera en bloques de datos de 64 bits.
- Utiliza una clave de 128 bits y una serie de operaciones matemáticas complejas para convertir el texto sin formato en texto cifrado.
- El cifrado IDEA usa una red Feistel, que divide el texto sin formato en dos mitades y luego aplica una serie de rondas a cada mitad, usando una combinación de operaciones XOR, módulo y multiplicación.
- Este proceso crea una clave única para cada bloque de datos. (Nagaraj, 2023)

Funciona el cifrado IDEA

- El cifrado IDEA funciona tomando bloques de datos de 64 bits y dividiéndolos en dos mitades, cada una con 32 bits.
- Luego, estas dos mitades se pasan a través de una serie de rondas, donde se someten a una combinación de operaciones XOR, módulo y multiplicación.
- Este proceso crea una clave única para cada bloque de datos.
- La clave utilizada en el cifrado IDEA es una clave de 128 bits creada por el usuario.

- A continuación, la clave se divide en ocho subclaves de 16 bits. Estas subclaves luego se usan en el proceso de cifrado para producir el texto cifrado.
- Cada ronda del proceso de cifrado de IDEA implica el uso de seis de estas subclaves. (Nagaraj, 2023)

Puntos fuertes de IDEA Encryption:

El cifrado IDEA ofrece una serie de fortalezas, que incluyen:

- Fuerte seguridad: el cifrado IDEA utiliza una clave de 128 bits, lo que lo hace extremadamente difícil de descifrar. También es resistente a ataques diferenciales y lineales.
- Cifrado rápido: el cifrado IDEA es un algoritmo de cifrado rápido, lo que lo hace ideal para su uso en aplicaciones en tiempo real.
- Diseño simple: el cifrado IDEA utiliza un diseño simple, lo que facilita su implementación y uso (Nagaraj, 2023).

Debilidades de IDEA Encryption:

El cifrado IDEA también tiene algunas debilidades, que incluyen:

- Vulnerable a los ataques de fuerza bruta: aunque el cifrado IDEA se considera seguro, sigue siendo vulnerable a los ataques de fuerza bruta.
- Tamaño de clave limitado: el cifrado IDEA utiliza una clave de 128 bits, que es más pequeña que algunos otros algoritmos de cifrado (Nagaraj, 2023).

Aplicaciones de IDEA Encryption:

El cifrado IDEA tiene una amplia gama de aplicaciones, que incluyen:

- Comunicación segura: el cifrado IDEA se puede utilizar para asegurar la comunicación entre dos partes, como en aplicaciones de correo electrónico o mensajería instantánea.
- Almacenamiento de datos: el cifrado IDEA se puede utilizar para cifrar datos confidenciales almacenados en un disco duro u otros dispositivos de almacenamiento.

- Firmas digitales: el cifrado IDEA se puede usar para crear firmas digitales, que se pueden usar para verificar la autenticidad de los documentos digitales (Nagaraj, 2023).

4.5.8. Chacha20

El algoritmo ChaCha20 es un algoritmo de cifrado simétrico que soporta claves de 128 y 256 bits y de alta velocidad, a diferencia de AES que es un cifrado por bloques, ChaCha20 es un cifrado de flujo. Tiene características similares a su predecesor Salsa20, pero con una función primitiva de 12 o 20 rondas distintas. Su código fue publicado, estandarizado por la IETF en la RFC 7539 y en implementaciones de software, es mucho más eficiente y rápido que AES, por lo que rápidamente se ha hecho un hueco dentro de los algoritmos más usados en la actualidad.

Para comprender por qué este algoritmo ha adquirido tanta notoriedad, accederemos a través de Google, lo que facilitará una comprensión más eficaz. Las conexiones HTTPS se enfocan en proporcionar el más alto nivel de seguridad para los sitios web que visitamos diariamente, representando un paso adelante respecto al protocolo HTTP, que carecía de protección. El cifrado utilizado varía entre distintos navegadores. Durante varios años, Chrome para Android ha empleado el algoritmo de cifrado simétrico AES-GCM. No obstante, Google ha estado trabajando en cifrados más modernos, seguros y eficientes.

El aumento de popularidad ocurrió con la implementación en la versión de escritorio de Chrome, extendiéndose posteriormente a Android con la introducción de ChaCha20 para el cifrado y Poly1305 para la autenticación. Este esfuerzo colosal resultó en un algoritmo simétrico que garantiza mayor seguridad y se muestra inmune a diversos tipos de ataques. De manera notable, ChaCha20 logra un rendimiento tres veces superior a protocolos más antiguos como AES. Este rendimiento optimizado permite una mejor utilización de las capacidades de la CPU, reduciendo el ancho de banda en un 16%, lo que maximiza la eficiencia de la conexión.

ChaCha20 se utiliza ampliamente en las conexiones HTTPS, actualmente si queremos tener la mejor seguridad podemos elegir entre AES o ChaCha20, no obstante, este último nos proporciona un mayor rendimiento, aunque tengamos aceleración de cifrado por hardware. Este protocolo también se utiliza en las conexiones SSH para administrar servidores, de esta forma, podremos no solamente administrarlos, sino hacer uso del protocolo de transferencia de ficheros basado en SSH que es SFTP, por lo que tendremos un gran rendimiento. Por último, otro protocolo muy popular que usa ChaCha20 es VPN WireGuard, de hecho, este protocolo de VPN solamente nos permite usar ChaCha20, por este motivo (entre otros) es mucho más rápido que OpenVPN o IPsec, aunque tengamos aceleración de cifrado por hardware.

Hasta aquí la explicación de la criptografía simétrica, hemos comentado los dos algoritmos que se usan frecuentemente en la actualidad, hay muchos más que en el pasado fueron muy relevantes, sobre todo para el desarrollo de los actuales, ya que las bases de los nuevos se asentaron sobre la experiencia de los viejos, sus errores y sus ventajas. Algoritmos como el DES, 3DES, RC5 o IDEA allanaron el camino a los nuevos para que hoy tengamos unos algoritmos de cifrado realmente fuertes y con capacidad para aguantar ataques y proteger toda nuestra información de manos indeseadas y malintencionadas. (López, 2021)

4.6. Algoritmos de encriptación asimétrico

Encriptación asimétrica RSA o Rivest-Shamir-Adleman

Considerado un elemento básico del cifrado asimétrico, diseñado por los ingenieros (Ron Rivest, Adi Shamir y Leonard Adleman) que le dieron su nombre en 1977, RSA utiliza la factorización del producto de dos números primos para ofrecer un cifrado de 1024 bits y una longitud de clave de hasta 2048 bits. Según una investigación realizada en 2010, se necesitarían 1.500 años de potencia de cálculo para descifrar su versión más pequeña de 768 bits. (Hernández, 2022)

Sin embargo, esto significa que es un algoritmo de cifrado más lento. Como requiere dos claves diferentes de una longitud increíble, el proceso de cifrado y

descifrado es lento, pero el nivel de seguridad que proporciona para la información sensible es incomparable. (Hernández, 2022)

¿Cómo funciona el algoritmo RSA?

La seguridad de este sistema se basa en el problema de factorización de números enteros, el cual consiste en encontrar el valor de dos números primos grandes a partir de su producto, conforme al avance de la tecnología, estos dos números deberían hacerse más y más grandes con el fin de dificultar la solución a dicho problema. De hecho, se cree que con el desarrollo de computación cuántica este se logrará resolver.

Ahora bien, para explicar el algoritmo, partiremos del clásico ejemplo con cofres para ilustrar cómo funciona un sistema de cifrado con clave pública.

Imagina que Alice le quiere enviar a Bob un mensaje secreto. Para lograrlo, Bob le envía un cofre con un candado abierto (clave pública) del cual solo él tiene la llave (clave privada). Alice pone el mensaje adentro del cofre, cierra el candado, por lo que ya nadie tiene acceso a la información secreta. Excepto Bob, quien tiene la llave desbloquear el cofre. Si entiendes este ejemplo, te será muy fácil comprender qué es RSA en criptografía. (KeepCoding, 2023)

Algoritmo RSA

En un rsa, Alice envía un mensaje en texto plano (M), en forma de un número m que es menor que n. El mensaje cifrado (c) se calcula por medio de la siguiente operación:

$$c=m^e \pmod n$$

Donde e es la clave pública de Bob.

La forma en la que Bob descifra el mensaje de Alice es mediante la siguiente operación:

$$m=c^d \pmod n$$

Donde d es la clave privada de Alice. (KeepCoding, 2023)

Ventajas y desventajas de RSA

Ventajas

- Resuelve el problema de la distribución de las llaves.
- Se puede usar para el manejo de firmas digitales.

Desventajas

- La seguridad del cifrado depende de la eficiencia computacional.
- Requiere mayor tiempo de ejecución que el cifrado simétrico.
- La llave privada debe ser cifrado por algún algoritmo simétrico. (Rivas, 2023)

4.6.1. Ecc o criptografía de curva elíptica

La criptografía basada en las matemáticas de las curvas elípticas no es un tema nuevo. A mediados de la década de los 1980, los desarrolladores Victor Miller de IBM y Neal Koblitz de la Universidad de Washington, hacen su primera propuesta sobre el uso de las curvas elípticas. En dicho estudio, destacan sus propiedades matemáticas para su uso en aplicaciones de criptografía altamente seguras. (Maldonado, 2020)

Desde ese momento y hasta la actualidad, la ECC ha demostrado su seguridad al soportar una generación de ataques. Esto debido al crecimiento del sector computacional y al advenimiento de la economía de las criptomonedas. Pero también relacionado con la ampliación del sector de dispositivos inalámbricos que requieren métodos de cifrado más amigables, pero manteniendo los estándares de seguridad y la tecnología de cifrado de datos basada en las curvas elípticas (ECC) ha estado ganando cada vez más terreno, sobre todo en empresas y espacios donde la seguridad y la privacidad son vitales. (Maldonado, 2020)

En este sentido, la ECC ha sido normalizada por el Instituto Americano de Estándares Nacionales (ANSI), el Instituto Nacional de Estándares y Tecnología (NIST) y por Estándares Federales de Procesamiento de la Información (FIPS). Con ello demuestra, que no solo es una tecnología de gran confianza, sino que también es madura y con gran aplicabilidad.

La criptografía de curva elíptica (ECC) es un método ampliamente utilizado en la criptografía de datos. Este método se enfoca en la creación de un sistema de cifrado asimétrico, o de clave pública/privada. Sin embargo, la ECC usa una estructura algebraica de curvas elípticas sobre campos finitos para garantizar la seguridad y fiabilidad de sus procesos criptográficos. De esa forma, la ECC permite que las claves sean más pequeñas en extensión en comparación con otros sistemas criptográficos. Y todo ello, sin renunciar en ningún momento a la seguridad del sistema.

Uno de los casos más famosos de uso de ECC es el algoritmo de firma digital de curva elíptica (ECDSA). Este es un algoritmo de firma ampliamente utilizado para la criptografía de clave pública que usa ECC. Un algoritmo que se usa en prácticamente la mayor parte de Internet, y por supuesto, en gran parte de los proyectos de criptomonedas como Bitcoin y Ethereum. (Maldonado, 2020)

¿Cómo se usan las curvas elípticas en criptografía?

En criptografía, no se usan las curvas elípticas basadas en números reales, ya que esto produce errores de redondeo en ordenadores. Por eso, se utilizan curvas elípticas definidas sobre cuerpos finitos, que se pueden representar por medio de la siguiente ecuación:

$$y^2 = x^3 + 10x + 2$$

Esta criptografía de curva elíptica se caracteriza por tener un número de puntos finito, cuyas coordenadas serán únicamente números enteros. Esa característica es de suma importancia para este algoritmo de cifrado, ya que permite hacer cálculos de forma eficiente y sin errores de redondeo. (KeepCoding, 2023)

Hay dos tipos de cuerpos finitos que se pueden utilizar en criptografía de curva elíptica:

- Cuerpos primos, que tienen un número primo de elementos.
- Cuerpos binarios, que tienen un número de elementos que es una potencia prima de 2.

La forma en la que se obtiene otro punto de la curva por este método es mediante la suma de un punto (x, y) muchas veces consigo mismo. De modo que:

$$Q = P + \ldots + P = n * P$$

Ventajas y desventajas de las ECC

Ventajas

- La criptografía asimétrica de clave pública (ECC) es compatible con la mayoría de los sistemas operativos y navegadores web modernos.
- Las claves que se obtienen mediante ECC son más pequeñas, lo que significa un mejor rendimiento con menor sobrecarga.
- El ECC escala mejor, a medida que las claves crecen el RSA se vuelve muy lento y pesado.
- Quantum Computing o la Computación cuántica, es un gran enemigo del RSA. Ya que permite romper las claves rápidamente. Por otro lado, el ECC es mucho menos vulnerable a esta nueva generación de computadoras. (Maldonado, 2020)

Desventajas

- Una de las principales desventajas de ECC que se ha reportado, es que aumenta significativamente el tamaño del mensaje cifrado, más que el cifrado RSA.
- El algoritmo ECC es más complejo y más difícil de aplicar que RSA. Esto aumenta la probabilidad de errores de implementación, reduciendo así la seguridad del algoritmo.
- La criptografía de clave pública es computacionalmente más costosa que el cifrado de clave privada, que emplea una clave de cifrado compartida única.
- En los dispositivos inalámbricos, el cifrado de clave pública puede acortar la vida útil de las baterías o de los propios dispositivos. (Maldonado, 2020)

4.7. Algoritmo de firma digital (DSA)

DSA es un estándar del Gobierno Federal de los Estados Unidos para firmas digitales. Fue propuesto por el instituto Nacional de Estándares y Tecnología (NIST) en agosto de 1991 para uso en su estándar de firma digital, especificando en FIPS 186 en 1993. Las etapas de los algoritmos DSA y los ejemplos que se describen a continuación están basados en las tutorías del Dr. Herong Yang. (Eduardo, 2018)

La primera parte del algoritmo DSA es generar la clave pública y generar la clave privada, que se describe de la siguiente manera.

- **a)** Elegir un número primo q, que se llama divisor principal.
- **b)** Elegir otro número primo q, tal que p-1 mod q = 0. P se denomina módulo primo.
- **c)** Calcula un número entero g, tal que 1<g <p, g^qmod p = 1 y g = h^(((p-1) /q)) mod
- **d)** p. q también se llama módulo de orden multiplicativo g de p.
- **e)** Elegir un número entero x, tal que 0<x <q.
- **f)** Calcular y como g^x mod p.
- **g)** Agrupamos nuestra clave pública como {p, q, g, y}.
- **h)** Agrupamos nuestra clave privada como {p, q, g, x}.

2. La segunda parte del algoritmo DSA es la generación y verificación de la firma, que

se describe como:

El lado del remitente debe realizar:

a) Generar el resumen del mensaje, usando un algoritmo hash como SHA1, se conoce como “h”.

b) Generar un número aleatorio k, tal que 0 <k <q.

c) Calcular un número r como (g^kmod p) mod q. Si r = 0, selecciona una k

d) diferente.

e) Calcular un número i, tal que k*i mod q = 1. i se llama inverso multiplicativo

f) modular de k modulo q.

g) Calcular s = i * (h + r * x) mod q. Si s = 0, selecciona una k diferente.

h) Agrupe la firma digital {r, s}.

3. Tercera parte, se verifica la firma de un mensaje:

a) Generar el resumen del mensaje (h), usando el mismo algoritmo hash.

b) Calcular w, de modo que s * w mod q = 1. w se denomina inverso modular

c) de s modulo q.

d) Calcular u1 = h * w mod q.

e) Calcular u2 = r * w mod q.

f) Calcular v = (((g^u1) * (yy^u2)) mod p) mod q.

g) Si v == r, la firma digital es válida. (Eduardo, 2018)

Ventajas y desventajas de algoritmo de firma digital (DSA)

Ventajas

- Tiene niveles de fuerza muy fuertes.
- También tiene pequeños estándares de firma digital.
- La velocidad de cálculo de la firma es muy inferior.
- No requiere un gran espacio en comparación con otros.
- No incluye ningún cargo y se puede utilizar de forma gratuita. (Bhandari, 2021)

Desventajas

- El proceso de autenticación requiere mucho tiempo ya que la verificación lleva mucho tiempo.
- La autenticación de datos se puede hacer en DSA. No se puede cifrar.
- DSA depende de SHA1. Por lo tanto, cualquier limitación o problema de este es el problema reflejado en DSA. (Bhandari, 2021)

Cifrado ElGamal

Fue diseñado en 1984 por Taher ElGamal puede realizar cifrado y firma, basado en la dificultad de calcular logaritmos discretos

Diffie-Hellman (DH)

Apareció en el año 1976 en New Directions in Cryptography

- Diseñado en 1977 por Diffie y Hellman.
- Claves de 512, 1024
- Basado en las propiedades de los logaritmos discretos
- Utilizado mayoritariamente para negociar claves
- Necesita autenticación adicional (man-in-the-middle)

4.8. Tipos de redes informáticos

De acuerdo con los requisitos de comunicación, hay varios tipos de conexiones de red disponibles. El tipo más básico de clasificación de red depende de la cobertura geográfica de la red (Kapoor, 2022).

A continuación, se mencionan diferentes tipos de redes:

- PAN (Red de área personal)
- LAN (red de área local)
- MAN (Red de Área Metropolitana)
- WAN (red de área amplia)
- Veamos cada uno de los tipos de red en detalle.

Red de área local (LAN)

La red de área local (LAN) está diseñada para conectar múltiples dispositivos y sistemas de red dentro de una distancia geográfica limitada. Los dispositivos están conectados mediante múltiples protocolos para intercambiar datos y servicios de manera adecuada y eficiente (Kapoor, 2022).

Atributos de la red LAN:

- La velocidad de transmisión de datos en la red LAN es relativamente más alta que en otros tipos de red, MAN y WAN.

- LAN utiliza direcciones de red privada para la conectividad de red para el intercambio de datos y servicios, y utiliza cable para la conexión de red, lo que reduce los errores y mantiene la seguridad de los datos.

Ventajas y desventajas de la red LAN

Ventajas

- La transmisión de datos y servicios es relativamente más alta que otras conexiones de red.
- El servidor de red actúa como una unidad central para toda la red.

Desventaja

- Necesita administración constante de ingenieros experimentados para su funcionamiento.
- Probabilidad de fuga de datos confidenciales por parte de la administración LAN.

Red de área metropolitana (MAN)

La Red de Área Metropolitana (MAN) es un tipo de red que cubre la conexión de red de una ciudad entera o la conexión de un área pequeña. El área cubierta por la red se conecta mediante una red cableada, como cables de datos. (Kapoor, 2022)

Atributos de la red MAN:

- La red cubre un área de pueblo completa o una parte de una ciudad.
- La velocidad de transmisión de datos es relativamente alta debido a la instalación de cables ópticos y conexiones por cable.

Ventajas y desventajas de la red MAN

Ventajas

- Proporciona transmisión de datos Full-Duplex en el canal de red para dispositivos.
- El área de conexión de la red cubre una ciudad entera o algunas partes utilizando los cables ópticos.

Desventajas

- Alta probabilidad de ataque de piratas informáticos y ciberdelincuentes debido a las grandes redes.
- La necesidad de hardware de buena calidad y el costo de instalación es muy alto.

Red de área amplia (WAN)

La red de área amplia (WAN) está diseñada para conectar dispositivos a grandes distancias, como estados o entre países. La conexión es inalámbrica en la mayoría de los casos y utiliza torres de radio para la comunicación.

La red WAN puede estar formada por varias redes LAN y MAN (Kapoor, 2022).

Atributos de la red WAN:

- La velocidad de la transferencia de datos WAN es menor que en comparación con las redes LAN y MAN debido a la gran distancia recorrida.
- La red WAN utiliza un medio satelital para transmitir datos entre varias ubicaciones y torres de red.

Ventajas y desventajas de la red WAN:

Ventajas

- Esta red cubre un área geográfica elevada y se utiliza para conexiones de larga distancia.
- También utilizan torres de radio y conectan canales para los usuarios.

Desventajas

- Alto costo para configurar la red y se necesita el apoyo de técnicos experimentados para mantener la red.
- Es difícil evitar la piratería y depurar una red grande. (Kapoor, 2022)

4.9. Protocolos de seguridad

Protocolos seguros que utilizan los algoritmos de encriptación para mantener nuestros datos seguros en una serie de situaciones diferentes.

TLS/SSL

La seguridad de la capa de transporte (TLS) aún se denomina a menudo por el nombre de su predecesor, capa de sockets seguros (SSL), pero en realidad es una versión actualizada de SSL con una variedad de mejoras de seguridad. TLS es uno de los protocolos seguros que encontrará con más frecuencia. Cada vez que vea "https" o el candado verde junto a una URL en la barra de direcciones de su navegador web, sabrá que TLS se está utilizando para asegurar su conexión al sitio web.

Se diferencia de los tres sistemas mencionados anteriormente en que TLS no es un algoritmo de cifrado, sino un protocolo que se ha convertido en un estándar de Internet para proteger los datos. Esto significa que TLS no es el mecanismo que realiza el cifrado; utiliza algoritmos como RSA, AES y otros para hacerlo. TLS es simplemente el sistema acordado que se utiliza para proteger los datos en una variedad de situaciones. TLS se puede utilizar para cifrar, autenticar y mostrar si los datos conservan su integridad original.

Se usa con mayor frecuencia sobre protocolos de capa de transporte como HTTP (lo que usamos para conectarnos a sitios web), FTP (lo que usamos para transferir archivos entre un cliente y un servidor) y SMTP (lo que usamos para el correo electrónico).

Agregar TLS a estos protocolos protege los datos que se transfieren, en lugar de dejarlos a la vista para que cualquiera que los intercepte acceda. Además de permitir que su navegador web se conecte de forma segura a un sitio web, TLS también se usa en las VPN para la autenticación y el cifrado.

TLS se compone de dos capas, el protocolo de protocolo de enlace y el protocolo de registro.

El protocolo Handshake se utiliza para iniciar la conexión. Cuando se establece la conexión, el cliente y el servidor deciden qué versión del protocolo se usará,

autentican los certificados TLS de cada uno (certificados que verifican la identidad de cada parte), eligen qué algoritmos se usarán para el cifrado y generan un clave a través del cifrado de clave pública.

Luego, el Protocolo de registro asegura los paquetes de datos que se transfieren con las claves compartidas que se generaron en el Protocolo de reconocimiento de datos. El cifrado de clave simétrica se utiliza para hacer que el proceso sea mucho más eficiente.

Además de cifrar los datos, el protocolo de registro se encarga de dividir los datos en bloques, agregar relleno, comprimir los datos y aplicar un código de autenticación de mensajes (MAC). También realiza todos estos procesos a la inversa para los datos que se reciben.

Como todos los protocolos, con el tiempo se descubrieron una serie de fallas en SSL, lo que condujo al desarrollo de TLS. TLS presenta una gama de adiciones que reforzaron la seguridad, pero se ha seguido actualizando con el tiempo. TLS 1.3 se definió en agosto de 2018, pero la versión 1.2 todavía se usa comúnmente (Lake, 2018).

IPsec

IPsec son las siglas de Internet Protocolo Security, y se usa principalmente en VPN, pero también se puede usar en enrutamiento y seguridad a nivel de aplicación. Utiliza una variedad de algoritmos criptográficos para cifrar datos y proteger su integridad, incluidos 3DES, AES, SHA y CBC.

IPsec se puede implementar en dos modos diferentes, modo túnel y modo transporte. En el modo de túnel, tanto el encabezado como la carga útil se cifran y autentican, luego se envían en un nuevo paquete con otro encabezado. Las VPN lo utilizan en las comunicaciones de host a host, de host a red y de red a red.

El modo de transporte solo encripta y autentica la carga útil y no el encabezado. Los datos transitan a través de un túnel L2TP, que proporciona seguridad de extremo a extremo. Generalmente se utiliza para conectar clientes y servidores, o una estación de trabajo a una puerta de enlace.

Cuando se trata de configuraciones de VPN , IPsec puede conectarse más rápido y ser más fácil de implementar, pero en muchos casos, usar TLS puede ser más ventajoso en general. Si bien las filtraciones de Snowden mostraron que la NSA estaba tratando de socavar la seguridad de IPsec, todavía se considera seguro de usar siempre que se implemente correctamente

SSH

Secure Shell (SSH) es otro protocolo seguro que se utiliza en una variedad de escenarios. Estos incluyen el acceso seguro a una terminal remota, como un túnel encriptado (de manera similar a una VPN) mediante el uso del proxy SOCKS, la transferencia segura de archivos, el reenvío de puertos y mucho más.

SSH se compone de tres capas separadas: la capa de transporte, la capa de autenticación de usuario y la capa de conexión. La capa de transporte permite que dos partes se conecten de forma segura, se autentiquen entre sí, cifren datos, validen la integridad de los datos y establezcan otros parámetros para la conexión.

En la capa de transporte, el cliente se pone en contacto con el servidor y las claves se intercambian mediante el intercambio de claves Diffie-Hellman. También se seleccionan un algoritmo de clave pública (como RSA), un algoritmo de clave simétrica (como 3DES o AES), el algoritmo de autenticación de mensajes y el algoritmo hash para la transmisión.

El servidor enumera los métodos de autenticación admitidos para el cliente, que pueden incluir contraseñas o firmas digitales. Luego, el cliente se autentica en la capa de autenticación utilizando el sistema que se haya acordado.

En la capa de conexión, se pueden abrir múltiples canales una vez que el cliente ha sido autenticado. Se utilizan canales separados para cada línea de comunicación, como un canal para cada sesión de terminal, y el cliente o el servidor pueden abrir un canal.

Cuando cualquiera de las partes desea abrir un canal, envía un mensaje al otro lado, con los parámetros previstos. Si el otro lado puede abrir un canal bajo esas

especificaciones, se abre y se intercambian datos. Cuando cualquiera de las partes desea cerrar el canal, envía un mensaje al otro lado y el canal se cierra.

Si bien un túnel SSH no es una VPN, se puede usar para lograr resultados similares. Puede usar un proxy SOCKS para cifrar su tráfico desde el cliente SSH al servidor SSH. Esto te permite encriptar el tráfico de cada aplicación, pero no ofrece la universalidad de una VPN.

Las filtraciones de Snowden contenían archivos que sugerían que la NSA podría descifrar SSH en algunas circunstancias. Si bien algunas implementaciones pueden ser vulnerables, el protocolo SSH en sí generalmente se considera seguro de usar.

PGP

Es el último protocolo de seguridad del que hablaremos hoy. Permite a sus usuarios cifrar sus mensajes, así como firmarlos digitalmente para probar su autenticidad e integridad. Desde principios de los noventa, ha sido una herramienta importante para proteger la información confidencial en los correos electrónicos.

El protocolo en sí se llama OpenPGP, pero PGP tiene una historia larga y complicada que involucra al programa inicial y a PGP Inc., una compañía que se formó en torno al desarrollo. Desde entonces, PGP Inc. ha sido adquirida por otras corporaciones varias veces, y algunos de sus activos ahora son propiedad de Symantec y otras compañías.

El estándar OpenPGP se desarrolló en 1997 para que PGP pudiera convertirse en un sistema interoperable y de uso mundial. Se puede implementar libremente en una variedad de clientes de correo electrónico, pero una de las configuraciones más utilizadas involucra Gpg4win , un paquete de cifrado de código abierto para Windows.

OpenPGP se puede usar con varios algoritmos diferentes, como RSA o DSA para el cifrado de clave pública; AES, 3DES y Twofish para cifrado de clave simétrica; y SHA para hashing.

En el transcurso de su desarrollo, se han encontrado una serie de vulnerabilidades en varias implementaciones de OpenPGP. Las nuevas versiones han abordado estas fallas de seguridad, la última de las cuales, EFAIL, se descubrió este año.

Siempre que la visualización de HTML y JavaScript estén deshabilitados mientras se visualizan los correos electrónicos y se detenga la recarga automática de contenido externo, PGP seguirá considerándose seguro. Algunos clientes como Thunderbird también han lanzado actualizaciones que mitigan estos problemas.

4.10. Diferencia entre gns3 y cisco packet tracer

Figura 4

Diferencia entre Gns3 y Packet Tracer

Fuente*:* (Otero, 2022).

Cisco Packet Tracer y GNS3 son dos programas populares de administración y simulación de red que pueden usarse para prepararse para pruebas de certificación o pruebas de características de red sin la necesidad de comprar derechos costosos técnicas. Las dos piezas de software fueron construidas para satisfacer distintos propósitos. Entre ambos, GNS3 es un simulador de red de código abierto.

Pueden sonar similares, pero están equipados con bastantes características que los distinguen entre sí. Este artículo se centra en las diferencias entre los dos programas de simulación de red (Otero, 2022).

Tabla 1

Cuadro comparativo de Gns3 VS Cisco Packet Tracer.

	GNS3	CISCO PACKET TRACER
Compatibilidad	Es compatible con una amplia gama de dispositivos de red, incluidos Cisco, Juniper y otros proveedores	Por otro lado, se enfoca solo en dispositivos Cisco.
Complejidad	GNS3 es una herramienta más compleja que requiere más conocimientos técnicos para su configuración y uso.	Está diseñado para ser fácil de usar y, a menudo, se usa en entornos educativos para enseñar conceptos de redes.
Realismo:	Es más realista en términos de cómo simula redes, ya que utiliza imágenes de dispositivos reales y emula sus sistemas operativos.	Es más, una simulación simplificada y es posible que no represente con precisión el comportamiento de la red en el mundo real.
Costo:	Es una herramienta gratuita y de código abierto	Requiere una cuenta de Cisco NetAcademy para descargar y usar.
Simulación o emulación	Emulación de la mayoría de los dispositivos, simulación de interruptores	Solo simulación.

Consumo de RAM	Consume la memoria RAM real del dispositivo. El consumo por cada router se estima en unos 512 MB de RAM.	No consume la memoria RAM real del dispositivo.
Ventajas:	• Es fácil de instalar. El proceso de instalación comienza en el asistente y proporciona opciones fáciles de configurar que se explican por sí mismas. No necesita ninguna configuración adicional después de la instalación. • Admite todos los enrutadores, conmutadores, PC y dispositivos de red esenciales de Cisco que necesita para practicar los temas del examen CCNA.	• Es software libre. • Es compatible con múltiples entornos de proveedores. • Puede usarlo con o sin software de virtualización. Si desea usarlo con software de virtualización, es compatible con software de virtualización gratuito y de pago. • Es compatible de forma nativa con Linux. Significa que puede usarlo en Linux sin ningún software de virtualización. • Incluye muchos dispositivos simulados preconfigurados y optimizados.
Desventajas:	• Necesita una cuenta activa de la academia de	• No proporciona imágenes de IOS. Tienes que obtener

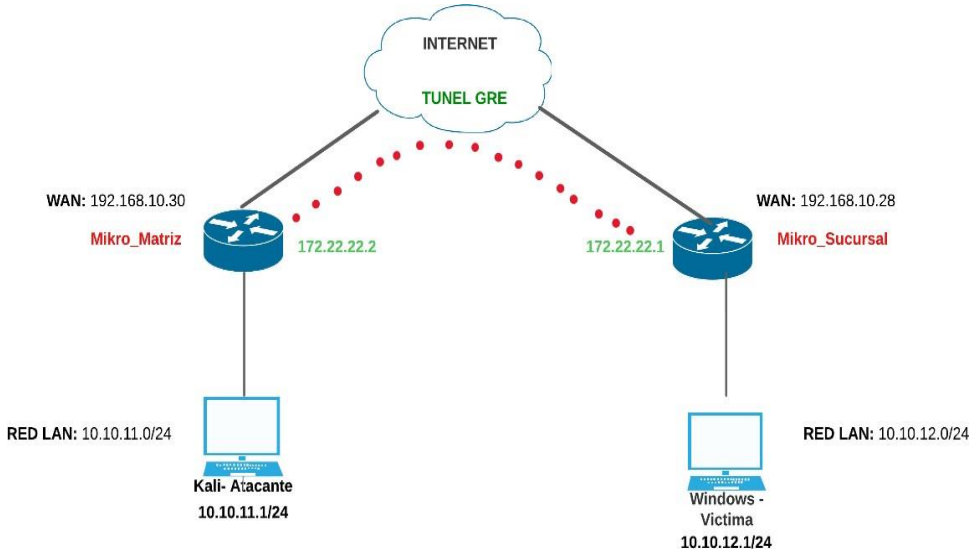
	Cisco para usarla. Debe iniciar sesión en la cuenta de la academia de Cisco para guardar las topologías en ella. • Incluye solo enrutadores y conmutadores de Cisco. No puede agregar enrutadores y conmutadores de otros proveedores.	las imágenes de IOS por tu cuenta. • Necesita una instalación local para funcionar. • Si su sistema tiene menos configuración de hardware, GNS3 no funcionará correctamente.

Elaborado por: Chela E & Utitiaja J.

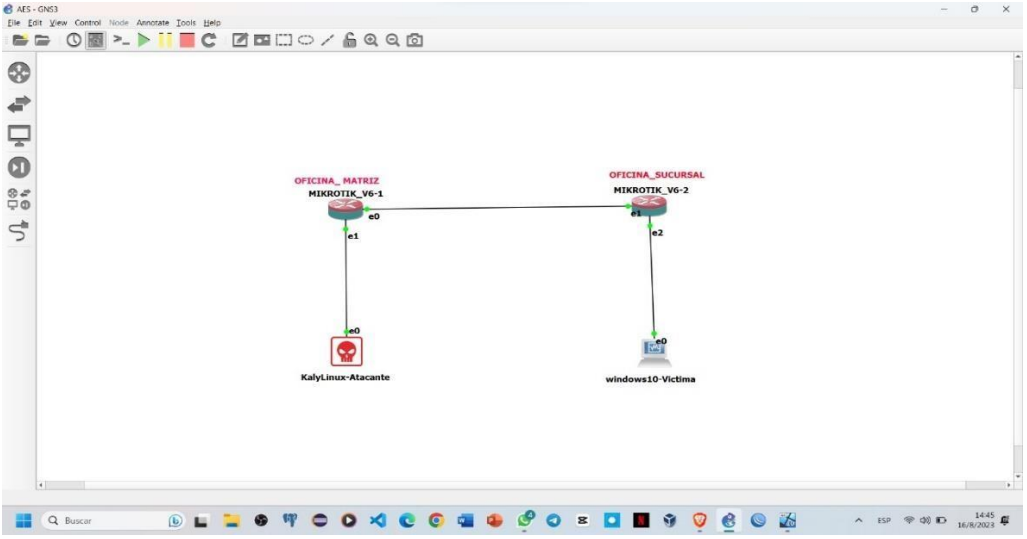
4.11. Practica experimental de encriptación (algoritmos y protocolos) con: AES, DES y 3DES

Figura 5

Topología de la red con VPN SITE TO SITE con túneles GRE+IPSEC.



Elaborado por: Chela E. & Utitiaja J.



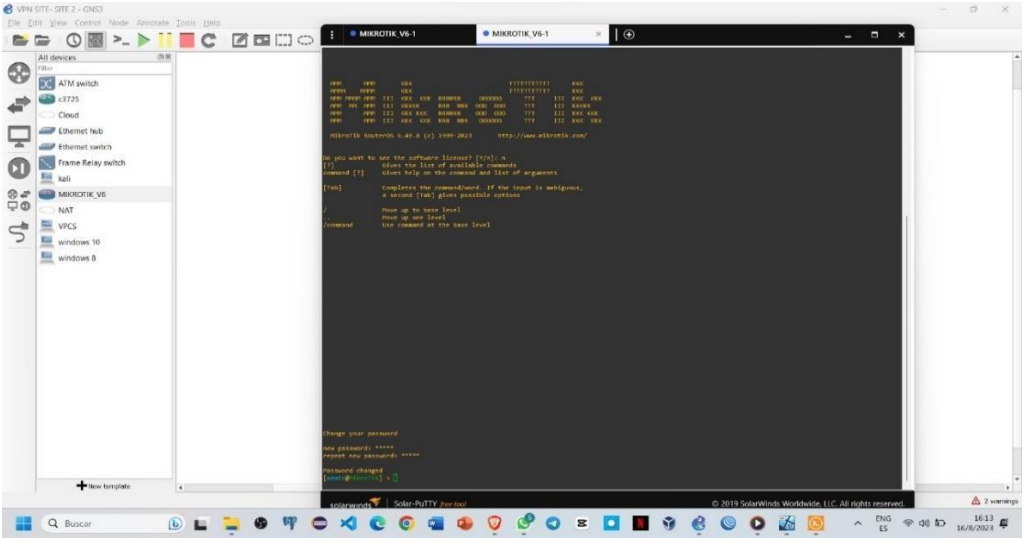
Elaborado por: Chela E. & Utitiaja J.

CONFIGURACION DE ROUTER MIKRO_MATRIZ

El router MIKRO_MATRIZ debe tener salida a internet: IP WAN, IP LAN, DNS, RUTA POR DEFAULT, NAT WAN; se configurará la interfaz eth1 con una ip privada (simulando una dirección ip publica fija en el equipo); también se sugiere configurar el protocolo SNTP en el equipo, y una ip en la interfaz ETH2

Figura 6

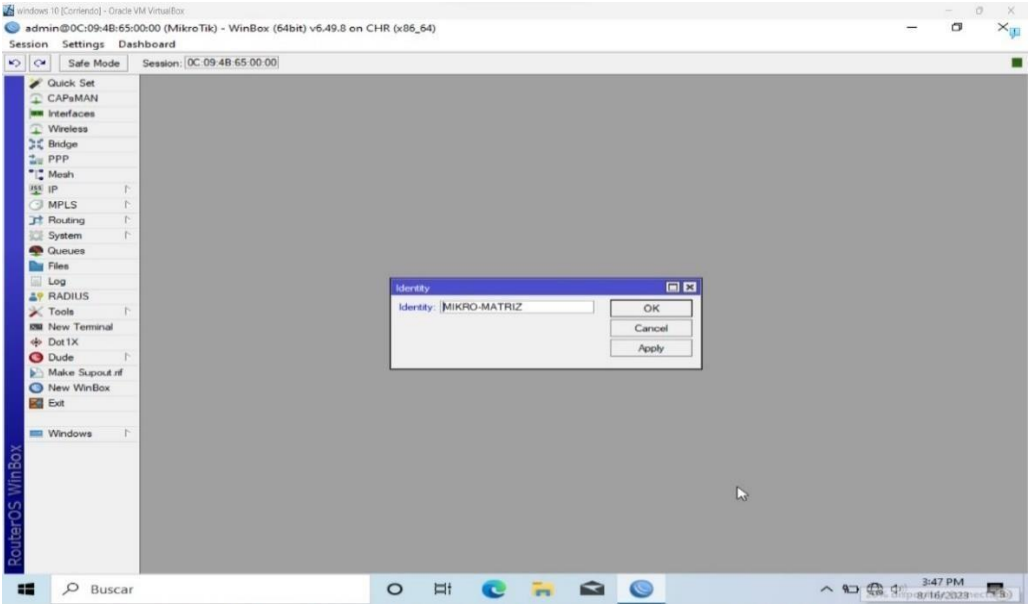
Encendemos el router



Elaborado por: Chela E. & Utitiaja J.

Figura 7

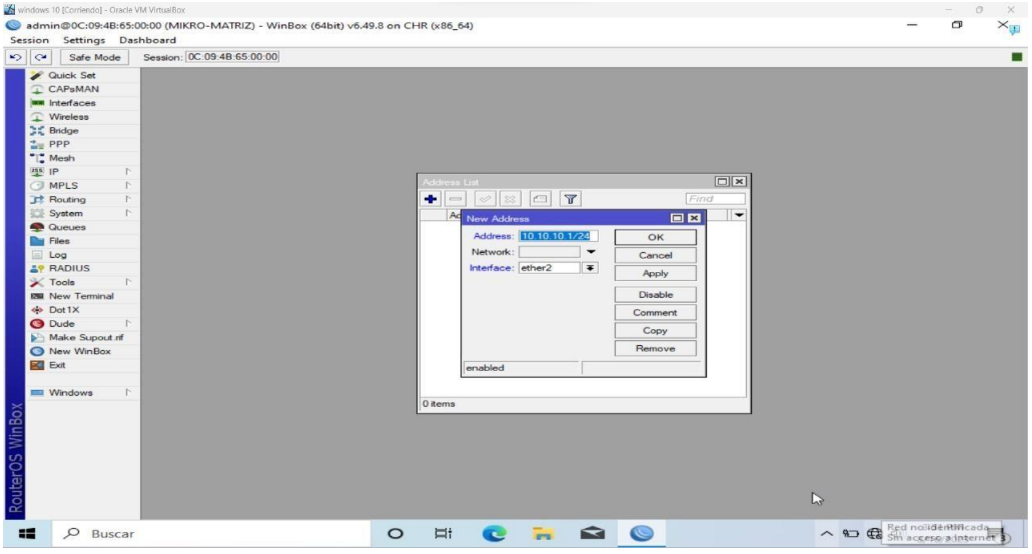
Iniciamos la configuración colocar el nombre MIKRO_MATRIZ para poder diferenciarlo al otro router.



Elaborado por: Chela E. & Utitiaja J.

Figura 8

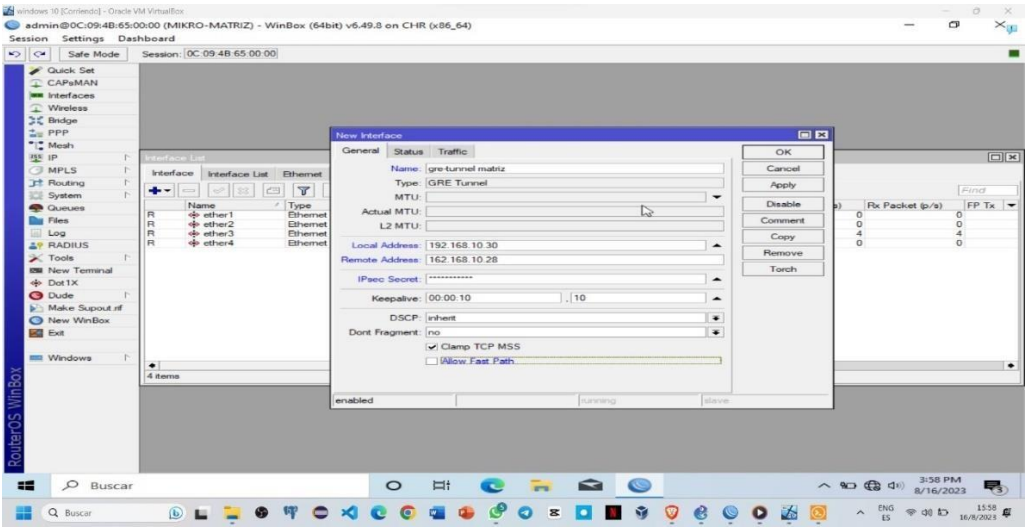
Dirigimos a Ip address a continuación seleccionamos la ethernet 2 y colocamos la Ip 192.168.10.1/24



Elaborado por: Chela E. & Utitiaja J.

Figura 9

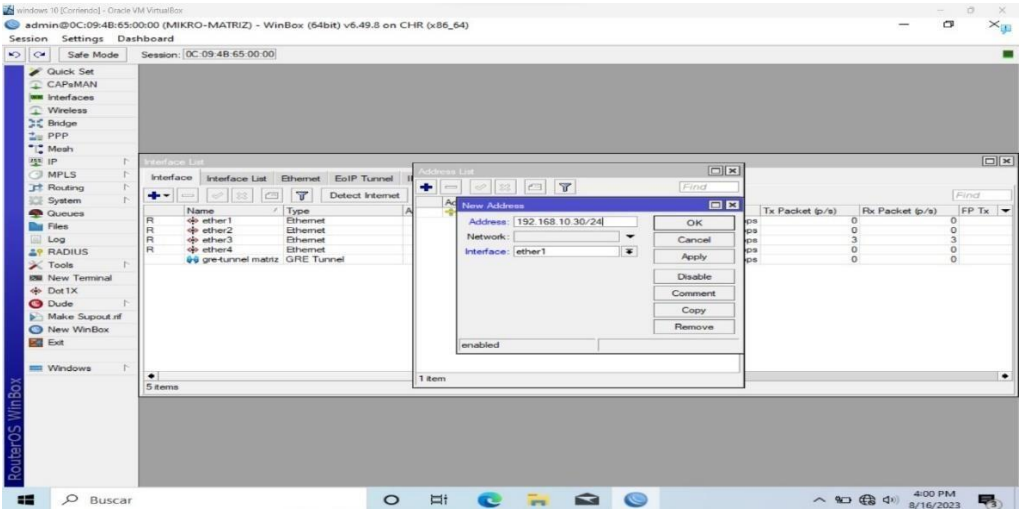
El router MIKRO_MATRIZ seleccionamos en interface, GRE TUNNEL, clic en más, y se completan los campos indicados a continuación, tome en cuenta que la dirección ip local y remota corresponden a las ips de las interfaces WAN del router Matriz y router Local, además de la clave IPSEC



Elaborado por: Chela E. & Utitiaja J.

Figura 10

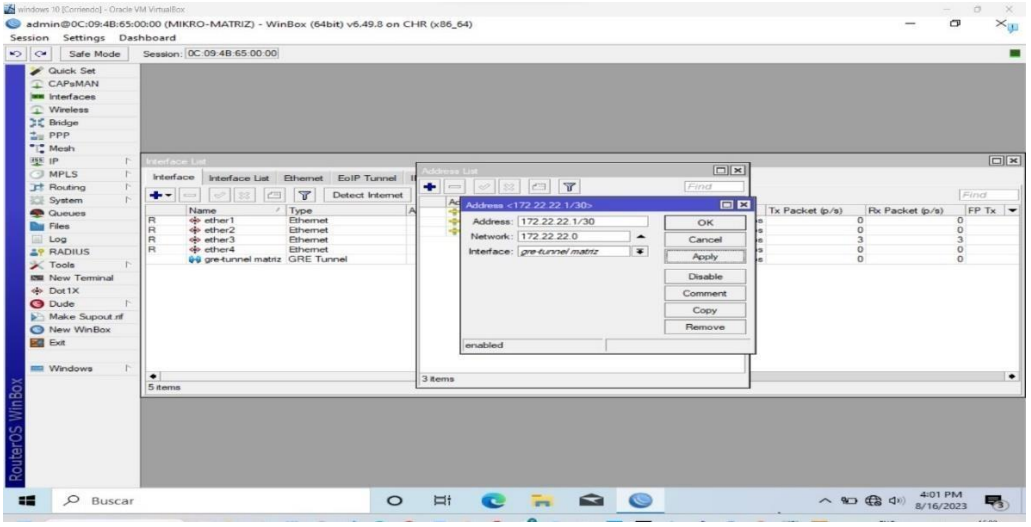
Dirigimos a Ip address a continuación seleccionamos la ethernet 1 y colocamos la Ip 192.168.10.30/24



Elaborado por: Chela E. & Utitiaja J.

Figura 11

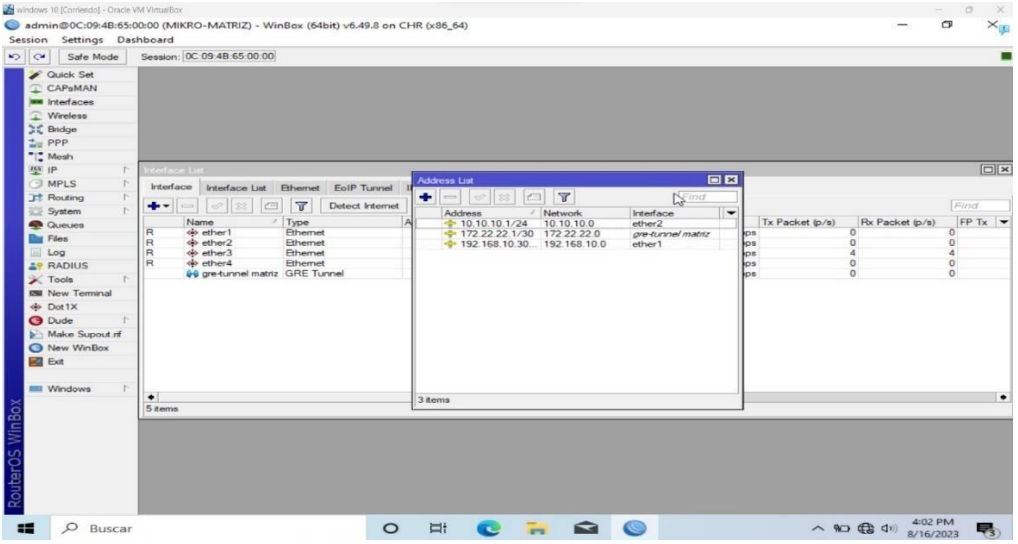
Se asigna una dirección ip a la interfaz del túnel EoIP creado recientemente, dirigimos a Ip address y colocamos una ip al túnel 172.22.22.1/30 y seleccionamos la interface gre tunnel matriz.



Elaborado por: Chela E. & Utitiaja J.

Figura 12

Dirigimos al ip address y observamos que ya está agregado la interface 2, interface virtual que es la fast 1.



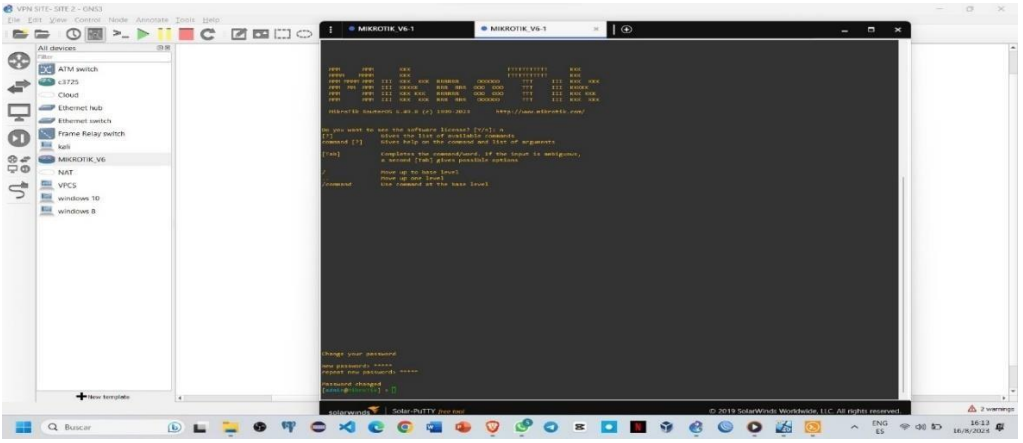
Elaborado por: Chela E. & Utitiaja J.

ROUTER_SUCURSAL

En este equipo es necesario configurar el acceso a internet: dirección ip en la interfaz WAN, dirección ip en la interfaz LAN, ruta por default, DNS, NAT; comprobar el acceso a internet desde este equipo. Considere configurar la interfaz ETH2 (red LAN) del equipo con el direccionamiento: 10.10.12.1/24

Figura 13

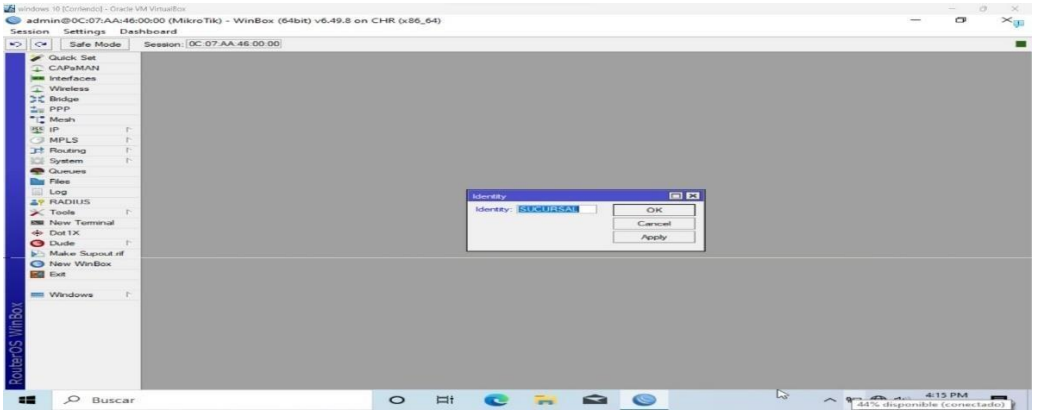
Encendemos el router y asignamos un usuario y una contraseña para continuar con la configuración del router MikroTik.



Elaborado por: Chela E. & Utitiaja J.

Figura 14

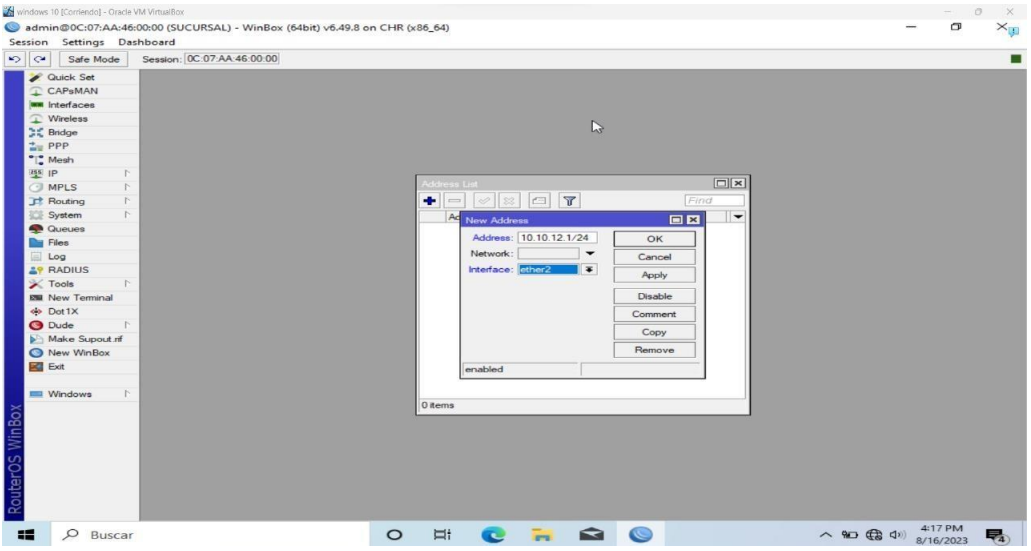
Iniciamos la configuración colocar el nombre SUCURSAL para poder diferenciarlo al otro router.



Elaborado por: Chela E. & Utitiaja J.

Figura 15

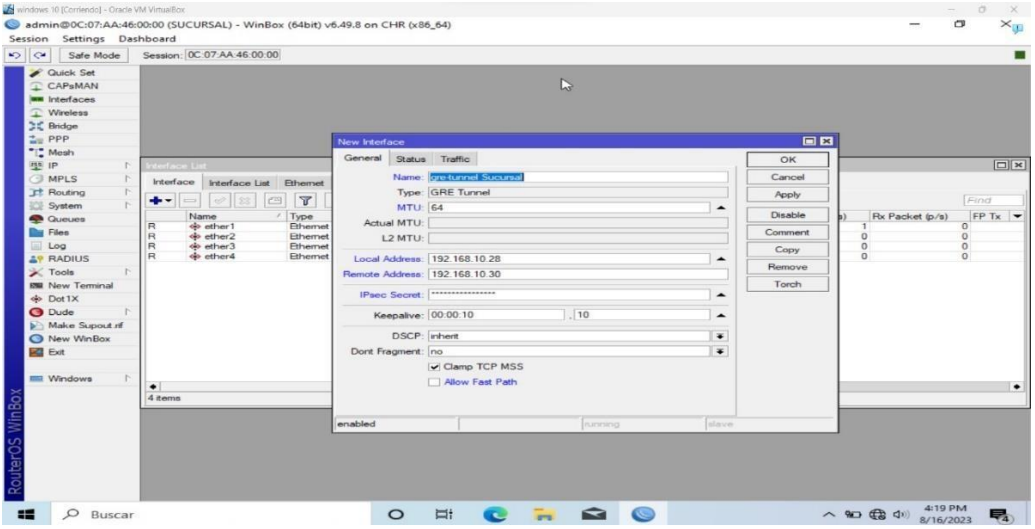
Dirigimos a Ip address a continuación seleccionamos la ethernet 2 y colocamos la Ip 10.10.12.1/24



Elaborado por: Chela E. & Utitiaja J.

Figura 16

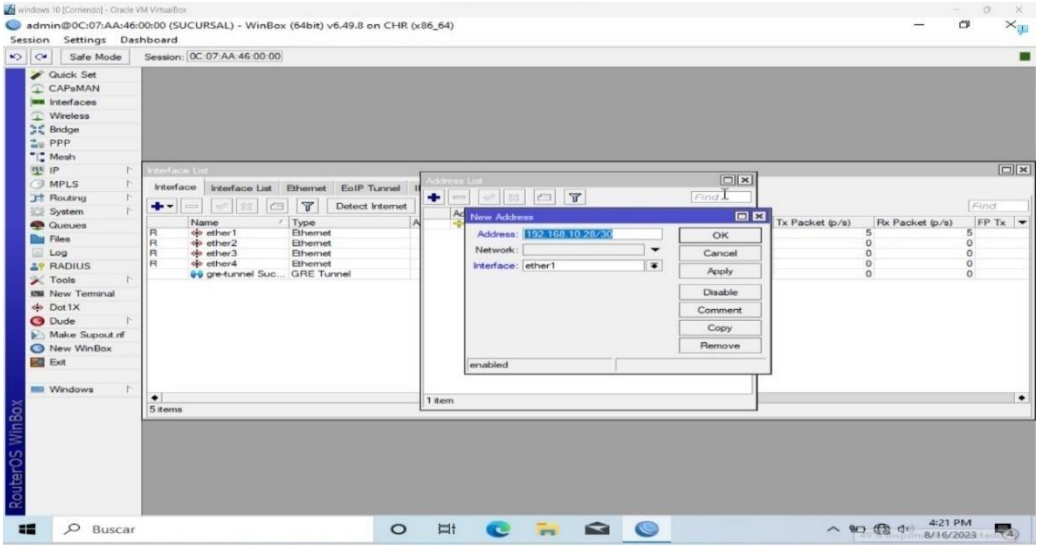
El router MIKRO_MATRIZ seleccionamos en interface, GRE TUNNEL, clic en más, y se completan los campos indicados a continuación, tome en cuenta que la dirección ip local y remota corresponden a las ips de las interfaces WAN del router Matriz y router Local, además de la clave IPSEC



Elaborado por: Chela E. & Utitiaja J.

Figura 17

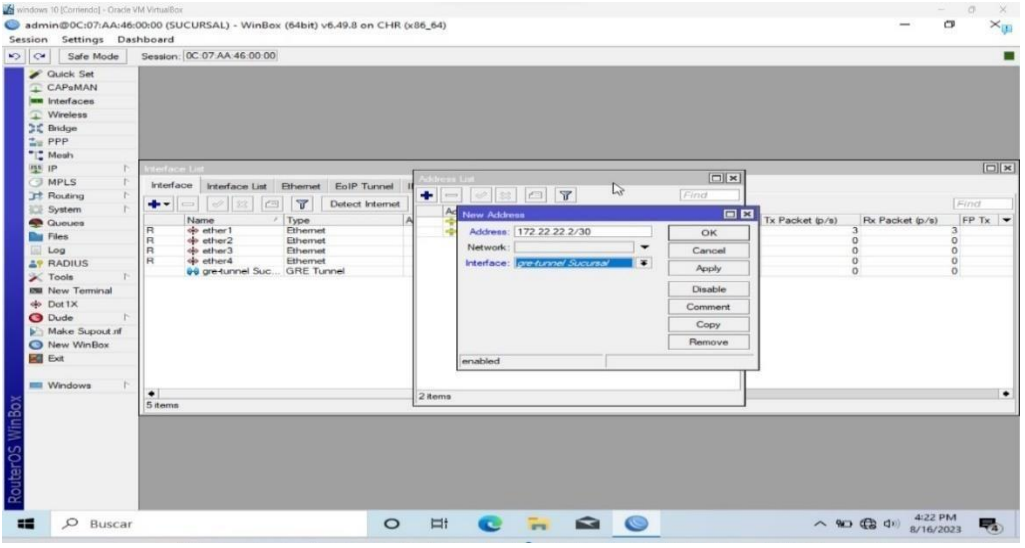
Dirigimos a Ip address a continuación seleccionamos la ethernet 1 y colocamos la Ip 192.168.10.28/30



Elaborado por: Chela E. & Utitiaja J.

Figura 18

Se asigna una dirección ip a la interfaz del túnel EoIP creado recientemente, dirigimos a Ip address y colocamos una ip al túnel 172.22.22.1/30 y seleccionamos la interface gre tunnel matriz.

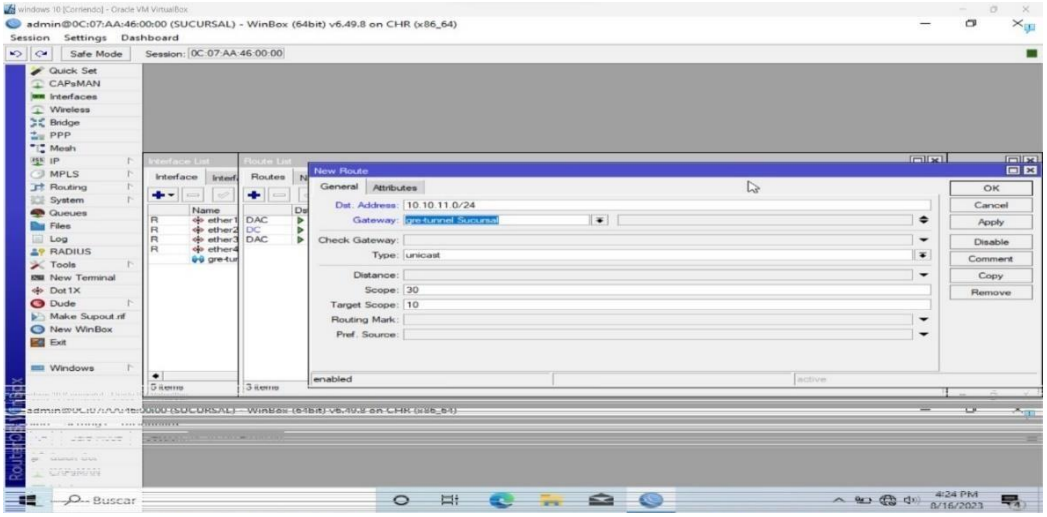


Elaborado por: Chela E. & Utitiaja J.

Figura 19

Es necesario agregar una ruta estática en el equipo, siendo el destino la red LAN de la Matriz de la empresa, y el siguiente salto la interfaz EoIP creada recientemente, aplicar los cambios

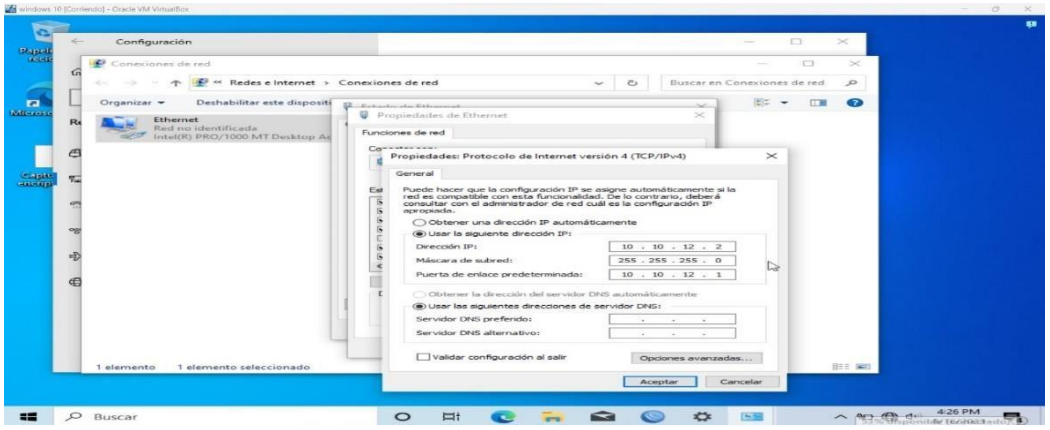
Dirigimos a ip Route y colocamos la ruta estática 10.10.11.0/24 en el Gateway gre-tunnel sucursal.



Elaborado por: Chela E. & Utitiaja J.

Figura 20

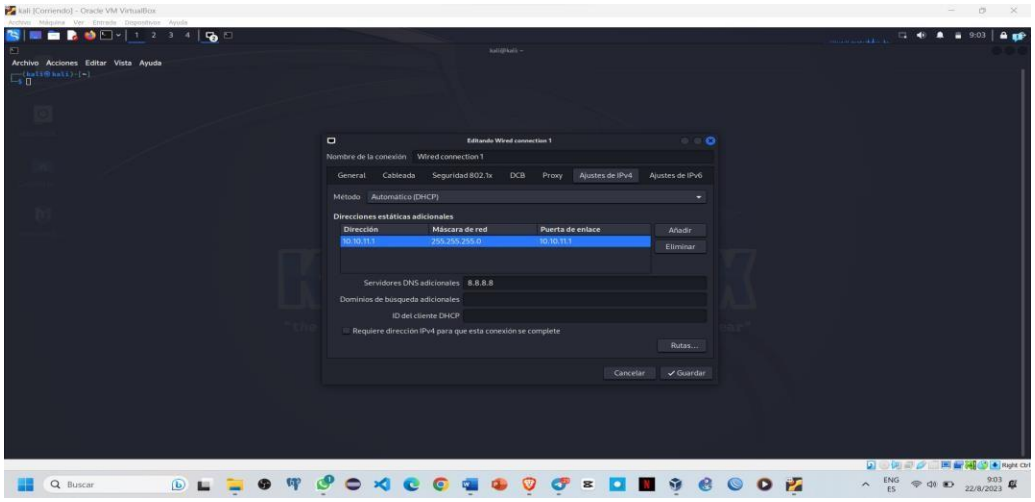
Abrimos la tarjeta de red de Windows para colocar la siguiente ip 10.10.11.2, mascara de res 255.255.255.0 y la puerta de enlace 10.10.12.1 que es la ip del router.



Elaborado por: Chela E. & Utitiaja J.

Figura 21

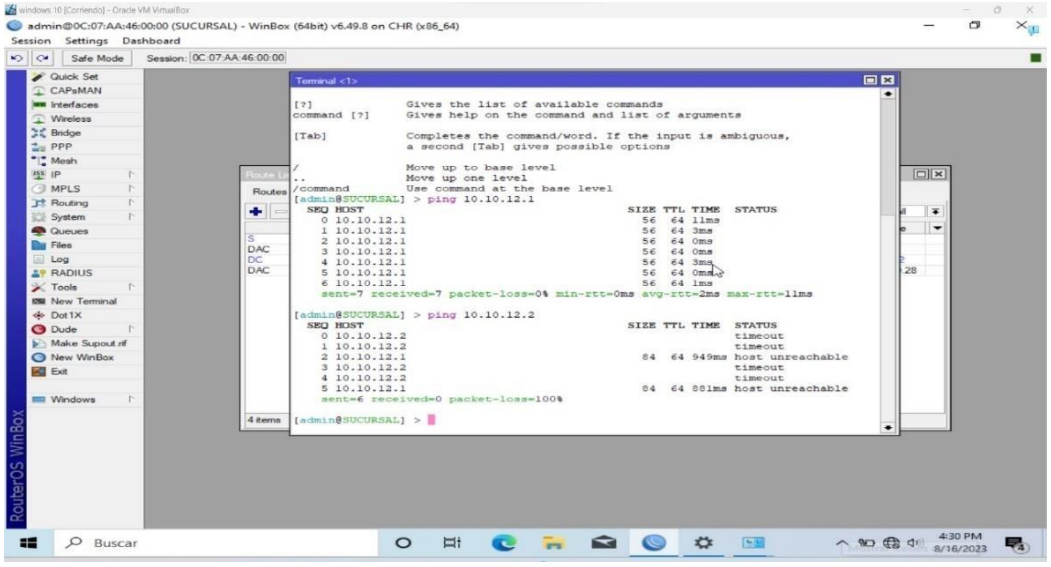
Abrimos la tarjeta de red de Windows para colocar la siguiente ip 10.10.11.1, mascara de res 255.255.255.0 y la puerta de enlace 10.10.11.1 que es la ip del router.



Elaborado por: Chela E. & Utitiaja J.

Figura 22

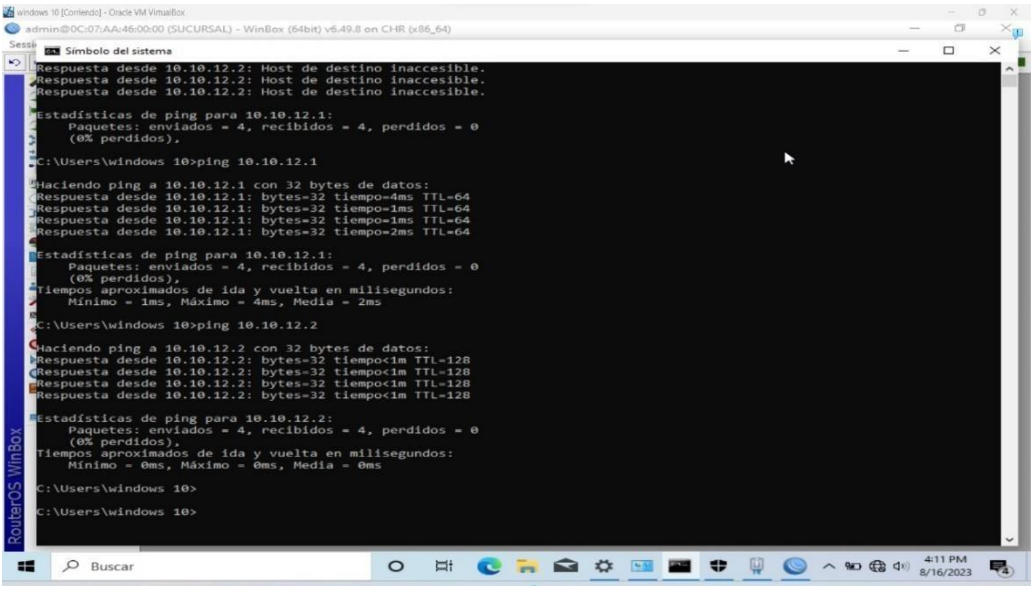
Ingresamos al terminal de winbox y realizamos in ping al 10.10.12.1 y al 10.10.12.2 y observamos que ya tienen la conectividad.



Elaborado por: Chela E. & Utitiaja J.

Figura 23

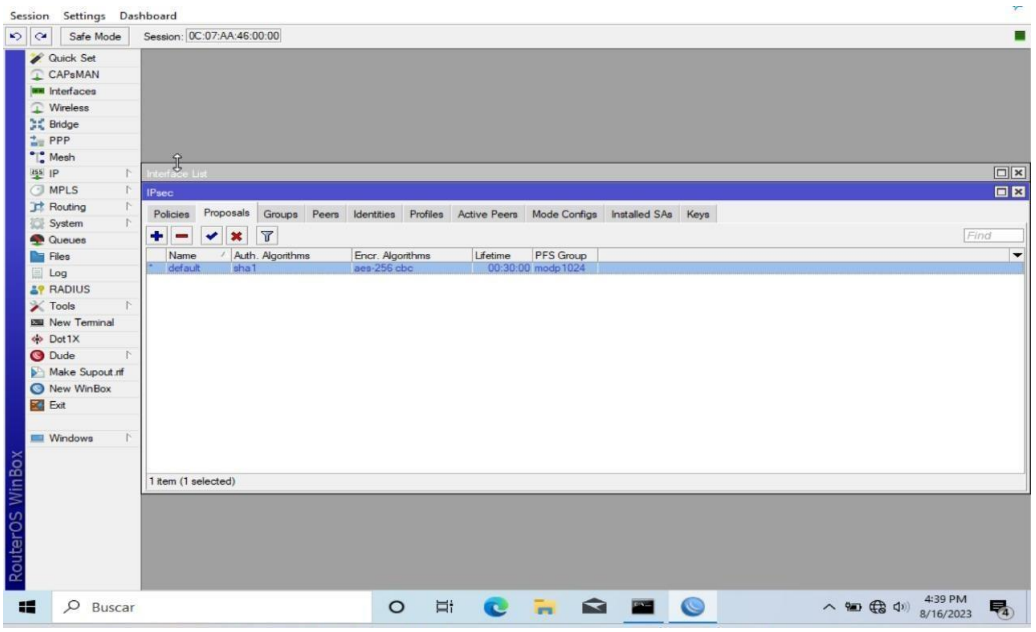
Ingresamos al terminal de Windows 10 y realizamos en ping al 10.10.12.1 y al 10.10.12.2 y observamos que ya tienen la conectividad.



Elaborado por: Chela E. & Utitiaja J.

Figura 24

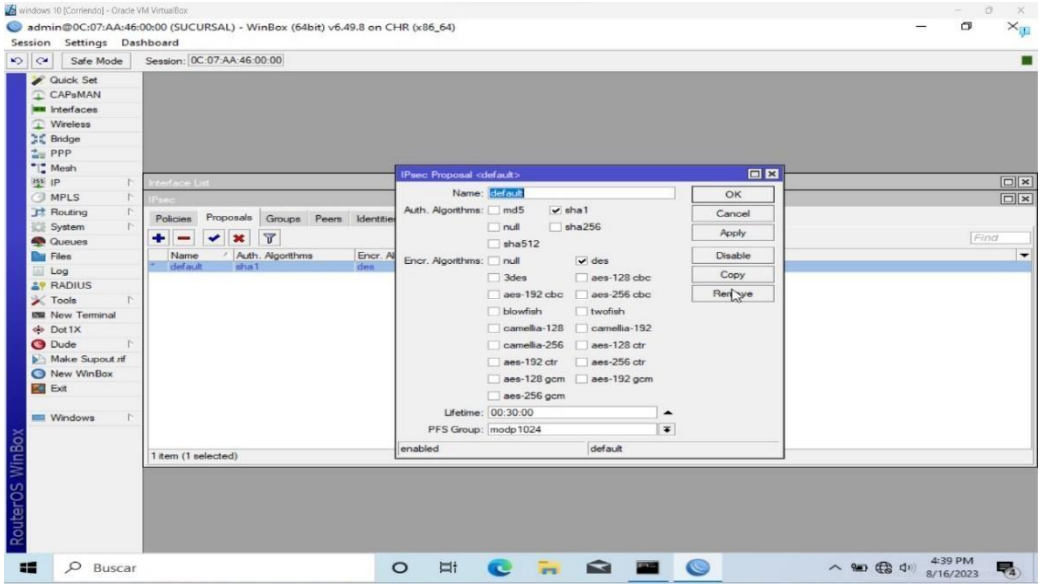
En la primera instancia aplicamos el algoritmo de encriptación Aes de 256 bits



Elaborado por: Chela E. & Utitiaja J.

Figura 25

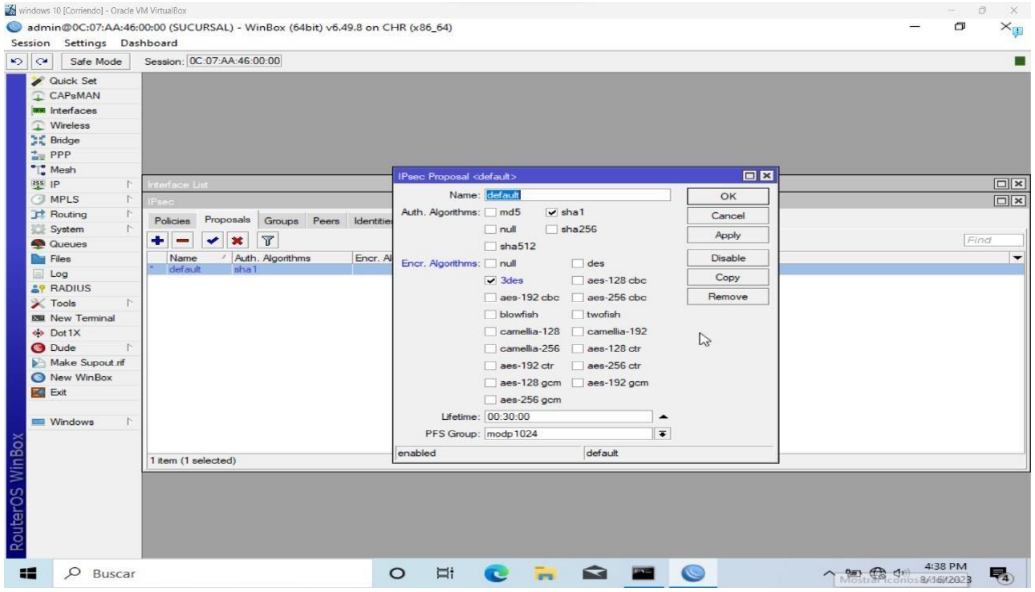
En segunda instancia aplicamos el algoritmo de encriptación Des.



Elaborado por: Chela E. & Utitiaja J.

Figura 26

En segunda instancia aplicamos el algoritmo de encriptación 3DES.



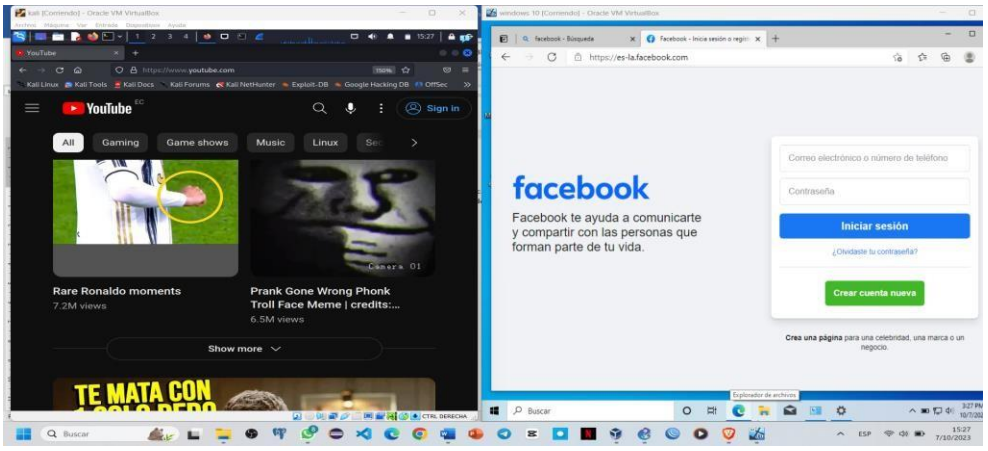
Elaborado por: Chela E. & Utitiaja J.

4.12. Ataque de denegación de servicio kali linux ettercap y ping a la maquina victima windows

- **Router mikrotik con encriptación DES**

Figura 27

Router mikrotik con encriptación DES

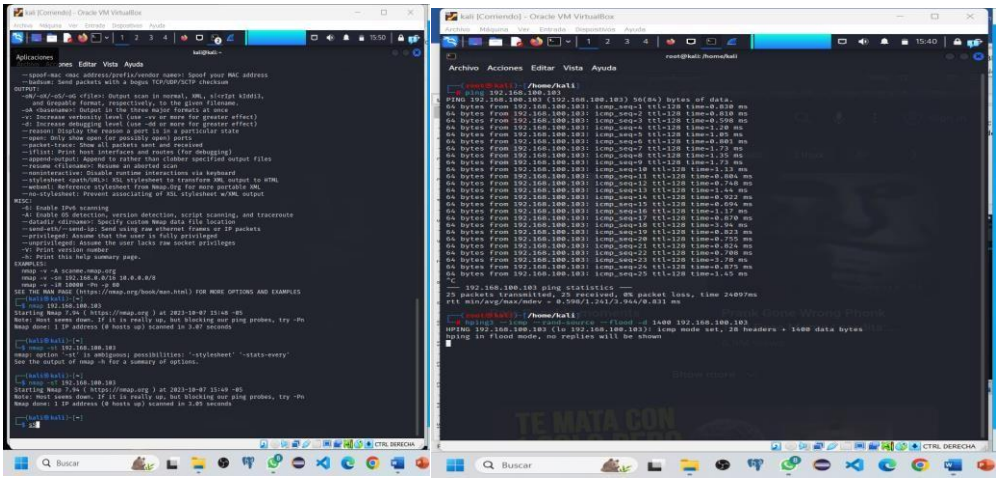


Elaborado por: Chela E. & Utitiaja J.

Podemos observar ambas maquinas conectadas a la misma red, por lo cual el ataque de denegación de servicio trata de enviar varios paquetes hasta que un servidor colapse o alguna computadora colapse de algún sitio especifico. Podemos usar varios métodos

Figura 28

Escaneos de puertos.

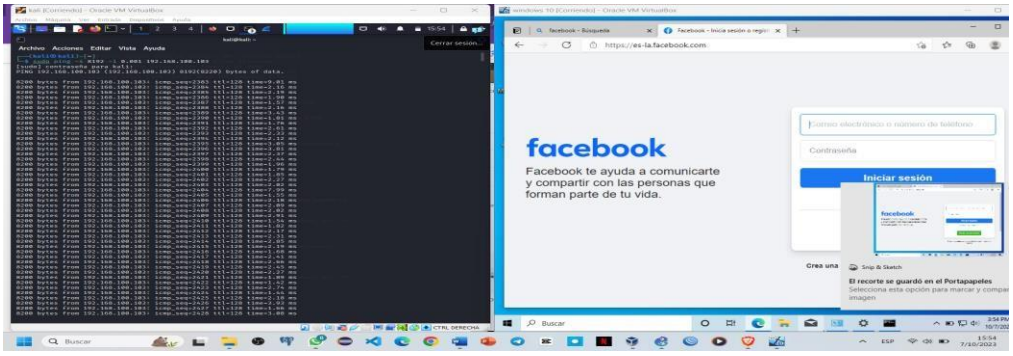


Elaborado por: Chela E. & Utitiaja J.

Primeramente, realizaremos un ping al ip de la víctima en este caso será un dispositivo que está conectado a la misma red a continuación, escaneamos puertos para visualizar que puerto esta vulnerable para eso ingresamos el siguiente código con la ip de la víctima que quiero atacar y dando a conocer que puerto está abierto.

Figura 29

Ping de la muerte.

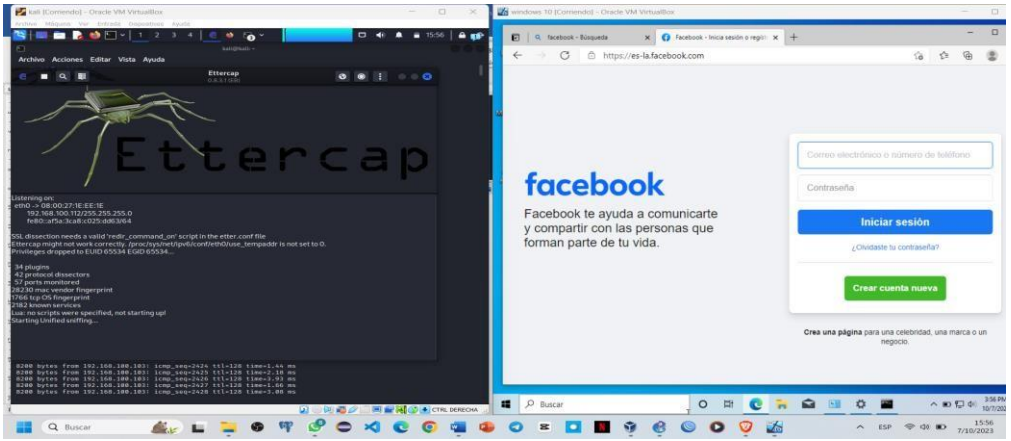


Elaborado por: Chela E. & Utitiaja J.

Ahí varios tipos de ataques en este caso vamos a realizar el ping de la muerte para esto ingresamos el siguiente código en el terminal de Linux sudo ping -s 8190 -i 0.001 192.168.100.103 y empieza a enviar un sin número de paquetes este es un tipo de ataque.

Figura 30

Ingresamos al programa ettercap

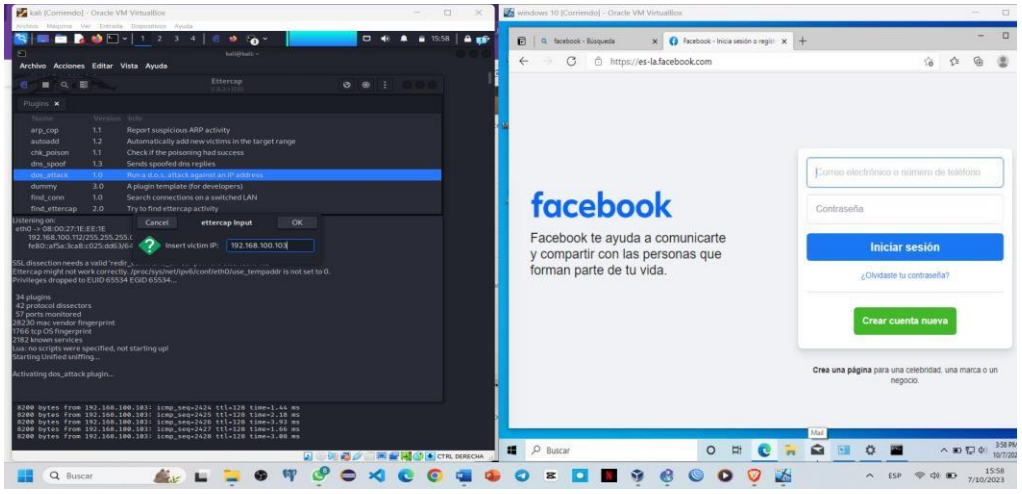


Elaborado por: Chela E. & Utitiaja J.

Ingresamos al programa ettercap donde iniciamos y comienza asiendo un barrido la misma aplicación.

Figura 31

El ataque Dos.

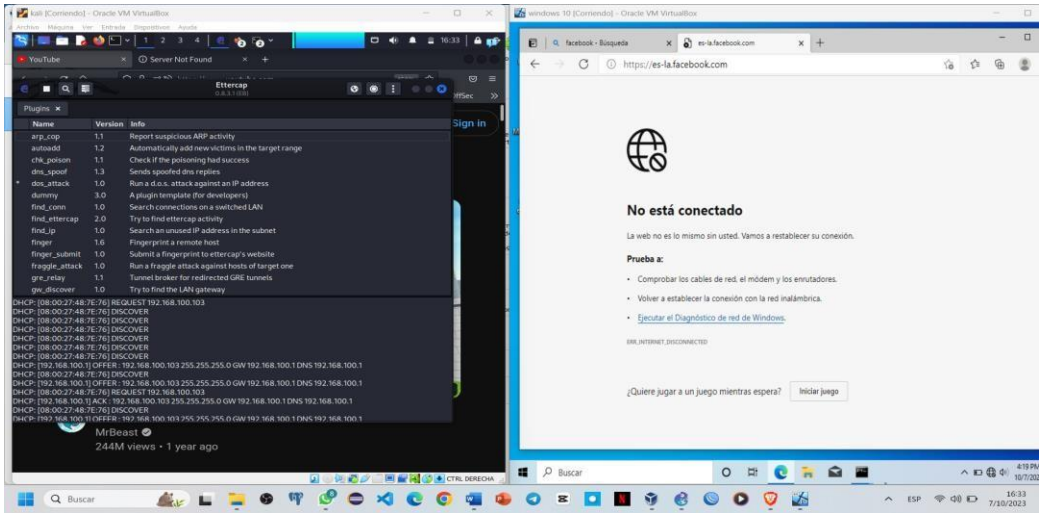


Elaborado por: Chela E. & Utitiaja J.

Para el siguiente procedimiento seleccionamos el ataque Dos en la cual ingresamos la ip de la maquina víctima y damos clik en ok y automáticamente comienza el ataque

Figura 32

El ataque de denegación de servicio.



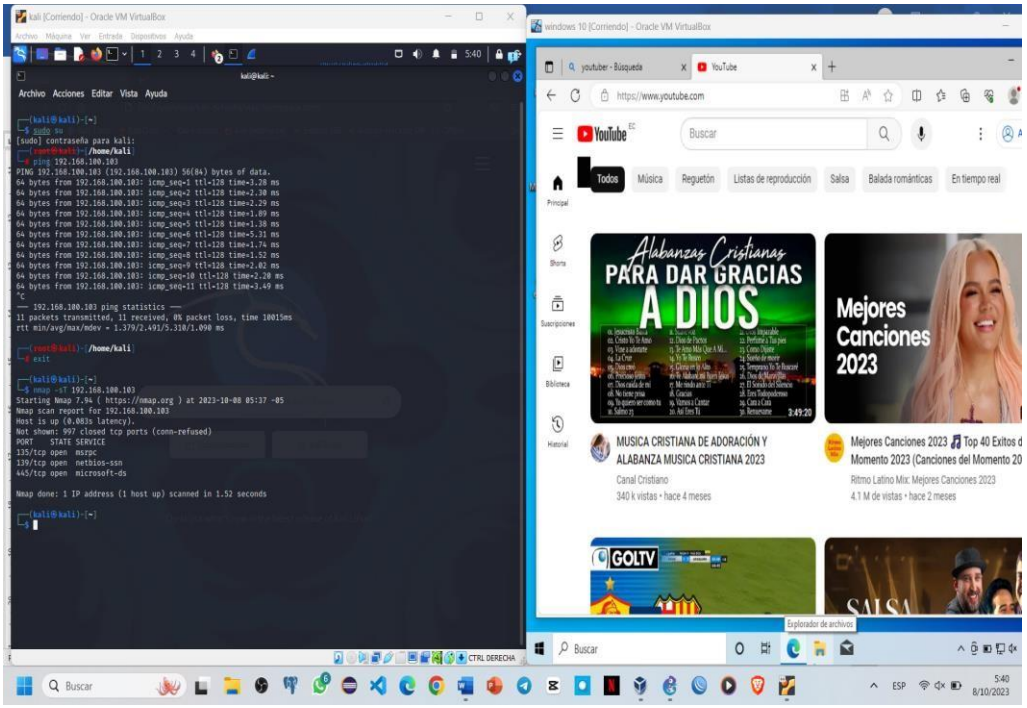
Elaborado por: Chela E. & Utitiaja J.

Podemos notar a través de la herramienta Ettercap que se está llevando a cabo un ataque de denegación de servicio dirigido al PC con Windows, donde se encuentra una página precargada de Facebook. Si intentamos recargar la página, resulta evidente que el servicio de Internet ya no está disponible, ya que el ataque de denegación de servicio ha enviado múltiples paquetes con el objetivo de saturar la máquina, lo que impide la carga de cualquier contenido en el navegador.

Router mikrotik con encriptación 3DES

Figura 33

Escaneos de puertos.

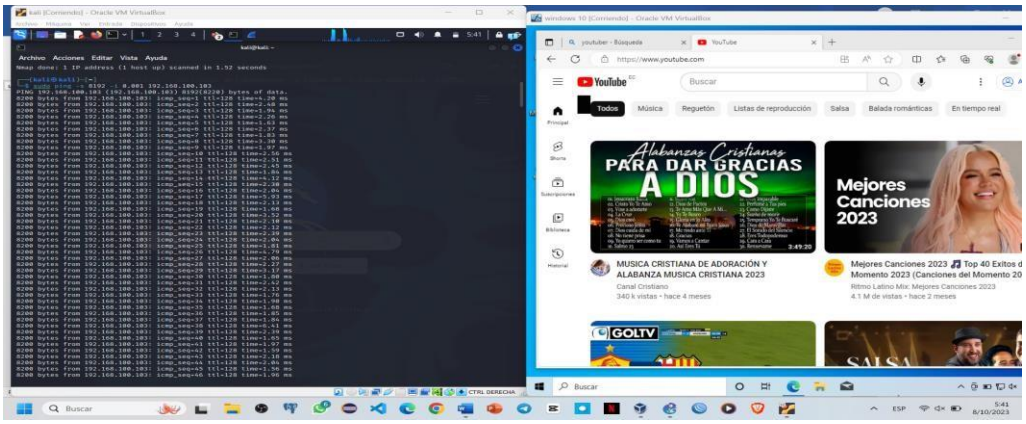


Elaborado por: Chela E. & Utitiaja J.

Primero, llevaremos a cabo un ping al dispositivo víctima, que se encuentra en la misma red. A continuación, realizaremos un escaneo de puertos para identificar posibles vulnerabilidades. Para ello, emplearemos el siguiente código con la dirección IP del dispositivo objetivo, lo que nos permitirá determinar qué puerto se encuentra accesible.

Figura 34

Ping de la muerte.

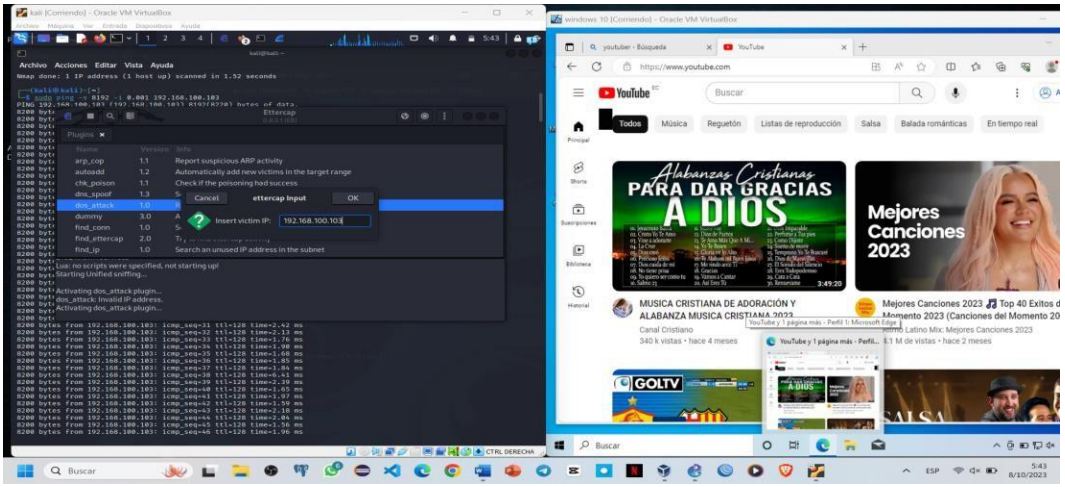


Elaborado por: Chela E. & Utitiaja J.

Ahí varios tipos de ataques en este caso vamos a realizar el ping de la muerte para esto ingresamos el siguiente código en el terminal de Linux sudo ping -s 8190 -i 0.001 192.168.100.103 y empieza a enviar un sin número de paquetes este es un tipo de ataque.

Figura 35

Programa ettercap

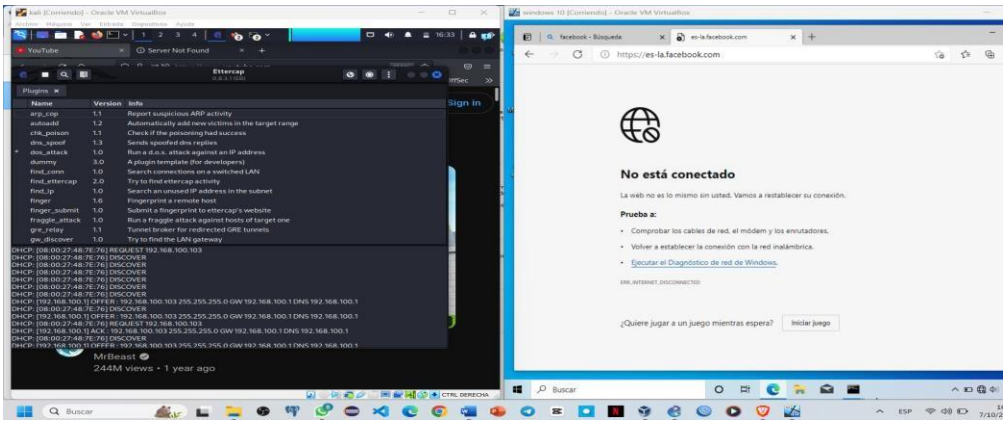


Elaborado por: Chela E. & Utitiaja J.

Ingresamos al programa ettercap donde iniciamos y comienza asiendo un barrido la misma aplicación en la cual ingresamos la ip de la maquina victima que quien va a hacer atacado.

Figura 36

El ataque de denegación de servicio.



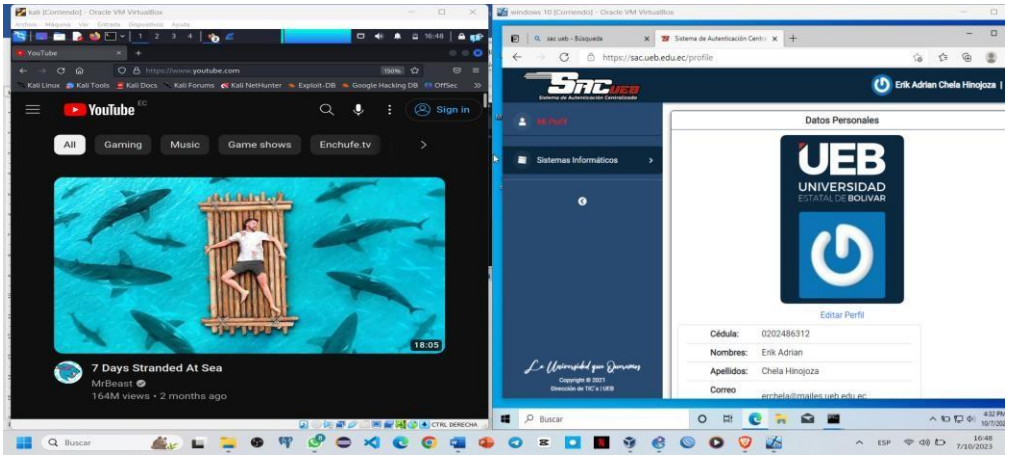
Elaborado por: Chela E. & Utitiaja J.

Como podemos observar que atreves de ettercap que está realizando el ataque de denegación de servicio que mandamos al pc de Windows en la cual se encuentra la página precargada de YouTube, si nuevamente le recargamos la página podemos observar que no tiene servicio a internet ya que el ataque de denegación de servicio envié varios paquetes en este caso se realizó que se colapse esta máquina que no cargue nada en el navegador.

- **Router mikrotik con encriptación AES.**

Figura 37

Router mikrotik con encriptación AES.

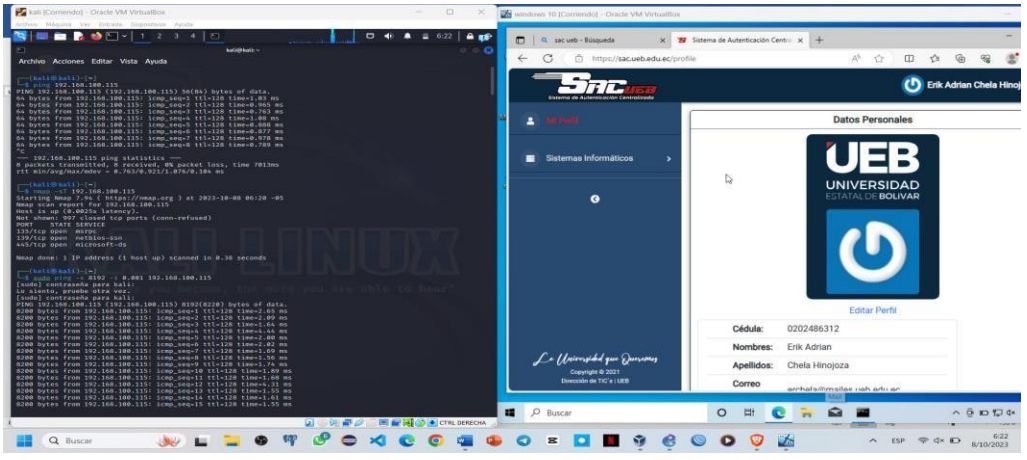


Elaborado por: Chela E. & Utitiaja J.

Podemos observar ambas maquinas conectadas a la misma red, por lo cual el ataque de denegación de servicio trata de enviar varios paquetes hasta que un servidor colapse o alguna computadora colapse de algún sitio especifico. Podemos usar varios métodos.

Figura 38

Ping de la muerte.

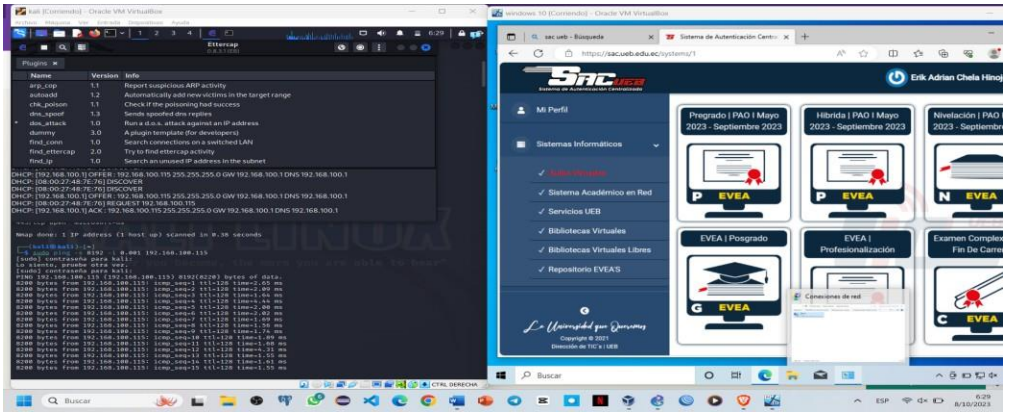


Elaborado por: Chela E. & Utitiaja J.

Ahí varios tipos de ataques en este caso vamos a realizar el ping de la muerte para esto ingresamos el siguiente código en el terminal de Linux sudo ping -s 8190 -i 0.001 192.168.100.103 y empieza a enviar un sin número de paquetes este es un tipo de ataque.

Figura 39

Denegación de servicios.



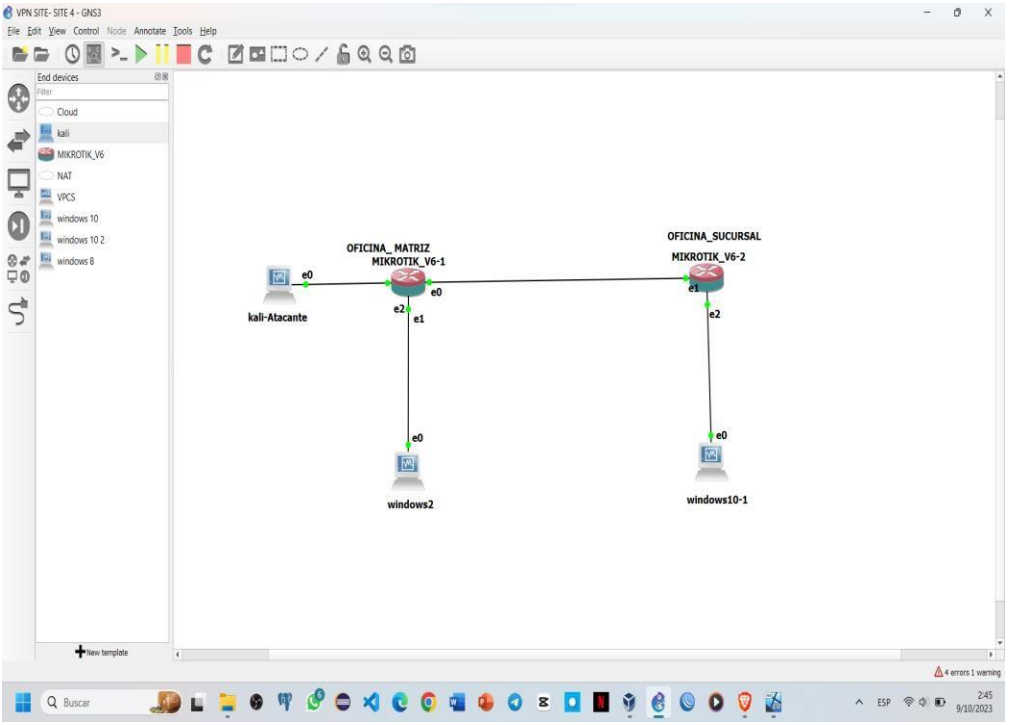
Elaborado por: Chela E. & Utitiaja J.

Como podemos observar que atreves de ettercap que está realizando el ataque de denegación de servicio que mandamos al pc de Windows en la cual se encuentra la página precargada de SAC-UEB, si nuevamente le recargamos esta página va a estar con acceso a internet en este caso el ataque de denegación de servicio no tuvo éxito no se colapsó la maquina ni el navegador, por lo cual podemos concluir que la encriptación AES es más segura que las demás encriptaciones.

4.13. Ataque del hombre en el medio

Figura 40

Ataque del hombre en el medio



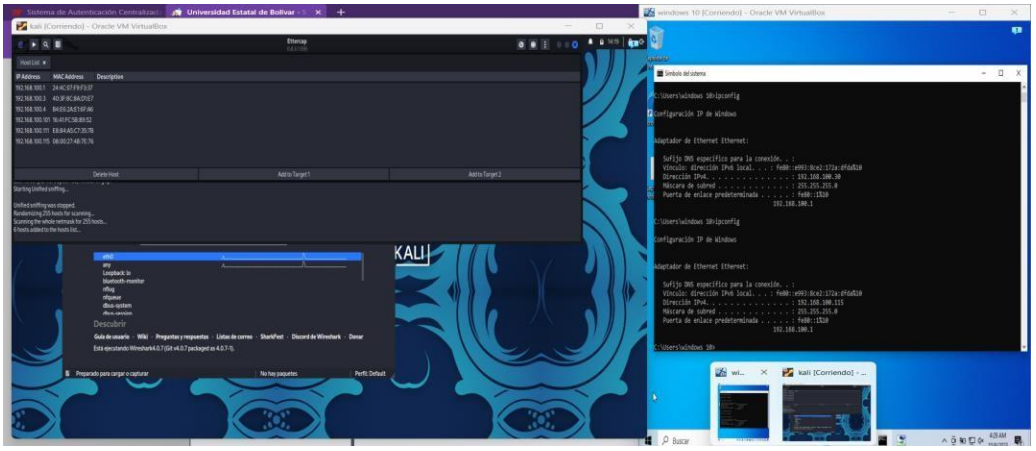
Elaborado por: Chela E. & Utitiaja J.

Para comprender este tipo de ataque, consideramos la siguiente topología en la que dos equipos están comunicándose, y un tercero actúa como intermediario interceptando las comunicaciones. Este intermediario también efectúa la captura del tráfico de red entre el equipo y su puerta de enlace, lo que le permite identificar los destinos de los sitios web a los que se accede.

ENCRIPTACION DES.

Figura 41

Encriptación DES.

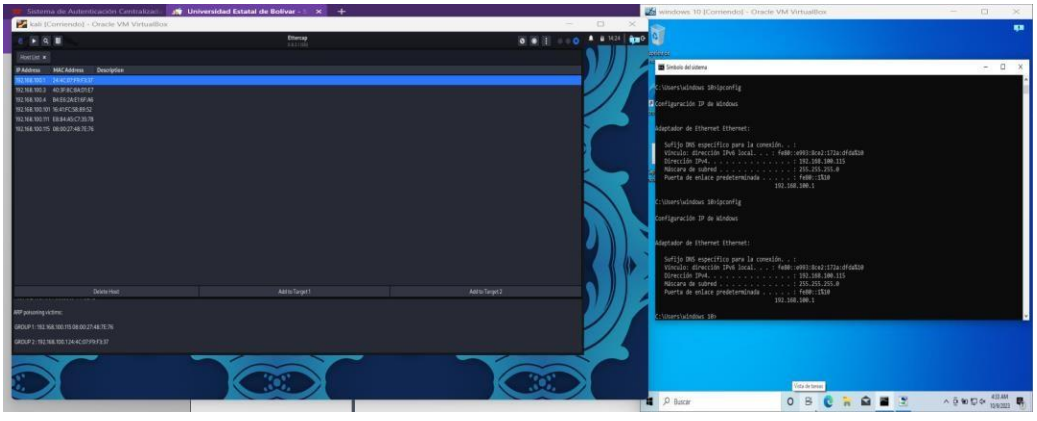


Elaborado por: Chela E. & Utitiaja J.

Nos conectamos con el usuario root en Linux y ejecutamos la herramienta ettercap quien nos ayudara a realizar diversos ataques en la cual iniciamos y realizamos un análisis de los equipos que están conectados y observamos los resultados de los análisis, por ende, nos dirigimos a la máquina de Windows para poder conocer la dirección ip de la maquina mencionada.

Figura 42

Seleccionamos la dirección ip del Windows 10.

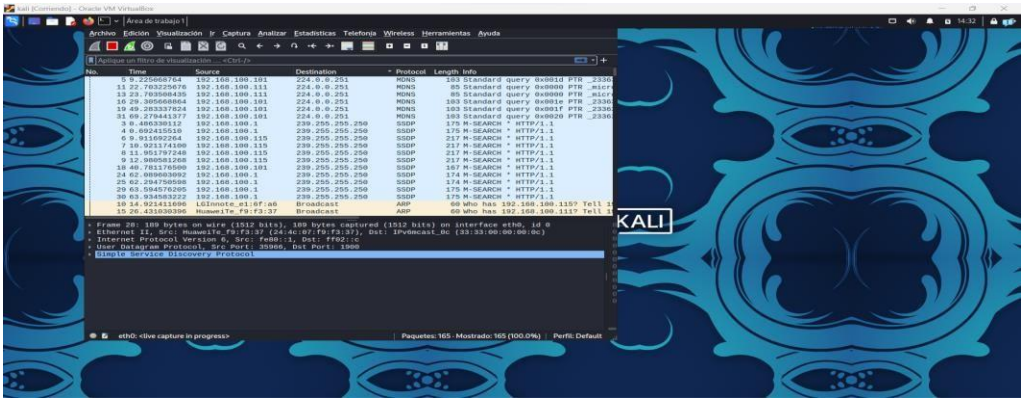


Elaborado por: Chela E. & Utitiaja J.

A continuación, seleccionamos la dirección Ip del Windows 10 y la dejamos como la primera tarjeta y la puerta de enlace como la segunda tarjeta donde vamos a estar seleccionando el ataque arp poisonig para así poder iniciar con el ataque.

Figura 43

Visualizar el tráfico de red ejecutamos wireshark.

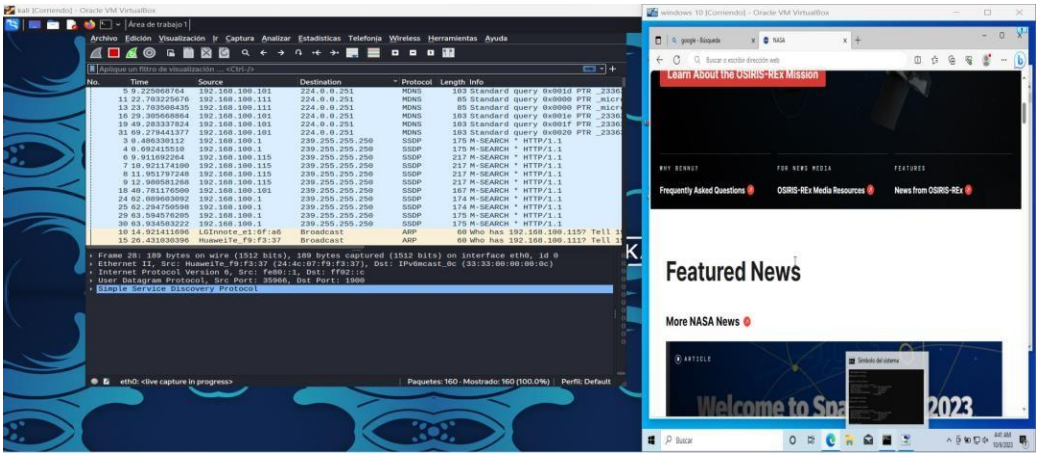


Elaborado por: Chela E. & Utitiaja J.

Para visualizar el tráfico de red, ejecutamos Wireshark y elegimos la tarjeta de red que deseamos monitorear. Esto permitirá capturar y analizar el tráfico de red en esa interfaz específica.

Figura 44

Tráfico de red en la máquina de Linux.

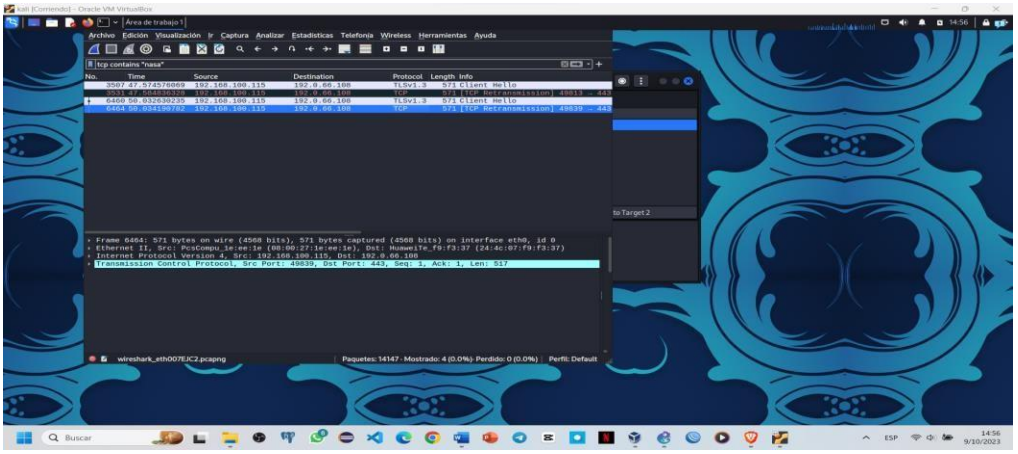


Elaborado por: Chela E. & Utitiaja J.

Al analizar el tráfico de red en la máquina de Linux ingresamos a la máquina de Windows donde ingresamos al navegador e ingresamos al sitio web de la nasa para posterior regresamos a la máquina de Kali Linux donde detenemos el análisis.

Figura 45

Búsqueda de wireshark

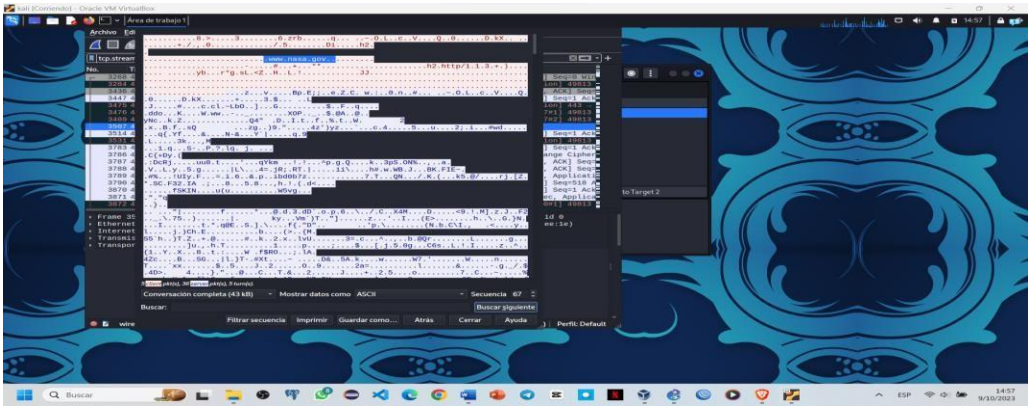


Elaborado por: Chela E. & Utitiaja J.

En el botón de búsqueda de wireshark ingresamos el siguiente comando tcp contains “nasa” donde vamos a visualizar los sitios capturados y realizamos un seguimiento.

Figura 46

Visualización de la navegación.



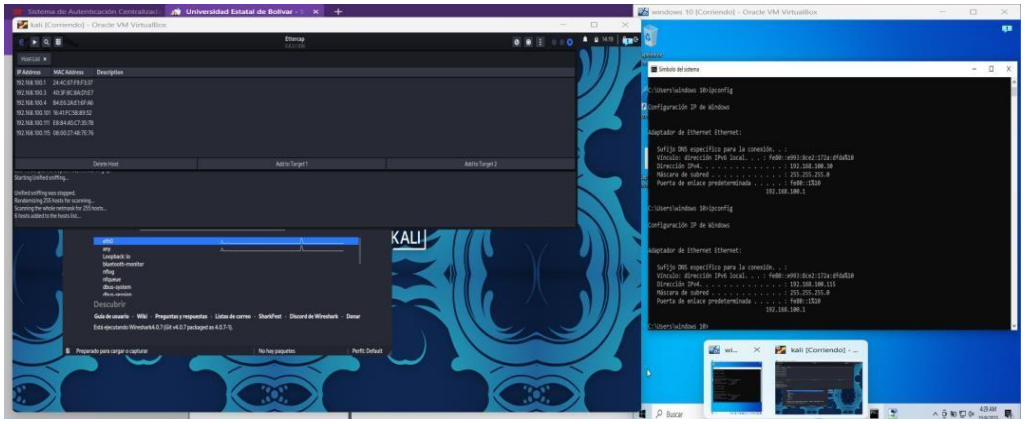
Elaborado por: Chela E. & Utitiaja J.

En este caso podemos visualizar la navegación que re realizo en la maquina víctima de Windows aparece en la ventana de seguimiento.

ENCRIPTACION 3DES

Figura 47

Usuario root en Linux.

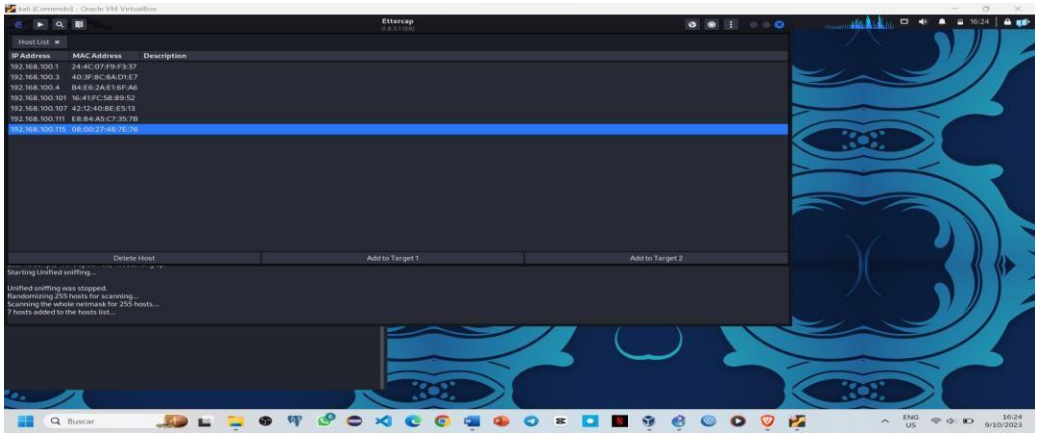


Elaborado por: Chela E. & Utitiaja J.

Nos conectamos con el usuario root en Linux y ejecutamos la herramienta ettercap quien nos ayudara a realizar diversos ataques en la cual iniciamos y realizamos un análisis de los equipos que están conectados y observamos los resultados de los análisis, por ende, nos dirigimos a la máquina de Windows para poder conocer la dirección Ip de la maquina mencionada.

Figura 48

Seleccionamos la dirección Ip del Windows 10.

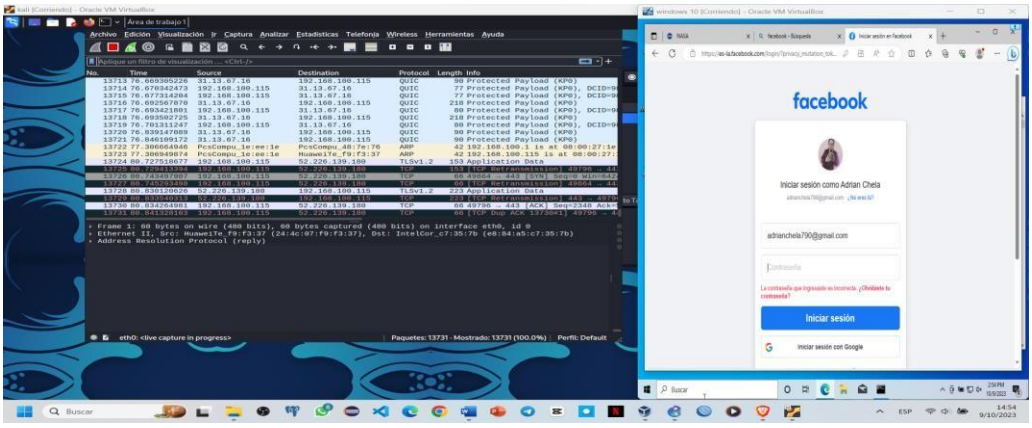


Elaborado por: Chela E. & Utitiaja J.

A continuación, seleccionamos la dirección Ip del Windows 10 y la dejamos como la primera tarjeta y la puerta de enlace como la segunda tarjeta donde vamos a estar seleccionando el ataque arp poisonig para así poder iniciar con el ataque.

Figura 49

Tráfico de red en la máquina de Linux.

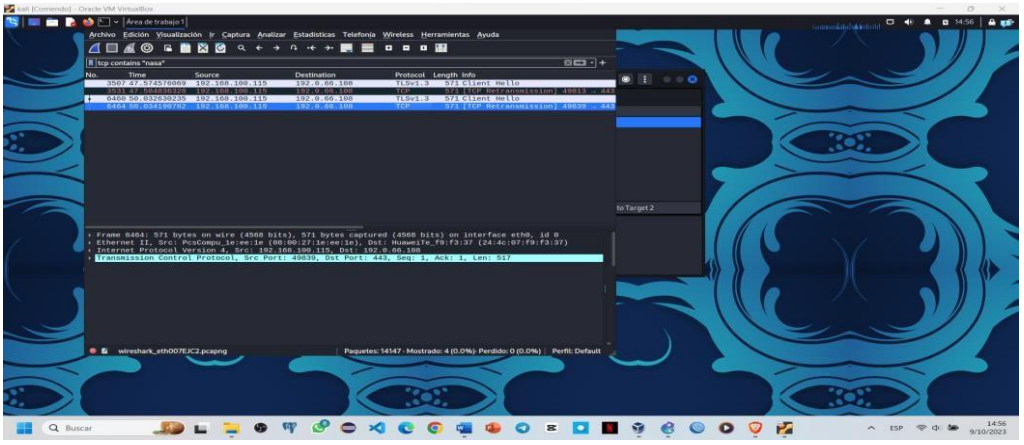


Elaborado por: Chela E. & Utitiaja J.

Al analizar el tráfico de red en la máquina de Linux ingresamos a la máquina de Windows donde ingresamos al navegador e ingresamos al sitio web de facebook para posterior regresamos a la máquina de Kali Linux donde detenemos el análisis.

Figura 50

Búsqueda de wireshark.

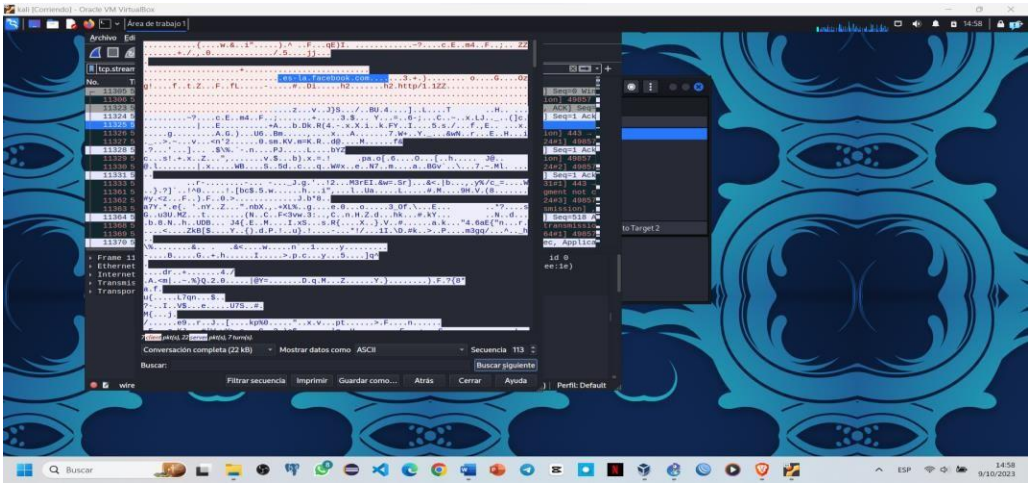


Elaborado por: Chela E. & Utitiaja J.

En el botón de búsqueda de wireshark ingresamos el siguiente comando tcp contains “facebook” donde vamos a visualizar los sitios capturados y realizamos un seguimiento.

Figura 51

Visualizar la navegación.

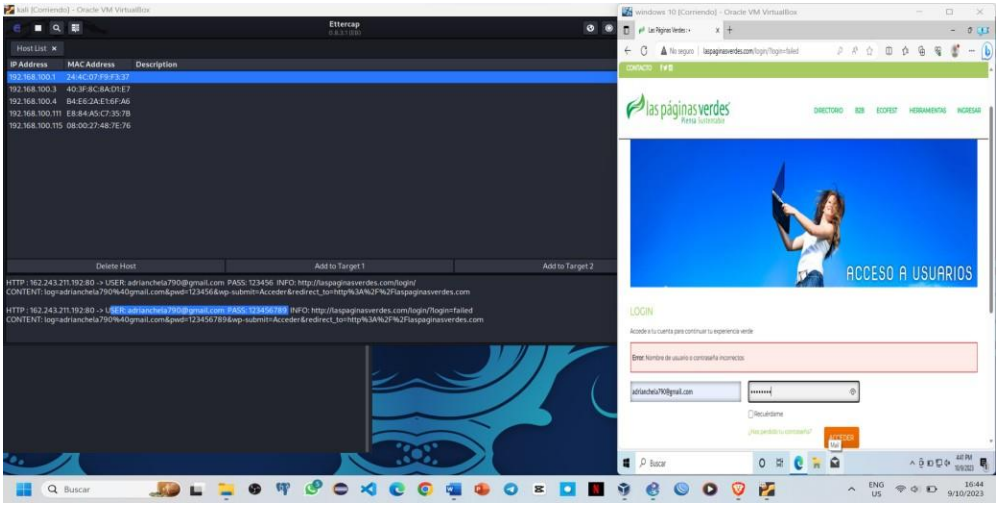


Elaborado por: Chela E. & Utitiaja J.

En este caso podemos visualizar la navegación que se realizó en la maquina víctima de Windows aparece en la ventana de seguimiento.

Figura 52

Ventana de seguimiento.

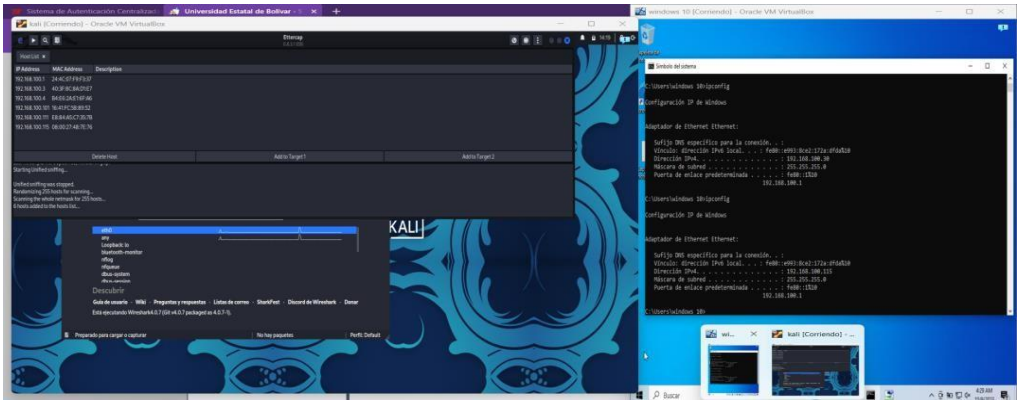


Elaborado por: Chela E. & Utitiaja J.

ENCRIPTACIÒN AES.

Figura 53

Encriptación AES.

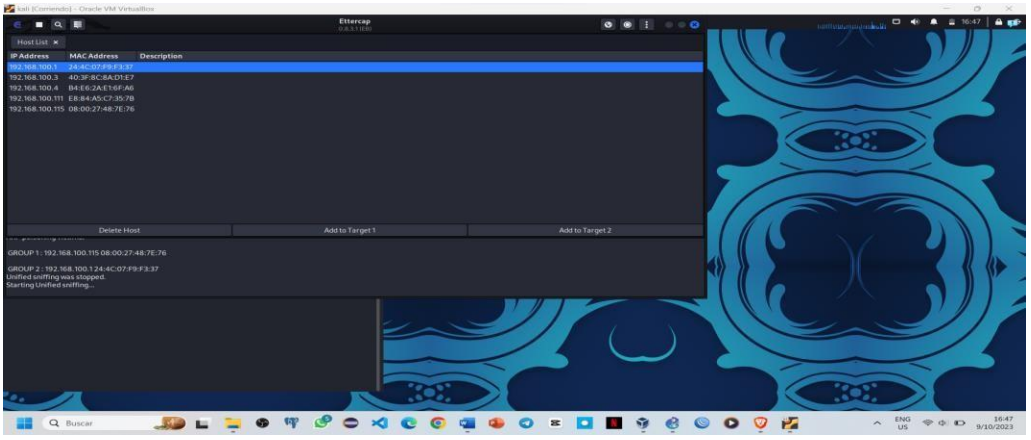


Elaborado por: Chela E. & Utitiaja J.

Nos conectamos con el usuario root en Linux y ejecutamos la herramienta ettercap quien nos ayudara a realizar diversos ataques en la cual iniciamos y realizamos un análisis de los equipos que están conectados y observamos los resultados de los análisis, por ende, nos dirigimos a la máquina de Windows para poder conocer la dirección Ip de la maquina mencionada.

Figura 54

Seleccionamos la dirección Ip del Windows 10.



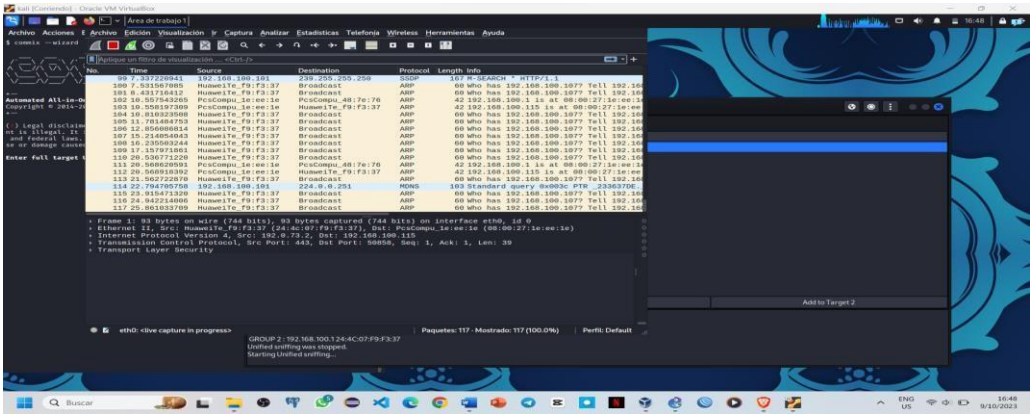
Elaborado por: Chela E. & Utitiaja J.

A continuación, seleccionamos la dirección ip del Windows 10 y la dejamos como la primera tarjeta y la puerta de enlace como la segunda tarjeta donde

vamos a estar seleccionando el ataque arp poisonig para así poder iniciar con el ataque. Para poder visualizar el tráfico de red ejecutamos wireshark y seleccionamos la tarjeta de la red en la cual vamos a monitorear en la cual desplazara los tráficos de red.

Figura 55

El tráfico de red en la máquina de Linux.

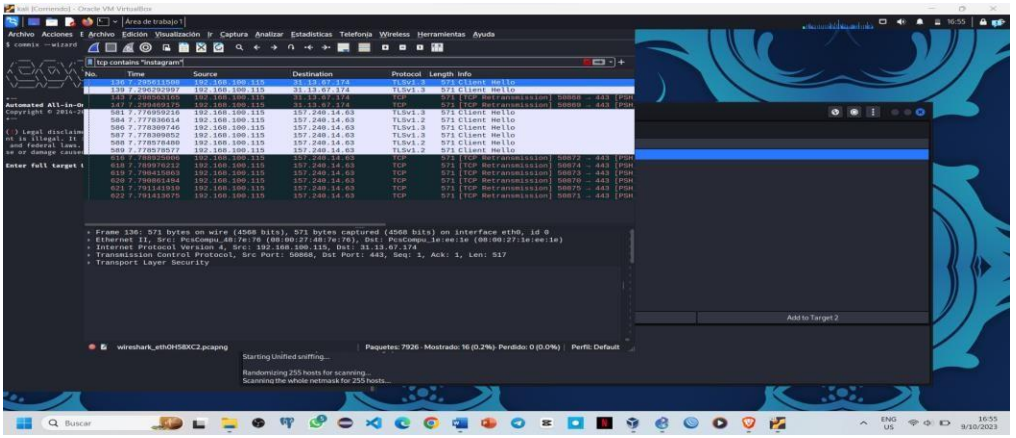


Elaborado por: Chela E. & Utitiaja J.

Al analizar el tráfico de red en la máquina de Linux ingresamos a la máquina de Windows donde ingresamos al navegador e ingresamos al sitio web de la nasa para posterior regresamos a la máquina de Kali Linux donde detenemos el análisis.

Figura 56

Búsqueda de wireshark.

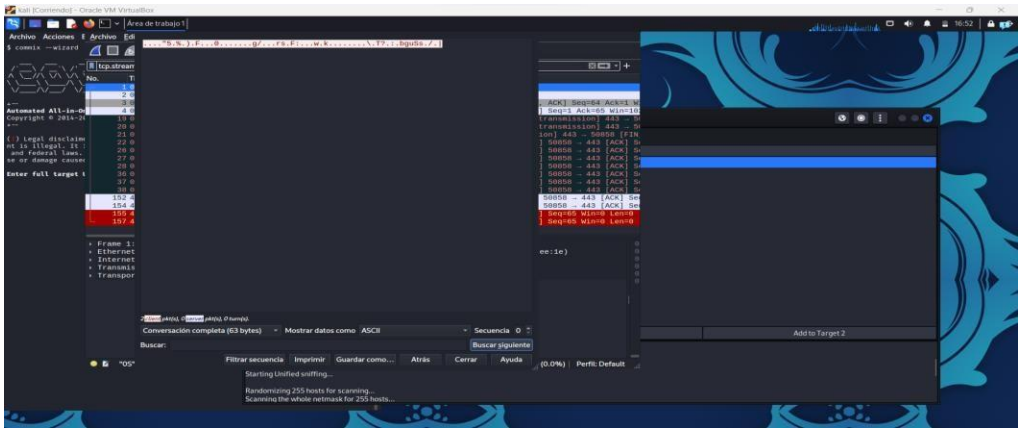


Elaborado por: Chela E. & Utitiaja J.

En el botón de búsqueda de wireshark ingresamos el siguiente comando tcp contains “instagram” donde vamos a visualizar los sitios capturados y realizamos un seguimiento.

Figura 57

Visualización de la navegación.



Elaborado por: Chela E. & Utitiaja J.

En este caso podemos visualizar que la navegación realizada en la maquina Windows no se observa al realizar el ataque con comparación del cifrado DES Y 3DES que aparece los sitios navegados de la maquina víctima.

4.14. Impacto de confidencialidad de las técnicas de encriptación (algoritmos y protocolos).

Nivel de impacto

Niveles de impacto de las técnicas de encriptación (algoritmos y protocolos)

Tabla 2

Niveles de impacto sobre las técnicas de encriptación (algoritmo y protocolos)

Niveles de impacto	
0%-25%	**Bajo**
26%-50%	**Medio**
51%-100%	**Alto**

Elaborado por: Chela E & Utitiaja J.

- **Simulación 1**

ATAQUE DE DENEGACION DE SERVICIO KALI LINUX ETTERCAP Y PING A LA MAQUINA VICTIMA WINDOWS

Tabla 3

Ficha de observación – AES – 256.

Código:	S-01	**Ficha N°:**	01
Descripción	La siguiente simulación es "Ataque de denegación de servicio kali linux ettercap y ping a la maquina victima windows "	**Hora inicial:**	2:00
Fecha:	08/10/2023	**Hora final:**	2:30
Tipos de encriptación:	AES		
Observadores:	Jhordan Utitiaja – Erik Chela		

AES - 256	**Porcentajes de impacto**				**Nivel de impacto**
	0%	**25%**	**50%**	**100%**	
Longitud de bits				**x**	**Alto**
La resistencia frente a ataques de fuerza bruta o criptoanálisis				**x**	**Alto**
La madurez (confiabilidad y estabilidad)				**x**	**Alto**
Velocidad y rendimiento				**x**	**Alto**

Gestión de claves				**x**	**Alto**
Cumplimiento normativo				**x**	**Alto**

Elaborado por: Chela E & Utitiaja J.

Tabla 4

Ficha de observación – 3DES-168.

Código:	S-02	**Ficha N°:**	02
Descripción	La siguiente simulación es "Ataque de denegación de servicio kali linux ettercap y ping a la maquina victima windows "	**Hora inicial:**	**2:30**
Fecha:	0/10/2023	**Hora final:**	**3:00**
Tipos de encriptación:	3DES- 168.		
Observadores:	Jhordan Utitiaja – Erik Chela		

3DES-168	**Porcentajes de impacto**				**Nivel de impacto**
	0%	**25%**	**50%**	**100%**	
Longitud de clave			**x**		Medio
La resistencia frente a ataques de fuerza bruta o criptoanálisis		**x**			Bajo
La madurez			**x**		Medio

Velocidad y rendimiento			**x**		Medio
Gestión de claves			**x**		Medio
Cumplimiento normativo				**x**	Alto

Elaborado por: Chela E & Utitiaja J.

Tabla 5

Ficha de observación – DES-56.

Código:	S-03	**Ficha N°:**	03
Descripción	La siguiente simulación es "Ataque de denegación de servicio kali linux ettercap y ping a la maquina victima windows "	**Hora inicial:**	**3:00**
Fecha:	08/10/2023	**Hora final:**	**3:00**
Tipos de encriptación:	DES-56 bits.		
Observadores:	Jhordan Utitiaja – Erik Chela		

DES-56 bits.	**Porcentajes de impacto**				**Nivel de impacto**
	0%	**25%**	**50%**	**100%**	
Longitud de clave		**x**			Bajo
La resistencia frente a ataques de fuerza bruta o criptoanálisis		**x**			Bajo

La madurez		**x**			Bajo
Velocidad y rendimiento		**x**			Bajo
Gestión de claves		**x**			Bajo
Cumplimiento normativo				**x**	Alto

Elaborado por: Chela E & Utitiaja J.

Descripción:

Discusión de los resultados.

Al finalizar la simulación de ataques a las encriptaciones (algoritmo y protocolo) como AES, 3DES, DES obtuvimos los siguientes resultados, que se plasmaron en la ficha de observación anexadas en las tablas 3,4,5 en donde determinamos que el algoritmo AES se destacó a los demás algoritmos de encriptación referente al ataque de denegación de servicio.

- **Simulación 2**

ATAQUE DEL HOMBRE EN EL MEDIO.

Tabla 6

Ficha de observación – AES-256 bits.

Código:	S-04	**Ficha N°:**	04
Descripción	La siguiente simulación es "Ataque del hombre en el medio"	**Hora inicial:**	**12:00**
Fecha:		**Hora final:**	**13:00**
Tipos de encriptación:	AES- 256 bits.		
Observadores:	Jhordan Utitiaja – Erik Chela		

AES	**Porcentajes de impacto**	

	0%	25%	50%	100%	Nivel de impacto
Longitud de clave				**x**	Alto
La resistencia frente a ataques de fuerza bruta o criptoanálisis				**x**	Alto
La madurez				**x**	Alto
Velocidad y rendimiento				**x**	Alto
Gestión de claves				**x**	Alto
Cumplimiento normativo				**x**	Alto

Elaborado por: Chela E & Utitiaja J.

Tabla 7

Ficha de observación - 3DES-168 bits.

Código:	S-05	**Ficha N°:**	05
Descripción	La siguiente simulación es "Ataque del hombre en el medio "	**Hora inicial:**	**13:00**
Fecha:	08/10/2023	**Hora final:**	**14:00**
Tipos de encriptación:	3DES		
Observadores:	Jhordan Utitiaja – Erik Chela		

DES	**Porcentajes de impacto**	

	0%	25%	50%	100%	Nivel de impacto
Longitud de clave			**x**		Medio
La resistencia frente a ataques de fuerza bruta o criptoanálisis		**x**			Bajo
La madurez			**x**		Medio
Velocidad y rendimiento			**x**		Medio
Gestión de claves			**x**		Medio
Cumplimiento normativo				**x**	Alto

Elaborado por: Chela E & Utitiaja J.

Tabla 8

Ficha de observación – DES-56bits.

Código:	S-06	**Ficha N°:**	06
Descripción	La siguiente simulación es "Ataque del hombre en el medio "	**Hora inicial:**	**14:30**
Fecha:	08/10/2023	**Hora final:**	**15:00**
Tipos de encriptación:	DES-56bits.		
Observadores:	Jhordan Utitiaja – Erik Chela		

DES-56bits	**Porcentajes de impacto**	

	0%	25%	50%	100%	Nivel de impacto
Longitud de clave		**x**			Bajo
La resistencia frente a ataques de fuerza bruta o criptoanálisis		**x**			Bajo
La madurez		**x**			Bajo
Velocidad y rendimiento		**x**			Bajo
Gestión de claves		**x**			Bajo
Cumplimiento normativo				**x**	Alto

Elaborado por: Chela E & Utitiaja J.

Descripción:

Discusión de los resultados.

Al finalizar la simulación de ataques a las encriptaciones (algoritmo y protocolo) como AES, 3DES, DES obtuvimos los siguientes resultados, que se plasmaron en la ficha de observación anexadas en las tablas 6,7,8 en donde determinamos que el algoritmo AES se destacó a los demás algoritmos de encriptación referente al ataque de hombre en el medio.

CAPITULO V

PROPUESTA

MANUAL CON LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN.

5.1. Presentación.

Después de haber realizar un análisis detallado con la ficha de observación anexada en la tabla 2 de las simulaciones de distintos tipos de encriptación en la herramienta GNS3, se ha podido determinar que el algoritmo AES es la mejor hoy en la actualidad.

El presente manual ha sido elaborado con la finalidad de brindar una guía tanto concisa como exhaustiva acerca de las mejores prácticas en el ámbito de la encriptación.

En un mundo cada vez más interconectado, la encriptación se convierte en un pilar fundamental para preservar la privacidad y la seguridad de datos críticos, desde conceptos básicos hasta técnicas avanzadas, este manual abarca la importancia de elegir algoritmos de encriptación robustos, la gestión segura de claves, la implementación adecuada de protocolos de seguridad y el aseguramiento de la integridad de los datos. Además, se exploran casos de uso en diferentes entornos, desde la comunicación en línea hasta el almacenamiento en la nube.

Este manual con las mejores prácticas de encriptación está dirigido tanto a expertos en ciberseguridad como a desarrolladores de software y usuarios finales que manifiesten inquietud por la preservación de su privacidad, este manual proporciona conocimientos esenciales y recomendaciones concretas.

El propósito es garantizar la confidencialidad y la protección de información delicada frente a las amenazas cibernéticas en constante desarrollo.

5.2. Objetivo general.

Desarrollar un manual completo que presente las mejores prácticas de encriptación, abordando desde conceptos fundamentales hasta técnicas avanzadas, con el propósito de capacitar a profesionales de ciberseguridad, desarrolladores de software y usuarios finales en la implementación efectiva de medidas de seguridad para proteger información sensible en entornos digitales.

5.3. Objetivos específicos.

- Analizar y explicar en detalle los diferentes tipos de algoritmos de encriptación disponibles, destacando sus fortalezas y debilidades, para permitir a los usuarios seleccionar la opción más adecuada para sus necesidades específicas.
- Proporcionar directrices claras y ejemplos prácticos sobre la gestión segura de claves, abordando aspectos como la generación, almacenamiento y rotación de claves, con el fin de prevenir accesos no autorizados.
- Detallar la implementación de protocolos de seguridad en diversos contextos, como la comunicación en línea y el almacenamiento en la nube, resaltando cómo configurar conexiones seguras y garantizar la integridad y confidencialidad de los datos transmitidos o almacenados.

5.4. ¿Por qué es importante la encriptación de datos?

La seguridad digital es un escenario en constante cambio, y es importante estar actualizados para evitar que los ataques maliciosos lo sorprendan a usted y a su negocio. A medida que los ciberataques y las infracciones se vuelven comunes, es más importante que nunca proteger tanto la computadora de su empresa como la suya propia. (Gutiérrez, 2020)

5.5. ¿Qué es la encriptación?

La encriptación es una técnica para garantizar que solo el personal autorizado pueda acceder a los datos en el contexto de la seguridad informática.

Básicamente es el proceso de convertir datos que de otro modo serían legibles en un formato ilegible (de texto sin formato a texto cifrado) mediante un algoritmo y una clave de cifrado. Sólo las personas con la clave de descifrado adecuada pueden descifrar y traducir la información cifrada a texto legible.

Para mantener la confidencialidad, integridad y autenticidad de los datos en una amplia gama o combinaciones de los mismos, se utiliza el cifrado. Se utiliza en varios escenarios, que incluyen:

Las comunicaciones por Internet, incluidos el correo electrónico, la mensajería instantánea y la navegación web segura (HTTPS), dependen del cifrado para salvaguardar las transmisiones de datos entre dispositivos. Esto se conoce como Comunicaciones Seguras. La información transmitida es impermeable a terceros no autorizados.

El almacenamiento seguro en dispositivos de almacenamiento, como discos duros, unidades USB y servicios en la nube, está protegido por los datos almacenados mediante cifrado. Incluso si un dispositivo es robado o perdido, los datos cifrados no se pueden recuperar sin la clave adecuada.

Para garantizar la autenticidad y seguridad de los documentos electrónicos, se emplea cifrado tanto en la autenticación de usuario como en la firma digital.

El uso de cifrado en redes Wifi garantiza que las comunicaciones inalámbricas sean seguras, evitando que usuarios no autorizados accedan a la red o intercepten datos.

En esencia, el cifrado es un componente vital para proteger los datos sensibles en el mundo digital, garantizando su protección durante el tránsito y el reposo.

5.6. Beneficios de implementar las mejores prácticas de encriptación en las empresas, organizaciones, instituciones y personas.

La implementación de las mejores prácticas de encriptación en empresas, organizaciones, instituciones y para personas en general conlleva una serie de beneficios significativos que abarcan tanto la seguridad de los datos como la protección de la privacidad. Aquí te presento cinco claves de beneficios:

Confidencialidad de Datos: La encriptación garantiza que la información sensible se mantiene confidencial. Solo las personas autorizadas con las claves adecuadas pueden acceder a los datos, lo que evita el acceso no autorizado y la divulgación no deseada de información confidencial.

Protección contra Amenazas Cibernéticas: Las mejores prácticas de encriptación ayudan a proteger los datos de amenazas cibernéticas, como el malware, el ransomware y los ataques de phishing. Incluso si un atacante logra acceder a los datos, estos seguirán siendo incomprensibles sin la clave de desencriptación.

Cumplimiento Normativo: Para muchas empresas e instituciones, el cumplimiento de las regulaciones de seguridad de datos y privacidad es obligatorio. La implementación adecuada de encriptación ayuda a cumplir con estos estándares legales y evita sanciones y multas asociadas con violaciones de datos.

Protección en Dispositivos Móviles: En un mundo donde los dispositivos móviles son omnipresentes, la encriptación protege los datos almacenados en teléfonos inteligentes y tabletas, impidiendo el acceso no autorizado en caso de pérdida o robo del dispositivo.

Seguridad en la Nube: Para las organizaciones que utilizan servicios en la nube para el almacenamiento y procesamiento de datos, la encriptación de extremo a extremo proporciona una capa adicional de seguridad, incluso cuando los datos están en tránsito y en reposo en servidores de terceros.

En resumen, la implementación de las mejores prácticas de encriptación en empresas, organizaciones, instituciones ya nivel personal es esencial para proteger la información y salvar la privacidad en un entorno digital cada vez más complejo y amenazante. Estos beneficios contribuyen a la integridad y seguridad de los datos, fortaleciendo la confianza en el manejo de la información.

5.7. Componentes del manual de las mejores prácticas de encriptación.

Para implantar el manual de las mejores prácticas de encriptación (MMPE) dentro de una empresas, organizaciones, instituciones y personas, se requiere integridad, responsabilidad, ética, paciencia, disciplina y confidencialidad.

A continuación, se detallará MMPE, a manera de consejos prácticos, para la gestión y uso eficiente de algoritmo de encriptación:

• AES 256

5.8. Uso eficiente del algoritmo de AES 256

El uso eficiente del algoritmo AES (Advanced Encryption Standard) es fundamental para garantizar la seguridad de la información en una red o sistema. AES es uno de los algoritmos de encriptación más sólidos y ampliamente utilizados, y su eficiencia radica en su capacidad para proporcionar una protección robusta de los datos sin comprometer el rendimiento. Aquí hay algunas prácticas para el uso eficiente de AES:

Recomendaciones.

- **Selección de Clave Adecuada:** Utilice claves seguras y robustas para AES. Las claves débiles son vulnerables a ataques de fuerza bruta. Se recomienda el uso de claves largas y complejas que sean difíciles de adivinar.

  Ejemplo: En lugar de usar una clave como "123456", se debe utilizar una clave robusta y compleja como "K#2aP&9$zQwX8!sE".

- **Modos de operación:** Elija el modo de operación AES adecuado según sus necesidades. Los modos comunes incluyen ECB (Electronic Codebook), CBC (Cipher Block Chaining) y GCM (Galois/Counter Mode), cada uno con sus propias características y aplicaciones.

  Ejemplo: Para proteger la confidencialidad de una comunicación por correo electrónico, se puede utilizar el modo de operación GCM de AES, que proporciona autenticación de mensajes además del cifrado.

- **Gestión de Claves:** Implementa una sólida gestión de claves. Esto incluye el almacenamiento seguro de claves y la rotación periódica de las

mismas. La gestión inadecuada de claves puede comprometer la seguridad de AES.

Ejemplo: Implementar un sistema de gestión de claves que rote automáticamente las claves cada 90 días y almacene las claves en un módulo de seguridad de hardware (HSM) para mayor protección.

- **Implementación Optimizada:** Utiliza bibliotecas de encriptación y herramientas de encriptación bien optimizadas. Esto ayuda a garantizar un rendimiento eficiente en la encriptación y desencriptación de datos.

  Ejemplo: Utilizar una biblioteca de criptografía ampliamente reconocida y optimizada, como OpenSSL o Bouncy Castle, para cifrar y descifrar datos de manera eficiente.

- **Actualizaciones Regulares:** Mantén tus implementaciones de AES actualizadas con las últimas recomendaciones y mejores prácticas de seguridad. Los estándares y las amenazas pueden cambiar con el tiempo, por lo que es importante mantenerse al día.

  Ejemplo: Mantener la implementación de AES actualizada con las últimas versiones de bibliotecas criptográficas y seguir las recomendaciones de seguridad emitidas por los proveedores.

- **Pruebas Rigurosas:** Realice pruebas exhaustivas de seguridad para detectar posibles vulnerabilidades en su implementación de AES. Las pruebas de penetración y las evaluaciones de seguridad son esenciales para identificar y corregir posibles puntos débiles.

  Ejemplo: Realizar pruebas de penetración en una aplicación web que utiliza AES para encriptar datos de usuarios, buscando posibles vulnerabilidades como inyección de código malicioso o debilidades en la gestión de claves.

- **Monitorización Continua:** Establece un sistema de monitorización continua para detectar y responder a actividades inusuales o intentos de acceso no autorizado. La detección temprana de amenazas puede prevenir incidentes de seguridad.

Ejemplo: Configurar un sistema de monitorización de seguridad que registre y alerte sobre cualquier intento de acceso no autorizado a los sistemas protegidos por AES.

- **Educación y Formación:** Capacita a tu equipo en las mejores prácticas de seguridad de AES. Un equipo bien informado es esencial para utilizar el algoritmo de manera efectiva y proteger los datos de manera adecuada. Ejemplo: Proporcionar formación regular en seguridad de datos y en el uso adecuado de AES a los empleados de una organización para garantizar un uso seguro y eficiente de la encriptación

El uso eficiente de AES implica un equilibrio entre seguridad y rendimiento. Al seguir estas prácticas, puedes aprovechar al máximo las capacidades de AES para proteger tus datos de manera sólida y eficiente en un entorno de red.

CONCLUSIONES

- En el presente estudio se analizó la aplicación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos, y se concluyó que la implementación de las mejores prácticas de encriptación es de vital importancia en el contexto actual, marcado por la creciente digitalización y la interconexión de dispositivos en redes de datos. La encriptación desempeña un papel fundamental al salvar la confidencialidad, integridad y disponibilidad de los datos, tanto durante su tránsito como en su almacenamiento. La cuidadosa de algoritmos y protocolos de encriptación es esencial para asegurar una protección efectiva de la información en un entorno donde la seguridad de los datos se ha convertido en una prioridad crítica.
- El análisis exhaustivo de las diversas técnicas de encriptación, incluyendo algoritmos y protocolos, ha revelado la importancia de elegir con sabiduría las soluciones de seguridad. Cada técnica presenta ventajas y desventajas específicas, lo que subraya la necesidad de una evaluación precisa en función de los requisitos de seguridad y los contextos de uso. Este objetivo ha resaltado la relevancia de comprender a fondo las características y aplicaciones de AES, DES, 3DES, RSA, entre otras, en la protección de datos en redes de datos. Además, se ha destacado la importancia de mantenerse actualizado sobre los avances en criptografía para tomar decisiones informadas en materia de encriptación de datos.
- La realización de simulaciones para demostrar la aplicación de las mejores prácticas de encriptación dentro de una institución de educación superior ha proporcionado valiosas lecciones sobre la efectividad y la importancia de estas prácticas en la protección de la información sensible. Estas simulaciones han permitido visualizar de manera concreta cómo los algoritmos y protocolos de encriptación, como AES, DES, 3DES, RSA y otros, pueden resguardar la confidencialidad de los datos en un entorno educativo. Además, han resaltado la necesidad de promover la conciencia de seguridad y la capacitación entre la comunidad académica, enfatizando la relevancia de la encriptación en la preservación de la integridad y la privacidad de los datos en una institución

educativa en la era digital. Además, el estudio realizado se evidenció que, el algoritmo AES es el más adecuado de tal manera que cumple con los requisitos necesarios para la seguridad y manejo de información, en un sistema informático.

- La creación del manual que contiene las mejores prácticas de encriptación ha resultado en una herramienta fundamental para guiar y establecer un marco sólido en la implementación de la seguridad de la información mediante la encriptación. Este manual representa una referencia valiosa que abarca desde la selección de algoritmos adecuados hasta la gestión de claves y el cumplimiento normativo. Su elaboración ha enfatizado la importancia de mantenerse actualizado en materia de seguridad de datos y criptografía para garantizar la relevancia continua de las prácticas recomendadas. La distribución y capacitación sobre el contenido del manual son esenciales para garantizar una comprensión y adopción efectiva de las mejores prácticas de encriptación en el entorno empresarial, institucional y personal.

RECOMENDACIONES

- Es esencial mantener actualizadas y adaptadas las prácticas de encriptación a medida que la tecnología avanza y las amenazas cibernéticas evolucionan. Además, se debe fomentar la concienciación y la capacitación en seguridad de la información entre profesionales y usuarios de redes de datos, fortaleciendo así las defensas contra posibles ataques. Mantenerse informado sobre las regulaciones y estándares de seguridad de datos pertinentes es crucial para garantizar un cumplimiento normativo sólido, lo que, a su vez, contribuye a proteger la integridad y la privacidad de la información en un entorno digital en constante cambio.
- Es fundamental llevar a cabo evaluaciones de riesgo periódicas para identificar las técnicas de encriptación más adecuadas según la naturaleza de los activos de datos. Asimismo, mantenerse al tanto de las investigaciones y avances en criptografía es esencial para tomar decisiones informadas sobre las técnicas de encriptación que mejor se adaptan a las necesidades cambiantes de seguridad, asegurando así una protección sólida y actualizada de la información sensible.
- Es crucial mantener la realización de simulaciones periódicas para asegurar que los procedimientos de encriptación sigan siendo efectivos y estén preparados para enfrentar nuevas amenazas. Además, es importante promover activamente la conciencia de seguridad entre la comunidad académica, fomentando la adopción de buenas prácticas de encriptación, lo cual contribuirá a fortalecer las defensas contra posibles riesgos ya garantizar un entorno más seguro para la información en entornos educativos y más allá.
- En relación a la propuesta del manual, se recomienda enfáticamente la adopción del algoritmo AES como elección principal, esto se debe a que AES se ha destacado entre otros algoritmos de encriptación por su capacidad para proporcionar un nivel superior de seguridad en la protección de datos. La incorporación de este contenido en el manual ayudará a garantizar que los usuarios estén plenamente informados y cumplan con las exigencias legales en el manejo de datos cifrados, fortaleciendo así la seguridad de la información.

BIBLIOGRAFÍA

Alvaro. (20 de Mayo de 2021). *AES y GOST: Criptografía simétrica moderna*. Obtenido de Just Cryptography: https://justcryptography.com/aes-y-gost-criptografia-simetrica-moderna/

Antonio, A., De Sucre, J., & Sánchez, J. (2021). Obtenido de Gob.ec: https://www.registrospublicos.gob.ec/wp-content/uploads/downloads/2021/05/resolucion_No_009-ng-dinardap-2021-signed1.pdf

Arias, E. R. (10 de Diciembre de 2020). Investigación de campo. *Economipedia*. Obtenido de https://economipedia.com/definiciones/investigacion-de-campo.html

Berhanu Aebissa, G. D. (2023). El efecto directo e indirecto de la justicia organizacional en la intención de los empleados de cumplir con la política de seguridad de la información: el caso de los bancos etíopes. (Elsevier,Ed.). *Informática y Seguridad.* Obtenido de https://www.sciencedirect.com/science/article/pii/S016740482300158X?vi

Blandonnet, C. d. (2018). ISO/IEC 27000. pág. 34. Obtenido de International Standard: www.iso.org

Canadas, R. (02 de Marzo de 2022). *Qué es la encriptación*. Obtenido de abdatum: https://abdatum.com/informatica/que-es-encriptacion

Carrillo, E. F. (Septiembre de 2022). *PROPUESTA DE MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA LA COMUNICACIÓN EN REDES DE CLIENTES CORPORATIVOS.* Obtenido de repositorio.pucesa.edu.ec: https://repositorio.pucesa.edu.ec/bitstream/123456789/3779/1/78213.pdf

CARVAJAL, E. T. (2018). *TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS.* https://doi.org/http://dx.doi.org/10.12795/IETSCIENTIA.2018.i01.03

Chávez, J. G. (2016). Análisis y modelos de datos de redes para seguridad. *Repositorio Academico*. Obtenido de https://repositorio.uchile.cl/handle/2250/138269

De, A. M. (s.f.). *GUIA PARA TRATAMIENTO DE DATOS PERSONALES EN ADMINISTRACION PUBLICA*. Obtenido de Gob.ec: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

Domingues, E. J. (2017). Os Ciberataques como um Novo Desafio para a Segurança: O Hacktivismo. Repositório Comum. Obtenido de http://hdl.handle.net/10400.26/15403

Encriptación, S. d. (9 de Abril de 2019). *Significados*. Obtenido de https://www.significados.com/encriptacion/

Félix, M. T. (2018). Unified cyber threat intelligence. *Universidade de Lisboa.* Obtenido de http://hdl.handle.net/10451/32642

García, D. (04 de Abril de 2023). *3DES: características, usos e implementación - MSMK University*. Obtenido de MSMK: https://msmk.university/ciberseguridad/3des

Gómez, B. (18 de Abril de 2021). *AES-256 ¿Qué es? ¿Cómo funciona? (Mejor explicación)*. Obtenido de Profesional Review: https://www.profesionalreview.com/2021/04/18/aes-256/

Gutiérres, N. (05 de Marzo de 2020). *Prey*. Obtenido de https://preyproject.com/es/blog/la-encriptacion-de-datos-una-guia-para-buenas-practicas-de-seguridad

Harrison, K. (08 de Agosto de 2022). *Explicación del estándar de cifrado avanzado (AES) (2023)*. Obtenido de Web Hosting Professional: https://webhostingprof.com/es/explicacion-del-estandar-de-cifrado-avanzado-aes-2022/

Kidd, C. (11 de Noviembre de 2022). *Data encryption methods & types: Beginner's guide to encryption*. Obtenido de Splunk-Blogs: https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html

Knerl, L. (03 de Agosto de 2019). *What Are the Different Types of Encryption?* Obtenido de Www.hp.com: https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption

Lisboa Díaz, M. A. (2020). Predicción de áreas con usuarios vulnerables a ciberataques. .*Universidad Nacional Andrés bello*, 76. Obtenido de http://repositorio.unab.cl/xmlui/handle/ria/13990

López, A. (04 de Abril de 2021). *Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica*. Obtenido de RedesZone: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

Martinez, J. G. (07 de Julio de 2022). *Norma ISO 27001: Qué Es, Beneficios y Proceso de Certificación*. Obtenido de Deltaprotect.com: https://www.deltaprotect.com/blog/que-es-iso-27001

MC Lee, M. (6 de September de 2022). *Everything you need to know about AES-256 encryption*. Obtenido de Kiteworks | Your Private Content Network: https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/

Mkinsi, M. H. (2022). ISO/IEC 27002. ISO. Obtenido de https://www.iso.org/

Nagaraj, K. (19 de Marzo de 2023). *TwoFish Encryption: A comprehensive guide*. Obtenido de Medium: https://cyberw1ng.medium.com/twofish-encryption-a-comprehensive-guide-2023-b3ad0f8448

Nagaraj, K. (25 de February de 2023). *Understanding blowfish encryption algorithm*. Obtenido de Medium: https://cyberw1ng.medium.com/understanding-blowfish-encryption-algorithm-2023-24eb8f69f85b

Nagaraj, K. (05 de Marzo de 2023). *Understanding IDEA encryption: A comprehensive guide*. Obtenido de Medium: https://cyberw1ng.medium.com/understanding-idea-encryption-a-comprehensive-guide-2023-16839d1a9410

Noemy, M. V. (Noviembre de 2017). *Criptografía y mecanismos de seguridad* . Obtenido de Edu.co: https://digitk.areandina.edu.co/bitstream/handle/areandina/1423/Criptograf%C3%ADa%20y%20mecanismos%20de%20seguridad.pdf?sequence=1&isAllowed=y

Pacheco, D. S. (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. *Ingeniare. Revista chilena de ingeniería*, 215-217.

Que es la encriptación de la informática. (s.f.). Obtenido de Larevistainformatica.com: http://www.larevistainformatica.com/que-es-encriptacion-informatica.htm

Sampieri, R. H. (2010). *Ampiación y Fundamentación de los métodos mixtos.* México. https://doi.org/5ta Edición

Simplilearn. (17 de Junio de 2020). *What is DES (Data Encryption Standard)? DES algorithm and operation*. Obtenido de Simplilearn.com: https://www.simplilearn.com/what-is-des-article

Sirisilla, S. (02 de Febrero de 2023). *Bridging the Gap: Overcome these 7 flaws in descriptive research design*. Obtenido de Enago Academy: https://www.enago.com/academy/descriptive-research-design/

Tancara Q, C. (1993). LA INVESTIGACION DOCUMENTAL. *Temas Sociales, 17*, 91–106. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S0040-29151993000100008

Taylor, H. (30 de Mayo de 2023). *Data encryption 101: A guide to data security best practices*. Obtenido de Preyproject.com: https://preyproject.com/blog/data-encryption-101

Urrutia, D. (29 de Enero de 2020). *Qué es Encriptación*. Obtenido de Arimetrics: https://www.arimetrics.com/glosario-digital/encriptacion

ANEXOS

ANEXO1: CRONOGRAMA DE GANTT

Figura 1

Diagrama de actividades de Gantt.

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		Aplicación de las mejores prácticas de encriptación, para el manejo de la información en redes de datos, año 2023.					
2		**Fase 1**	**133 días**	**lun 12/06/23**	**mar 12/12/2**		
3		Analizar las diferentes técnicas de encriptación (algoritmo y protocolos) para redes.	10 días	lun 12/06/23	vie 23/06/23		Erik Chela,Jhordan Utitiaja
4		Recopilar información sobre diferentes técnicas de encriptación existentes, describir cómo funcionan y comparar sus fortalezas y debilidades.	5 días	lun 26/06/23	vie 30/06/23	3	Erik Chela,Jhordan Utitiaja
5		Elaborar el manual con las mejores prácticas de encriptación.	20 días	lun 03/07/23	vie 28/07/23	4	Erik Chela,Jhordan Utitiaja
6		Elaboración de la ficha de observación.	5 días	lun 31/07/23	vie 04/08/23	5	Erik Chela,Jhordan Utitiaja
7		Análisis e interpretación de los resultados.	5 días	lun 07/08/23	vie 11/08/23	6	Erik Chela,Jhordan Utitiaja
8		Revisión del análisis e interpretación de los resultados.	5 días	lun 14/08/23	vie 18/08/23	7	Erik Chela,Jhordan Utitiaja
9		Elaboración de una simulación sobre el uso de las mejores prácticas de encriptación (algoritmo y protocolos) dentro de una institución de educación superior.	30 días	lun 21/08/23	vie 29/09/23	8	Erik Chela,Jhordan Utitiaja
10		Revisión y corrección de la simulación.	10 días	lun 02/10/23	vie 13/10/23	9	Erik Chela,Jhordan Utitiaja
11		Revisión y corrección del proyecto de investigación.	10 días	lun 16/10/23	vie 27/10/23	10	Erik Chela,Jhordan Utitiaja
12		Elaboración de conclusiones y recomendaciones.	5 días	lun 30/10/23	vie 03/11/23	11	Erik Chela,Jhordan Utitiaja
13		Validación de errores del proyecto de investigación.	25 días	lun 06/11/23	vie 08/12/23	12	Erik Chela,Jhordan Utitiaja
14		Entrega formal del proyecto.	1 día	mar 12/12/23	mar 12/12/23	13	Erik Chela,Jhordan Utitiaja

Elaborado por: Chela E. & Utitiaja J.

ANEXO 2: PRESUPUESTO

Tabla 1

Presupuesto

Descripción	**Cantidad**	**Valor unitario**	**Valor Total**
Movilización	60	$ 0.30	$18
Alimentación	30	$ 2.00	$ 60
Carpetas	4	$ 0.50	$ 2.00
Impresiones, copias, anillados.	80	$ 0.05	$ 4.00
Computadoras	2	$ 600	$ 1200.00
CD con portada	2	$3	$ 6.00
Empastado	4	$ 50	$ 200.00
Total			1490

Elaborado por: Chela E. & Utitiaja J.

ANEXO 3: EVIDENCIAS DE REUNIONES CON EL DIRECTOR Y PARES ACADÉMICOS

Reuniones con el director.

Reuniones con los pares académicos.


HONOR X6s
50MP Triple Camera


HONOR X6s
50MP Triple Camera


HONOR X6s
50MP Triple Camera

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

ING. RODRIGO DEL POZO DURANGO, EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR.

CERTIFICA

Que el trabajo de integración curricular denominado "**APLICACIÓN DE LAS MEJORES PRÁCTICAS DE ENCRIPTACIÓN, PARA EL MANEJO DE LA INFORMACIÓN EN REDES DE DATOS, AÑO 2023",** presentado por Erik Adrian Chela Hinojoza y Jhordan Pablo Utitiaja Katan estudiantes de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta TURNITIN, reflejando un **porcentaje de similitud del 12%**, como se puede evidenciar en el documento adjunto.

Guaranda, 24 de octubre del 2023

Atentamente,

Firmado electrónicamente por: RODRIGO HUMBERTO DEL POZO DURANGO

Ing. Rodrigo Del Pozo Durango.
Director

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

Reporte de similitud

NOMBRE DEL TRABAJO
Proyecto Investigacion Final.docx

AUTOR
Jhordan Utitiaja

RECUENTO DE PALABRAS
23307 Words

RECUENTO DE CARACTERES
125344 Characters

RECUENTO DE PÁGINAS
130 Pages

TAMAÑO DEL ARCHIVO
24.4MB

FECHA DE ENTREGA
Oct 23, 2023 1:59 PM CST

FECHA DEL INFORME
Oct 23, 2023 2:01 PM CST

● **12% de similitud general**

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

- 8% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Cross
- 10% Base de datos de trabajos entregados

● **Excluir del Reporte de Similitud**

- Material bibliográfico
- Material citado
- Fuentes excluidas manualmente
- Bloques de texto excluidos manualmente