UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas y Computación

TESIS

Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información

PRESENTADO POR:

Bach. Simón Wilmer Mori Acero

Línea de Investigación de la Universidad:

Nuevas Tecnologías y Procesos

Línea de Investigación de la Escuela Profesional:

Ingeniería e infraestructura

PARA OPTAR TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

LIMA - PERÚ
2019

UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas y Computación

TESIS

Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información

PRESENTADO POR:

Bach. Simón Wilmer Mori Acero

PARA OPTAR TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

LIMA - PERÚ

2019

ASESORES

_____

ASESOR METODOLOGICO
Mg. ANSELMO ANICETO VALENZUELA ZEGARRA

_____

ASESOR TEMÁTICO
Ing. MABEL SUSANA YGNACIO GARCIA

Dedicatoria

El presente trabajo está dedicado a Dios por darme fuerzas para seguir adelante y a mis padres Gonzalo Mori Cuenca y Estela Acero Castillo, por su apoyo, consejos, comprensión, amor; a mi esposa Sarita Chumpitaz Arias por el apoyo incondicional para conseguir mis objetivos, a mi pequeño hijo Dylan Ichiro que siempre estuvo a mi lado acompañándome y a toda mi familia por su constante apoyo.

Agradecimiento

Agradecer a mis padres, esposa, hijos, hermanos y amigos por el apoyo brindado de manera incondicional y fortaleza para continuar hasta alcanzar mis objetivos, porque compartieron conmigo momentos de alegría, tristeza y porque me demostraron que podré contar con ellos siempre. Es muy grato agradecer a mi asesor metodólogo Mg. Anselmo Aniceto Valenzuela Zegarra, a mi asesor Temático Ing. Mabel Susana Ygnacio García porque compartieron conmigo experiencias, conocimientos y nuevas ideas. A todos los que permitieron superarme más y ser mejor cada día.

JURADOS DE SUSTENTACIÓN

_____

PRESIDENTE
Dr. CASIO AURELIO TORRES LOPEZ

_____

PRIMER JURADO
Dr. GAMARRA MORENO ABRAHAM ESTEBAN

_____

SEGUNDO JURADO
Mg. BLAS REBAZA MARUJA EMELITA

_____

TERCER JURADO
Ing. VIGO LOPEZ GIOVANNY SOCORRO

_____

SECRETARIO DOCENTE
MG. MIGUEL ÁNGEL CARLOS CANALES

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Esta investigación tuvo como problema general "¿Cuál será la influencia de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información?, el objetivo general fue "Implementar la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información"; y la hipótesis general que se contrastó fue "La optimización del algoritmo Estándar de Encriptación Avanzada (AES) mejorará la protección de la información"

El método general de investigación fue el método científico, el tipo de investigación fue aplicada, el nivel de investigación fue explicativo, el diseño Pre-experimental, la población de estudio corresponde a los todos los empleados de la empresa DIACSA en un total de 43 empleados (censado), no se tomó una muestra por ser una población reducida, por tanto se utilizó la técnica del censo.

Finalmente en base al análisis de los resultados obtenidos se llegó a la conclusión que la optimización del algoritmo Estándar de Encriptación Avanzada (AES) mejoró la protección de la información de los empleados de la empresa DIACSA.

Palabras clave: Criptografía, Criptoanálisis, algoritmo de encriptación, criptografía simétrica, criptografía asimétrica

ABSTRACT

This research had as a general problem “What will be the influence of the optimization of the Standard Advanced Encryption (AES) algorithm for the protection of information? The general objective was“ Implement the optimization of the Standard Advanced Encryption (AES) algorithm for the protection of information ”; and the general hypothesis that was contrasted was "The optimization of the Advanced Encryption Standard (AES) algorithm will improve the protection of information".

The general research method was the scientific method, the type of research was applied, the level of research was explanatory, the Pre-experimental design, the study population corresponds to all the employees of the company DIACSA in a total of 43 employees (censored), a sample was not taken because it was a small population, therefore the census technique was used.

Finally, based on the analysis of the results obtained, it was concluded that the optimization of the Advanced Encryption Standard (AES) algorithm improved the protection of the information of the employees of the company DIACSA.

Keywords: Cryptography, Cryptanalysis, encryption algorithm, symmetric cryptography, asymmetric cryptography

INTRODUCCION

Los problemas de seguridad de la información aparecen con más énfasis con los nuevos desarrollos Tecnológicos, la era de la tecnología de información, las comunicaciones digitales aumentan, por lo tanto aparecen también nuevas amenazas que tratan de vulnerar a estos medios de comunicación y datos almacenados en medios informáticos, computadoras, servidores o base de datos, dando origen así a aparición de técnicas utilizadas por hackers, cibercriminales, etc., para vulnerar los sistemas de la información; por lo que personas, empresas, gobiernos, organizaciones son conscientes de este tipo de ataque y de las vulnerabilidades que presentan los sistemas de información, algunas organizaciones están elaborando estrategias de defensa para enfrentar a estos ataques, o ante cualquier tipo de vulnerabilidad de los sistemas de información, y ya no es sólo de interés de las redes militares de defensa, inteligencia o logística, sino también de uso personal y de redes de infraestructuras críticas absolutamente dependientes.

Una de las propuestas más comunes en la actualidad es que tanto personas u organizaciones están optando por el uso de algoritmos criptográficos propios o personalizados para garantizar la seguridad y protección de la información de sus computadores, servidores o bases de datos.

Esta investigación tiene como base la tesis de pregrado "Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información" desarrollada por el suscrito, y se enfoca en la optimización del algoritmo criptográfico de AES al cual se realizó una implementación para poder medir y recoger información de manera independiente acerca de la efectividad y seguridad que proporciona para proteger la información en los usuarios.

El algoritmo Advanced Encryption Standard (AES) fue seleccionado de varios algoritmos por el Instituto Nacional de Normas y Tecnología (NIST) en el año 1997 el cual sería capaz de proteger la información durante los próximos años y en la actualidad el algoritmo AES ha llegado a ser un algoritmo de mayor uso en criptografía simétrica adoptado y soportado en hardware y software.

Algunas acciones de ataques de criptoanálisis contra AES hasta la fecha han sido inalcanzables debido a que tiene flexibilidad para incorporar una longitud de llave que puede ser incrementada que permite tener un grado de escalabilidad en el futuro contra el progreso en la capacidad de realizar exhaustivas búsquedas de llaves o ataques por fuerza bruta. Sin embargo, la seguridad AES está solo si se hace una correcta implementación y una buena gestión de llaves.

Esta investigación está desarrollada en 5 Capítulos:

En el Capítulo I de esta investigación, se hizo el planteamiento de los problemas actuales en la criptografía moderna, que se han tenido que describir para poder comprender la importancia y los beneficios de los resultados sobre todo por el impacto causado en el área de seguridad de la información de la empresa Digital Automation & Control S.A. (DIACSA) al tenerse como objetivos mejorar nivel de seguridad y aumentar la eficiencia en la protección de la información, nos centraremos específicamente en el algoritmo AES y sus problemas, analizamos sus funciones y complejidad computacional, después planteamos una modificación de sus funciones y análisis de su complejidad, comparándola con el algoritmo original.

En el Capítulo II están descritos los antecedentes previos, aspectos específicos teóricos en los que basamos esta investigación, como otros trabajos encontrados sobre encriptación y seguridad de la información, la descripción del algoritmo AES, las herramientas y métodos que se usaron para el análisis de este, haciendo la definición de términos para una mejor comprensión y en base a los planteamientos teóricos se planteó la hipótesis general, especificas así como las variables y su operacionalización.

En el Capítulo III se hizo una descripción del diseño metodológico de la investigación, donde se optó por desarrollar una metodología pre-experimental correlacional por la manipulación de las variables, se usó el tipo de investigación aplicada por que se hizo en base a conocimientos teóricos relacionados a encriptación; asimismo, esta investigación se desarrolló en la empresa DIACSA teniendo como población y muestra tomadas a los empleados de dicha empresa y para el análisis y procesamiento de los datos se usó el software de estadística SPSS.

En el Capítulo IV se hizo el análisis y evaluación exhaustiva de las características del algoritmo logrando determinar sus fortalezas y debilidades para poder hacer la optimización y presentarlo a los usuarios para obtener una respuesta del grado y nivel de seguridad que brinda esta optimización pudiendo hacer la interpretación de los resultados obtenidos en la investigación después de aplicar técnicas y los instrumentos.

En el Capítulo V se presentaron los resultados obtenidos de la aplicación de los instrumentos de medición, del impacto que presento la implementación de la optimización del algoritmo.

Finalmente se tiene las conclusiones de los resultados, recomendaciones, referencias bibliográficas y anexos.

Bach: Simón Wilmer Mori Acero

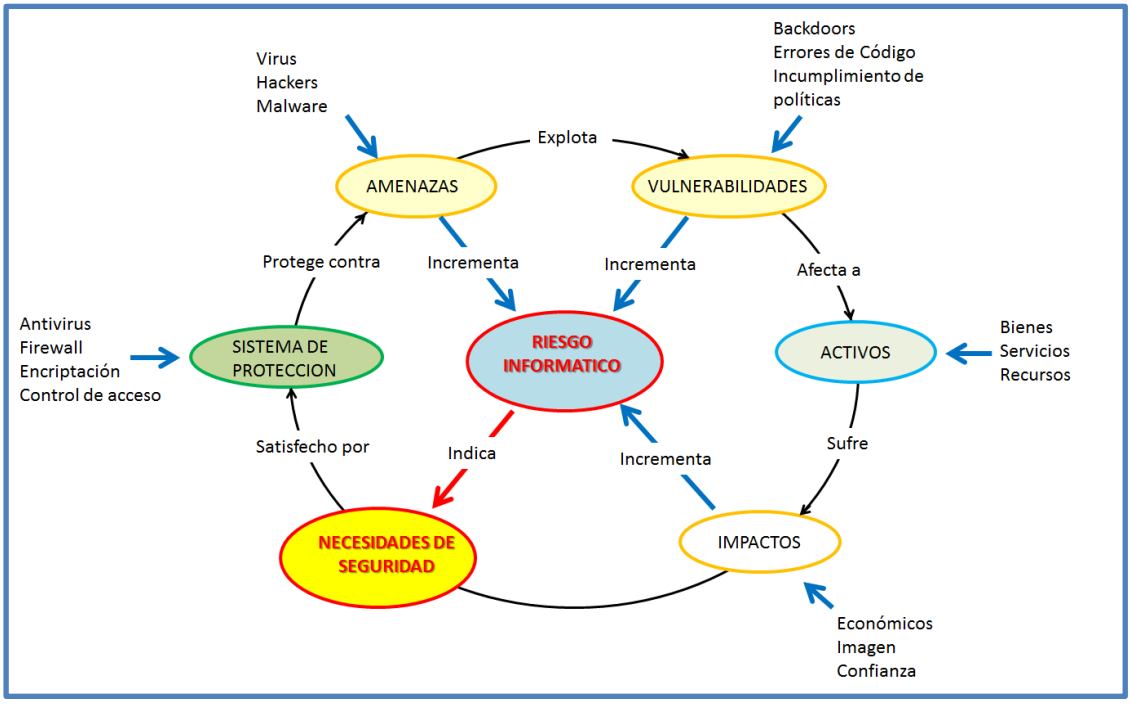
CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema:

En la actualidad existe un gran riesgo de que la información pueda ser sustraída desde las bases de datos o de un computador personal por medio de dispositivos de almacenaje de uso personal o por intrusión a las redes informáticas intranet o internet debido a que no se encuentra con ningún tipo de protección para evitar ser copiados o abiertos por personas no autorizadas.

Figura 1 Riesgo informático



Fuente: Elaboración propia

Al respecto, diversas empresas u organizaciones, como medida preventiva para proteger la información de computadores de uso personal o base de datos, han adaptado sistemas de seguridad, entre ellos: antivirus, firewall, copias de seguridad, etc., aunque a veces estas medidas no son las suficientes debido a que se administra información compartida, en algunos casos de manera integral y en otros de manera aislada.

La empresa DIACSA es una de las empresas que manipula información confidencial propia de la empresa y de los proyectos o investigaciones que se realizan, cuenta con medios informáticos implementados en las redes donde la información está disponible para todos los usuarios; esta información nunca era protegida permitiendo de esa manera poder se víctimas del ataque de hackers o cibercriminales; ante esta necesidad se consideró necesario implementar medios de protección basados en la encriptación de la información.

La encriptación consiste en transformar un mensaje en otro, de tal manera que el mensaje original sólo puede ser recuperado por un determinado grupo de personas que conocen cómo desencriptar mensajes; sin embargo algunos inconvenientes que se pueden presentar al momento de emplear la encriptación para la protección de información, es que puede ocasionar recarga de trabajo o que la información una vez protegida no se encuentre disponible a los usuarios para ser usada cuando lo requieran y el aumento de la cantidad de datos en transita por las redes, también aumenta la responsabilidad de las empresas o de los usuarios por mantener la privacidad de los datos que manejan fuera del alcance de la ciberdelincuencia y de prácticas malintencionadas.

La protección de los datos es y será una de las funciones importantes dentro del entorno de la Tecnología de la Información y las Comunicaciones (TIC), es por eso que la encriptación o cifrado de datos ha dejado de ser de uso solo de militares y bancos convirtiéndose en una tecnología que puede ser de uso obligado para todo tipo de organizaciones sin importar el tamaño o rubro que sea, debido a que todas las organizaciones hacen gestión de datos sensibles, los que pueden ser sustraídos y utilizados de manera ilegal.

“La compañía peruana de seguridad Supra Networks estimó que los ciberataques se elevarán en 25% este año en América Latina. Pero ¿cuáles son las modalidades que más afectan a los usuarios y empresas en el Perú? Los expertos consultados coinciden que el ransomware, phishing y recientemente el cryptojacking generan cada vez más víctimas en el país.” (1)

La mayor amenaza, claramente, recae en los hackers que no sólo acceden redes y sistemas sin permiso, sino que también llevan a cabo ataques de phishing, ransomware

y crypto hacking con el fin de beneficiarse. Para poder ilustrar el estado actual de la seguridad informática tenemos los siguientes datos estadísticos: "…

1. El 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017. (Ponemon Institute)
2. 43% de los ciberataques afectan a pequeños negocios. (Small Business Trends)
3. 90% de los hackers cubren sus rastros utilizando encriptación. (Vanson Bourne)
4. El número de variantes de malware de crypto hacking creció de 8 en el 2017 a 25 en Mayo del 2018. (Quick Heal)
5. El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los $124 billones. (Computer Weekly)
6. El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos. (Accenture)
7. Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de $2.4 millones en defensa. (Accenture)
8. Ocurren más de 4,000 ataques de ransomware por día. (FBI)
9. El 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones. (KnowBe4)
10. En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. (CyberArk)…" (2)

En el Perú no está muy difundido el empleo de herramientas de encriptación para la protección de información, debido a la falta de promoción por parte de los organismos responsables de la seguridad y los pocos que las usan en algunos casos han presentado inconvenientes para la recuperación de la información una vez encriptado, quizás por el poco conocimiento de la forma adecuada del empleo de la encriptación para la protección de la información; Asimismo, la empresa privada viene usando algoritmos de encriptación comercial de manera indirecta implementada dentro de dispositivos informáticos como servidores, routers, switches y otros.

1.2. Formulación del problema

1.2.1. Problema General

¿Cuál será la influencia de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información?.

1.2.2. Problemas Específicos

a) ¿Cuál será impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para incrementar la **efectividad** de la protección de la información?

b) ¿Cuál será impacto de la optimización e implementación del algoritmo Estándar de Encriptación Avanzada (AES) para aumentar el nivel de **seguridad** en la protección de la información?

1.3. Justificación

1.3.1. Social o practica

En la práctica esta investigación es de beneficio tanto para las empresas u organizaciones y a la sociedad en general porque les va a permitir proteger todo tipo de información evitando inconvenientes por pérdida de información privada o sensible, producto de investigaciones, trabajos realizados, información personal o familiar, que se encuentran en dispositivos informáticos con acceso a internet o redes sociales. Esta solución ayuda a la sociedad a continuar obteniendo herramientas que van a garantizar la seguridad de la información.

1.3.2. Metodológica

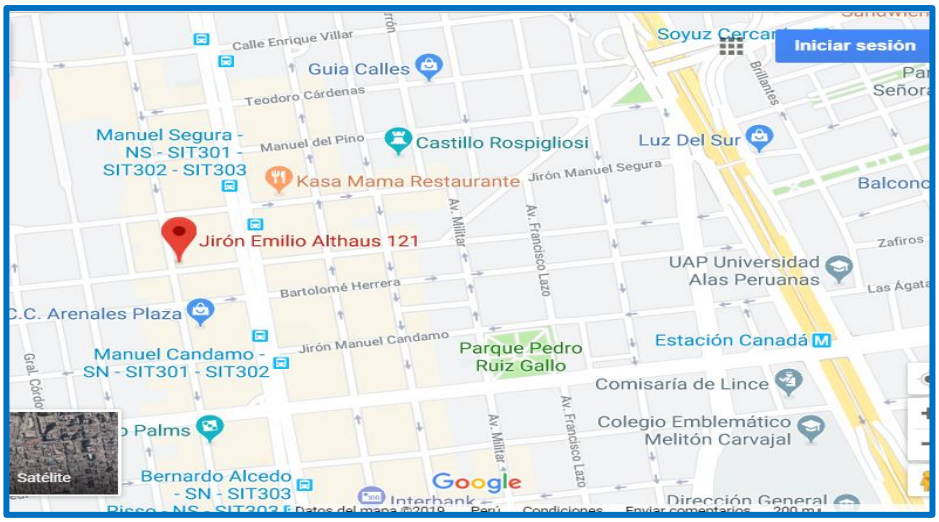
Se usó una metodología de seguridad de tecnologías de información y comunicaciones, que permitió la implementación del algoritmo de encriptación, la importancia metodológica de esta investigación es que se pondrá en práctica además de los métodos tradicionales de recopilación de información, se usarán normas y estándares que guían en diferente medida el cumplimiento de la seguridad de las tecnologías de información y comunicaciones basadas en el estándar del algoritmo y de la NTP-ISO 27001

1.4. Delimitación del problema

1.4.1. Espacial

La presente investigación se desarrolló haciendo el análisis y evaluación del algoritmo que usa la herramienta de encriptación Estándar de Encriptación Avanzada AES, que fue optimizado e implementado para dar protección a la información y a las comunicaciones dentro de la empresa Digital Automation & Control S.A (DIACSA) ubicada en Jr. Emilio Althaus 121-1001 distrito de Lince - http://www.diacsa.com/

Figura 2. Ubicación empresa Diacsa



Fuente: http://www.diacsa.com/servicios.html

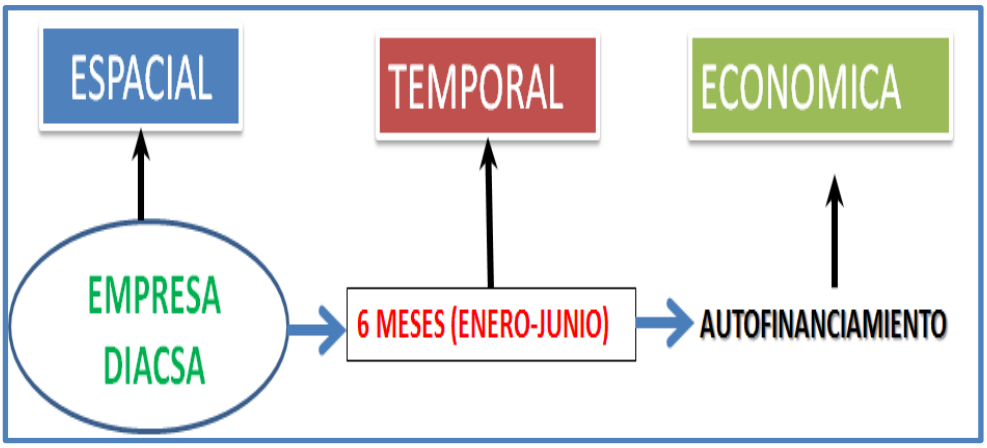
1.4.2. Temporal

Para la obtención de información relacionada al algoritmo de encriptación y su funcionamiento para el cifrado y descifrado así como para la obtención datos relacionados al impacto causado en los usuarios se tomó un periodo de tiempo promedio de seis (6) meses entre enero a junio del 2019.

1.4.3. Económico

Esta investigación se realizó mediante el autofinanciamiento, con recursos necesarios y de acuerdo a la disponibilidad de los mismos se tuvieron que racionalizar para poder llegar a la etapa final de dicha investigación.

Figura 3. Delimitación del problema de investigación



Fuente: Elaboración propia

1.5. Limitaciones

Una de las principales limitaciones de esta investigación es que es necesario una mayor cantidad de tiempo para realizar la optimización y la implementación de los prototipos del algoritmo de encriptación con diferentes usuarios. Asimismo, existe una limitación económica ya que toda la inversión de esta investigación es autofinanciada por el suscrito.

1.6. Objetivos

1.6.1. Objetivo General

Implementar la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información.

1.6.2. Objetivos Específicos:

a) Determinar cuál es el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para incrementar la **efectividad** de la protección de la información.

b) Establecer cuál es el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para aumentar el nivel de **seguridad** en la protección de la información.

CAPÍTULO II

MARCO TEÓRICO

Como parte del Marco Teórico de esta investigación, se ha seleccionado los conceptos básicos relacionados con herramientas de encriptación y la seguridad de la información que deben ser de conocimiento de los empleados de esta empresa u organización en donde se desarrollara dicha investigación.

2.1. Antecedentes

La necesidad de mantener la información guardada en bases de datos o computadoras personales y envió o recepción de grandes cantidades de información produce una gran repercusión en los sistemas de comunicación, este envió o recepción de información requiere soporte de redes, protocolos de comunicación y de medidas de seguridad adecuadas que le permitan llegar de forma segura a sus destinos finales, sin ser vulneradas en su integridad, contenido y autenticidad. Es por esa razón es necesario que la información pueda estar disponible en todo momento, trasmitiendo y recibiendo a cada instante que se requiera pero que esta se encuentre asegurada mediante el uso de la encriptación.

2.1.1. Antecedentes Nacionales.

"Análisis y Optimización del algoritmo de encriptación Rijndael en el que se basa el Estándar de Encriptación Avanzada AES (Advanced Encryption Standard)" Dávila Torres Juan Carlos (Puno-2017)

Esta investigación plantea como **objetivo principal**, realizar la modificación del algoritmo Rijndael para que se convierta en una herramienta de encriptación más fuerte y fortalecida contra los ataques de fuerza bruta, donde los datos sean totalmente aleatorios. Al realizarse la evaluación de la complejidad del algoritmo inicial, se decidió realizar una modificación en la estructura de la función KeyExpansion que es donde se originan las llaves a usar en la siguientes rondas de acuerdo al tamaño de la llave y al realizarse esta modificación también puede calcular los movimientos para cada una de las

rondas, y ShiftRow que es una de las principales funciones para difusión de los caracteres, en la modificación de esta función se pueden realizar movimientos de acuerdo a los calculados en la función KeyExpansion.

Hipótesis General: El nuevo algoritmo encriptación basado en el estándar de encriptación avanzada AES (Advanced Encryption Standard) ofrece una mayor independencia matemática en los bloques crípticos y no se afectó la complejidad temporal del algoritmo original.

Tipo y Diseño de Investigación: Esta investigación es tipo descriptiva ya que se describen las diferentes funciones del algoritmo de encriptación AES, así como la modificación de estas y el impacto que tiene sobre el proceso de encriptación y desencriptación de datos

Una vez realizada la modificación se ha tenido que hacer un análisis asintónico de la modificación para poder **comparar** los **resultados** obtenidos con los que son producto del análisis asintótico del algoritmo inicial.

Siguiendo como base esta investigación de tipo descriptiva se pudo determinar y conocer cada una de las etapas en las que se puede optimizar el algoritmo AES para realizar la optimización debido a que el algoritmo Rijndael es el que dio origen al algoritmo AES.

“Análisis comparativo de algoritmos criptográficos para redes privadas virtuales” Capuñay Puican, Denys Ivan (Chiclayo-2016)

La manera de manejar la información de una forma más segura y confiable, es mediante las redes privadas virtuales (VPN), que permite unirnos y tener un enlace privado, el mismo que se va adecuando sobre una red pública que va a poder garantizar la integridad y confidencialidad de la información debido a los múltiples procesos de autenticación, encriptación y codificación, obteniendo un enlace que va a garantiza la privacidad.

Por eso, que la presente investigación a tratado de hacer el análisis comparativo de algoritmos criptográficos que son usados para redes privadas virtuales, debido a que el principal problema está en asegurar la integridad y seguridad que tiene la información al momento que sea otro equipo de manera remota. Esto se ha logrado al seleccionar los algoritmos para redes privadas virtuales (VPN), e implementándolo en una red donde se tuvo que hacer estudios y captura de tráfico que permite observar y analizar cual ofrece una mejor integridad y seguridad de la información.

El Objetivo general de esta Investigación es realizar un análisis comparativo de los algoritmos criptográficos que existen para redes privadas virtuales.

Esta investigación se desarrolló bajo la **metodología experimental**, porque permitió la manipulación de las variables en tal forma que permita la recolección de datos, lográndose conocer el tipo de encriptación que ofrece cada algoritmo. Luego de esto se evaluó cada algoritmo en una red implementada, se pudo determinar cuál de los algoritmos es más óptimo en tiempos, tamaño de paquetes, nivel de encriptación y desencriptación, grado de encapsulación, entre otros. Se obtuvo que el **algoritmo AES** puede dividir los datos en mayor número de paquetes y requiere menor tiempo de envió comparado con los otros algoritmos. Con respecto a los paquetes encriptados el algoritmo AES tiene igual cantidad de paquetes encriptados que el algoritmo DES, pero el algoritmo AES desencripta mas paquetes que el algoritmo DES utilizando menos recursos.

La Hipótesis propuesta es: con la implementación del algoritmos criptográfico mejora la integridad de una red privada virtual; Para poder validar dicha hipótesis y evaluar su impacto real del algoritmo en lo relacionado a la integridad y seguridad de los datos, se realizó el análisis y evaluación en una red privada virtual, en el que se realizaron ataques que consistieron en captura de tráfico y desencriptando, todo fue realizado simulando escenarios reales.

Entre las **conclusiones** se tiene que el AES está diseñado con el mejor protocolo de encriptamiento en relación a tiempo de envío, cantidad de

paquetes de encriptación y de paquetes de desencriptación, cantidad de paquetes de encapsulación y en el cantidad de paquetes de desencapsulación.

Este trabajo de investigación hace una comparación de la funcionalidad de otros algoritmos implementados en una red VPN en los que concluye que el algoritmo AES presenta mayores ventajas en relación al tiempo de envío, pero también hace referencia al tamaño de paquetes, al nivel de encriptación y desencriptación, al grado de encapsulación entre otros lo que nos permitió tomarlo como base para nuestra investigación.

"Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información" Samaniego Zanabria, Ana Liz (Lima-2018)

En esta Investigación "se realizó Evaluación de algoritmos criptográficos para mejorar la seguridad en la comunicación y almacenamiento de la información", se ha tenido que someter a **pruebas, herramientas**, enfoques y ataques a algoritmos criptográficos globalmente conocidos (AES, IDEA y RC5) y al algoritmo propio presentado en esta investigación ANN, con el fin de obtener resultados del grado de seguridad, fortaleza de llave, modo y diseño cifrado, rendimiento y resistencia de cada uno de ellos, con la finalidad de poder evidenciar cuál de ellos tiene implementado mecanismo que dan mayor seguridad en la comunicación y almacenamiento de la información, como solución al problema planteado en párrafos anteriores.

El objetivo general que se ha definido en la investigación es: Determinar qué algoritmo criptográfico proporciona mayor seguridad en la comunicación y almacenamiento de la información por lo que se tuvo que aplicar metodología de investigación - **teórica** debido a que proporcionará conocimientos que permiten mejorar la seguridad de la comunicación y almacenamiento de la información; Por otro lado se platea como hipótesis general: El algoritmo propio proporciona mayor seguridad en la comunicación y almacenamiento de la información en comparación con los algoritmos criptográficos globalmente conocidos.

En conclusión el algoritmo propio proporciona mayor grado y cantidad de almacenamiento de la información y seguridad en la comunicación al ser comparado con los algoritmos criptográficos globalmente conocidos, los ítems que sustentan este resultado son la resistencia y capacidad de almacenamiento.

De esta investigación se obtuvo parámetros de seguridad y fortalezas de otros algoritmos criptográficos lo que nos ha permitido analizar mejor nuestras propuestas de mejora del algoritmo AES.

"Establecimiento, Implementación, Mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una Empresa de Consultoría de Software" Santos Llanos, Daniel Elías (Lima – 2016)

Esta investigación tiene como Objetivo General "Desarrollar un Sistema de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013"

En la actualidad, empresas de consultoría y desarrollo de software cuentan con retos propios de este negocio. Entre los que destacan son los relacionados a seguridad de la información, debido al intercambio constante de información entre la empresa y los clientes, donde van aparecer algunos potenciales riesgos que podrían comprometer el éxito y la subsistencia de la empresa u organización. **La solución** que se ha planteado para resolver este problema es la implementación de Sistema de Gestión de Seguridad de Información (SGSI), el mismo que deberá contar con el estándar ISO 27001:2013 como parte del marco formal de los requisitos que debe cumplir. Este sistema servirá para que los directivos y los demás colaboradores puedan gestionar y puedan tomar las decisiones correctas con respecto a la seguridad de información de la empresa u organización, esta permitirá asegurar de que este sistema cuente con niveles adecuados en relación a aspectos de confidencialidad, integridad y disponibilidad de la información importante que se usa como parte de su

operación. Con este informe se ha podido especificar cuatro fases cíclicas de un SGSI: **el establecimiento**, que es donde las bases del sistema se van a integrar a los procesos del negocio**; la implementación**, que es donde se desarrolla los mecanismos para una correcta administración de lo relacionado a seguridad; **el mantenimiento**, que es donde se pueden detectar fallos que pueden ocurrir en la empresa, organización o en el mismo sistema; **y la mejora**, que va a permite cerrar el ciclo mediante la aplicación de correcciones y optimizaciones que hayan sido detectadas. Este modelo va a permitir que este sistema pueda operar bajo el principio de mejora continua, que será de beneficio permanentemente para la organización, favoreciendo a que se realice un adecuado manejo de la seguridad de la información.

Finalmente después del desarrollo de esta investigación se tiene como resultado que el estándar 27001 necesariamente se tiene que complementar con otros estándares ISO, por lo tanto para la elaboración adecuadamente todos los componentes que van a permitir cumplir los requisitos del estándar 27001 se tienen que considerar los estándares que, aunque no han sido referenciados, ya forman parte del dominio de los requisitos del SGSI y para el resultado del proyecto y sus interesados, se han tenido que elaborar algunas propuestas innovadoras asociadas a: la metodología de la gestión de los riesgos, la normalización de planes del sistema y verificación integral de cumplimiento de todos los componentes requeridos por la ISO/IEC 27001:2013.

Esta investigación plantea que para la realización de la implementación de un SGSI es necesario contar con requisitos basados en los procedimientos y los estándares de seguridad establecidos en las normas ISO en las que consideran temas relacionados a criptografía para la protección de la información.

“Metodología para la Seguridad de Tecnologías de Información y Comunicaciones en la Clínica Ortega” Guzmán Pacheco, Goyo Francisco (Huancayo – 2015)

Existen varios estándares que se han desarrollado para la gestión de la seguridad de la información, algunos son más generales que otros, otros están

centrados solo en la gestión de los riesgos (serie ISO/IEC 27.000), y en algunos casos tienen una tendencia al desarrollo de un modelo de madurez de la seguridad de la información (ejemplo ISM3); sin embargo, en las especificaciones no se afrontan en su aplicación a un grupo empresarial, lo cual requiere algunas consideraciones adicionales.

En este trabajo, como parte de la investigación se han hecho **análisis a diferentes enfoques de estos estándares**, para poder proponer la metodología para la implementación, gestión y mejora en la seguridad de tecnologías de información y las comunicaciones en la clínica Ortega. Se presentan también otras alternativas estratégicas y se ha discutido sobre su conveniencia o no. Se analizaron varios métodos que se conocen como análisis y gestión de los riesgos.

Esta investigación ha tenido como objetivo general "Determinar cuál es el nivel de importancia de las metodologías de seguridad de tecnologías de información y comunicaciones que va a permitir la continuidad de procesos de la clínica Ortega cuyos principales servicios van a depender de la tecnología.

Esta investigación es tipo **descriptiva** debido a que pretende medir o obtener información de manera independiente o en conjunto en lo relacionado a los conceptos o variables a que se han referido y de tipo explicativa porque se parte de un diagnóstico para poder proponer una alternativa de solución, explicándose paso a paso todo lo que se va realizando en el desarrollo de dicha investigación.

El Método utilizado es **Analítico o Explicativo**, debido a que permitió analizar y explicar todas las metodologías de seguridad de tecnología de información y comunicación, sus vulnerabilidades y controles para la protección.

Como **Hipótesis General** se planteó "El análisis de riesgo y los controles de seguridad van a permitir definir la metodologías de seguridad de tecnologías de información y comunicaciones para la continuidad de los procesos de información de la clínica Ortega".

Como **conclusión** para poder definir el modelo de metodología de seguridad en tecnologías de información y comunicaciones se ha tenido que realizar el análisis de los riesgos lo que ha permitido detectar algunas amenazas a los que están sometidos los activos de la información y los requerimientos de seguridad que se han presentado, han permitido delimitar el ámbito del modelo y su estructura. Para poder desarrollar el modelo de seguridad de tecnologías de información y comunicaciones se ha tenido que tomar en cuenta Normas técnicas y recomendaciones del modelo ISO; además, se ha realizado una evaluación económica del mismo el cual ha podido ser tomado como referencia para poder considerar que el proyecto relacionado con las metodologías de seguridad de tecnologías de información y comunicaciones es factible económicamente.

De esta investigación obtuvimos la idea de que para hacer una mejora de la seguridad de la información es necesario el desarrollar un modelo de seguridad de tecnología de la información y comunicaciones que esté basado en implementación de Normas técnicas y recomendaciones del modelo ISO.

2.1.2. Antecedentes Internacionales.

"Diseño e Implementación de un Nuevo Algoritmo Criptográfico Simétrico para Mensajería Instantánea en un Entorno Web" Cushpa Guamán, Ana Lucila (QUITO – 2018)

El **objetivo** fue el diseñar e implementar de un nuevo algoritmo criptográfico simétrico para mensajería instantánea en entorno web, para incrementar la seguridad de la información que se transmite a través de canales inseguros de información utilizando la criptografía. Se realizó una revisión de las características que presentan los algoritmos criptográficos simétricos más utilizados que permitió determinar el algoritmo simétrico AES (Advanced Encryption Standard) como algoritmo base para obtener los parámetros para hacer una comparación con otros algoritmos simétricos donde se generó el Prototipo I, después esto ha permitido hacer el desarrollo de un nuevo algoritmo criptográfico que reúne nuevas funciones lo que ha generado el

Prototipo II. En la implementación se utilizó Netbeans como ambiente de desarrollo de los prototipos llamados de escritorio con los cuales se pueden realizar las pruebas de entropía a los mensajes cifrados por cada uno de los prototipos y utilizando el software R Stadistical se pudieron obtener algunos datos estadísticos de las pruebas realizadas para poder hacer la validación del algoritmo propuesto y su incorporación en los prototipos web que serán aplicados en un chat del que se requiere del apoyo postgreSQL que servirá de motor a su base de datos. Al realizar la implementación del Prototipo I y Prototipo II se hizo la comparación de los resultados que fueron obtenidos del análisis de las características de los algoritmos y con el apoyo de la herramienta Cryptool se tuvieron que realizar pruebas de criptoanálisis para poder hacer la medición y comparar los indicadores considerados en las variables. Al aplicar la estadística descriptiva e inferencial para la comprobación de la **hipótesis** se pudo concluir que el **nuevo algoritmo** propuesto **incrementó el nivel** de seguridad en 53% al compararlo con el algoritmo simétrico AES base esto se debe a que este presenta mayor difusión en el cifrado de los mensajes. La modificación de las funciones que ejecuta el algoritmo o el incremento de nuevas funciones ayudan a difuminar más el mensaje.

Para la demostración de la **Hipótesis** "La implementación del nuevo algoritmo criptográfico simétrico para mensajería instantánea en el entorno web mejorará el nivel de seguridad de la información" se realizó una investigación tipo **cuasi-experimental** debido a que, en base a características que se definen en el estudio, se escogerá un algoritmo criptográfico simétrico que servirá de base para crear el nuevo algoritmo criptográfico simétrico y aplicará el **método analítico** porque que se realizará un análisis de los algoritmos criptográficos simétricos existentes, su funcionalidad y características para determinar un algoritmo criptográfico simétrico base y **método inductivo** porque a partir del algoritmo criptográfico base seleccionado, se diseñará un nuevo algoritmo que mejore el nivel en la seguridad de la información

Del análisis de algoritmos criptográficos se determinó el algoritmo AES como base para el desarrollo del nuevo algoritmo criptográfico debido a sus ventajas

en la resistencia a criptoanálisis y contra fuerza bruta, además permite la utilización de claves de longitud de 128 bits, 192 bits y 256 bits así como también tamaños de bloque variable.

“Paralelización de los algoritmos de cifrado simétrico AES-CTR y AES-OTR sobre un kit de desarrollo NVIDIA Jetson TK1”Torres González, Daniel Alberto (México – 2016)

El principal **objetivo** de la tesis es generar nuevos diseños e implementaciones paralelas optimizadas del algoritmo de cifrado simétrico estandarizado AES-CTR y del algoritmo de cifrado simétrico en competencia AES-OTR sobre un kit de desarrollo NVIDIA Jetson TK1, de tal forma que, para una entrada de datos, los algoritmos sean capaces de ejecutar varias instancias de AES en paralelo sobre la CPU o sobre la GPU, para así disminuir los tiempos de ejecución del proceso de cifrado/descifrado de datos, registrando todos los resultados y comparándolos contra una implementación secuencial de AES-CTR hecha con las bibliotecas estandarizadas de OpenSSL y contra una implementación secuencial de AES-OTR escrita por el autor, para finalmente corroborar que el rendimiento de los algoritmos criptográficos ha sido mejorado.

Actualmente muchas corporaciones y agencias gubernamentales se encuentran investigando nuevas formas de asegurar grandes volúmenes de información considerada sensible en intervalos de tiempo cortos. Para lograr esta tarea se requiere cifrar la información con un algoritmo criptográfico, el cual puede requerir de operaciones computacionales bastante costosas y por ende degradar el desempeño del equipo de cómputo en el que se ejecuta. La constante demanda de soluciones criptográficas eficientes ha crecido continuamente en diversas áreas durante la última década, como consecuencia del uso del Internet. En esta tesis se discuten implementaciones paralelas eficientes de los algoritmos criptográficos AES-CTR y AES-OTR. También se discute una optimización del modo de operación OTR. Las implementaciones se realizaron sobre un equipo móvil, el kit de desarrollo NVIDIA Jetson TK1, que cuenta

con una arquitectura para una versión multinúcleo y una versión en muchos núcleos.

Los resultados obtenidos en la arquitectura móvil muestran una aceleración de 3,92 y un rendimiento de 2,67 Gb/s en el modo de operación CTR, una aceleración de 2,32 y un rendimiento de 1,41 Gb/s en el modo de operación OTR, y una aceleración de 2,91 y un rendimiento de 1,68 Gb/s en la optimización propuesta al modo de operación OTR. Además, con la finalidad de demostrar que las implementaciones de los algoritmos paralelos son eficientes, se muestran pruebas realizadas sobre un servidor que incluye un microprocesador Intel I7 una tarjeta gráfica Tesla C2070. Los resultados obtenidos en el servidor muestran una aceleración de 21,105 y un rendimiento de 12,89 Gb/s en el modo de operación CTR, una aceleración de 2,303 y un rendimiento de 2,86 Gb/s en el modo de operación OTR, y una aceleración de 8,86 y un rendimiento de 11,01 Gb/s en la optimización propuesta al modo de operación podrán OTR. Al contar con estas nuevas implementaciones los dispositivos que incluyan en sus arquitecturas componentes multinucleo y GPU serán capaces de cifrar de una manera más eficiente una entrada de bytes proporcionados. Por consiguiente, AES-CTR y/o AES-OTR podrán realizar el cifrado de datos considerados sensibles en intervalos de tiempo cortos, permitiendo a otras aplicaciones aprovechar mayormente el uso de CPU como también de GPU, para poder incrementar la cantidad de información a ser cifrada/descifrada y ser transferida a través de un canal de comunicación si así se desea.

En esta tesis se generaron nuevos diseños paralelos optimizados de los algoritmos criptográficos AES-CTR y AES-OTR, con su respectiva implementación sobre una plataforma móvil. Estos diseños son capaces de invocar varias instancias de AES en paralelo, tanto en CPU como en GPU, para transformar grandes volúmenes de datos en una forma más eficiente que los algoritmos secuenciales clásicos y así, disminuyen los tiempos de ejecución del proceso criptográficos.

De esta investigación hemos podido obtener la conclusión que la velocidad de cifrado y descifrado no dependen de la complejidad del algoritmo o el lenguaje de programación sino del modo de operación y la infraestructura donde sea implementado.

“Desarrollo de una Aplicación para encriptar información en la transmisión de datos en un aplicativo de mensajería web” Moya Caza, Johanna Beatriz y Franklin Andrés Escobar Erazo (QUITO - 2015)

Es muy común hoy en día la vulnerabilidad en la información. Razón por la cual en los últimos años ha tomado importancia el estudio y la implementación de modelos de encriptación para poder asegurar la confidencialidad al hacer el intercambio de información. Convirtiéndose en una especie de “tentación” para la adquisición de productos ayuden a minimizar este problema; es por eso que resulta ser de mucha importancia encontrar **e implementar medidas de seguridad que puedan garantizar la integridad** de la misma (objetivo principal de esta investigación).

Un claro ejemplo que puede ser de gran ayuda para poder evitar este tipo de vulnerabilidad en la información real en la trasmisión de datos es **la aplicación de la encriptación** que un proceso mediante el cual la información o texto sin ningún formato puede ser cifrado de tal forma que el resultado es ilegible a menos que se conozcan algunos datos necesarios para poder hacer su interpretación, convirtiéndose así en una medida de seguridad que se usa para que al momento que se almacena o transmite información real o sensible ésta no va a ser obtenida con facilidad por intrusos, además opcionalmente debe existir un proceso de “des-encriptación” mediante el cual la información va a ser interpretada o descifrada y devuelta de nuevo a su estado original, beneficiando a las organizaciones respecto a costos bajos pero con beneficios mayores en seguridad de la información real en la trasmisión de datos.

Esta investigación de tipo **aplicada** aborda la protección pero desde un punto de vista que proporciona información del funcionamiento de los algoritmos de cifrado.

Se puede aplicar toda la información que se haya podido investigar para el desarrollo de esta disertación, se utilizaran metodologías que se conocen como **método de SCRUM** debido a que los entregables son pequeños y pueden hacerse revisiones de forma periódica, pudiendo hacerse de manera más efectiva la identificación de los errores y de los cambios, además Scrum se enfoca en entrega de productos sin importar la calidad del código como XtremeProgramming, como no se hace algo que parte desde cero y más bien se adapta a nuestras preferencias además que se va a reutilizar herramientas que ya existen en caso de que se necesiten. Para alcanzar el desarrollo tendremos que ir probando algunas herramientas como Dreamweaver, PHP, HTML, Visual Studio, ASP. NET y algunos relacionados a gestores de bases de datos como MySQL, Microsoft SQL Server, PostgreSQL que permiten realizar cambios hasta obtener el objetivo final para esta disertación.

En conclusión así como esta investigación existe otras donde presentan gran variedad de funciones para hacer encriptamiento, de las que es necesario ser realicen análisis y pruebas respectivas para la utilización individual o combinada de estos según requerimientos y seleccionar de manera adecuada la metodología y herramientas, permitiendo que el desarrollo de un aplicativo pueda manejar un código privado para que se mantenga la privacidad tanto emisor y receptor, asegurando de esa manera la confidencialidad y evitando ser intersectada por terceros no autorizados.

"Análisis en Seguridad Informática y Seguridad de la Información Basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros" Bermúdez Molina, Kelly Gabriela - Bailón Sánchez, Edber Rafael (Ecuador – 2015)

El objetivo de esta investigación es Analizar procesos críticos de Credigestión con respecto a gestiones de seguridad que sean las adecuadas para poder garantizar la confidencialidad, integridad y disponibilidad de información, mediante formulación de recomendaciones relacionadas a seguridad y controles que están basados en la Norma ISO/IEC 27001.

Teniendo como hipótesis que mediante los controles de seguridad basados en la norma ISO/IEC 27001 se pueden establecen algunos mecanismos adecuados para poder mitigar los riesgos que se puedan presentar durante el uso de sistemas de información y el manejo de la información.

Se utilizó el tipo de investigación **de campo** debido a que se apoya en la información levantada, que es obtenida mediante observaciones en el mismo lugar donde se desarrolla cada uno de los procesos, las reuniones con Gerentes y Supervisores de cada área; la investigación es de tipo **descriptiva** porque detalla cada una de las actividades que se llevan a cabo en los todos los procesos manejados en el objeto de estudio, permitiendo de esta manera conocer en forma sistemática las principales falencias que se presentan en los mismos; investigación también es de tipo **no experimental** debido a que el objeto de estudio de la investigación no se puede modificar de manera deliberada, porque se basa principalmente en la observación de los eventos para que estos puedan ser posteriormente analizados; investigación de tipo **explicativa** ya que trata de establecer aspectos que causan el objeto de la investigación, asimismo, se plantea una valoración de hipótesis para que ayude a comprender mejor las causas de los eventos que se hayan presentado.

Mediante la realización de la elaboración de análisis de seguridad de la información y seguridad informática que se basa en la norma ISO/IEC 27001, este trabajo tuvo como finalidad poder conocer las vulnerabilidades a las que se expone la información por falta de **aplicación de controles de seguridad**.

Este análisis estaba dirigido a una empresa financiera, del que se tiene como **objetivo principal realizar el estudio de seguridad en los procesos críticos**. Mediante la realización de reuniones, revisión de la documentación, las consultas, observación, realización de encuestas y ejecución de entrevistas con los directivos que poseen un amplio conocimiento del negocio, se pudo identificar los riesgos actuales a los que están expuestos tanto físicos, lógicos y sistemas donde se procesa la información.

La **ejecución del análisis de los riesgos** pueden dar a conocer el nivel de impacto que va a tener la ocurrencia de las amenazas ya identificadas en cada activo de la información y pueden afectar datos relevantes utilizados o los resultados producto de la ejecución de las actividades propias del negocio.

Esta investigación nos ha permitido comprender que los **resultados** que se han obtenido nos dan a conocer que para poder minimizar los riesgos existentes, también va a ser necesario implementar controles de seguridad, lo cual ayudan a fortalecer tres aspectos muy importantes: la confidencialidad, integridad y disponibilidad de la información. Pero para fortalecer estos aspectos es necesaria la implementación de algoritmos de encriptación como parte de los controles para proteger la información.

"Diseño de un modelo de Seguridad de Información en redes LAN" Tufiño Galán, Ana Cristina (Quito, 2018)

El presente trabajo de disertación tiene como finalidad Diseñar un Modelo de Seguridad de Información para Redes LAN, basadas en ataques y vulnerabilidades que pueda tener una red al momento de intercambiar información entre sí.

Objetivo general: Diseñar un modelo de seguridad para la Interconexión de Sistemas Abiertos (OSI), que permita establecer mecanismos de protección en las 7 capas.

Se desarrolló a través de un **método científico** los cuales aplican conceptos puntuales sobre redes, sistemas operativos, hacking ético incluida sus aplicaciones, análisis de tráfico, escaneo de puertos, entre otros.

Las herramientas que se han utilizado son: Oracle VM Virtual Box, Máquina Virtual Kali Linux, Máquina Virtual Metaexploitable 2, Máquina Virtual Windows 7, Máquina Virtual, Windows XP, Wireshark, Ettercap, Yersinia, John de Ripper, Zenmap Linux, Nmap, Consola de comandos de cada uno de los sistemas operativos, Simuladores de red GNS3 y Cisco PacketTracer,

Firewall Untangle siendo utilizados con el objetivo de simular posibles ataques y mitigaciones hacia la red.

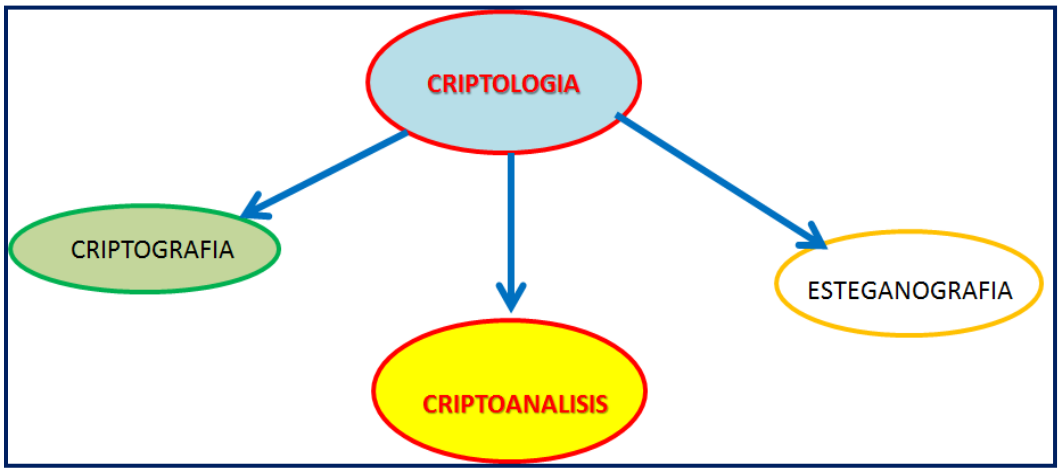
Como **resultado** de todo este análisis se obtiene las mejores medidas preventivas para ser una posible guía en el diseño y construcción de redes para cualquier tipo de empresa basadas en la familia de la ISO 270001. Por otro lado, el uso de la máquina virtual Kali Linux permitió realizar este análisis gracias a sus herramientas incluidas ya que se ha creado con el objetivo de auditar y asegurar cualquier red, además **Wireshark** fue la aplicación más utilizada para analizar el trafico antes y después de cada uno de los ataques desarrollados.

2.2. Marco Conceptual

2.2.1. Algoritmos de Encriptación

"La Criptología (proviene del griego krypto: 'oculto' y logos: 'estudio') es y será tradicionalmente, una disciplina que se dedica principalmente al estudio de la escritura secreta, se puede decir que estudia los mensajes que son procesados de cierta manera y se convierten en difíciles o imposibles de poder leer por entidades no autorizadas. Los campos en los que se divide la criptología son:" (3)

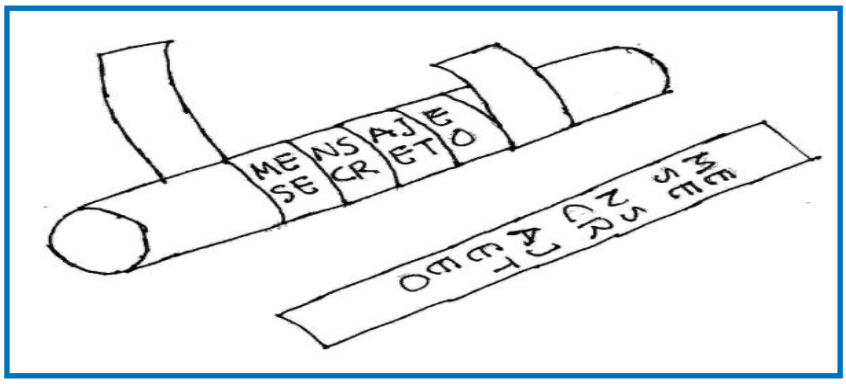
Figura 4. Campos de la Criptología



Fuente: Elaboración propia

- “**Criptografía.** (del griego: kryptos = oculto + graphein = escritura) se considera como el arte de poder escribir con clave secreta o de modo enigmático, se ocupa también del estudio de algoritmos, protocolos y sistemas que son utilizados para poder proteger la información y ofrecer seguridad a las comunicaciones y a las entidades que se comunican. Es el arte de poder escribir con clave secreta o de un modo enigmático. Aportando así una visión más específica, la criptografía consiste en la creación de técnicas tanto para el cifrado de datos como para el descifrado. Y tiene como objetivo conseguir la confidencialidad de los mensajes. Al ser la criptografía la creación de mecanismos para cifrar datos, entonces el criptoanálisis son los métodos para “romper” estos mecanismos y poder obtener la información. Una vez que nuestros datos hayan pasado un proceso criptográfico decimos que la información se encuentra cifrada” (4)

Figura 5. Cifrado Skytale



Fuente: http://www.math.com.mx/criptografia.html

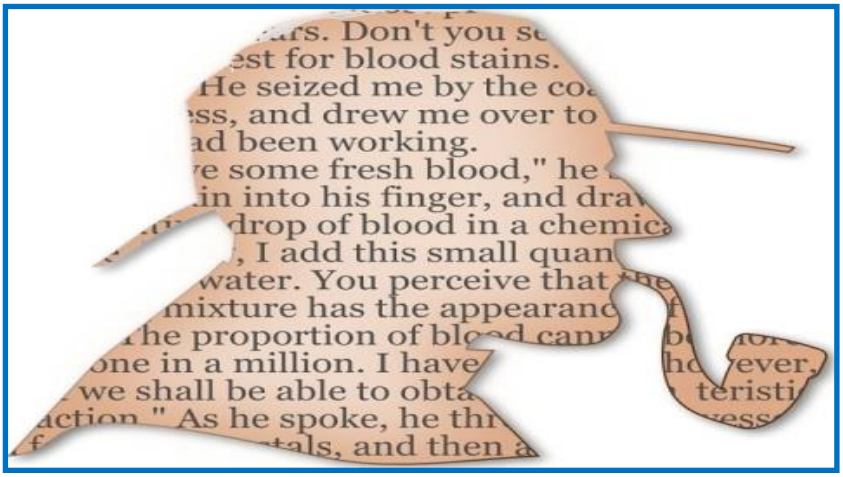
- “**Criptoanálisis.** Se ocupa principalmente de conseguir capturar el significado de los mensajes construidos mediante criptografía sin tener ninguna autorización para ello. Se puede decir que el criptoanálisis tiene un objetivo contrario a la criptografía. Su objetivo principal es buscar el punto débil o vulnerable de las técnicas criptográficas aplicadas para poder explotarla y así reducir o eliminar la seguridad que aportaba esa técnica criptográfica. A cualquier intento de criptoanálisis se le conoce como ataque. Se dice que un ataque tiene éxito y que el sistema se ha roto, cuando el atacante ha conseguido romper la seguridad que la técnica o método criptográfico aporta al sistema.” (5).

Figura 6. Criptoanálisis

Fuente: https://www.emezeta.com/articulos/criptoanalisis-las-tablas-rainbow

- "**Esteganografía**. Esta técnica se encarga de ocultar mensajes con información privada que viajan por un canal no seguro, de tal forma que el mensaje no sea ni siquiera percibido. Habitualmente el mensaje está escondido dentro de datos con diferentes formatos de video, imágenes, audio o mensajes de texto. Los usos más comunes de estas técnicas son: transmitir información entre entidades sin ser detectada por terceros no autorizados, se puede incluir información imperceptible en objetos digitales (Ej. imágenes, vídeos, audios)". (6)

Figura 7. Esteganografia



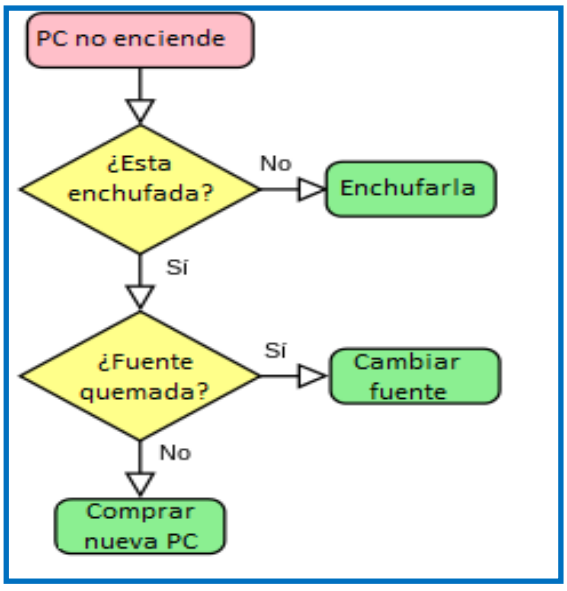
Fuente: https://rootear.com/windows/ocultar-archivos-esteganografia

“La Criptología es la ciencia que se ocupa de las comunicaciones secretas, dividiéndose en dos partes, una referida a la preparación y producción de códigos y claves (Criptografía) y otra referida al estudio e indagación de documentos y criptogramas para encontrar las claves que permitan descubrir el texto en el lenguaje claro (Criptoanálisis). El uso de las claves y de los códigos debe responder a la situación en que se encuentran los sucesos y por consiguiente atender a la táctica y la estrategia para restablecer así la prioridad de los requisitos de rapidez seguridad y simplicidad referente al mantenimiento del secreto de las claves y códigos, sea de tránsito prolongado que dan origen a la criptografía táctica, cuando se trata de operaciones limitadas en el tiempo, cuya clave debe cambiarse cada vez que sea necesario, o criptografía estratégica en la que el mantenimiento del secreto debe conservarse por un tiempo prolongado con códigos y claves perfeccionados para ser empleados en niveles superiores de la administración y servicios diplomáticos”. (7).

2.2.1.1. Algoritmos simétricos

Algoritmo: “Es el conjunto finito y ordenado de operaciones que van a permitir obtener una solución a un problema, esta es la definición de la Real Academia española” (8)

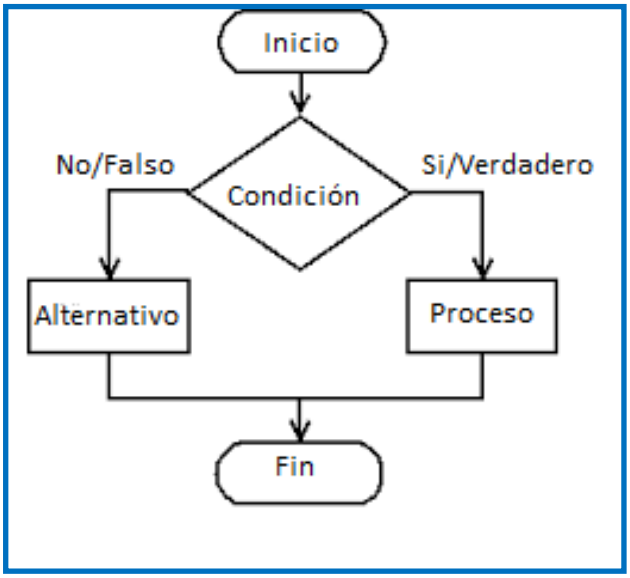
Figura 8. Algoritmo



Fuente: Elaboración propia

“Tanto para la matemática, lógica, ciencias de la computación y otras disciplinas relacionadas, algoritmo (del griego y latín, dixit algorithmus y del griego arithmos, significa «número», talvez también con influencia del matemático persa Al-Juarismi) viene a ser un conjunto pre-establecido de instrucciones o reglas bien definidas, ordenadas y finitas que van a permitir realizar una actividad mediante algunos pasos de manera sucesiva y que no generen dudas a quienes van a realizar dicha actividad. Dados una entrada y un estado de inicio y siguiendo los pasos de manera sucesiva se llega al estado final y la obtención de una solución” (9)

Figura 9. Diagrama de flujo algoritmo

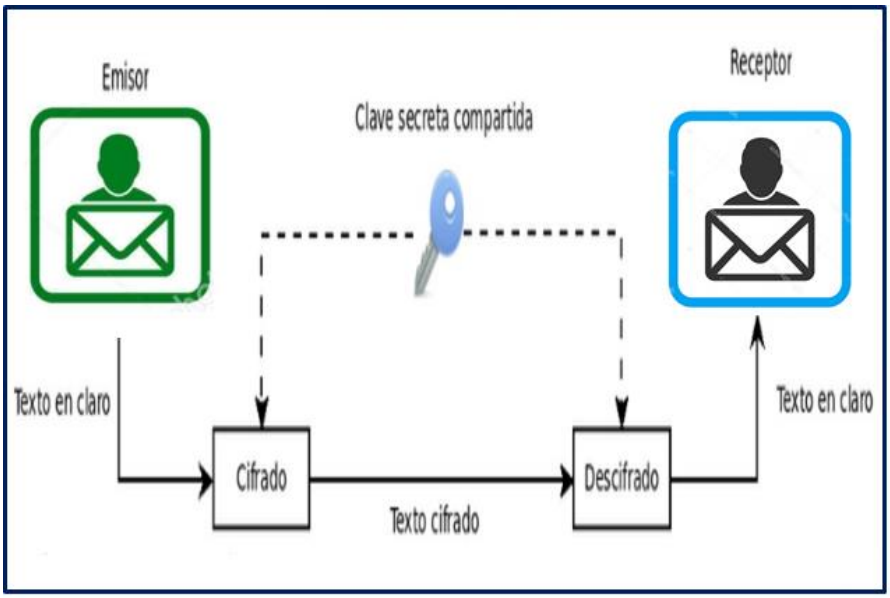


Fuente:https://proyectohomo.blogspot.com/2017/03/que-es-un-algoritmo.html

“La criptografía Simétrica se refiere a un método criptográfico, que usa la misma llave tanto para cifrar y para descifrar. Esto conlleva a un grave problema al momento de hacer el intercambio entre emisor y receptor, debido que si es escuchado por una tercera persona esta podría obtener la llave que es usada para el cifrado. Es muy importante que la llave sea difícil y que no se pueda adivinar y que el método de cifrado a emplearse sea también el adecuado. En la actualidad, con la potencia computacional disponible y el empleo de

algoritmos adecuados, dependiendo del método de cifrado que se ha empleado se puede obtener una llave fácilmente.” (10)

Figura 10. Algoritmo simétrico



Fuente:https://es.slideshare.net/leidyjohanagarciaortiz/presentacin-criptografa-17521554

Entre los algoritmos Simétricos más conocidos tenemos: DES, 3DES, AES, etc.

“DES: El algoritmo conocido como DES (Data Encryption Standard) es un algoritmo para el cifrado que fue desarrollado por la NSA, y ha sido escogido como FIPS (Federal Information Processing Standard) el año 1976, su uso se ha extendido por todo el mundo. El DES es un algoritmo que realiza un cifrado por bloques. Un bloque de longitud fija de bits lo transforma mediante diferentes de operaciones básicas en otro bloque cifrado pero de la misma longitud. El tamaño del bloque es de 64 bits. La llave también tiene 64 bits además 8 de estos bits son usados para la comprobación de la paridad, haciendo así que la longitud efectiva de la llave sea 56 bits. Está compuesto de 16 fases o rondas. Al inicio y al final se realiza una permutación. Estas permutaciones no son muy significativas criptográficamente, pero han sido incluidas para facilitar la carga y descarga de los bloque al hardware. Antes de realizar cada ronda

cada bloque se divide en mitades de 32 bits y se procesan alternativamente.” (11)

“AES: El algoritmo AES (Advanced Encryption Standard) también se le conoce como Rijndael que ha sido el ganador del concurso convocado en el año 1997 por el NIST (Instituto Nacional de Normas y Tecnología) con la finalidad de seleccionar un nuevo algoritmo de cifrado. Asimismo el 2001 fue tomado como FIPS y el 2002 se convirtió en un estándar efectivo. Desde el 2006 se ha convertido en el algoritmo más popular empleado para criptografía simétrica. Este algoritmo opera con una matriz de 4x4 bytes. Con el uso de un algoritmo se reordenan los bytes de la matriz. El cifrado es de llave simétrica, la misma llave aplicada para el cifrado es aplicada en el descifrado. Está basado en el algoritmo Rijndael, que consiste en una red de sustitución y permutación, mas no una red de Feistel. AES es tiene rapidez tanto en software como en hardware, es fácil de implementar y no requiere mucha memoria. El algoritmo AES funciona bajo una serie de bucles repetitivos. Consta de 10 ciclos para llaves de 128 bits, 12 para 192 y 14 para 256.

Expansión de la clave usando el esquema de claves de Rijndael.

En la etapa inicial:

1. AddRoundKey

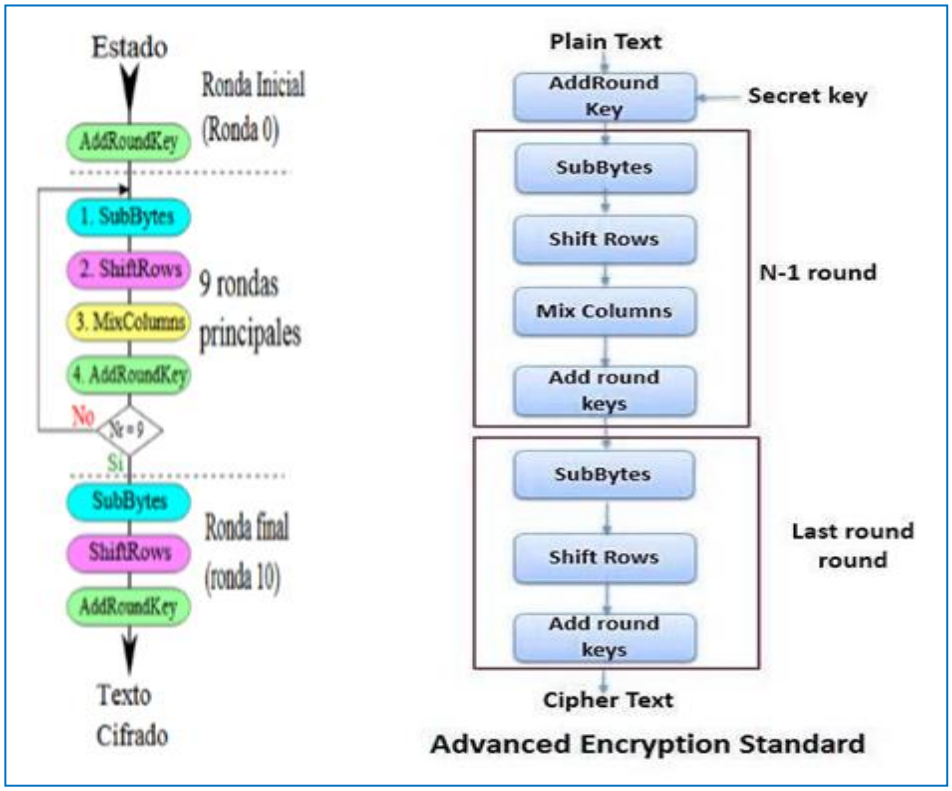
En las Rondas:

1. SubBytes; en este paso se hace una sustitución no lineal en el que cada byte es reemplazado por otro de acuerdo a una tabla de búsqueda.
2. ShiftRows; en este paso se hace una transposición en el que a cada fila del «state» se hace una rotación de manera cíclica un número de veces determinado.
3. MixColumns; en esta operación de mezclado que opera en las columnas del «state», se hace combinando cuatro bytes en cada columna en el que se usa una transformación lineal.
4. AddRoundKey; cada byte del «state» es combinado con la llave «round»; cada llave «round» se deriva de la llave de cifrado usando una iteración de la llave.

En la etapa final:

1. SubBytes
2. ShiftRows
3. AddRoundKey" (11)

Figura 11. Esquema algoritmo AES



Fuente: https://pc-solucion.es/2018/04/19/aes/

Algoritmo Advanced Encryption Standard (AES)

"Este algoritmo es uno de los más conocido entre muchos de los usuarios de routers, debido a que WPA opera con AES como principal método de cifrado; este método de cifrado se puede implementar tanto para sistemas hardware como para software. Este sistema criptográfico AES opera en bloques y llaves de longitudes variables, existe AES de 128bits, de 192 bits y de 256 bits. El resultado parcial del cifrado consiste en una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le aplica una serie de bucles de cifrado que están basados en operaciones matemáticas (sustitución no lineal de bytes, desplazamiento de filas,

combinaciones de las columnas mediante multiplicaciones lógicas y sumas en XOR en base a llaves intermedias). ” (12)

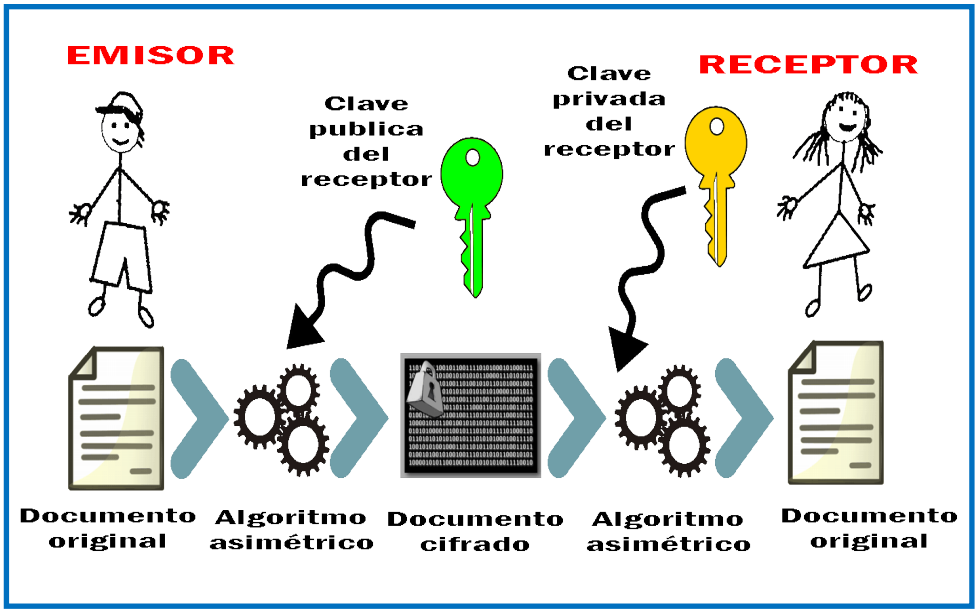
“Aplicaciones AES: El AES abarca campos como: • Protección de las comunicaciones digitales: Internet, TV digital, comunicaciones móviles, redes de datos y de voz. •Transferencia de documentos EDI (Electronic Data Interchange) y Comercio electrónico EC (Electronic Commerce). • Garantizar la seguridad y protección del software. • La mensajería militar en la red de mando y control (S/MIME). • Aplicación del DNI digital, con firma digital, y firma digital de documentos.” (13)

Criptografía Simétrica: Los algoritmos usados en criptografía simétrica se refieren a que van a usar la misma llave tanto en el cifrado y el descifrado; Son algoritmos fáciles de usar y a la vez son muy eficientes debido a su rapidez porque para el proceso de cifrado y descifrado utilizan un tiempo mínimo necesario, generalmente son usados como algoritmos de cifrado en tiempo real, entre ellos el más usado en la actualidad en aplicaciones web, correo electrónico, telegram, Instagram, watsapp es el **Advanced Encryption Standard (AES)** por su versatilidad y funcionalidad.

2.2.1.2. Algoritmos Asimétricos

Criptografía Asimétrica: Se le conoce también como criptografía de llave pública, debido a que usa llaves diferentes en cada punto de la comunicación, es decir que un usuario tiene que tener una llave llamada pública y otra llave llamada privada en donde la llave privada tendrá que estar en un lugar seguro sin acceso a personas no autorizadas, bien guardada por el usuario, se mantendrá realmente en secreto sin que nadie pueda conocer de su existencia como tal; sin embargo la llave pública tendrá que ser accesible y estar disponible para todos los usuarios dela red de comunicación para poder ser usada cuando se requiera.

Figura 12. Algoritmo Asimétrico



Fuente:http://instintologico.com/introduccion-a-la-criptografia-simetrica-asimetrica/

Entre los algoritmos Asimétricos tenemos: RSA, Diffie-Hellman, DSA, Funciones Hash, etc.

"Algoritmo Asimétrico (RSA) Algoritmo que se le conoce como "Criptografía de llave Pública" que consiste en la alteración de los datos de un documento con la finalidad de alcanzar características de seguridad como la de autenticación, integridad y de confidencialidad. Este algoritmo no se basa en una sola llave sino que usa un par de llaves: una pública y otra privada. Estas dos llaves pertenecen a la misma persona o usuario que ha enviado un mensaje. Una llave es pública y se puede entregar a cualquier usuario, sin embargo la llave privada el propietario debe guardarla para que nadie tenga acceso a ella. Si el remitente usa una llave pública del destinatario para el cifrado del mensaje, una vez que es cifrado, solo la llave privada del destinatario podrá descifrar el mensaje, debido a que es el único que conoce la llave. Por esta razón se logra la confidencialidad del envío de los mensajes, nadie excepto el destinatario puede descifrarlo." (14)

"El sistema RSA, ha sido desarrollado en el MIT (Instituto Tecnológico de Massachusetts), por Ronald Rivest, Leonard Adleman y Adi Shamir, y su nombre se debe a las iniciales de los apellidos de cada uno de sus creadores. El sistema, permite el cifrado y el firmado digital. Los datos que son cifrados y enviados utilizando este algoritmo, son representados mediante números. El funcionamiento toma el producto de 2 números primos seleccionados al de forma aleatoria, al azar y son mantenidos de manera secreta, los que deben ser mayores que 10100. Con el resultado obtenido, es que se genera la llave de cifrado y descifrado. La seguridad del RSA se encuentra en el problema matemático para factorizar números demasiado grandes, pues no existen maneras rápidas de poder obtener resultados favorables, haciendo uso de una computadora tradicional. Actualmente de los algoritmos que usan clave pública, RSA es el más empleado, además se prevé que el tamaño de los números primos seleccionados para la generación de las llaves, aumente debido al incremento" (15)

"Diffie-Hellman: Este algoritmo ha sido de los primeros de llave pública que desarrollaron Whitfield Diffie y Martin Hellman en el año 1976, de ahí el nombre. También es conocido como algoritmo de Intercambio Exponencial Diffie-Hellman, el que basa su seguridad por la dificultad para calcular logaritmos discretos en campos finitos y es usado para la distribución de llaves, más no para el cifrado y descifrado; **DSA (Digital Signature Algorithm):** Este algoritmo tiene como finalidad firmar documentos electrónicos, de ninguna manera cifra información. Fue desarrollado por el NIST agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos y **Funciones Hash:** En el campo de la criptografía las funciones Hash tienen una importancia mayúscula, ya que se enfocan principalmente a solventar los problemas relacionados a la integridad de los mensajes, como también a la autenticidad de los mensajes y de su origen. Las funciones Hash viene a ser las funciones que matemáticamente realizan el resumen

de un documento a firmar, de manera que para ellos comprimen el documento en un solo bloque de una longitud fija, bloque del que su contenido resulta ilegible y no tiene ningún sentido real.” (16)

En general todos los algoritmos asimétricos basan su seguridad en funciones matemáticas que no son muy complicadas para ser resueltas en un sentido, pero son muy difíciles a momento de ser resueltas en sentido inverso, claro está que si se conoce la llave no habrá estas complicaciones. Asimismo, siempre se requiere de dos llaves una llave pública y una llave privada que deben ser generadas de manera simultánea y en estricta relación una de la otra, pero con una complejidad suficiente como para evitar que se pueda realizar algún cálculo o función matemática para obtener una llave privada a partir de la obtención de la llave pública.

“Inconvenientes del uso de algoritmos asimétricos

- **Son poco eficientes:** debido a que toman mucho tiempo en aplicar las llaves para poder generar los documentos cifrados, sobre todo debido a que las llaves deben ser largas para asegurar una independencia matemática entre ellas.
- **Utilizar las llaves privadas repetidamente**: se pone en riesgo debido a que algunos ataques criptográficos están basados en el análisis de paquetes cifrados. Estos paquetes serían capturados en la red o directamente el atacante podría elaborar un software malicioso que generase paquetes de tamaño y contenido elegidos cuidadosamente y conseguir enviarlos a nuestro servidor para que los devolviera cifrados con su clave privada.
- **Hay que proteger la llave privada.** No es suficiente con dejarla en un archivo de una carpeta del disco duro en la cuenta de algún usuario o cliente; cualquier otro usuario con permisos de administrador podría llegar hasta él. Por este motivo, las llaves privadas se deben guardar juntas en un fichero llamado keyring (archivo de llaves, llavero), y este fichero debe estar protegido mediante cifrado simétrico. Es decir, que para poder hacer uso

de la llave privada, hay que introducir una llave que pueda descifrar el llavero y permita leerla.

- **Hay que transportar la llave privada**. En cifrado simétrico, si se ha enviado el fichero cifrado a otro ordenador o máquina y necesitamos descifrarlo, suficiente con recordar la llave e introducirla. Pero en la llave privada esto no es posible (porque son cientos de símbolos que no tienen sentido). Se debe transportar el llavero, asumiendo el con el riesgo que supone (si lo perdemos, alguien podría intentar hacer un ataque por fuerza bruta en contra del cifrado simétrico).” (17)

Entonces se puede decir que con el cifrado asimétrico no se debe cifrar todos los paquetes intercambiados en una red local debido a que produce un bajo rendimiento del algoritmo que haría lenta la trasmisión de los datos. En vez de este se sugiere utilizar ambos, es decir un sistema mixto:

- Criptografía asimétrica se usaría únicamente en inicio de sesión y al momento que se genere un canal seguro se debe acordar la llave simétrica que se usará en esa comunicación.
- Criptografía simétrica se usará en la transmisión, usando la llave simétrica que fue acordada cuando se generó el canal seguro al inicio de la sesión. Por políticas de seguridad es necesario cambiar la llave simétrica en un tiempo determinado (minutos) y de esa manera hacer difícil el criptoanálisis en caso de intrusos en la comunicación.

Se puede decir que, si A necesita tener una conversación con B, en A se va a generar en ese momento una llave simétrica. Para enviarla a B de modo seguro, A la cifrara usando un algoritmo asimétrico con la llave pública de B. y Cuando B reciba la llave simétrica cifrada, la descifrara con su llave privada y desde ese instante pueden continuar el diálogo cifrando con el algoritmo simétrico establecido y la llave simétrica recibida.

2.2.2. Protección de la Información

"La información viene a ser un activo tan importante como otros activos del negocio, tiene mucho valor para la organización y en consecuencia requiere una adecuada protección. Esto es de gran importancia en el creciente ambiente interconectado de los negocios. Como resultado de la creciente interconectividad, la información siempre va está expuesta a riesgos, amenazas haciéndolo vulnerable. La información puede adoptar diversas formas; puede estar en digital, impresa o escrita en papel, almacenada en medios electrónicos, transmitida por mensajería o por medios electrónicos, mostrada en videos o audios en conversación. Debe ser protegida adecuadamente cualquiera de las formas que tome o los medios por los que se tenga que compartir o almacenar." (18)

Figura 13. Seguridad de la información

Fuente: https://www.agro.uba.ar/uti/servicios/seguridad_informacion

"Seguridad de la información; Para asegurar la continuidad del negocio, con la seguridad de la información se protege a ésta de un amplio rango de amenazas, se minimizaran los daños a la organización y maximizaran el retorno de las inversiones y las oportunidades de negocios.

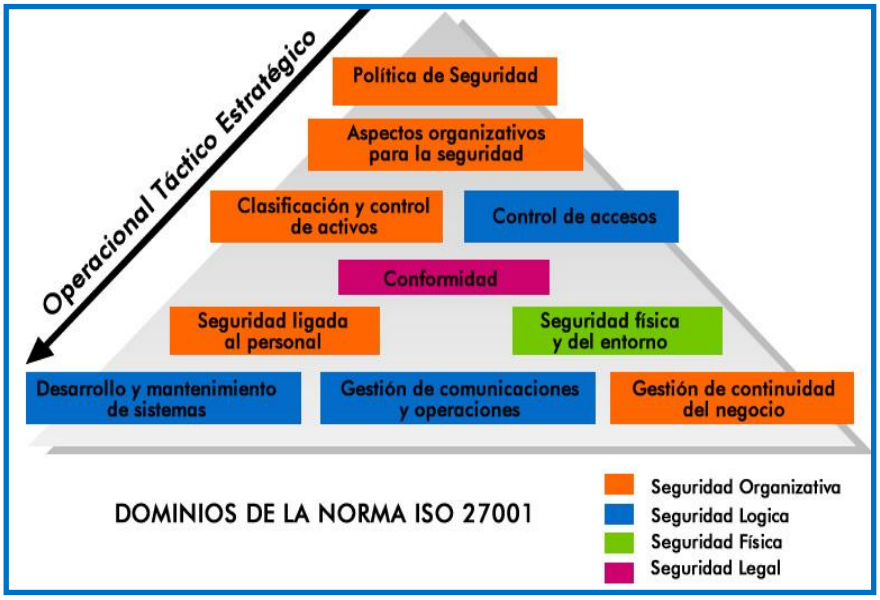
ISO 27001 ¿En qué se basa la política de seguridad de la información? En explicar la política de seguridad de la información de acuerdo a la norma ISO 27001 y da a conocer lo que debe incluir. Sin embargo, es importante recordar la definición de seguridad de la información, que no es más que un conjunto procedimientos y medidas que son puestos en marcha por las empresas para

poder proteger la confidencialidad, la disponibilidad e integridad de los datos.” (19)

Figura 14. ISO 27001

Fuente: https://ada.co/noticia/adaobtiene-certificaci-n-iso-27001

Figura 15. Dominios de la Norma ISO 27001



Fuente: Consultores en Tecnología Colombia S.A.S. (CETECO)

“La seguridad de la información viene a ser el conjunto de métodos y herramientas establecidos para proteger la información y los sistemas informáticos ante cualquier amenaza, es un proceso en el que es necesario la participación de las personas.” (20).

Figura 16. Seguridad Informática y Seguridad de la información

Fuente:https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/

"La seguridad de la información se consigue implantando un conjunto de controles, políticas, prácticas, procedimientos, estructuras organizativas, funciones de software y hardware. Los controles necesitaran ser establecidos, implementados, monitoreados, revisados y mejorados donde y cuando sea necesario, de esa manera poder asegurar que se cumplan los objetivos específicos relacionados a seguridad y negocios de la organización." (21)

"La seguridad de la información debe ser flexible, eficaz y dar soporte al modelo de negocio de la compañía:

- El acceso a la información debe ser controlado y estar basado en el rol de la personal en la empresa.
- Los servicios proporcionados deben ser seguros desde cualquier punto de acceso cuando se conecte a la infraestructura de la compañía.
- Las medidas de seguridad deben garantizar todos los requisitos relacionados a la confidencialidad, la integridad y la disponibilidad de información y servicios.
- Las medidas de seguridad deberán garantizar la privacidad y protección de los datos personales de acuerdo a la legislación que se encuentre vigente.

- La seguridad de la información debe estar alienada con la empresa, los requisitos de seguridad de nuestros clientes y las buenas prácticas de la industria". (22)

"Sistema de Gestión de Seguridad de Información. Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de políticas, implantación de procedimientos, establecimiento de directrices, asignación de recursos asociados y actividades, gestionadas colectivamente por o para una organización, en el afán por encontrar la protección de sus activos de información. Un SGSI es un enfoque del punto de vista sistemático para poder establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad y la protección de la información de una empresa u organización para poder alcanzar los objetivos del negocio. Está basada en la evaluación del riesgo y de los niveles de aceptación del riesgo de la organización, es diseñada para poder tratar y gestionar los riesgos de forma efectiva. Debe analizar los requisitos para la protección de los activos de información y aplicar los controles adecuados para poder garantizar su protección, según sea necesario, esto contribuye a la implementación con éxito de un SGSI". (23)

"Seguridad de información. En la seguridad de información se incluyen tres dimensiones principales: la confidencialidad, disponibilidad e integridad. Esto consiste en la adecuada aplicación y gestión de medidas de seguridad apropiadas, lo va a implicar la consideración de la existencia de una gran cantidad de amenazas, con la finalidad de garantizar el éxito y asegurar la continuidad del negocio, de forma sostenida, y alcanzar la minimización de los impactos de incidentes de seguridad de la información. Esto se puede lograr mediante la implementación de un conjunto aplicable de adecuados controles, que son seleccionados a través del proceso de gestión de los riesgos y son administrados utilizando un SGSI; esto incluye las políticas, procesos, procedimientos, estructuras organizacionales, software y hardware destinados para proteger los activos de información identificados. Los controles deben ser especificados, implementados, monitoreados, revisados y mejorados cuando sea necesario, para poder asegurar que se cumplan los objetivos específicos de seguridad de información y del negocio sean logrados. Es esperado que los

controles de seguridad de la información relevantes se puedan integrar a la perfección con todos los procesos de negocio de la organización". (24)

"Política de seguridad de la información: Consiste en dirigir y dar soporte a la gestión de la seguridad de la información. La gerencia deberá estar en la capacidad de establecer de forma clara y efectiva las líneas de la política de actuación y poder manifestar su apoyo y su compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad de la organización". (25)

2.3. Definición de Términos

- **Algoritmo.** Conjunto de instrucciones o reglas definidas, ordenadas y finitas para realizar una actividad mediante pasos sucesivos. Dados un estado inicial y una entrada, se llega a un estado final y se obtiene una solución.
- **Texto llano:** Texto seleccionado o mensaje que requiere ser protegido que será usado en la operación de cifrado en combinación con la llave.
- **Llave**. Consiste generalmente en una palabra, frase o párrafo más o menos extenso de un libro, que regula directamente la operación de cifrar un mensaje y que permite asimismo la operación de descifrar un criptograma
- **Cifrar.** Transcribir guarismos, letras, símbolos en relación a una llave, un mensaje que se quiere ocultar.
- **Llave Privada**. Un Sistema Asimétrico de cifrado esta llave es conocida solo por el emisor del mensaje para cifrar o descifrar el mensaje.
- **Llave Pública**. En un Sistema Asimétrico de Cifrado es la llave que todos conocen para Cifrar o descifrar el mensaje.
- **Criptogramas.** Mensaje obtenido producto de un método de cifrado utilizando un sistema de códigos o claves secretas.
- **Modo enigmático.** Oculto o escondido de manera que no se puede predecir su origen, no se tiene indicios de su significado
- **FIPS** (Federal Information Processing Standard) publicación 140-2, es el estándar para la seguridad de los ordenadores del gobierno de los Estados Unidos para obtener la acreditación de los módulos criptográficos.

- **NIST** (National Institute of Standards and Technology), agencia de Administración de Tecnología del Departamento de Comercio de los Estados Unidos. Emitió la serie de publicaciones FIPS 140 para poder coordinar los requerimientos y estandarización de los módulos criptográficos en los que se incluyen componentes de hardware y software.
- **Hacking:** "Hacking" o "Hacker" persona con profundos conocimientos sobre ordenadores que realizan funciones de cómputo y se dedican a realizar estafas a gran escala sobre bancos y/o grandes multinacionales.
- **Seguridad de la Información:** Permite la preservación de la confidencialidad, integridad y disponibilidad de la información y otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad.
- **ISO (International Organization for Standarization):** Organización no gubernamental que desarrollada estándares, se ocupa de los sistemas de información, ha desarrollado el modelo de referencia OSI y protocolos estándares para varios niveles de este modelo.
- **LAN:** Local Area Network, Red de área local. Red que conecta los ordenadores en un área relativamente pequeña y predeterminada.
- **MAN:** Metropolitan Area Network, Red de área metropolitana. Red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa.
- **WAN:** Wide Area Network. Red de área amplia. Red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km.

2.4. Hipótesis

2.4.1. Hipótesis General

La optimización del algoritmo Estándar de Encriptación Avanzada (AES) mejorará la protección dela información.

2.4.2. Hipótesis Específicas

a) La optimización del algoritmo Estándar de Encriptación Avanzada (AES) incrementará la **efectividad** de la protección de la información.

b) La optimización e implementación del algoritmo Estándar de Encriptación Avanzada (AES) aumentará el nivel de **seguridad** en la protección de la información.

2.5. Variables

2.5.1. Definición Conceptual de la variable

VARIABLE INDEPENDIENTE (X): Algoritmo de Encriptación

Los algoritmos de encriptación son programas, aplicaciones, dispositivos, etc. usados en sistemas informáticos que mediante su aplicación permiten que la información este protegida.

VARIABLE DEPENDIENTE (Y): La protección de la información

Son los métodos, procedimientos establecidos destinados a proteger la información de manera efectiva y con un buen nivel de seguridad ante cualquier riesgo o amenaza.

2.5.2. Definición operacional de las variables

Proceso a través del cual los algoritmos de encriptación mediante programas, aplicaciones, dispositivos, etc. sumados a los métodos, procedimientos, políticas de seguridad establecidas destinadas a proteger la información van a permitir que esta se encuentre protegida de manera efectiva y con un buen nivel de seguridad.

2.5.3. Operacionalización de la variable

Tabla 1. Operacionalización de las variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSION	ITEM/INDICADOR
Independiente: Algoritmo de encriptación	Los algoritmos de encriptación son programas, aplicaciones, dispositivos, etc. usados en sistemas informáticos que mediante su aplicación permiten que la información este protegida	Proceso a través del cual los algoritmos de encriptación mediante programas, aplicaciones, dispositivos, etc. sumados a los métodos, procedimientos, políticas de seguridad establecidas destinadas a proteger la información van a permitir que esta se encuentre protegida de manera efectiva y con un buen nivel de seguridad.		
VARIABLE	**DEFINICION CONCEPTUAL**	**DEFINICION OPERACIONAL**	**DIMENSION**	**ITEM/INDICADOR**
Dependiente: La protección de la información	La protección de la información son los métodos, procedimientos establecidos destinados a protegerla de manera efectiva y con un buen nivel de seguridad ante cualquier riesgo o amenaza.	Proceso a través del cual los algoritmos de encriptación mediante programas, aplicaciones, dispositivos, etc. sumados a los métodos, procedimientos, políticas de seguridad establecidas destinadas a proteger la información van a permitir que esta se encuentre protegida de manera efectiva y con un buen nivel de seguridad.	Efectividad	Cantidad de información protegida
				Políticas de seguridad establecidas
				Frecuencia de uso de encriptación
			Seguridad	Herramientas de encriptación a usar.
				Nivel de conocimiento de herramientas de encriptación.
				Porcentaje cumplimiento de Políticas de seguridad establecidas.

Fuente: Elaboración propia

CAPÍTULO III

METODOLOGÍA

Tiene un enfoque cuantitativo debido a que las conclusiones están basadas en porcentajes de comparación entre las variables que presenta el proyecto; el diseño pre-experimental permitió la manipulación de las variables en función a los datos recolectados, conociéndose así el nivel de seguridad de la encriptación que ofreció el algoritmo y la efectividad de la protección de la información.

3.1. Método de investigación

Esta investigación se desarrolló aplicando el método científico, en el que se pudo observar el comportamiento de las variables en función los información obtenida en la recolección de datos numéricos producto de la aplicación de los instrumentos a la muestra seleccionada; asimismo en base al análisis empleado bajo el enfoque cuantitativo se pudo establecer la relación existente entre las variables debido a que la información obtenida en porcentajes permitió determinar los niveles de seguridad del algoritmo de encriptación y la efectividad en la protección de la información.

3.2. Tipo de investigación

Aplicada, debido a que esta investigación se realizó en base a conocimientos teóricos relacionados a encriptación en el que después de hacer una análisis y evaluación al algoritmo de encriptación se pudo identificar sus fortalezas y debilidades de las cuales para poder hacer una optimización de dicho algoritmo se usó los conocimientos adquiridos sobre algoritmos de encriptación para disminuir las debilidades de dicho algoritmo lográndose esta optimización que podrá ser utilizada en el área de las TIC de cualquier organización o persona en general.

3.3. Nivel de investigación

Explicativo pues con esta investigación se busca explicar la relación existente y su comportamiento relacionado a la interacción de causa y efecto entre la variable independiente y variable dependiente, es decir que con la optimización del algoritmo de encriptación (VI) se logra mejorar la protección de la información (VD).

3.4. Diseño de investigación

Para el desarrollo de esta tesis se utilizó el diseño **Pre-experimental** debido a que se tuvo que evaluar el comportamiento de las variables haciendo una evaluación previa a nuestra investigación y luego otra evaluación después de la implementación para comparar los resultados y poder demostrar nuestra hipótesis.

Tabla 2. Diseño de la Investigación

Var. Independiente	Var. Dependiente	Resultado
Algoritmo de encriptación AES	**Para protección de la información**	- Con el análisis del algoritmo criptográfico AES y su optimización se logró un algoritmo más seguro. - Con la implementación de la optimización del algoritmo AES se incrementa la seguridad de la información - El aumento del nivel de seguridad se logró con la optimización del algoritmo - Con la implementación de la optimización del algoritmo AES se incrementa la efectividad en la protección de la información.

Fuente: Elaboración propia

3.5. Población y muestra

Para nuestra investigación la población corresponde a los todos los Empleados de la empresa DIACSA en un total de 43 empleados (censado) quienes tiene diferentes niveles de capacitación profesional entre ingenieros de sistemas, ingenieros electrónicos y personal administrativos que trabajan en todas las áreas de dicha empresa; no se tomó una muestra por ser una población reducida, por tanto se utilizó la técnica del censo.

3.6. Técnicas e instrumentos de recolección de datos

Para obtener información se aplicó un procedimiento sistemático usando Técnicas e Instrumentos de medición tipo encuesta aplicando cuestionarios de preguntas de acuerdo a los indicadores de las variables y los resultados se obtuvieron del procesamiento de esta información obtenida de la muestra lo que permitió demostrar lo planteado en la hipótesis de esta investigación.

3.7. Procesamiento de la información

Para el procesamiento de la información producto de la recolección de datos se hizo mediante herramientas informáticas de estadística que me permiten obtener resultados exactos presentados en histogramas donde se muestra la información en porcentajes de cada una de las preguntas planteadas de acuerdo a las variables de esta investigación.

3.8. Técnicas y análisis de datos

Los datos obtenidos pasaran por un proceso de Análisis comparativo usando las herramientas correspondientes. (Software:= SPSS) y con el fin de seleccionar la prueba de hipótesis en el presente trabajo de investigación, los datos se sometieron a una prueba de normalidad para validar su distribución por lo que fue necesario realizar la prueba rangos de Wilcoxon para cada uno de los indicadores.

CAPÍTULO IV

RESULTADOS

4.1 Especificaciones Básicas del algoritmo AES

Tabla 3. Especificaciones básicas AES

ESPECIFICACIONES BÁSICAS AES	
Aplicación:	Cifrador que opera con bytes en vez de bits, usa funciones invertibles y bloques enteros.
Modalidad:	Algoritmo que agrupa tantos bits dependiendo de la longitud del bloque, los bits contiguos se agrupan de ocho en ocho, y forman bytes, una tabla de cuatro filas y columnas
Seguridad de información de llaves:	Fuere resistencia ante ataques conocidos, un diseño sencillo, implementación compacta basada en parámetros de velocidad y adaptabilidad.
Mecanismo de protección:	Implementado empleando lógica combinacional suplementada con registros, memorias y multiplexores, en su modo de operación emplea rondas que tienen diferentes secuencias de operaciones.
Capacidad de generación de llaves:	En el proceso de cifrado, carga inicial de las llaves y en el proceso de generación de las subclaves.
Seguridad:	Resistente a análisis lineal y análisis diferencial.

Fuente: Elaboración propia

4.2 Análisis comparativo de AES con otros algoritmos

Tabla 4. Comparación de AES con otros algoritmos

Característica	AES	DES	T-DES
Tipo	Algoritmo simétrico	Algoritmo simétrico	Algoritmo simétrico
Algoritmo	Publico	Publico	Publico
Longitud de clave (bits)	128, 192 o 256 bits	40 y 56 bits	128 bits
Vector de inicialización	No considera	No considera	No considera
Tamaño de bloque	128 bits	64 bits	64 bits
Numero de Rondas	10, 12 o 14	48 rondas	16 rondas
Operaciones	XOR ⊕, Desplazamiento, Transposición	XOR ⊕, Desplazamiento,	XOR ⊕, Desplazamiento, Transposición

		Transposición	
Basado	Sustituciones, permutaciones y transformaciones lineales	Sustituciones, permutaciones y transformaciones lineales	Sustituciones, permutaciones y transformaciones lineales
Caja	S (Tabla)	Tablas de sustitución	Tablas de sustitución
Sistema	Irrompible 256 bits	64 bits vulnerables por fuerza bruta	64 bits vulnerables por fuerza bruta
Confusión	Matriz mixcolums	No considera	No considera
Efectividad	Radica en su llave	Radica en su llave 54 bits	Radica en su llave 54 bits
Seguridad	Tamaño de llave	Tamaño de llave débil que es salir en DES	Tamaño de llave aplica 3veces DES
Criptogramas	Alfanuméricos	Alfanuméricos	Alfanuméricos
Permite	Reutilización	Reutilización	Reutilización
Ataques por fuerza bruta	Imposible por la longitud y complejidad de la llave	Vulnerable al criptoanálisis diferencial y fuerza Bruta. Podría ser Analizada de texto llano con Criptoanálisis diferencial	Vulnerables a criptoanálisis diferencial y lineal. Tablas de sustitución Débiles
No permite	Invertir el algoritmo cifrado	----------	----------
Implementación	HW y SW	SW	SW

Fuente: Elaboración propia

4.3 Principales características del Algoritmo Criptográfico AES optimizadas

Basándonos en el objetivo de esta investigación y en relación a nuestras variables e indicadores propuestos para poder lograr la optimización de dicho algoritmo y a la vez demostrar lo planteado en nuestra hipótesis general se ha tenido que hacer una evaluación exhaustiva a dicho algoritmo pero por la existencia de gran cantidad de información respecto al algoritmo AES, se pudo hacer un análisis de las características

de este algoritmo, donde se pudo obtener los siguientes resultados mostrados en la siguiente tabla:

Tabla 5. Características AES

CARACTERISTICAS AES		
Item	**Características AES**	**Características optimización**
Tipo	Algoritmo simétrico	Algoritmo simétrico
Algoritmo	Publico	Propietario
Longitud de clave (bits)	128, 192 o 256 bits	256, 512 bits
Vector de inicialización	No considera	**Basado en CryptoGenRandom api Windows**
Tamaño de bloque	128 bits	128 bits
Numero de Rondas	10, 12 o 14	10, 12 o 14
Operaciones	XOR ⊕, Desplazamiento, Transposición	XOR ⊕, Desplazamiento, Transposición
Basado	Sustituciones, permutaciones y transformaciones lineales	Sustituciones, permutaciones y transformaciones lineales
Caja	S (Tabla)	**S (Tabla definida en programa)**
Sistema	Irrompible 256 bits	Irrompible 256, 512 bits
Confusión	Matriz mixcolums	**Variación de Matriz mixcolums**
Efectividad	Radica en su llave	Radica en su llave
Seguridad	Tamaño de llave	Tamaño de llave
Criptogramas	Alfanuméricos	Alfanuméricos
Permite	Reutilización	Reutilización
Ataques por fuerza bruta	Imposible por la longitud y complejidad de la llave	Imposible por la longitud y complejidad de la llave
No permite	Invertir el algoritmo cifrado	Invertir el algoritmo cifrado
Implementación	HW y SW	SW
Tiempo de ejecución cifrado	1539.7 Mb/s	Menor tiempo en procesadores modernos
Tiempo de ejecución descifrado	1519.9 Mb/s	Menor tiempo en procesadores modernos
Criptoanálisis con texto cifrado conocido	634 segundos	Menor tiempo en procesadores modernos o computación paralela

Fuente: Elaboración propia

Estas características técnicas del algoritmo nos sirvieron para poder obtener una mejor solución y lograr la optimización del algoritmo por lo que en nuestra investigación se ha considerado mantener el mayor porcentaje de las características técnicas para continuar con el estándar del algoritmo, más por el contrario nuestro trabajo consistió

en fortalecer parámetros de seguridad y **disponibilidad** de los componentes como la **Caja S**, el tamaño de llave que se adecue a nuestro algoritmo incluyendo la implementación del Algoritmo Hash Seguro 1 (SHA1) para la comprensión de datos si fuera necesario, cambios en la **matriz del procedimiento de generación del Mixcolums**, el número de rondas que se usen serán las que se encuentran en el algoritmo original del AES dependiendo del tamaño de llave y por último y de mayor importancia **un generador de llaves aleatorio** basado en api Windows CryptoGenRandom para la carga inicial de la llave y vector de inicialización; debido a que al ser AES conocido su forma de funcionamiento los hackers o criptoanalistas centraran sus esfuerzos en los que ya conocen y si nosotros implementamos un algoritmo basado en AES con ciertos cambios, será más difícil su rompimiento con ataques con cualquiera de las técnicas de criptoanálisis disponibles.

Tabla 6. Características a fortalecer en AES

Caja	S (S-BOXES)
Longitud de llave (bits)	128, 192 o 256 bits
Mixcolums	Variación del orden de la matriz
Numero de Rondas	10, 12 o 14
Generador de llaves	Aleatorio de un solo uso

Fuente: Elaboración propia

Caja S (S-BOXES) "En criptografía, una Caja-S (Caja de Sustitución) es el componente básico de los algoritmos de llave simétrica los cuales van a realizar sustitución. En los codificadores de bloques son comúnmente usados para obscurecer la relación entre la llave y el texto cifrado, esta es una propiedad de confusión de Claude Shannon" (26).

En este caso lo que se ha optimizado es que estos valores de la tabla son implementados de manera fija dentro del programa del algoritmo y de esta manera el algoritmo al momento de hacer el cifrado no tiene que hacer ningún proceso ni cálculo matemático si no que solo toma los valores de la tabla y los remplaza por el correspondiente valor, de esta manera esta función se hace más rápida mejorando el tiempo de cifrado o descifrado de manera más eficiente.

Caja S (S-BOXES) para el cifrado

Figura 17. Caja S para cifrado

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	3B	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	F7	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	2D
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1E	9E
E	E1	F8	98	11	69	D9	E8	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fuente: Javier Martínez de la Torre (2016), Cifrado de Clave privada: AES

Caja S (S-BOXES) invertida para el descifrado

Figura 18. Caja S invertida para descifrado

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	OC	7D

Fuente: Javier Martínez de la Torre (2016), Cifrado de Clave privada: AES

La tabla S-Boxes en el programa en lenguaje C++ se encuentra implementada de forma fija dentro del programa con la finalidad de que ya no se haga ningún cálculo matemático para obtener los datos de dicha tabla ya que se encuentran definidos en el programa de la siguiente manera:

```
Unsigned char S[256] ={
//0        1       2     3     4        5       6       7      8       9      A      B      C      D      E      F
0x63,  0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76,      //0 15
0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0,   //1 30
0xB7,  0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC, 0x34, 0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15,      //2 45
0x04,  0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75,      //3 60
0x09,  0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84,      //4 75
0x53,  0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A, 0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF,   //5 90
0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D, 0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8,     //6 105
0x51,  0xA3, 0x40, 0x8F,  0x92, 0x9D, 0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2,  //7 120
0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73,    //8 135
0x60,  0x81,  0x4F,  0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46, 0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB, //9 150
0xE0,  0x32, 0x3A, 0x0A, 0x49, 0x06, 0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79,    //A 165
0xE7,  0xC8, 0x37, 0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08, //B 180
0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A,//C 195
0x70,   0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6,  0x0E, 0x61, 0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E,    //D 210
0xE1,   0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF,    //E 225
0x8C,  0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16
};//f
```

Longitud de llave (bits) Se puede observar que el tamaño de la llave hace que el algoritmo este más fortalecido ante cualquier tipo de ataque de criptoanálisis, a mayor tamaño de llave mayor fortaleza y dependiendo del tamaño de la llave corresponderá al **número de rondas** establecido. Si se usa una llave de mayor cantidad de bits (256 ó más) se requiere la implementación del algoritmo de comprensión de datos Secure Hash Algorithm - 1 (SHA-1) es una función hash criptográfica ampliamente utilizado, que genera un 160 bits (20 bytes) hash a partir de cualquier valor de entrada.

Generador de llaves randómico, en este algoritmo se realiza una carga de llaves inicial, lo que se requiere que esta llave sea obtenga a partir de un dispositivo de aleatoriedad para evitar que la llave se repita por lo que tendrá que tener características para un solo uso, esto se logró usando un programa generador de llaves que una vez generada la llave haga una mescla con datos externos obtenidos del mismo programa en combinación con otros parámetros de entrada.

Para realizar esta función dentro del programa se usa un generar vectores de inicialización aleatorios y valores de sal que consiste en generadores de números aleatorios de software que funcionan siempre de la misma manera es decir que

comienzan con un número aleatorio, conocido como semilla y luego usan un algoritmo para generar una secuencia pseudoaleatoria de bits basada en esta semilla. Lo más importante y lo más complicado de este proceso es obtener una semilla que sea verdaderamente aleatoria y generalmente se basa en la latencia de entrada del usuario o la fluctuación de fase de uno o más componentes de hardware por lo que fue necesario implementar la solución que presenta Microsoft.

"Microsoft presenta una solución, **CryptGenRandom** que utiliza el generador de números aleatorios que son utilizados por otros componentes de seguridad. Esto permite que muchos procesos contribuyan a una semilla de todo un sistema. CryptoAPI puede almacenar una semilla aleatoria intermedia para cada usuario. Para formar esta semilla en el generador de números aleatorios, la aplicación de llamada suministra los bits que pueden tener por ejemplo, una entrada de tiempo de mouse o teclado, que luego esta se combinan con la semilla almacenada y otros datos del sistema y datos del usuario, como la identificación de proceso y el ID del hilo, el reloj del sistema, la hora del sistema, el contador del sistema, el estado de la memoria, los grupos de discos libres, el bloque de entorno de usuario hash, etc. El resultado se utiliza para inicializar el generador de números pseudoaleatorios (PRNG). En Windows Vista con Service Pack 1 (SP1) y posteriores, se usa la implementación del PRNG basado en modo contador AES especificado en la Publicación Especial 800-90 de NIST. En Windows Vista, Windows Storage Server 2003 y Windows XP, se usa el PRNG especificado en el Estándar de procesamiento de información federal (FIPS) 186-2. Si una aplicación accede a una buena fuente aleatoria, llenara el búfer pbBuffer con datos aleatorios antes de llamar a **CryptGenRandom.** El CSP usa estos datos para aleatorizar aún más su semilla interna. Es aceptable omitir el paso de inicializar el búfer pbBuffer antes de llamar a **CryptGenRandom"**. (27)

CryptGenRandom código programado en lenguaje C++

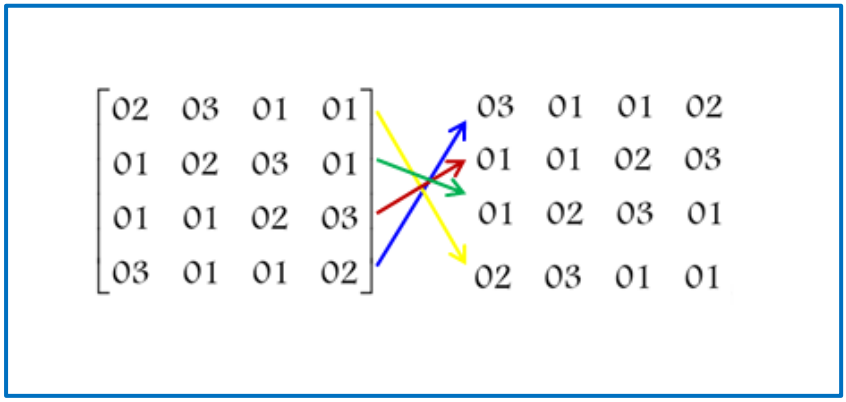
```
void GetRnd(void *RndBuf, size_t BufSize)
 {      byte *p = (byte*)RndBuf;
        HCRYPTPROV hProv;

        bool Succes = ::CryptAcquireContextW(&hProv, 0, 0, PROV_RSA_FULL,
        CRYPT_VERIFYCONTEXT | CRYPT_SILENT) && ::CryptGenRandom(hProv, BufSize, p);
        if (Succes)
                ::CryptReleaseContext(hProv, 0);
```

```
else
{       std::random_device rd;
        std::mt19937 eng(rd());
        std::uniform_int_distribution<unsigned short> distr(0, 255);
        for (size_t m = 0; m < BufSize; m++)
                p[m] = static_cast<byte>(distr(eng));
        }
}
```

El Mixcolums; este procedimiento está desarrollado en base a la matriz obtenida de los valores pre-establecidos de las tablas L-Table y E-Tables y una matriz de 4 x 4 para desplazamientos a la que se hizo una variación con respecto a orden de la matriz para mayor confusión cambiando la primera fila hacia la última y la segunda hacia la tercera tanto la matriz de cifrado y descifrado como se muestra en la figura:

Figura 19. Variación de Matriz Mixcolums



Fuente: Elaboración propia

El Mixcolums se programa de la siguiente manera utilizando lenguaje de programación C++:

```
inline void genera::MixColumns(uint32_d* p)
{ short i;
  uint32_d Temp;
  for (i = 0; i < Nb; i++)
  {
          // 03 01 01 02
          // 01 01 02 03
          // 01 02 03 01
          // 02 03 01 01
Temp = ((uint32_d)(((Multiply_03[(p[i] >> 24) & 0xFF]) ^ ((p[i] >> 16) & 0xFF) ^ ((p[i] >> 8) & 0xFF) ^ (Multiply_02[p[i] & 0xFF])) << 24)) + ((uint32_d)((((p[i] >> 24) & 0xFF) ^ ((p[i] >> 16) & 0xFF) ^ (Multiply_02[(p[i] >> 8) & 0xFF]) ^ (Multiply_03[p[i] & 0xFF])) << 16)) + ((uint32_d)((((p[i] >> 24) & 0xFF) ^
```

```
(Multiply_02[(p[i] >> 16) & 0xFF]) ^ (Multiply_03[(p[i] >> 8) & 0xFF]) ^ (p[i] & 0xFF)) << 8)) +((uint32_d)((Multiply_02[(p[i] >> 24) & 0xFF]) ^ (Multiply_03[(p[i] >> 16) & 0xFF]) ^ ((p[i] >> 8) & 0xFF) ^ (p[i] & 0xFF)));
            p[i] = Temp;
  }
}

inline void genera::InvMixColumns(unsigned long* p)
{
  short i;
  uint32_d Temp;
  for (i = 0; i < Nb; i++)
  {         // 09 0D 0B 0E
            // 0D 0B 0E 09
            // 0B 0E 09 0D
            // 0E 09 0D 0B
  Temp =          ((uint32_d)(((Multiply_09[(p[i] >> 24) & 0xFF]) ^ (Multiply_0D[(p[i] >> 16) & 0xFF]) ^ (Multiply_0B[(p[i] >> 8) & 0xFF]) ^ (Multiply_0E[p[i] & 0xFF])) << 24)) + ((uint32_d)(((Multiply_0D[(p[i] >> 24) & 0xFF]) ^ (Multiply_0B[(p[i] >> 16) & 0xFF]) ^ (Multiply_0E[(p[i] >> 8) & 0xFF]) ^ (Multiply_09[p[i] & 0xFF])) << 16)) +((uint32_d)(((Multiply_0B[(p[i] >> 24) & 0xFF]) ^ (Multiply_0E[(p[i] >> 16) & 0xFF]) ^ (Multiply_09[(p[i] >> 8) & 0xFF]) ^ (Multiply_0D[p[i] & 0xFF])) << 8)) +((uint32_d)(((Multiply_0E[(p[i] >> 24) & 0xFF]) ^ (Multiply_09[(p[i] >> 16) & 0xFF]) ^ (Multiply_0D[(p[i] >> 8) & 0xFF]) ^ (Multiply_0B[p[i] & 0xFF])) << 0));
  p[i] = Temp;
  }
}
```

4.4 Estructura de AES para encriptar

El algoritmo AES funciona con 10, 12 ó 14 rondas dependiendo del tamaño de la Llave y dentro de cada una de esas rondas hay una serie de etapas que son:

Byte sustitución layer: sirve para añadir confusión al proceso, realiza una transformación no lineal en cada uno de los elementos del estado.

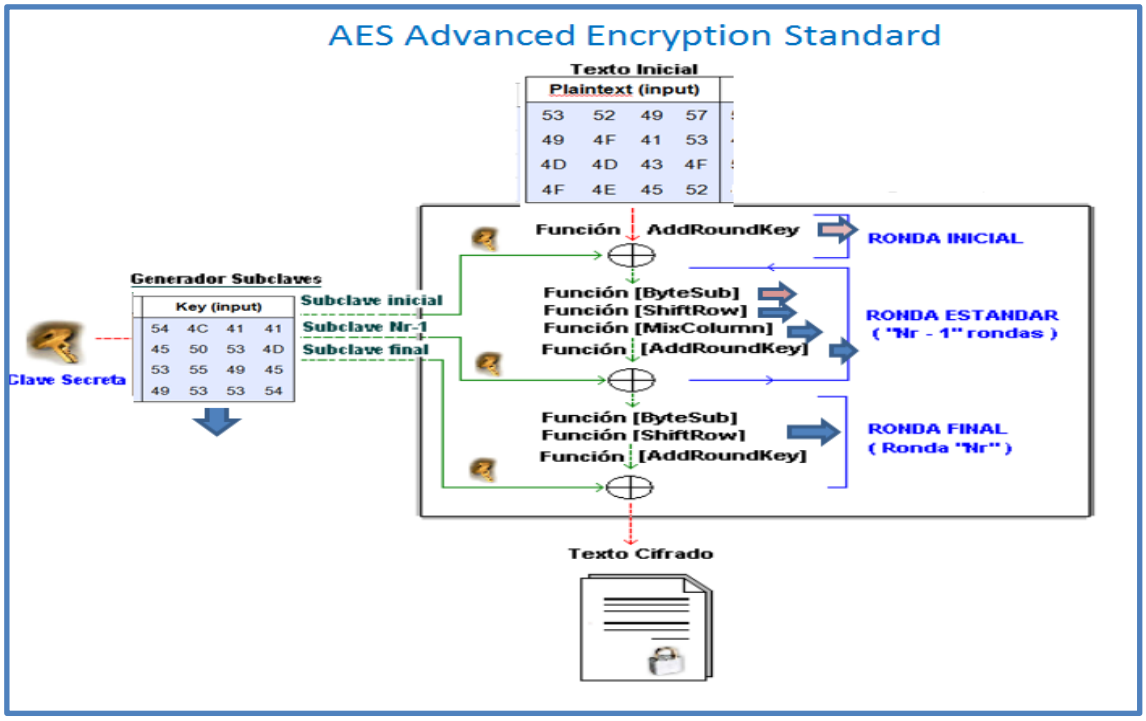
ShiftRows layer: permuta los elementos del estado.

MixColumn layer: realiza operaciones con una matriz constante y la de estado.

Key addition layer: hace un XOR de la subLlave y del estado actual.

Para la etapa de Key addition, donde se utilizan subllaves, es necesario generar dichas subllaves. Estas subllaves se generan a partir de la llave original y se crean en una etapa llamada key Schedule. Dependiendo de la llave original habrá más o menos rondas y por tanto será necesario generar más o menos subllaves. (28)

Figura 20. Esquema de encriptación con AES



Fuente: Javier Martínez de la Torre, Cifrado de llave privada: AES - 2015

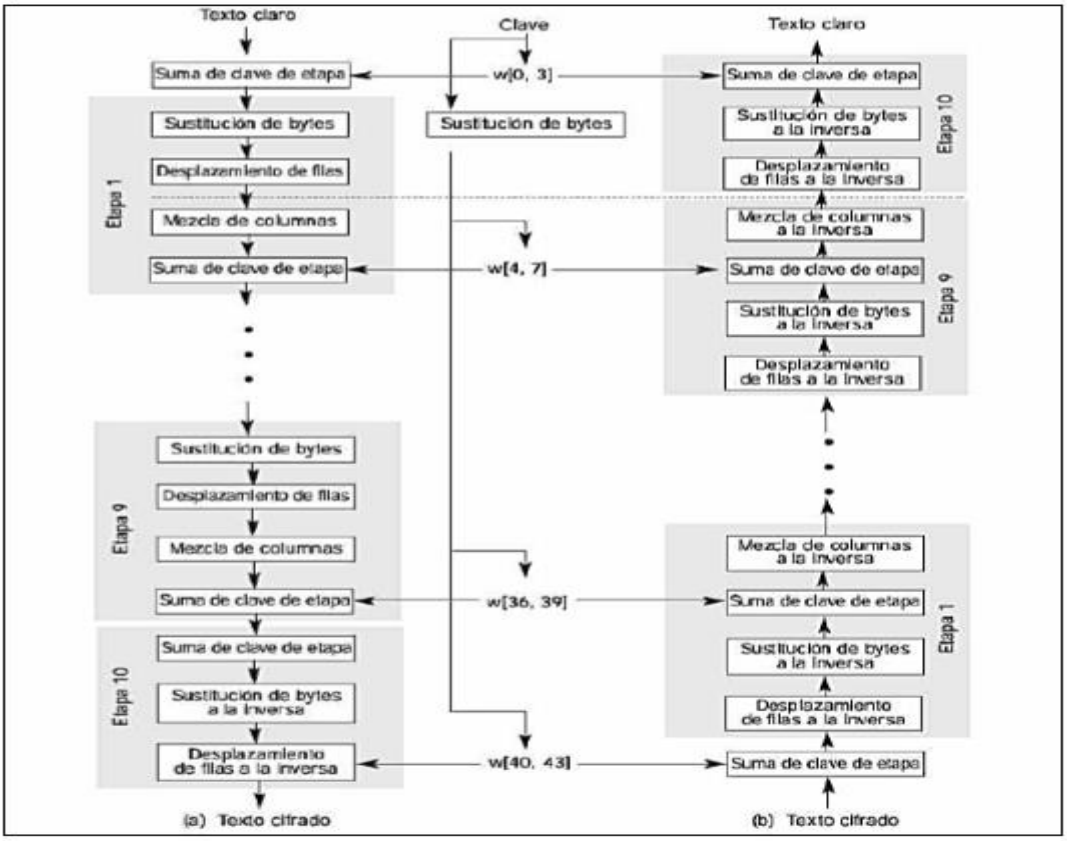
Modo de empleo del AES

a. Se utilizan cuatro fases diferentes para cifrar, una de permutación y tres de sustitución:

   - Sustitución de bytes: Se usa una tabla denominada caja S4, que realizar una sustitución byte a byte del bloque.
   - Desplazamiento de filas: Permutación realizada fila por fila.
   - Mezcla de columnas: Sustitución que altera cada byte de una columna en función de todos los bytes de la columna.
   - Suma de la llave de etapa: Operación XOR bit a bit del bloque actual con una porción de la llave expandida.

b. Proceso de generación de las subllaves.

Figura 21. Cifrado y Descifrado AES



Fuente: Denis Iván Capuñay (2016) Análisis comparativo de algoritmos Criptográficos

4.5 Evaluación de Seguridad de AES

Se ha podido determinar que la seguridad de AES se basa en el tamaño de la llave y la cantidad de rondas que realiza para el cifrado, por lo tanto mientras mayor es el tamaño de llaves mayor será el número de rondas que debe realizar el cifrador y eso implica mayor número de operaciones que realiza el algoritmo.

Una de las formas de realizar un ataque para encontrar las llaves del AES es una búsqueda llave por llave es decir un ataque por fuerza bruta, lo que se tendrá que realizar la búsqueda para cada tamaño de llave (128 bits, 192 bits y 256 bits) las veces que sea necesario y la cantidad de rondas correspondiente de acuerdo a cada tamaño de llave utilizada.

Este tipo de búsqueda si conectamos varias supercomputadoras con procesadores trabajando en paralelo aun en la actualidad puede tomar demasiado tiempo, esto es debido al gran número de operaciones que se deben realizar para encontrar la llave; por lo tanto por la dificultad que se tiene para obtener una llave mediante este tipo de búsqueda se puede medir que la fortaleza del AES se encuentra en el tamaño de su llave.

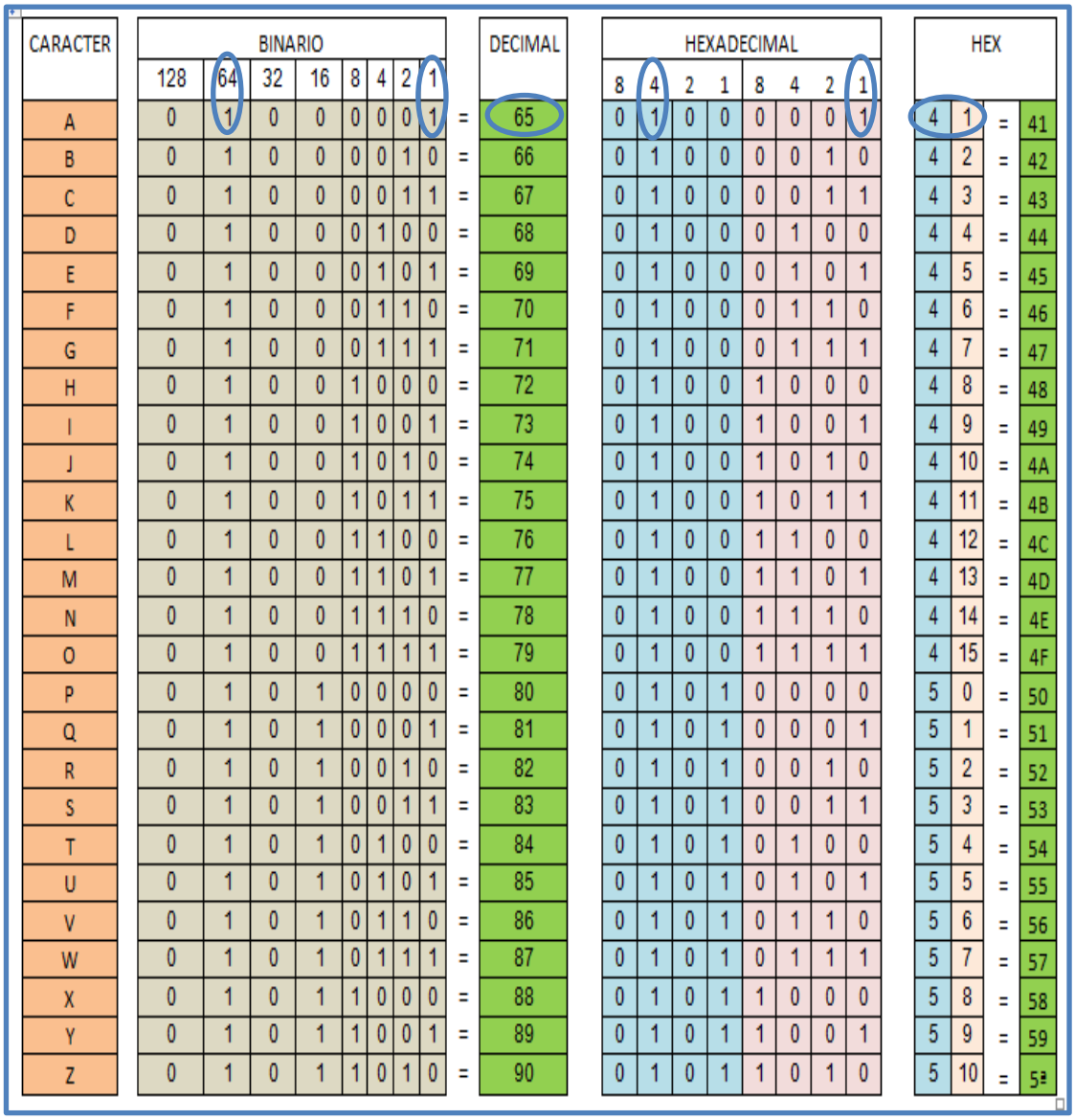
Existen algoritmos que consiguen reducir el número de rondas lo que hace que se haga una reducción en el tiempo. Sin embargo, continúa siendo computacionalmente imposible obtener la Llave (ataque por fuerza bruta). Por otro lado se sabe que la mayor parte de los ataques se centran en los dispositivos sobre los que se implementa AES y buscan obtener datos que pueda dejar el algoritmo temporalmente en las memorias y por tanto puedan ser utilizados para revelar algunos datos que ayuden a romper el algoritmo (ataque lateral). Además AES con el uso de la inversa sobre campos finitos en las s-cajas hace que los ataques lineales y diferenciales se vuelvan muy complicados.

Para realizar un ataque al algoritmo AES se debe definir una potencial víctima que puede ser una persona u organización que tenga implementado un sistema de seguridad de información en el que incluya método de encriptación AES, después de esto debe conocer el funcionamiento del algoritmo para identificar los puntos vulnerable del AES y sus fortalezas, luego recién se podrá definir el tipo de ataque se puede realizar y si existen posibilidades de tener resultados favorables.

4.6 Presentación de la simulación de AES

Se realiza la carga inicial del texto llano cualquiera que para el ejemplo es un texto que solo tiene letras del alfabeto pero que también podrían ser números o cualquier caracter del código ASCII; de la misma manera se realiza la carga inicial de la llave. Tanto el texto llano como la llave se tienen que convertir las letras o caracteres a código binario y luego a código hexadecimal como se muestra en la siguiente imagen.

Figura 22. Representación de carácter ASCII a Hexadecimal

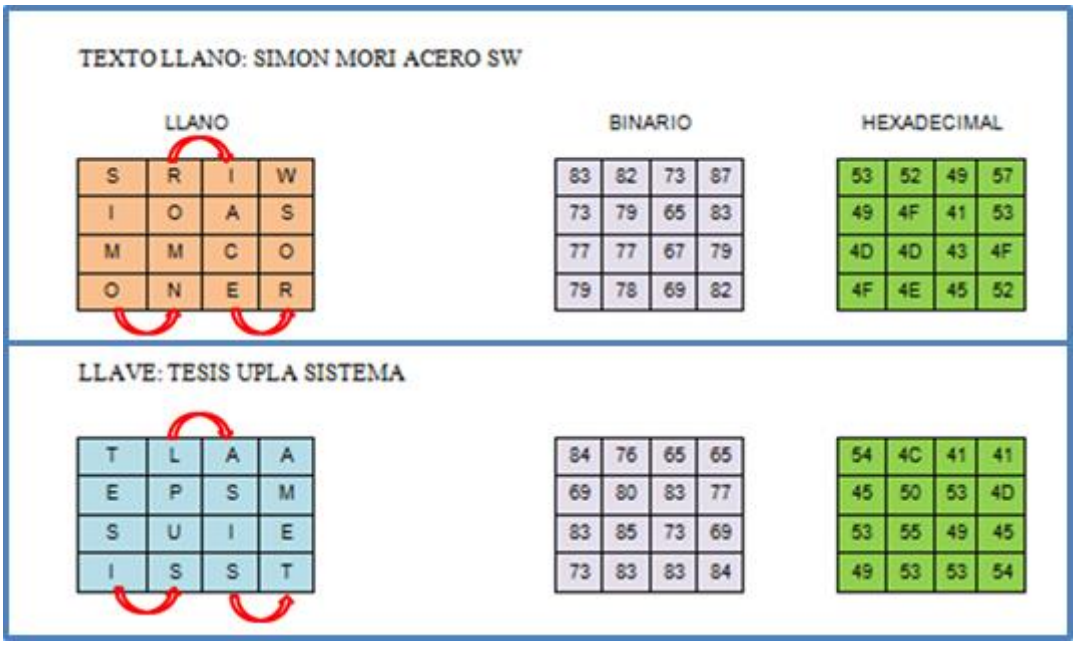


CARACTER	BINARIO									DECIMAL	HEXADECIMAL									HEX			
	128	64	32	16	8	4	2	1			8	4	2	1	8	4	2	1					
A	0	1	0	0	0	0	0	1	=	65	0	1	0	0	0	0	0	1		4	1	=	41
B	0	1	0	0	0	0	1	0	=	66	0	1	0	0	0	0	1	0		4	2	=	42
C	0	1	0	0	0	0	1	1	=	67	0	1	0	0	0	0	1	1		4	3	=	43
D	0	1	0	0	0	1	0	0	=	68	0	1	0	0	0	1	0	0		4	4	=	44
E	0	1	0	0	0	1	0	1	=	69	0	1	0	0	0	1	0	1		4	5	=	45
F	0	1	0	0	0	1	1	0	=	70	0	1	0	0	0	1	1	0		4	6	=	46
G	0	1	0	0	0	1	1	1	=	71	0	1	0	0	0	1	1	1		4	7	=	47
H	0	1	0	0	1	0	0	0	=	72	0	1	0	0	1	0	0	0		4	8	=	48
I	0	1	0	0	1	0	0	1	=	73	0	1	0	0	1	0	0	1		4	9	=	49
J	0	1	0	0	1	0	1	0	=	74	0	1	0	0	1	0	1	0		4	10	=	4A
K	0	1	0	0	1	0	1	1	=	75	0	1	0	0	1	0	1	1		4	11	=	4B
L	0	1	0	0	1	1	0	0	=	76	0	1	0	0	1	1	0	0		4	12	=	4C
M	0	1	0	0	1	1	0	1	=	77	0	1	0	0	1	1	0	1		4	13	=	4D
N	0	1	0	0	1	1	1	0	=	78	0	1	0	0	1	1	1	0		4	14	=	4E
O	0	1	0	0	1	1	1	1	=	79	0	1	0	0	1	1	1	1		4	15	=	4F
P	0	1	0	1	0	0	0	0	=	80	0	1	0	1	0	0	0	0		5	0	=	50
Q	0	1	0	1	0	0	0	1	=	81	0	1	0	1	0	0	0	1		5	1	=	51
R	0	1	0	1	0	0	1	0	=	82	0	1	0	1	0	0	1	0		5	2	=	52
S	0	1	0	1	0	0	1	1	=	83	0	1	0	1	0	0	1	1		5	3	=	53
T	0	1	0	1	0	1	0	0	=	84	0	1	0	1	0	1	0	0		5	4	=	54
U	0	1	0	1	0	1	0	1	=	85	0	1	0	1	0	1	0	1		5	5	=	55
V	0	1	0	1	0	1	1	0	=	86	0	1	0	1	0	1	1	0		5	6	=	56
W	0	1	0	1	0	1	1	1	=	87	0	1	0	1	0	1	1	1		5	7	=	57
X	0	1	0	1	1	0	0	0	=	88	0	1	0	1	1	0	0	0		5	8	=	58
Y	0	1	0	1	1	0	0	1	=	89	0	1	0	1	1	0	0	1		5	9	=	59
Z	0	1	0	1	1	0	1	0	=	90	0	1	0	1	1	0	1	0		5	10	=	5ª

Fuente: Elaboración propia

El texto llano y la llave se han cargado en una matriz de 4 x 4 al que se le ha colocado su respectiva representación binaria y hexadecimal de acuerdo a lo indicado en la ilustración que se presenta para mayor detalle:

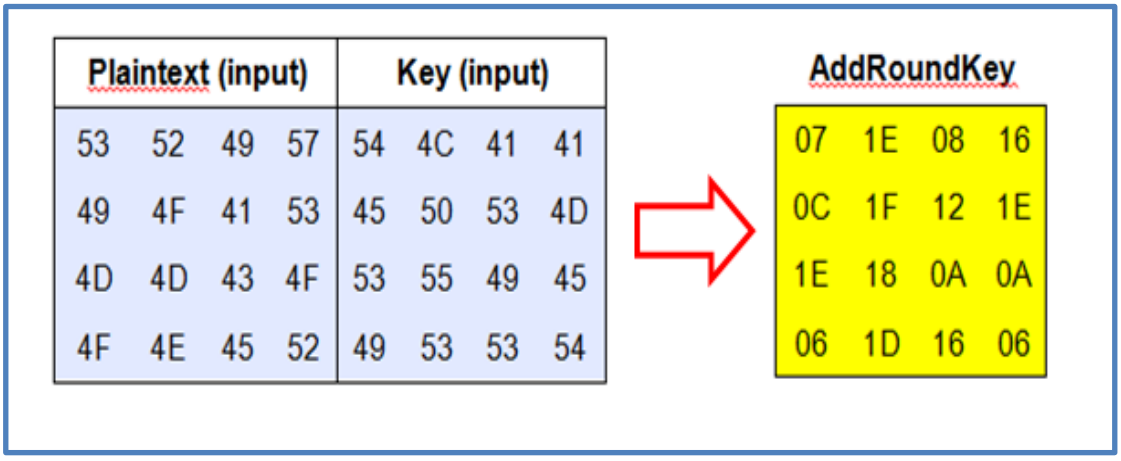
Figura 231. Representación llano y llave de Binario a Hexadecimal



Fuente: Elaboración propia

Luego de este proceso se realiza el AddRoundKey que corresponde a una operación XOR entre el texto llano y la llave siguiendo el esquema de la matriz de 16 números hexadecimales.

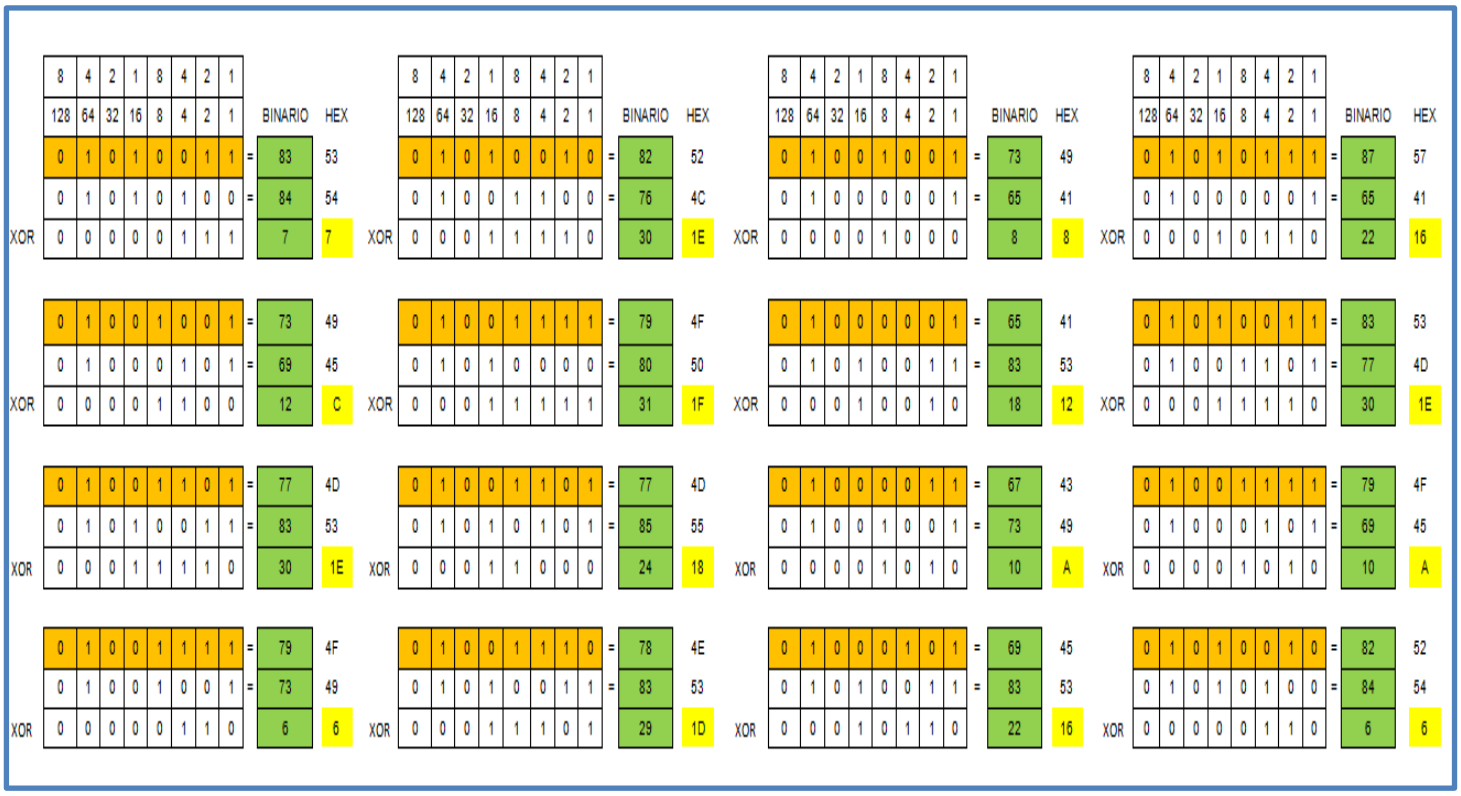
Figura 24. Resultado generación AddRoundKey



Fuente: Elaboración propia

En esta imagen se muestra el proceso de las operaciones XOR para la obtención del AddRoundKey, los resultados de cada operación están resaltados de color amarillo, los mismo que se utilizaron para comprobar la correcta operación de cada paso del algoritmo.

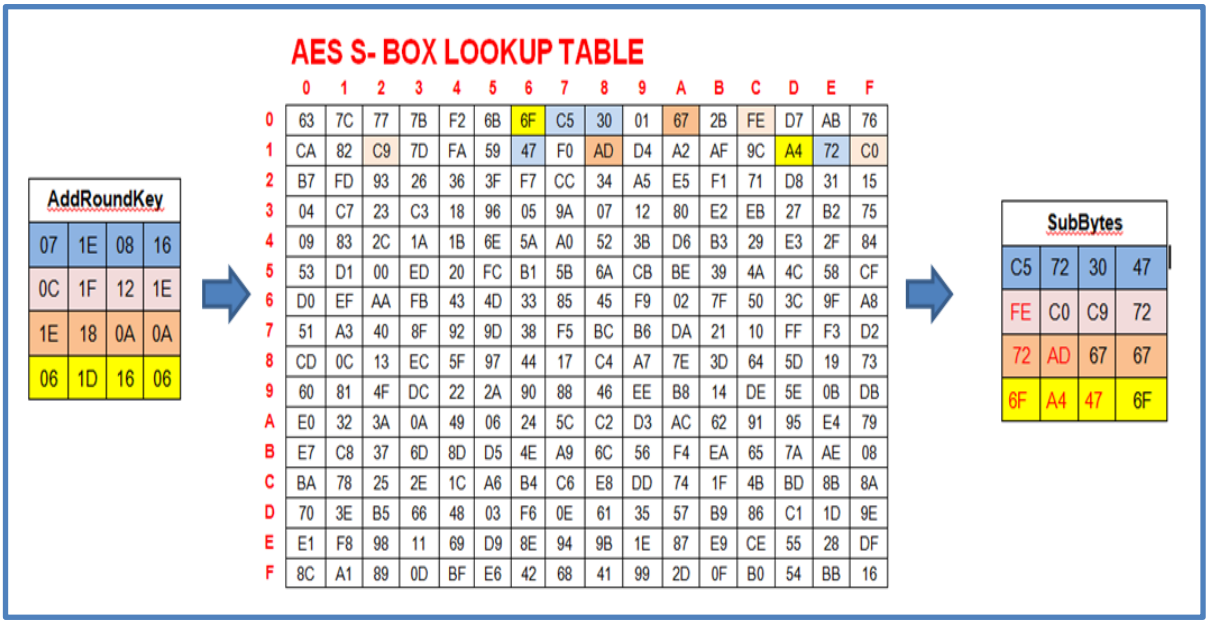
Figura 252. Operaciones XOR generación AddRoudKey



Fuente: Elaboración propia

Después de haber obtenido el AddRoundKey se procedió a realizar el siguiente procedimiento que corresponde a la generación de la matriz subbytes y se obtiene haciendo una sustitución de los números hexadecimales por otros que se encuentran pre-establecidos en la tabla de la caja S (S-Boxes) Ejemplo: el 07 de la matriz AddRoundKey está representado por C5 la tabla S y así sucesivamente con los demás caracteres de la matriz.

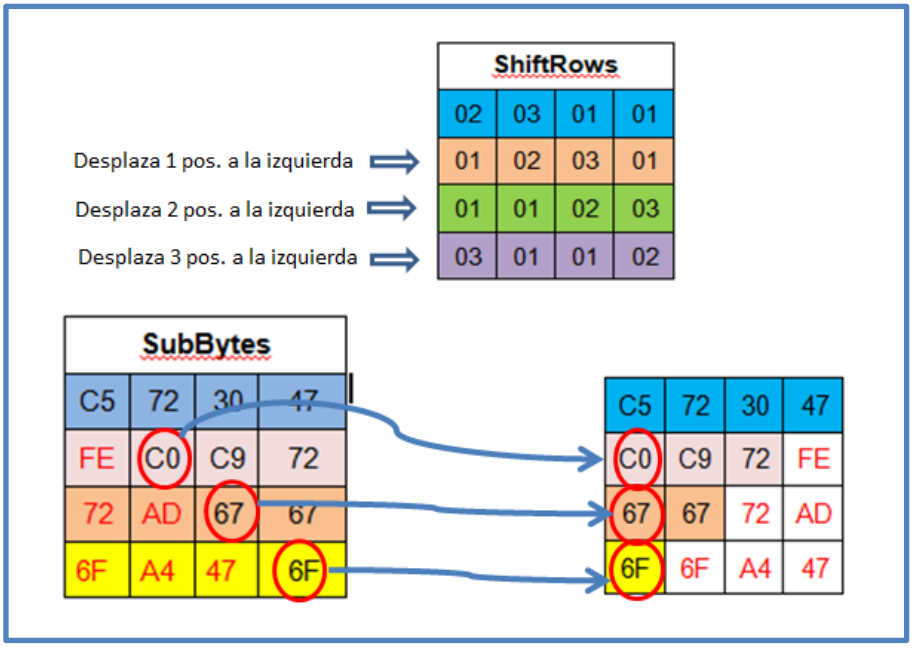
Figura 263. Generación matriz SubBytes



Fuente: Elaboración propia

Otro de los procedimientos es el llamado shiftrows que corresponde un desplazamiento de las posiciones de la matriz subBytes

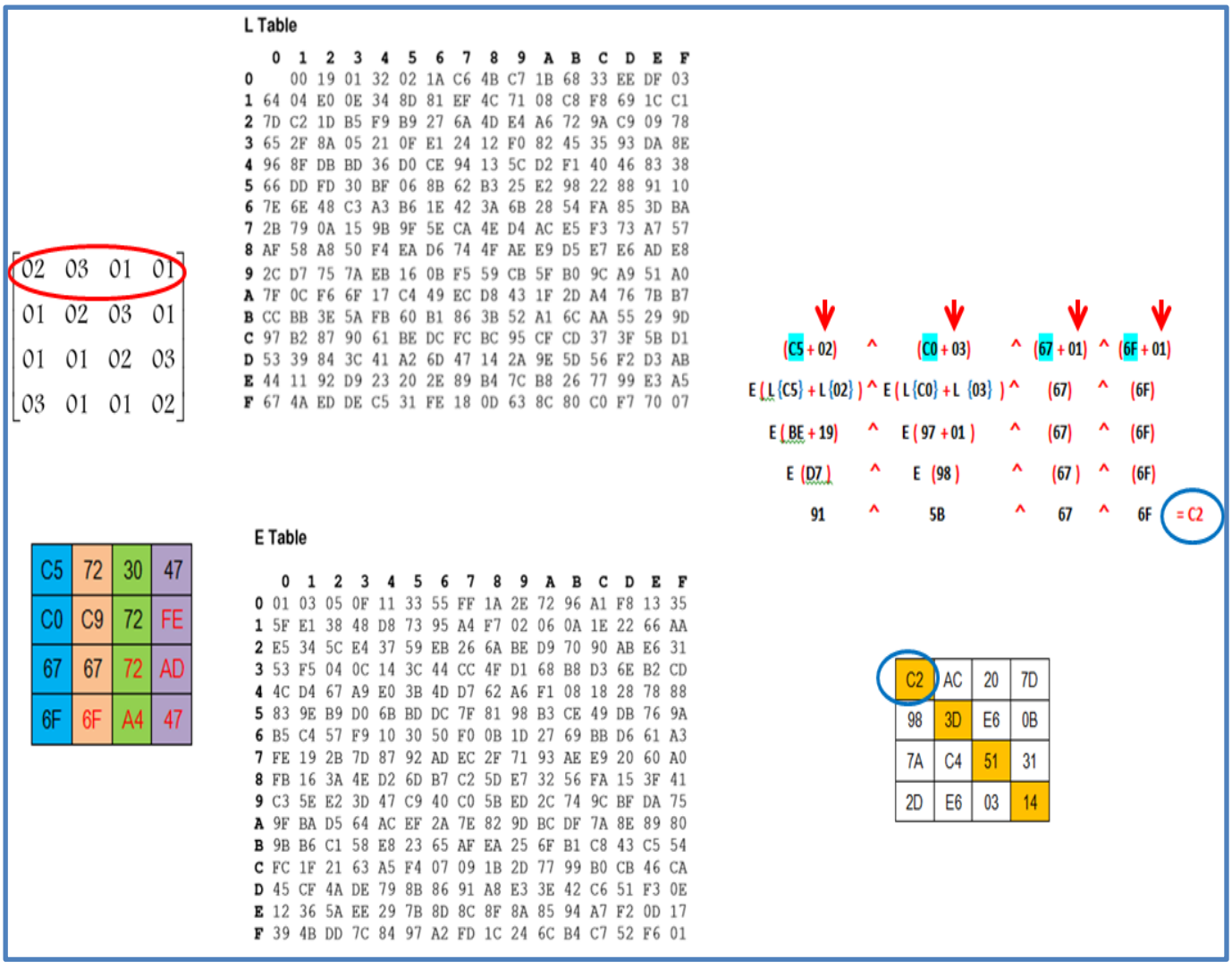
Figura 27. Matriz ShiftRows



Fuente: Elaboración propia

Luego tenemos el procedimiento Mixcolums que está desarrollado en base a la matriz obtenida del proceso shiftrows y consiste en operaciones de suma y XOR de los resultados del shiftrows con su representación de las tablas pre-establecidas L-Table y E-Tables además de una matriz de desplazamientos usada en el shiftrow según se muestra en la siguiente figura.

Figura 28. Generación matriz MixColums



Fuente: Elaboración propia

Procedimiento Mixcolums para obtener cada uno de los datos de la matriz 4 x 4 se muestran a continuación:

- Procedimiento para obtener la primera columna de la matriz MixColums

(C5 + 02) ^ (C0 + 03) ^ (67 + 01) ^ (6F + 01)

E (L {C5} + L {02}) ^ E (L {C0} + L {03}) ^ (67) ^ (6F)

E (BE + 19) ^ E (97 + 01) ^ (67) ^ (6F)

E (D7) ^ E (98) ^ (67) ^ (6F)

91 ^ 5B ^ 67 ^ 6F = C2

(C5 + 01) ^ (C0 + 02) ^ (67 + 03) ^ (6F + 01)

(C5) ^ E (L {C0} + L {02}) ^ E (L {67} + L {03}) ^ (6F)

(C5) ^ E (97 + 19) ^ E (42 + 01) ^ (6F)

(C5) ^ E (B0) ^ E (43) ^ (6F)

C5 ^ 9B ^ A9 ^ 6F = 98

(C5 + 01) ^ (C0 + 01) ^ (67 + 02) ^ (6F + 03)

(C5) ^ (C0) ^ E (L {67} + L {02}) ^ E (L {6F} + L {03})

(C5) ^ (C0) ^ E (42 + 19) ^ E (BA + 01)

(C5) ^ (C0) ^ E (5B) ^ E (BB)

C5 ^ C0 ^ CE ^ B1 = 7A

(C5 + 03) ^ (C0 + 01) ^ (67 + 01) ^ (6F + 02)

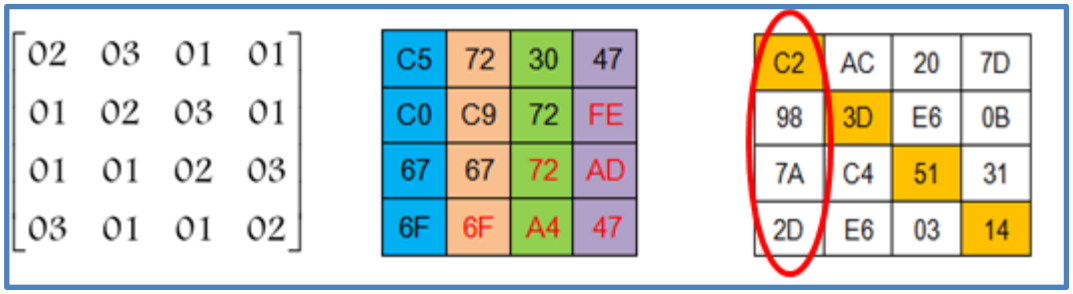
E (L {C5} + L {03}) ^ (C0) ^ (67) ^ E (L {6F} + L {02})

E (BE + 01) ^ (C0) ^ (67) ^ E (BA + 19)

E (BF) ^ (C0) ^ (67) ^ E (D3)

54 ^ C0 ^ 67 ^ DE = 2D

Figura 29. Generación primera columna matriz MixColums



Fuente: Elaboración propia

- Procedimiento para obtener la segunda columna de la matriz MixColums

(72 + 02) ^ (C9 + 03) ^ (67 + 01) ^ (6F + 01)

E (L {72} + L {02}) ^ E (L {C9} + L {03}) ^ (67) ^ (6F)

E (0A + 19) ^ E (95 + 01) ^ (67) ^ (6F)

E (23) ^ E (96) ^ (67) ^ (6F)

E4 ^ 40 ^ 67 ^ 6F = AC

(72 + 01) ^ (C9 + 02) ^ (67 + 03) ^ (6F + 01)

(72) ^ E (L {C9} + L {02}) ^ E (L {67} + L {03}) ^ (6F)

(72) ^ E (95 + 19) ^ E (42 + 01) ^ (6F)

(72) ^ E (AE) ^ E (43) ^ (6F)

72 ^ 89 ^ A9 ^ 6F = 3D

(72 + 01) ^ (C9 + 01) ^ (67 + 02) ^ (6F + 03)

(72) ^ (C9) ^ E (L {67} + L {02}) ^ E (L {6F} + L {03})

(72) ^ (C9) ^ E (42 + 19) ^ E (BA + 01)

(72) ^ (C9) ^ E (5B) ^ E (BB)

72 ^ C9 ^ CE ^ B1 = C4

(72 + 03) ^ (C9 + 01) ^ (67 + 01) ^ (6F + 02)

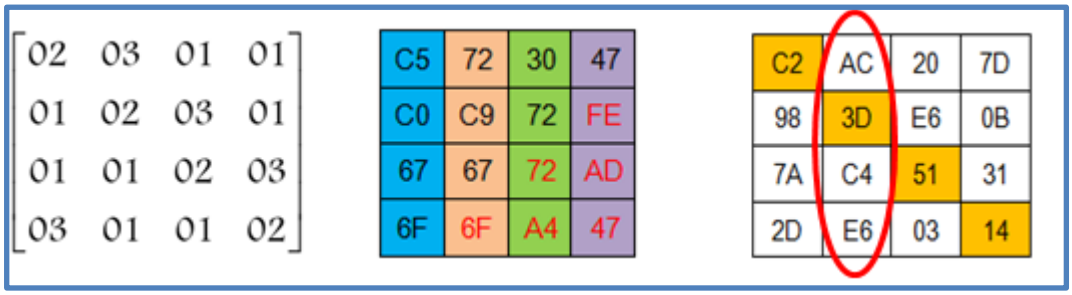
E (L {72} + L {03}) ^ (C9) ^ (67) ^ E (L {6F} + L {02})

E (0A + 01) ^ (C9) ^ (67) ^ E (BA + 19)

E (0B) ^ (C9) ^ (67) ^ E (D3)

96 ^ C9 ^ 67 ^ DE = E6

Figura 30. Generación segunda columna matriz MixColums



Fuente: Elaboración propia

- Procedimiento para obtener la tercera columna de la matriz MixColums

(30 + 02) ^ (72 + 03) ^ (72 + 01) ^ (A4 + 01)

E (L {30} + L {02}) ^ E (L {72} + L {03}) ^ (72) ^ (A4)

E (65 + 19) ^ E (0A + 01) ^ (72) ^ (A4)

E (7E) ^ E (0B) ^ (72) ^ (A4)

60 ^ 96 ^ 72 ^ A4 = 20

(30 + 01) ^ (72 + 02) ^ (72 + 03) ^ (A4 + 01)

(30) ^ E (L {72} + L {02}) ^ E (L {72} + L {03}) ^ (A4)

(30) ^ E (0A + 19) ^ E (0A + 01) ^ (A4)

(30) ^ E (23) ^ E (0B) ^ (A4)

30 ^ E4 ^ 96 ^ A4 = E6

(30 + 01) ^ (72 + 01) ^ (72 + 02) ^ (A4 + 03)

(30) ^ (72) ^ E (L {72} + L {02}) ^ E (L {A4} + L {03})

(30) ^ (72) ^ E (0A + 19) ^ E (17 + 01)

(30) ^ (72) ^ E (23) ^ E (18)

30 ^ 72 ^ E4 ^ F7 = 51

(30 + 03) ^ (72 + 01) ^ (72 + 01) ^ (A4 + 02)

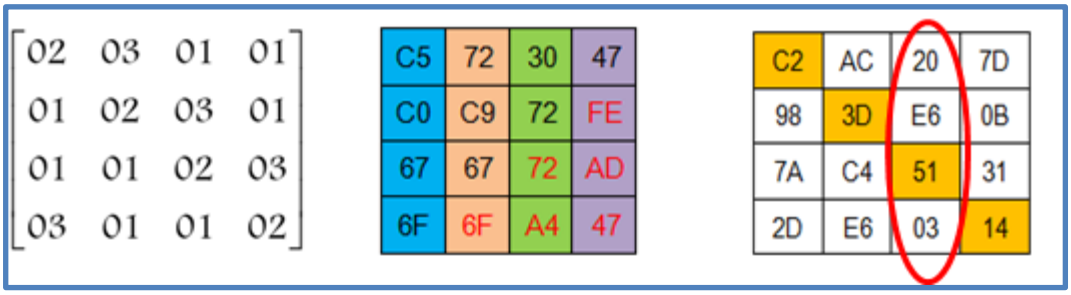
E (L {30} + L {03}) ^ (72) ^ (72) ^ E (L {A4} + L {02})

E (65 + 01) ^ (72) ^ (72) ^ E (17 + 19)

E (66) ^ (72) ^ (72) ^ E (30)

50 ^ 72 ^ 72 ^ 53 = 03

Figura 31. Generación tercera columna matriz MixColums



Fuente: Elaboración propia

- Procedimiento para obtener la cuarta columna de la matriz MixColums

(47 + 02) ^ (FE + 03) ^ (AD + 01) ^ (47 + 01)

E (L {47} + L {02}) ^ E (L {FE} + L {03}) ^ (AD) ^ (47)

E (94 + 19) ^ E (70 + 01) ^ (AD) ^ (47)

E (AD) ^ E (71) ^ (AD) ^ (47)

8E ^ 19 ^ AD ^ 47 = 7D

(47+ 01) ^ (FE + 02) ^ (AD + 03) ^ (47 + 01)

(47) ^ E (L {FE} + L {02}) ^ E (L {AD} + L {03}) ^ (47)

(47) ^ E (70 + 19) ^ E (76 + 01) ^ (47)

(47) ^ E (89) ^ E (77) ^ (47)

47 ^ E7 ^ EC ^ 47 = 0B

(47 + 01) ^ (FE + 01) ^ (AD + 02) ^ (47 + 03)

(47) ^ (FE) ^ E (L {AD} + L {02}) ^ E (L {47} + L {03})

(47) ^ (FE) ^ E (76 + 19) ^ E (94 + 01)

(47) ^ (FE) ^ E (8F) ^ E (95)

47 ^ FE ^ 41 ^ C9 = 31

(47 + 03) ^ (FE + 01) ^ (AD + 01) ^ (47 + 02)

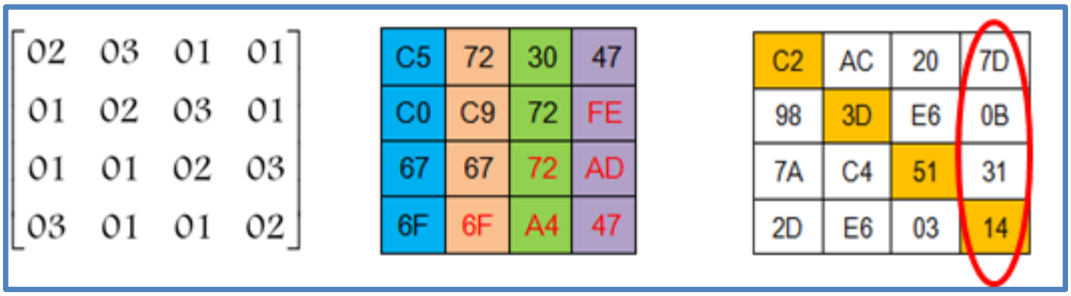
E (L { 47} + L {03}) ^ (FE) ^ (AD) ^ E (L {47} + L {02})

E (94 + 01) ^ (FE) ^ (AD) ^ E (94 + 19)

E (95) ^ (FE) ^ (AD) ^ E (AD)

C9 ^ FE ^ AD ^ 8E = 14

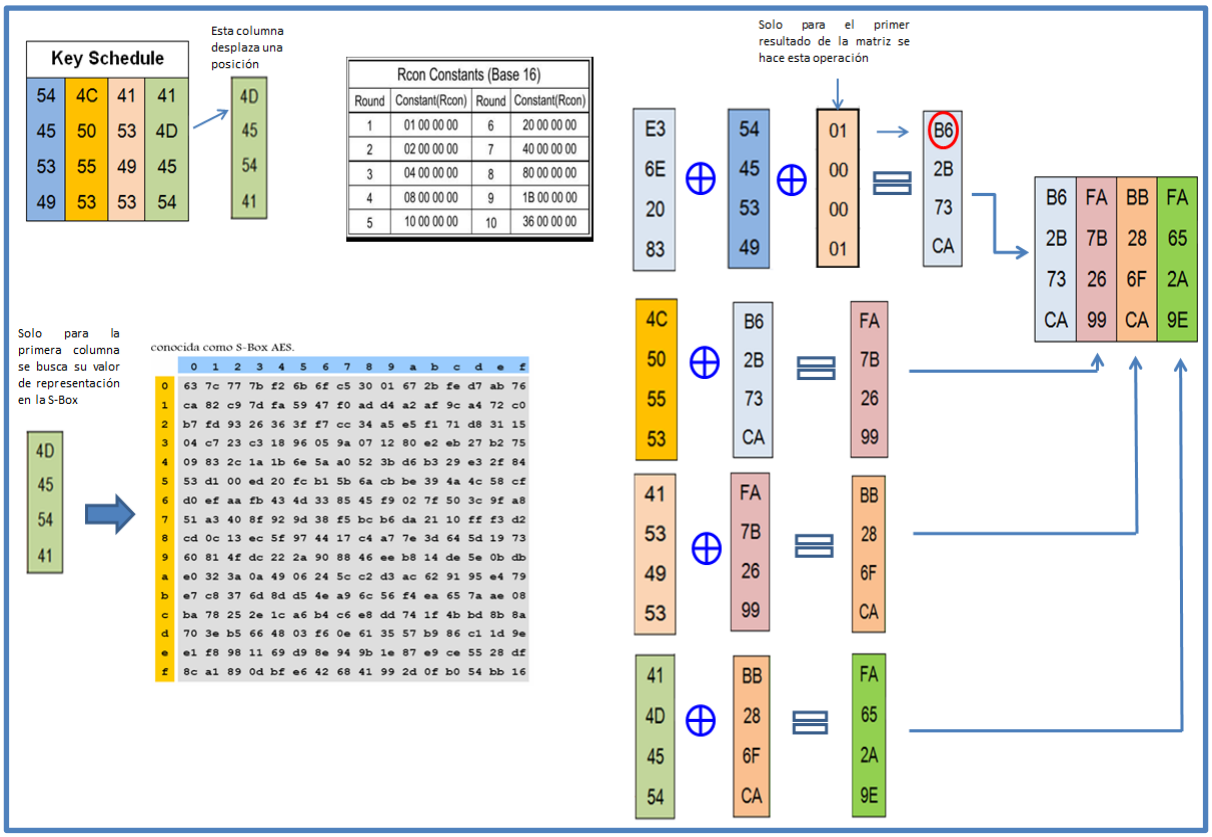
Figura 32. Generación cuarta columna matriz MixColums



Fuente: Elaboración propia

Luego del procedimiento MixColums se requiere obtener el nuevo keySchedule que está desarrollado en base a la matriz del keySchedule inicial mediante operaciones XOR de las diferentes posiciones de la matriz más una R constant como se muestra a continuación.

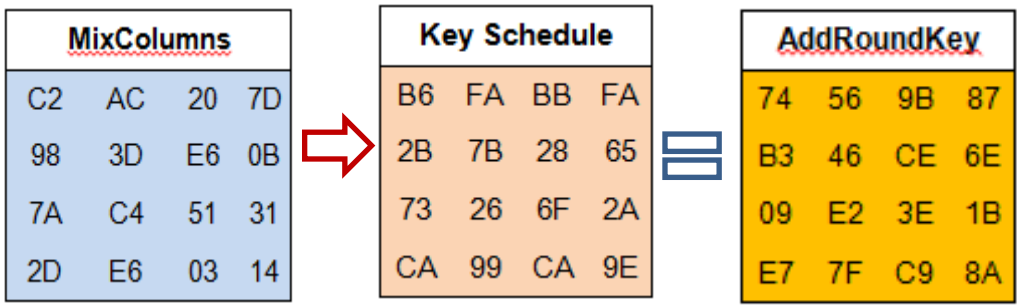
Figura 33. Generación nuevo KeySchedule



Fuente: Elaboración propia

Para continuar con el procedimiento de completar los rondas, se requiera calcular el nuevo AddRounkKey por lo que será necesario hacer una operación entre el Key Schedule obtenido con el MixColumns y de esa manera se obtiene el AddRoundKey nuevo que es punto de partida para la siguiente ronda.

Figura 34. Nuevo AddRounkKey



Fuente: Elaboración propia

El procedimiento continua repetidamente hasta completar la última ronda en la que se obtiene el cifrado.

Figura 35. Representación resultados de Cifrado

Plaintext (input)				Key (input)				Ciphertext (output)				String Representations	
53	52	49	57	54	4C	41	41	90	0C	5B	7A	Plaintext:	53494D4F524F4D4E4941434557534F52
49	4F	41	53	45	50	53	4D	FA	0A	76	36	Key:	544553494C50555341534953414D4554
4D	4D	43	4F	53	55	49	45	35	93	69	CB	Ciphertext	90FA350E0C0A93285B7669DC7A36CB07
4F	4E	45	52	49	53	53	54	0E	28	DC	07		

Fuente: Elaboración propia

Figura 36. Representación completa del proceso de cifrado

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0					02	03	01	01					07	1E	08	16	54	4C	41	41	
					01	02	03	01					0C	1F	12	1E	45	50	53	4D	
					01	01	02	03					1E	18	0A	0A	53	55	49	45	
					03	01	01	02					06	1D	16	06	49	53	53	54	
Round 1	C5	72	30	47	C5	72	30	47	C2	AC	20	7D	74	56	9B	87	B6	FA	BB	FA	01
	FE	C0	C9	72	C0	C9	72	FE	98	3D	E6	0B	B3	46	CE	6E	2B	7B	28	65	
	72	AD	67	67	67	67	72	AD	7A	C4	51	31	09	E2	3E	1B	73	26	6F	2A	
	6F	A4	47	6F	6F	6F	A4	47	2D	E6	03	14	E7	7F	C9	8A	CA	99	CA	9E	
Round 2	92	B1	14	17	92	B1	14	17	1D	C4	41	DC	E4	C7	F9	9E	F9	03	B8	42	02
	6D	5A	8B	9F	5A	8B	9F	6D	95	C2	E0	A3	5B	77	7D	5B	CE	B5	9D	F8	
	01	98	B2	AF	B2	AF	01	98	35	D8	E4	2D	4D	86	D5	36	78	5E	31	1B	
	94	D2	DD	7E	7E	94	D2	DD	B9	DF	1D	6D	5E	A1	A9	47	E7	7E	B4	2A	
Round 3	69	C6	99	0B	69	C6	99	0B	75	D0	B3	CA	C9	6F	B4	8F	BC	BF	07	45	04
	39	F5	FF	39	F5	FF	39	39	3D	74	E7	66	5C	A0	AE	D7	61	D4	49	B1	
	E3	44	03	05	03	05	E3	44	61	DB	2B	D4	FC	18	D9	3D	9D	C3	F2	E9	
	58	32	D3	A0	A0	58	32	D3	16	1B	0E	DD	DD	AE	0F	F6	CB	B5	01	2B	
Round 4	DD	A8	8D	73	DD	A8	8D	73	ED	9A	47	E3	91	59	83	62	7C	C3	C4	81	08
	4A	E0	E4	0E	E0	E4	0E	4A	1B	D3	BE	7D	64	78	5C	2E	7F	AB	E2	53	
	B0	AD	35	27	35	27	B0	AD	91	5A	CF	E2	FD	F5	92	56	6C	AF	5D	B4	
	C1	E4	76	42	42	C1	E4	76	2D	B9	E1	9E	88	A9	F0	A4	A5	10	11	3A	
Round 5	81	CB	EC	AA	81	CB	EC	AA	C0	26	17	E0	41	64	91	E7	81	42	86	07	10
	43	BC	4A	31	BC	4A	31	43	7A	53	A1	91	88	0A	1A	79	F2	59	BB	E8	
	54	E6	4F	B1	4F	B1	54	E6	78	AF	1B	B1	94	EC	05	1B	EC	43	1E	AA	
	C4	D3	8C	49	49	C4	D3	8C	F9	2E	F7	43	50	97	5F	D1	A9	B9	A8	92	
Round 6	83	43	81	94	83	43	81	94	E1	87	72	65	DB	FF	8C	9C	3A	78	FE	F9	20
	C4	67	A2	B6	67	A2	B6	C4	CE	A5	18	81	90	A2	A4	D5	5E	07	BC	54	
	22	CE	6B	AF	6B	AF	22	CE	70	51	F0	9D	D3	B1	0E	C9	A3	E0	FE	54	
	53	88	CF	3E	3E	53	88	CF	EE	6E	07	28	82	BB	7A	C7	6C	D5	7D	EF	
Round 7	B9	16	64	DE	B9	16	64	DE	4A	39	41	15	10	1B	9D	30	5A	22	DC	25	40
	60	3A	49	03	3A	49	03	60	ED	EB	22	87	93	92	E7	16	7E	79	C5	91	
	66	C8	AB	DD	AB	DD	66	C8	9F	CB	8E	40	E3	57	EC	76	7C	9C	62	36	
	13	EA	DA	C6	C6	13	EA	DA	D6	88	06	7E	23	A8	5B	CC	F5	20	5D	B2	
Round 8	CA	AF	5E	04	CA	AF	5E	04	DB	FC	A6	15	80	85	03	95	5B	79	A5	80	80
	DC	4F	94	47	4F	94	47	DC	56	F2	21	73	2D	F0	E6	25	7B	02	C7	56	
	11	5B	CE	38	CE	38	11	5B	DF	21	66	25	94	F6	D3	A6	4B	D7	B5	83	
	26	C2	39	4B	4B	26	C2	39	52	0A	2B	F9	98	E0	9C	FC	CA	EA	B7	05	
Round 9	CD	97	7B	2A	CD	97	7B	2A	D8	DE	74	BB	29	56	59	16	F1	88	2D	AD	1B
	D8	8C	8E	3F	8C	8E	3F	D8	D4	BA	82	99	43	2F	D0	9D	97	95	52	04	
	22	42	66	24	66	24	22	42	46	9B	38	0F	66	6C	7A	CE	20	F7	42	C1	
	46	E1	DE	B0	B0	46	E1	DE	DD	84	49	43	DA	69	13	1C	07	ED	5A	5F	
Round 10	A5	B1	CB	47	A5	B1	CB	47					90	0C	5B	7A	35	BD	90	3D	36
	1A	15	70	5E	15	70	5E	1A					FA	0A	76	36	EF	7A	28	2C	
	33	50	DA	8B	DA	8B	33	50					35	93	69	CB	EF	18	5A	9B	
	57	F9	7D	9C	9C	57	F9	7D					0E	28	DC	07	92	7F	25	7A	
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Fuente: Elaboración propia

La criptografía computacional se visualiza de manera sencilla con el uso de lenguajes de programación que permiten para este caso poder hacer un seguimiento paso por paso de los proceso del algoritmo como lo que se muestra en el siguiente programa en leguaje C++, que admite una cadena con una clave criptográfica definida por el usuario para validar el acceso al programa y luego se realiza el proceso de encriptación con la optimización del algoritmo AES.

```
void AES::blockEncrypt(uint32_d* pBuffer, uint32_d lSize)
{
  uint32_d w[4], iv[4];
  uint32_d RoundKey[(Nr + 1)* Nk];
  uint32_d m, i, block = lSize / Nb;
  // Desciframos el Bloque de memoria donde está la llave :v
  SecHideData(Key, sizeof(Key), false, true);
  for (i = 0; i < Nb; i++) iv[i] = this->IV[i];
  for (m = 0; m < block; m += Nb)
  {       // Regenerando la Llave !
            ExpansionK(Key, RoundKey);
            // Primera ronda...
            w[0] = pBuffer[m + 0] ^ iv[0] ^ RoundKey[0];
            w[1] = pBuffer[m + 1] ^ iv[1] ^ RoundKey[1];
            w[2] = pBuffer[m + 2] ^ iv[2] ^ RoundKey[2];
            w[3] = pBuffer[m + 3] ^ iv[3] ^ RoundKey[3];
            // Rondas de [1] - [9]
            for (i = 1; i < Nr; i++)
            {         SubBytes(w);
                      ShiftRows(w);
                      MixColumns(w);
                      w[0] ^= RoundKey[i * Nk];
                      w[1] ^= RoundKey[i * Nk + 1];
                      w[2] ^= RoundKey[i * Nk + 2];
                      w[3] ^= RoundKey[i * Nk + 3];
            }
            // Ronda[10] - No se realiza MixColumns
            SubBytes(w);
            ShiftRows(w);
            pBuffer[m + 0] = w[0] ^ RoundKey[i * Nk];
            pBuffer[m + 1] = w[1] ^ RoundKey[i * Nk + 1];
            pBuffer[m + 2] = w[2] ^ RoundKey[i * Nk + 2];
            pBuffer[m + 3] = w[3] ^ RoundKey[i * Nk + 3];
            // Actualizamos el Vector.. y la LLave para la nueva Regeneración :v
            for (i = 0; i < Nb; i++)
            {         iv[i]  = pBuffer[m + i];
                      Key[i] = RoundKey[Nr * Nk + i];
            }
  }
  CleanData(Key, sizeof(Key));
  CleanData(iv, sizeof(iv));
  CleanData(RoundKey, sizeof(RoundKey));
  return;   }
```

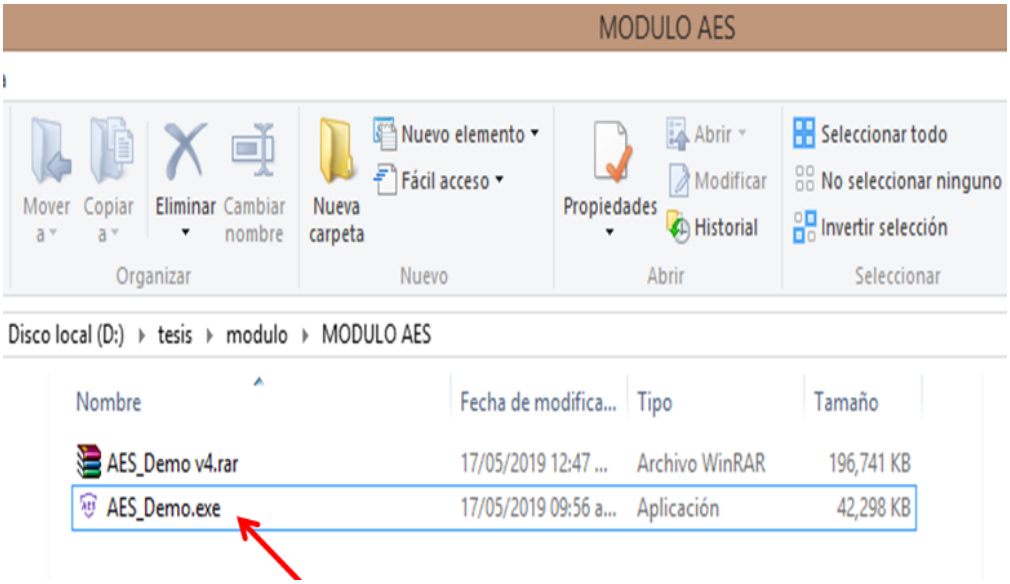
Después de haber simulado cada fase del proceso de cifrado de algoritmo de encriptación AES se ha logrado hacer una evaluación de la seguridad del algoritmo permitiendo de esa manera determinar cuáles son sus fortalezas y debilidades; asimismo, se observa una efectividad en la encriptación de datos, siempre y cuando no se presenten fallas en las que se modifiquen, agreguen o supriman bits ocasionando errores en la interpretación final de los datos.

Por lo que se pudo comprobar es altamente improbable que existan llaves débiles o semidébiles en AES, debido a la estructura de su diseño, que busca eliminar la simetría en las subclaves. También se ha comprobado que es resistente a criptoanálisis, tanto lineal como diferencial. En cuanto a los ataques por fuerza bruta, se entiende que la resistencia del algoritmo es proporcional a la longitud de la llave usada.

Con respecto a la velocidad del proceso de encriptación o desencriptacion para esta investigación no ha sido relevante debido a que se hizo la implementación del algoritmo usando lenguaje de programación de manera más óptima obteniéndose resultados que no se ajustan a la realidad debido a que la velocidad de encriptación o desencriptacion van a depender netamente del hardware en el que este implementado.

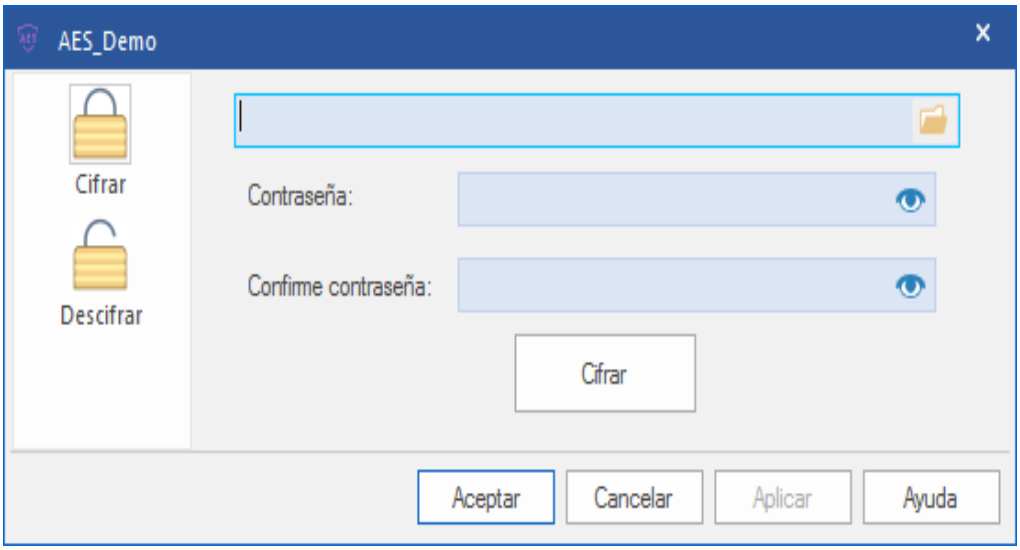
4.7 Presentación de AES Optimizado

Figura 37. Interface Acceso directo modulo AES



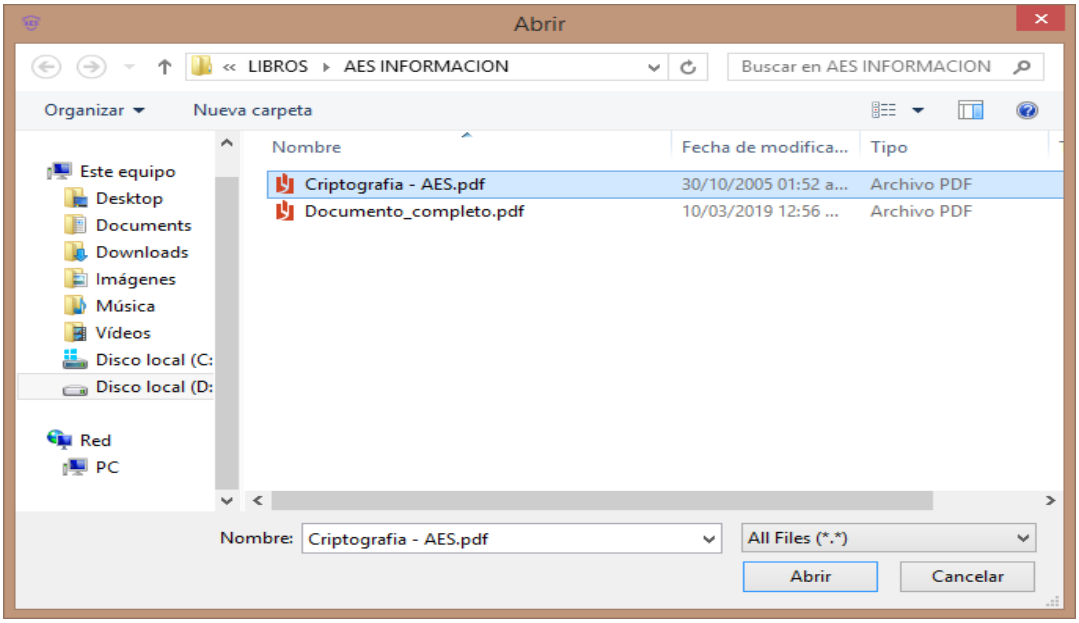
Fuente: Elaboración propia

Figura 38. Interface Módulo de carga de archivos a cifrar/descifrar



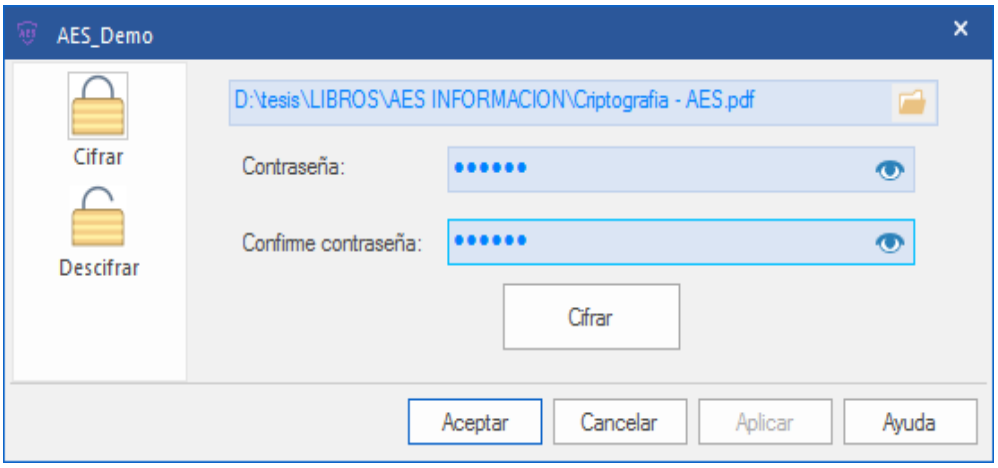
Fuente: Elaboración propia

Figura 39. Interface Seleccionar archivo a cifrar/descifrar



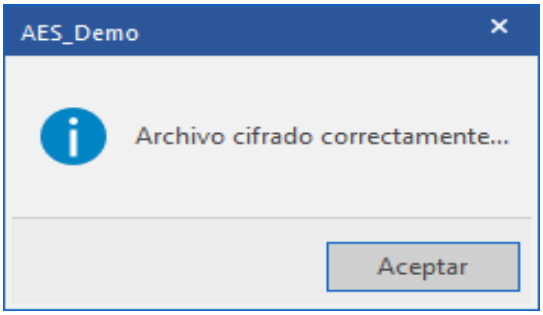
Fuente: Elaboración propia

Figura 40. Interface Seleccionar cifrar/descifrar



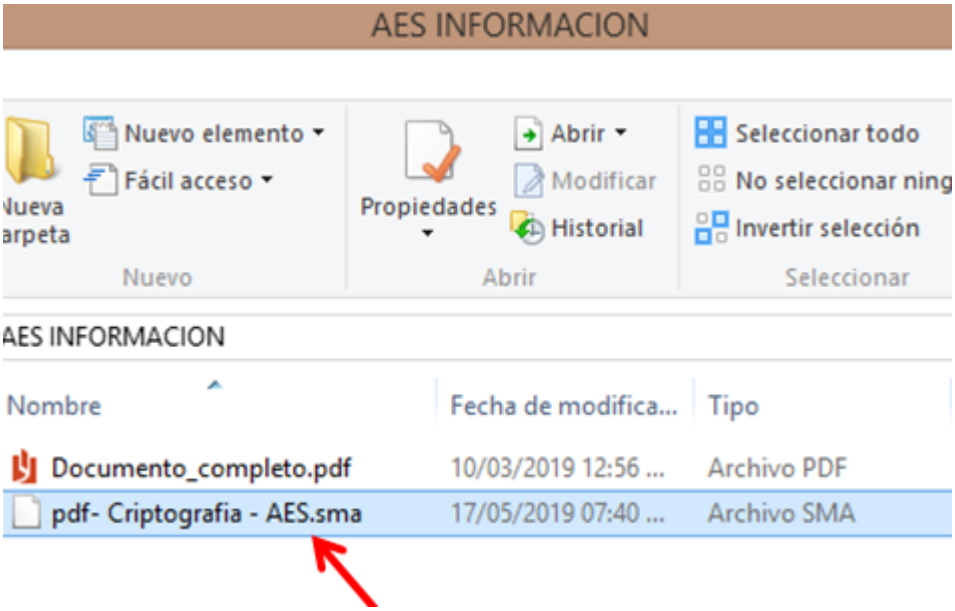
Fuente: Elaboración propia

Figura 41. Interface mensaje Archivo cifrado/descifrado



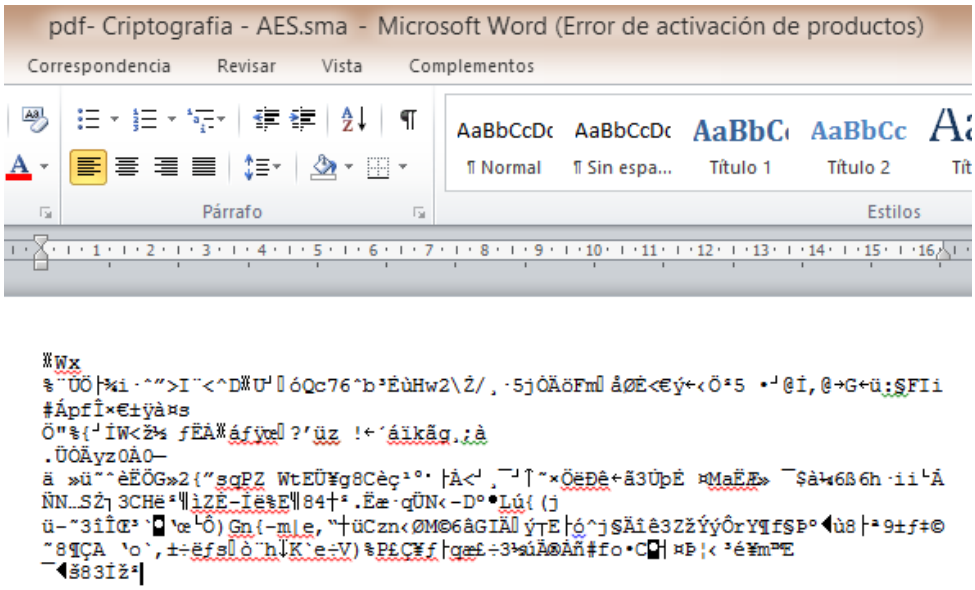
Fuente: Elaboración propia

Figura 42. Archivo cifrado extensión .sma



Fuente: Elaboración propia

Figura 43. Contenido Archivo cifrado



Fuente: Elaboración propia

4.8 Evaluación de la optimización del algoritmo AES

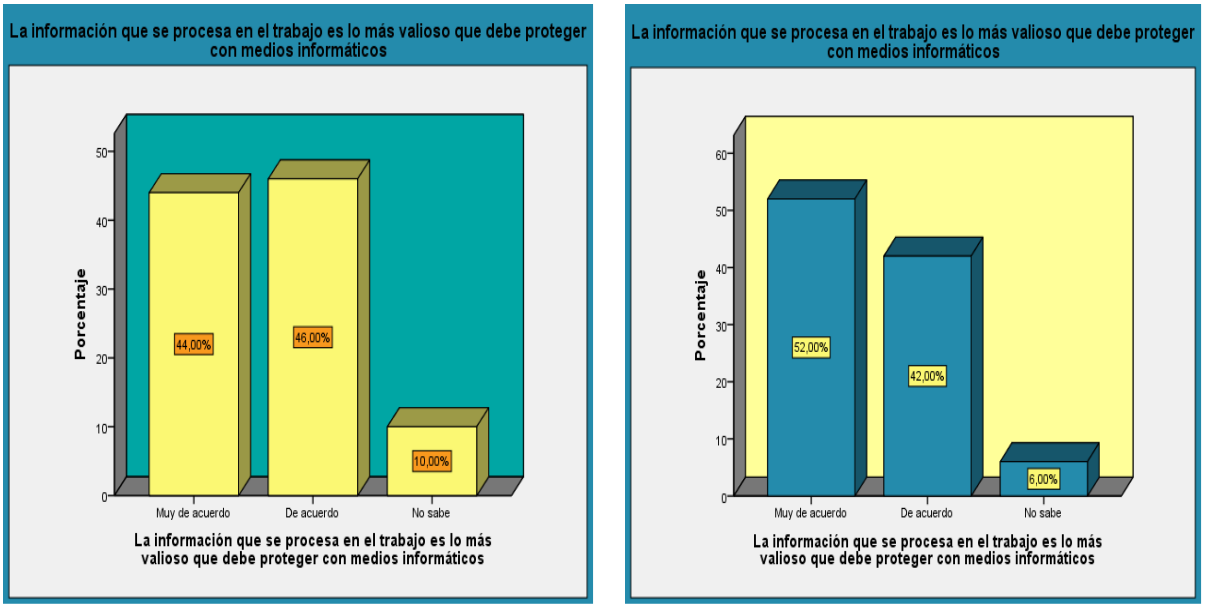
Después de haber realizado la implementación de la Optimización del Algoritmo AES se consideró necesario hacer una evaluación Pre y Post – implementación para obtener información del impacto causado en los usuarios de acuerdo a la muestra establecida. Se aplicó una de las técnicas de recolección de datos que consistió en hacer un cuestionario de preguntas relacionadas a las variables planteadas en esta investigación de la siguiente manera:

CUESTIONARIO ANTES Y DESPUES DE LA IMPLEMENTACION DE LA OPTIMIZACIÓN DEL ALGORITMO AES

Los resultados para cada pregunta son presentados en los histogramas de barras a lado izquierdo de color amarillo corresponde a los resultados Pre-implementación y al lado derecho de color azul corresponde a los resultados Pos-implementación.

1. Para Ud. la información que se procesa en el trabajo es lo más valioso que debe proteger con medios informáticos.

Figura 44. Distribución porcentual Valoración de la información



Fuente: Elaboración propia

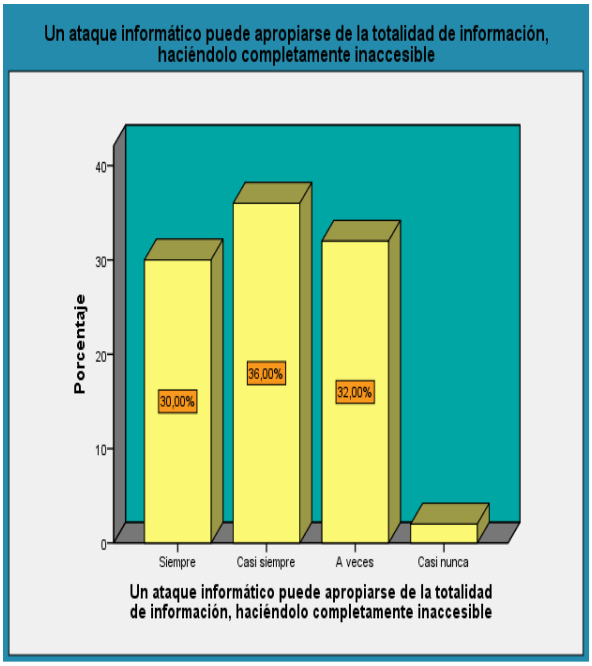
Análisis de los resultados: Del total de 43 encuestados el **44%** está **Muy de acuerdo** que la información que se procesa en el trabajo es lo más valioso que debe proteger con medios informáticos.

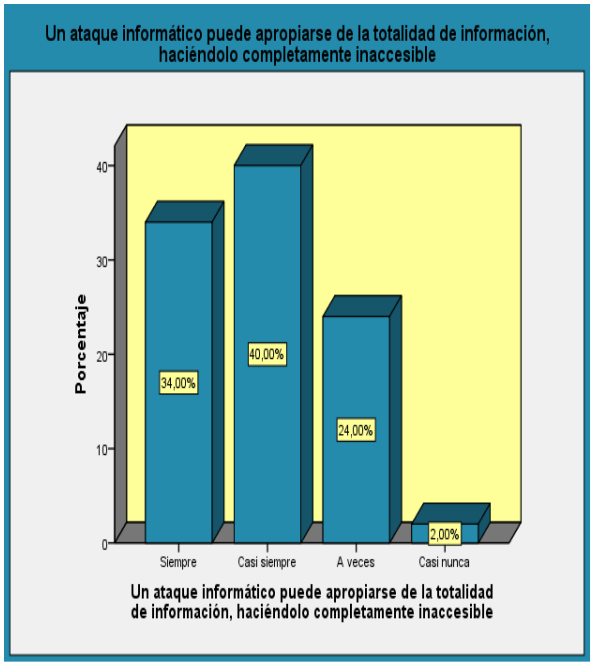
Análisis de los resultados: Del total de 43 encuestados el **52**% está **Muy de acuerdo** que la información que se procesa en el trabajo es lo más valioso que debe proteger con medios informáticos.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **8%** con respecto a que los encuestados consideran estar **Muy de acuerdo** que la información que se procesa en el trabajo es lo más valioso que debe proteger con medios informáticos; esto se debe a que la implementación del algoritmo ha ocasionado un impacto en la protección de la información.

2. Sabe Ud. que un ataque informático puede apropiarse de la totalidad de información, haciéndolo completamente inaccesible.

Figura 45. Distribución porcentual efectos de ataque informático





Fuente: Elaboración propia

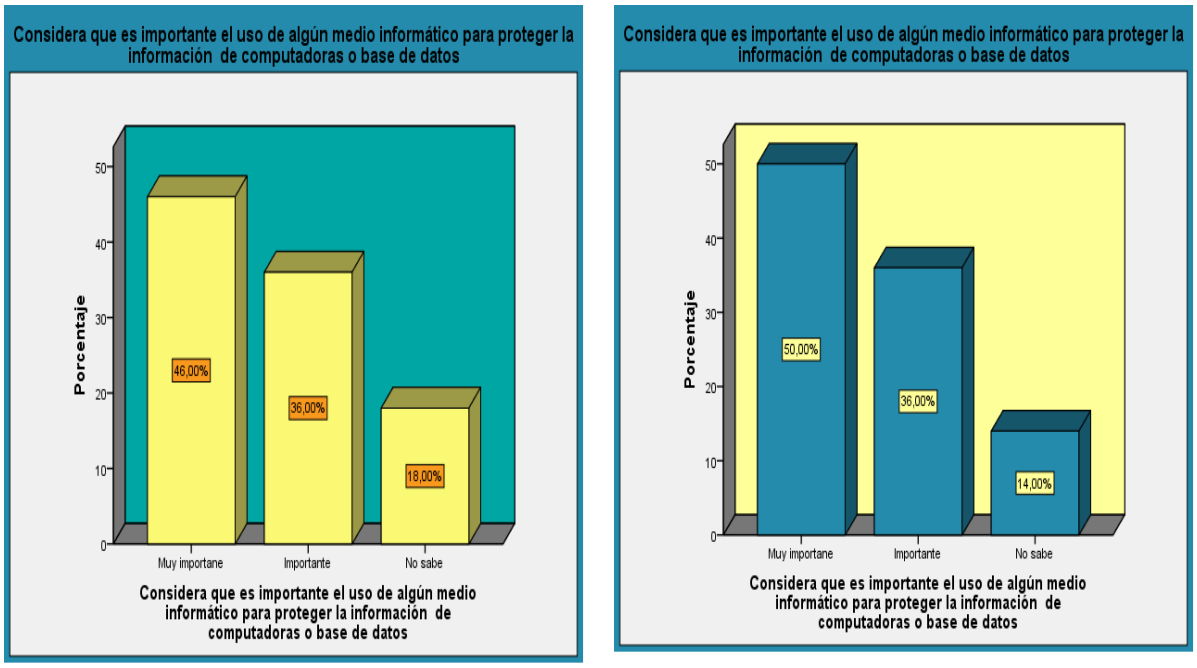
Análisis de los resultados: Del total de 43 encuestados el **36%** indica que **casi siempre** un ataque informático puede apropiarse de la totalidad de información, haciéndolo completamente inaccesible.

Análisis de los resultados: Del total de 43 encuestados el **40**% considera que un ataque informático **casi siempre** puede apropiarse de la totalidad de información, haciéndolo completamente inaccesible.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados consideran que un ataque informático **casi siempre** puede apropiarse de la totalidad de información, haciéndolo completamente inaccesible y esto se debe a que con la implementación del algoritmo los encuestados han tomado conocimiento de la importancia de la protección de la información.

3. Dentro de las medidas de seguridad que debe aplicar, considera que es importante el uso de algún medio informático para proteger la información de computadoras o base de datos.

Figura 46. Distribución porcentual importancia uso de medios informáticos



Fuente: Elaboración propia

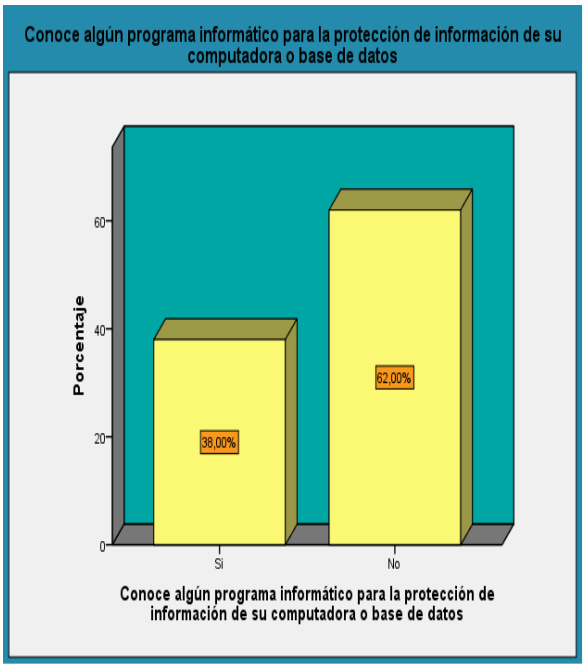
Análisis de los resultados: Del total de 43 encuestados el **46**% considera que es **muy importante** el uso de algún medio informático para proteger la información de computadoras o base de datos

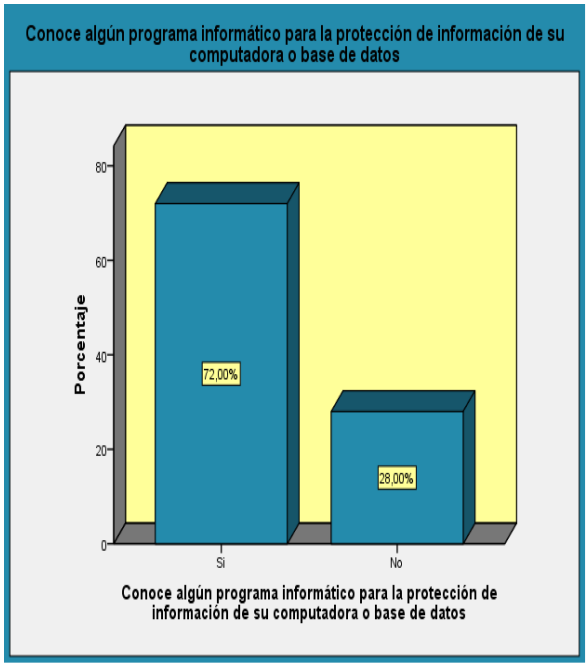
Análisis de los resultados: Del total de 43 encuestados el **50**% considera que es **muy importante** el uso de algún medio informático para proteger la información de computadoras o base de datos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados consideran que el uso de un medio informático es **Muy importante** para proteger la información de computadoras o base de datos; esto se debe a que con la implementación del algoritmo los encuestados valoraron más la importancia de la protección de la información.

4. Conoce algún programa informático para la protección de información de su computadora o base de datos.

Figura 47. Distribución porcentual conocimiento de programas informáticos





Fuente: Elaboración propia

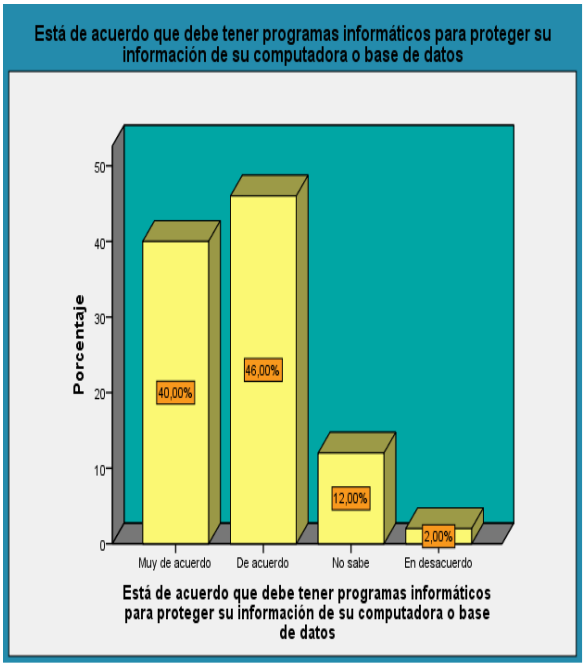
Análisis de los resultados: Del total de 43 encuestados solo el **38**% de encuestados responde que **SI** conoce algún programa informático para la protección de información de su computadora o base de datos.

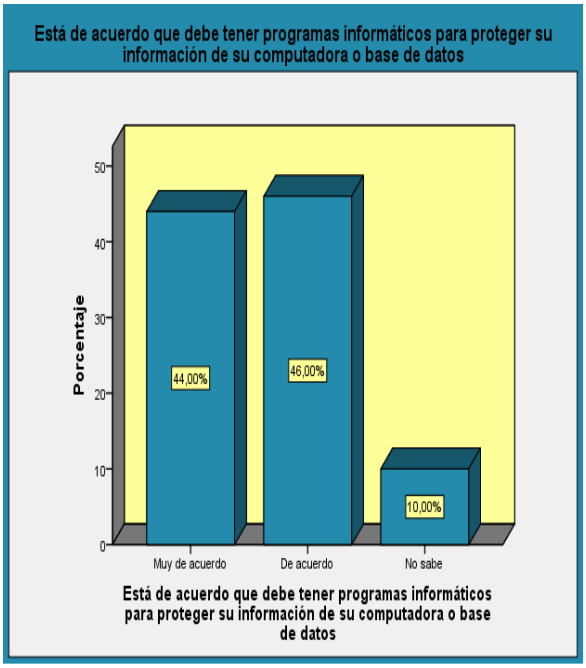
Análisis de los resultados: Del total de 43 encuestados el **72**% de encuestados responde que **SI** conoce algún programa informático para la protección de información de su computadora o base de datos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **34%** con respecto a que los encuestados responde que **SI** conoce algún programa informático para la protección de información de su computadora o base de datos; esto se debe a que con la implementación del algoritmo ha permitido que los encuestados conozcan programas informáticos para la mejorar la protección de la información.

5. Ud. está de acuerdo que debe tener programas informáticos para proteger su información de su computadora o base de datos

Figura 48. Distribución porcentual aceptación de uso de programas informáticos





Fuente: Elaboración propia

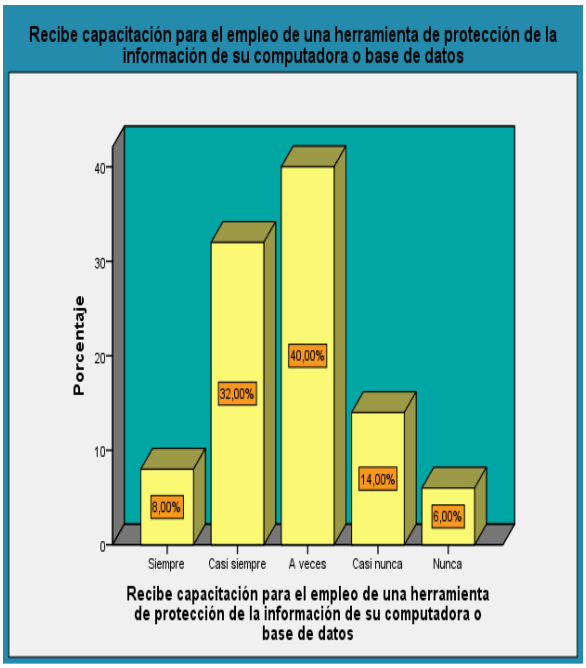
Análisis de los resultados: Del total de 43 encuestados un total de **86%** está **Muy de acuerdo** y **de acuerdo** que debe tener programas informáticos para proteger su información de su computadora o base de datos

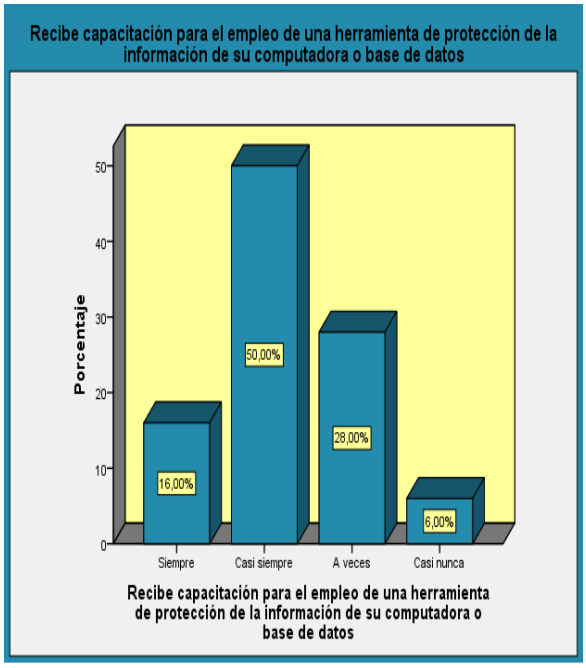
Análisis de los resultados: Del total de 43 encuestados un total de **90%** está **Muy de acuerdo** y **de acuerdo** que debe tener programas informáticos para proteger su información de su computadora o base de datos.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados están **Muy de acuerdo** y **de acuerdo** que debe tener programas informáticos para proteger su información de su computadora o base de datos; esto se debe a que con la implementación del algoritmo los encuestados protegen mejor su información.

6. Dentro de su área de trabajo recibe capacitación para el empleo de una herramienta de protección de la información de su computadora o base de datos.

Figura 49. Distribución porcentual capacitación sobre herramientas criptográficas





Fuente: Elaboración propia

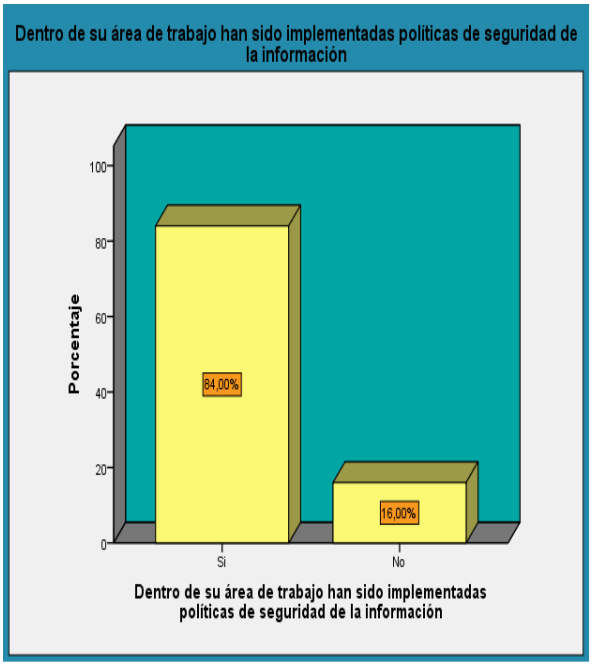
Análisis de los resultados: Del total de 43 encuestados un total de **40%** indica que **siempre** y **casi siempre** reciben capacitación para el empleo de una herramienta de protección de la información de su computadora o base de datos

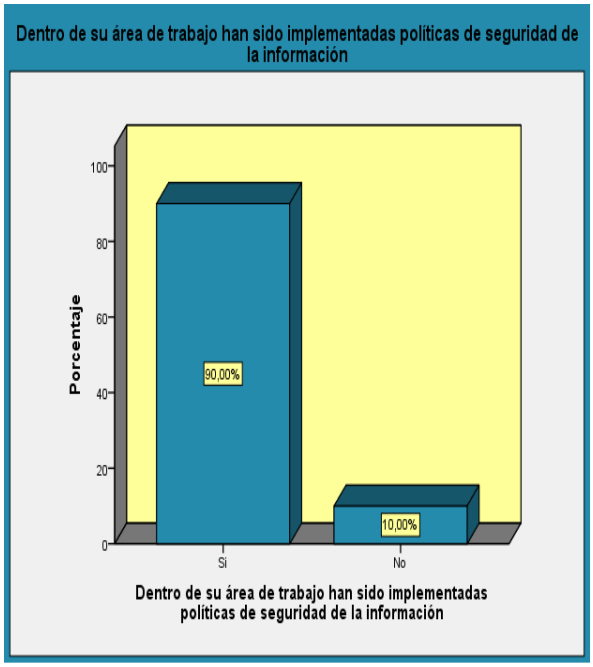
Análisis de los resultados: Del total de 43 encuestados un total de **66%** indica que **siempre** y **casi siempre** reciben capacitación para el empleo de una herramienta de protección de la información de su computadora o base de datos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **26%** con respecto a que los encuestados **siempre** y **casi siempre** reciben capacitación para el empleo de una herramienta de protección de la información de su computadora o base de datos; esto se debe a que con la implementación del algoritmo se ha generado el interés por capacitar a los encuestados en el empleo de una herramienta de protección de la información de su computadora o base de datos debido a que esta permite mayor seguridad en la protección de la información .

7. Dentro de su área de trabajo han sido implementadas políticas de seguridad de la información.

Figura 50. Distribución porcentual implementación políticas de seguridad





Fuente: Elaboración propia

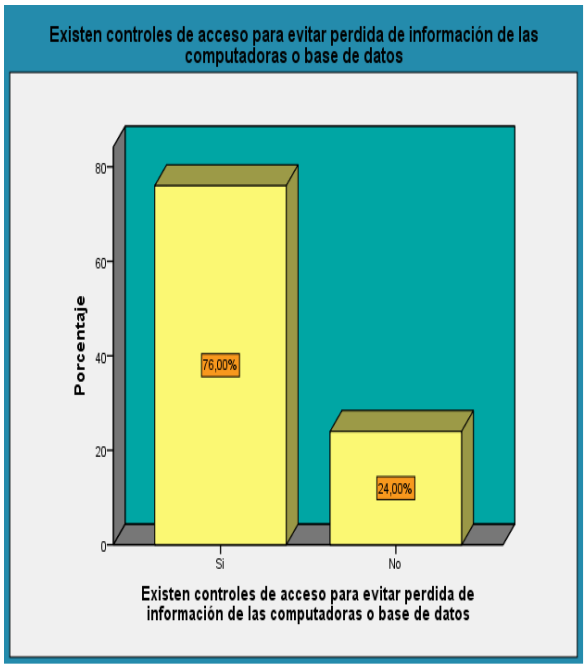
Análisis de los resultados: Del total de 43 encuestados el **84**% indica que en su área de trabajo han sido implementadas políticas de seguridad de la información

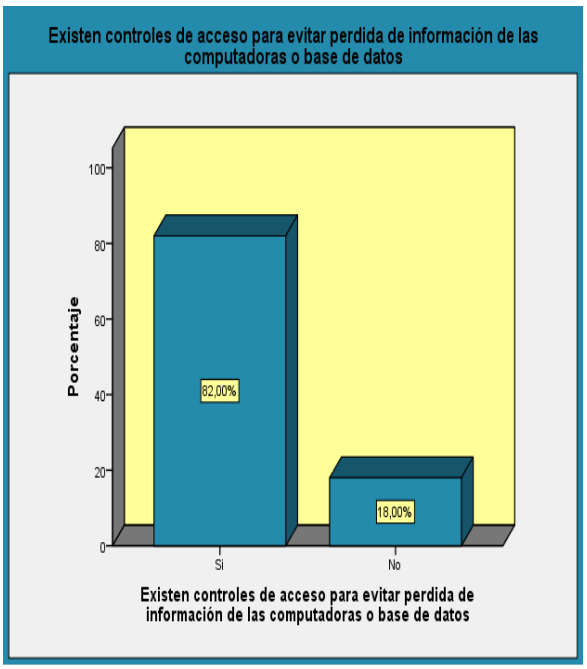
Análisis de los resultados: Del total de 43 encuestados el **90**% indica que en su área de trabajo han sido implementadas políticas de seguridad de la información

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **6%** con respecto a que los encuestados indican que en su área de trabajo han sido implementadas políticas de seguridad de la información; esto se debe a que con la implementación del algoritmo es necesario aplicar las políticas de seguridad de información implementadas.

8. Existen controles de acceso para evitar perdida de información de las computadoras o base de datos.

Figura 51. Distribución porcentual implementación controles de acceso





Fuente: Elaboración propia

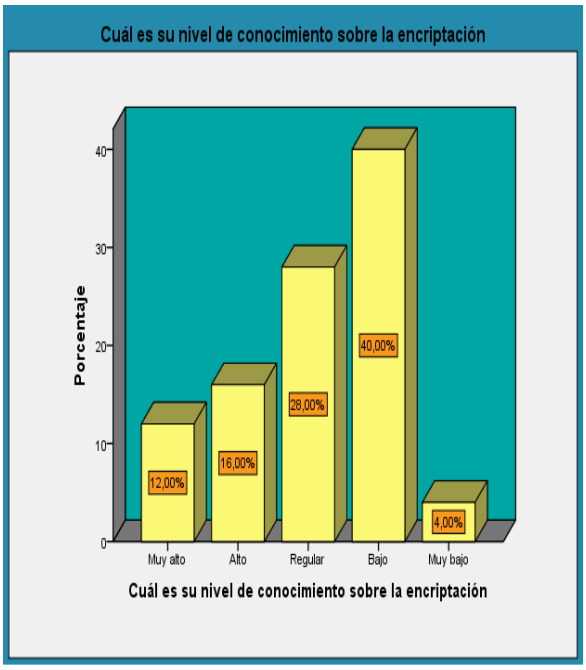
Análisis de los resultados: Del total de 43 encuestados el **76**% indica que **SI** existen controles de acceso para evitar perdida de información de las computadoras o base de datos

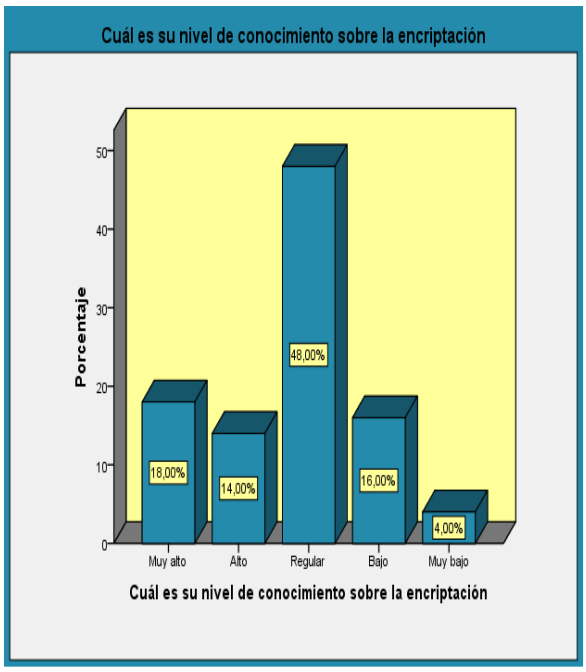
Análisis de los resultados: Del total de 43 encuestados el **82**% indica que **SI** existen controles de acceso para evitar perdida de información de las computadoras o base de datos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **6%** con respecto a que los encuestados indican que **SI** existen controles de acceso para evitar perdida de información de las computadoras o base de datos; esto se debe a que con la implementación del algoritmo estos controles de acceso se hacen más evidentes porque por que no permiten el acceso a información que se encuentra protegida con nuestro algoritmo.

9. ¿Cuál es su nivel de conocimiento sobre la encriptación?

Figura 52. Distribución porcentual grado de conocimiento de encriptación





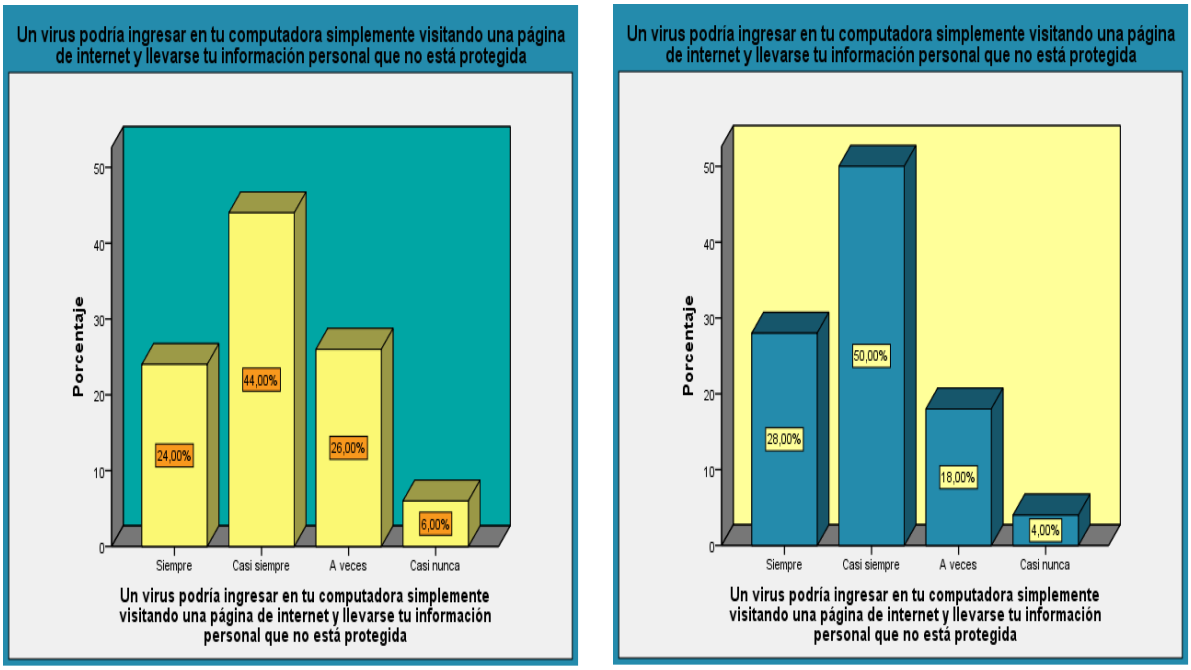
Análisis de los resultados: Del total de 43 encuestados un total de **56%** indica que su nivel de conocimiento sobre encriptación es **Muy alto, Alto y Regular.**

Análisis de los resultados: Del total de 43 encuestados un total de **80%** indica que su nivel de conocimiento sobre encriptación es **Muy alto, Alto y Regular.**

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **24%** con respecto a que los encuestados indican tener conocimiento sobre encriptación; esto se debe a que con la implementación del algoritmo aumentó el nivel de conocimiento sobre encriptación y esto indica que existe un incremento en el nivel de seguridad de la información.

10. Sabe Ud. que un virus podría ingresar en tu computadora simplemente visitando una página de internet y llevarse tu información personal que no está protegida

Figura 53. Distribución porcentual efectos que causa un virus



Fuente: Elaboración propia

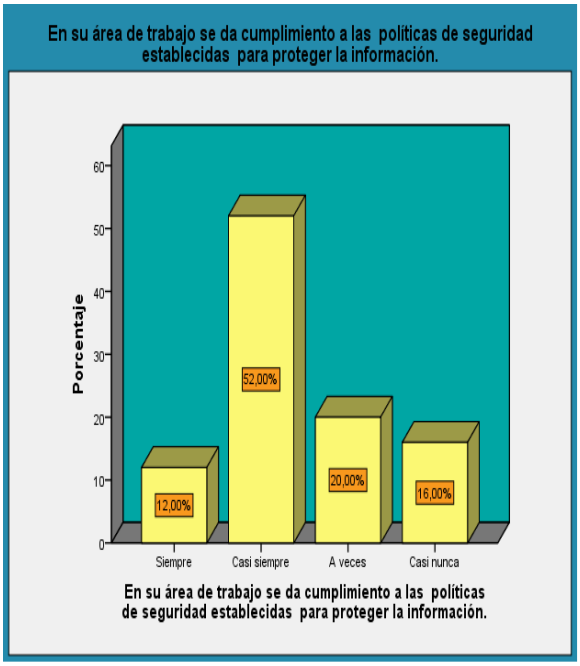
Análisis de los resultados: Del total de 43 encuestados el **44**% indica que **casi siempre** un virus podría ingresar en su computadora simplemente visitando una página de internet y llevarse tu información personal que no está protegida

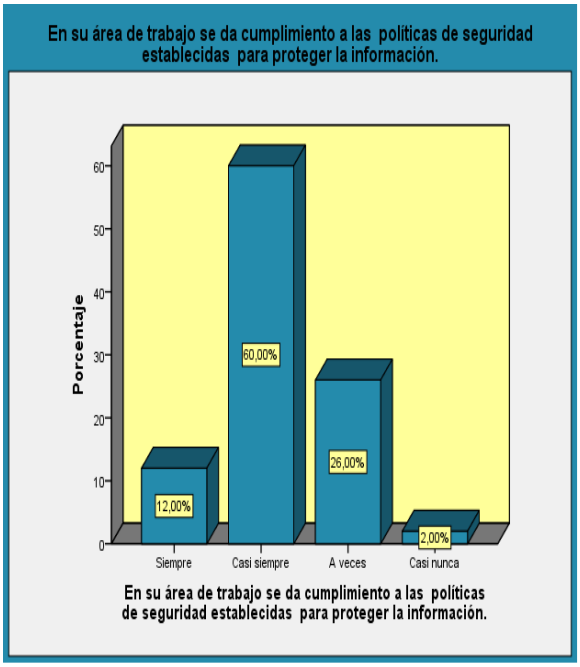
Análisis de los resultados: Del total de 43 encuestados el **50**% indica que **casi siempre** un virus podría ingresar en su computadora simplemente visitando una página de internet y llevarse tu información personal que no está protegida

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **6%** con respecto a que los encuestados indican que **casi siempre** un virus podría ingresar en su computadora simplemente visitando una página de internet y llevarse tu información personal que no está protegida; esto se debe a que con la implementación del algoritmo aumenta la eficiencia en la protección de la información porque la que la información está encriptada.

11. En su área de trabajo se da cumplimiento a las políticas de seguridad establecidas para proteger la información.

Figura 54. Distribución porcentual del cumplimiento políticas de seguridad





Fuente: Elaboración propia

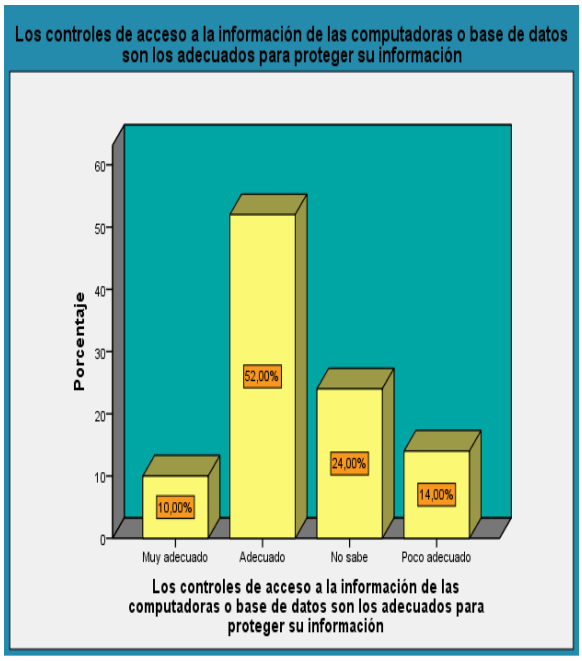
Análisis de los resultados: Del total de 43 encuestados el **52**% indica que **casi siempre** en su área de trabajo se da cumplimiento a las políticas de seguridad establecidas para proteger la información

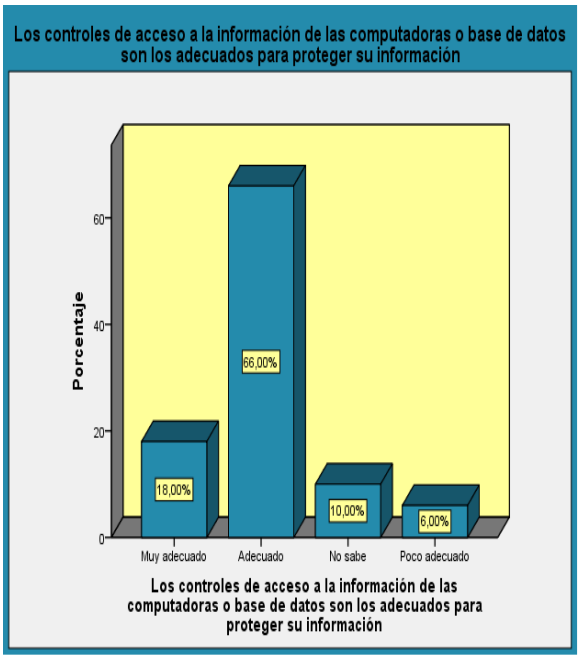
Análisis de los resultados: Del total de 43 encuestados el **60**% indica que **casi siempre** en su área de trabajo se da cumplimiento a las políticas de seguridad establecidas para proteger la información

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **8%** con respecto a que los encuestados indican que **casi siempre** en su área de trabajo se da cumplimiento a las políticas de seguridad establecidas para proteger la información; esto se debe a que con la implementación del algoritmo se está dando cumplimiento a las políticas se seguridad de la información.

12. Los controles de acceso a la información de las computadoras o base de datos son los adecuados para proteger su información.

Figura 55. Distribución porcentual control de accesos adecuados





Fuente: Elaboración propia

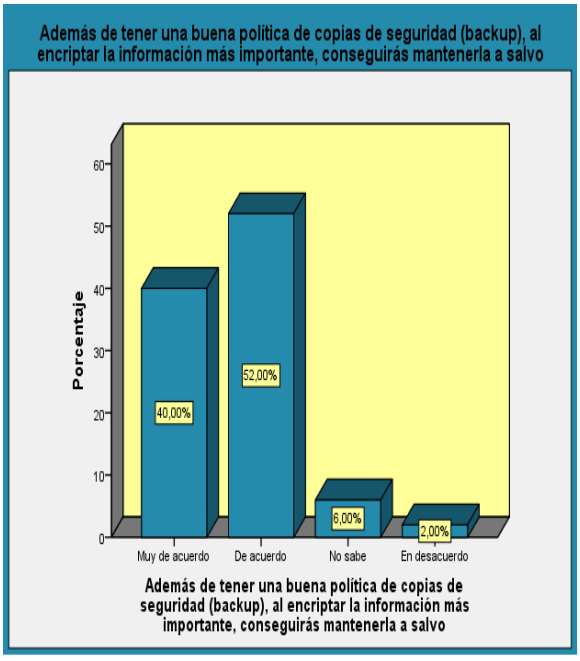
Análisis de los resultados: Del total de 43 encuestados el **52**% indica que los controles de acceso a la información de las computadoras o base de datos son **adecuados** para proteger su información.

Análisis de los resultados: Del total de 43 encuestados, el **66**% indica que los controles de acceso a la información de las computadoras o base de datos son **adecuados** para proteger su información.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **14%** con respecto a que los encuestados ; indican que los controles de acceso a la información de las computadoras o base de datos son **adecuados** para proteger su información; esto se debe a que con la implementación del algoritmo se hace más difícil los acceso a la información de personas no autorizadas, esto se debe a que la información está protegida con la encriptación.

13. Cree Ud. que además de tener una buena política de copias de seguridad (backup), al encriptar la información más importante, conseguirás mantenerla a salvo.

Figura 56. Distribución porcentual copias de seguridad y encriptación



Fuente: Elaboración propia

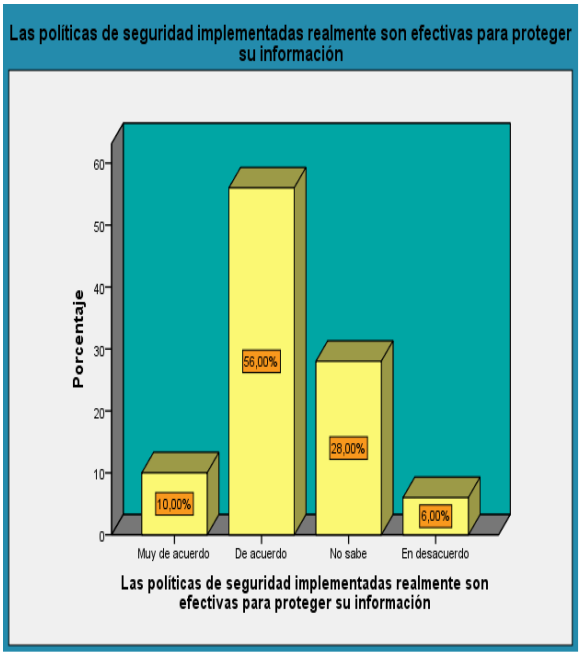
Análisis de los resultados: Del total de 43 encuestados el **48**% está **de acuerdo** que además de tener una buena política de copias de seguridad, al encriptar la información más importante, conseguirá mantenerla a salvo.

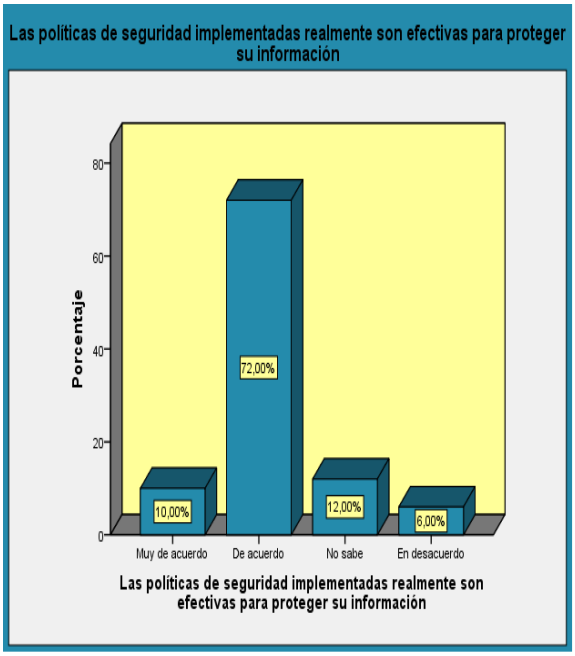
Análisis de los resultados: Del total de 43 encuestados el **52**% está **de acuerdo** que además de tener una buena política de copias de seguridad, al encriptar la información más importante, conseguirá mantenerla a salvo.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados indican que están **de acuerdo** que además de tener una buena política de copias de seguridad, al encriptar la información más importante, conseguirá mantenerla a salvo; esto se debe a que con la implementación del algoritmo se está protegiendo la información como parte de la política de seguridad de la información.

14. Las políticas de seguridad implementadas realmente son efectivas para proteger su información.

Figura 57. Distribución porcentual efectividad de las políticas de seguridad





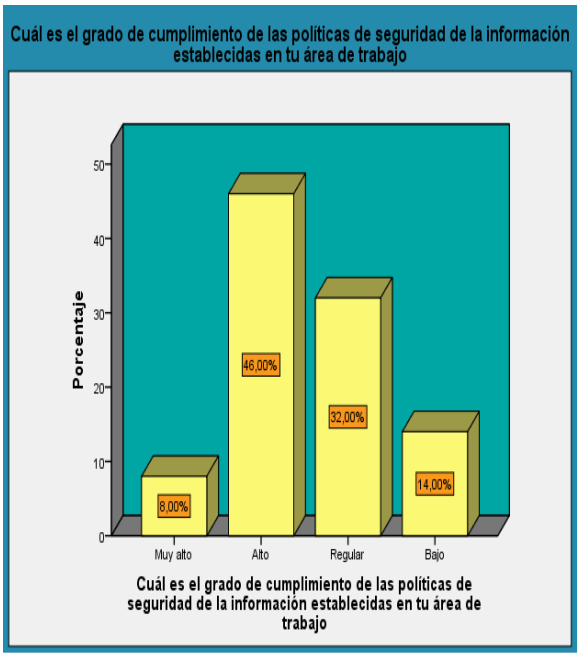
Análisis de los resultados: Del total de 43 encuestados el **56**% está **de acuerdo** que las políticas de seguridad implementadas realmente son efectivas para proteger su información

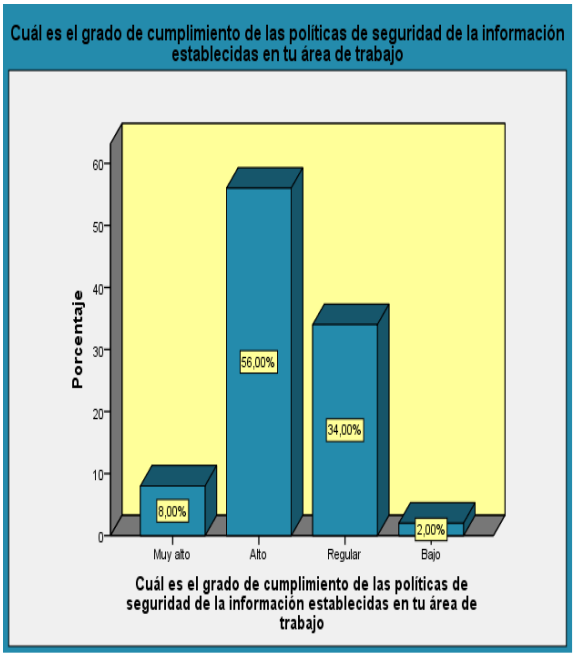
Análisis de los resultados: Del total de 43 encuestados el **72**% está **de acuerdo** que las políticas de seguridad implementadas realmente son efectivas para proteger su información.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **16%** con respecto a que los encuestados indican que están **de acuerdo** que las políticas de seguridad implementadas realmente son efectivas para proteger su información; esto se debe a que la implementación del algoritmo y las políticas de seguridad se complementan para una mejor protección de la información.

15. Cuál es el grado de cumplimiento de las políticas de seguridad de la información establecidas en tu área de trabajo.

Figura 58. Distribución porcentual grado de cumplimiento de políticas de seguridad





Fuente: Elaboración propia

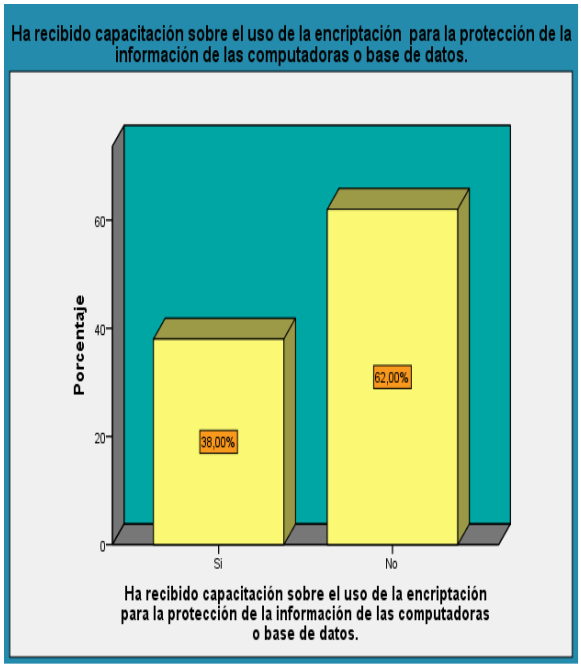
Análisis de los resultados: Del total de 43 encuestados el **46**% indica que el grado de cumplimiento de las políticas de seguridad de la información establecidas en su área de trabajo es **alto.**

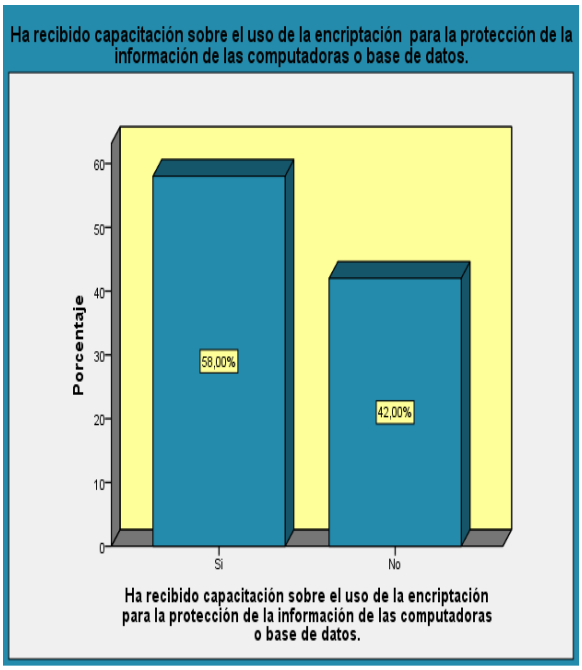
Análisis de los resultados: Del total de 43 encuestados el **56**% indica que el grado de cumplimiento de las políticas de seguridad de la información establecidas en su área de trabajo es **alto.**

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **10%** con respecto a que los encuestados indican que el grado de cumplimiento de las políticas de seguridad de la información establecidas en su área de trabajo es **alto**; esto se debe a que la implementación del algoritmo ha impulsado a tener que cumplir las políticas de seguridad de la información.

16. Ha recibido capacitación sobre el uso de la encriptación para la protección de la información de las computadoras o base de datos.

Figura 59. Distribución porcentual nivel capacitación recibida sobre encriptación





Fuente: Elaboración propia

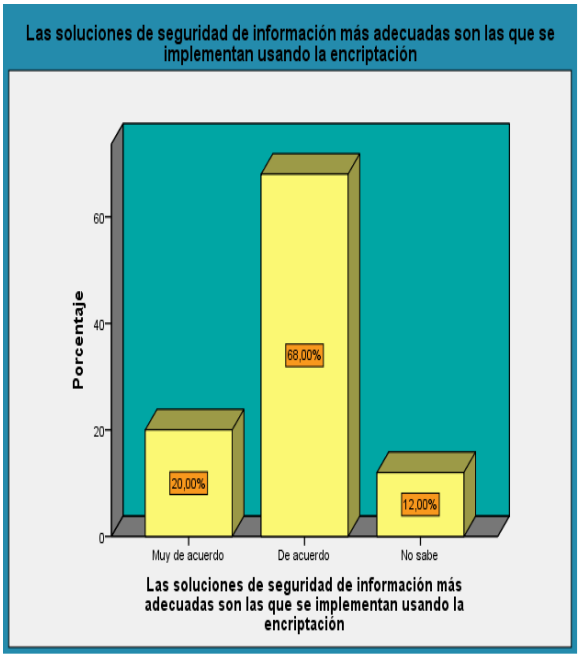
Análisis de los resultados: Del total de 43 encuestados solo el **38%** indica que **SI** ha recibido capacitación sobre el uso de la encriptación para la protección de la información de las computadoras o base de datos.

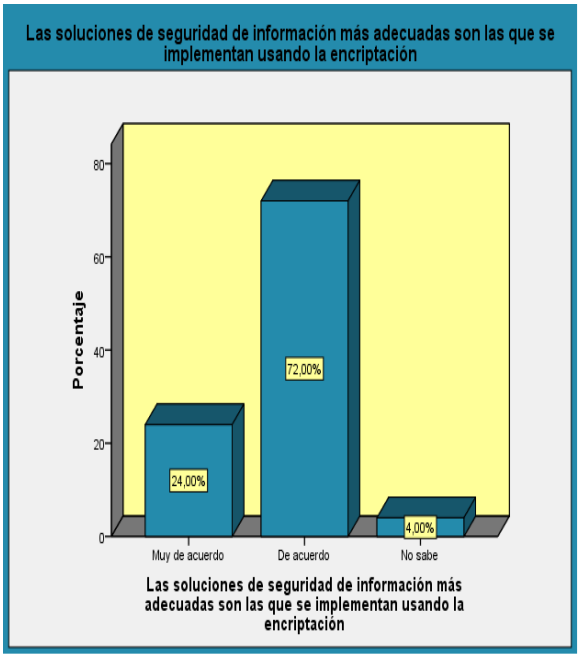
Análisis de los resultados: Del total de 43 encuestados el **58%** indica que ha recibido capacitación sobre el uso de la encriptación para la protección de la información de las computadoras o base de datos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **20%** con respecto a que los encuestados indican que han recibido capacitación sobre el uso de la encriptación para la protección de la información de las computadoras o base de datos; esto se debe a que con la implementación del algoritmo ha sido necesario capacitar y despertar el interés en los encuestados de aumentar sus conocimientos en temas relacionados a encriptación y medios de protección de la información.

17. Las soluciones de seguridad de información más adecuadas son las que se implementan usando la encriptación.

Figura 60. Distribución porcentual soluciones de seguridad





Fuente: Elaboración propia

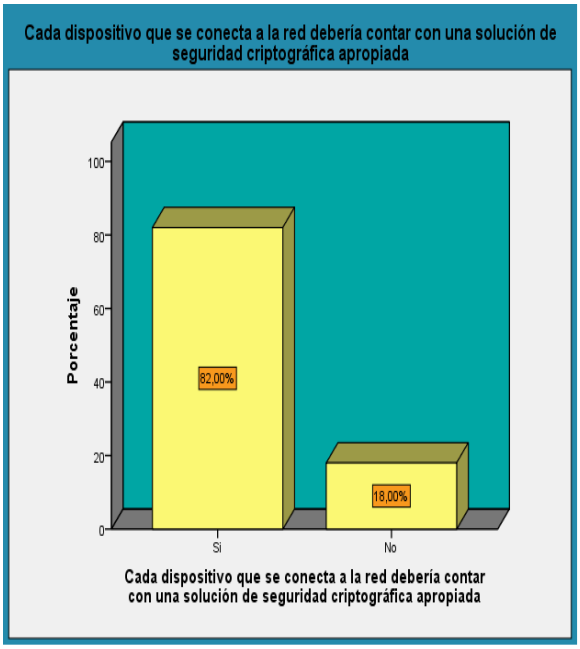
Análisis de los resultados: Del total de 43 encuestados el **68%** está **de acuerdo** que las soluciones de seguridad de información más adecuadas son las que se implementan usando encriptación.

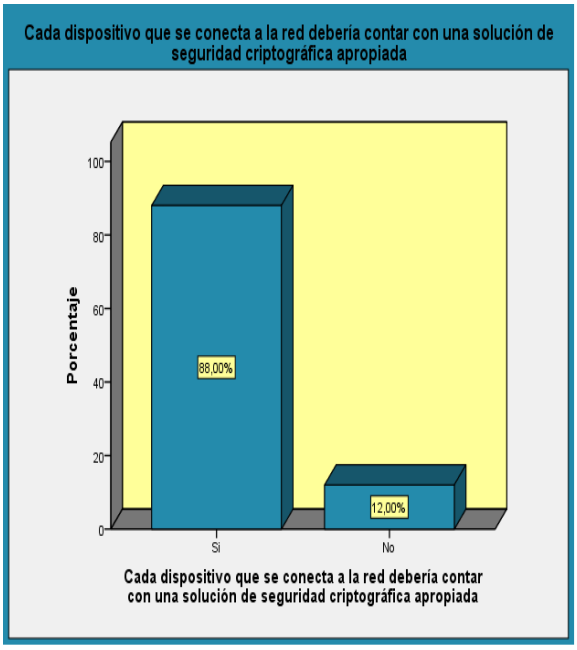
Análisis de los resultados: Del total de 43 encuestados el **72%** está **de acuerdo** que las soluciones de seguridad de información más adecuadas son las que se implementan usando encriptación.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados indican que están **de acuerdo** que las soluciones de seguridad de información más adecuadas son las que se implementan usando encriptación; esto se debe a que con la implementación del algoritmo han podido comprobar que la encriptación realmente ha mejorado la protección de la información.

18. Cada dispositivo que se conecta a la red de tu área de trabajo debería contar con una solución de seguridad criptográfica apropiada

Figura 61. Distribución porcentual solución de seguridad criptográfica





Fuente: Elaboración propia

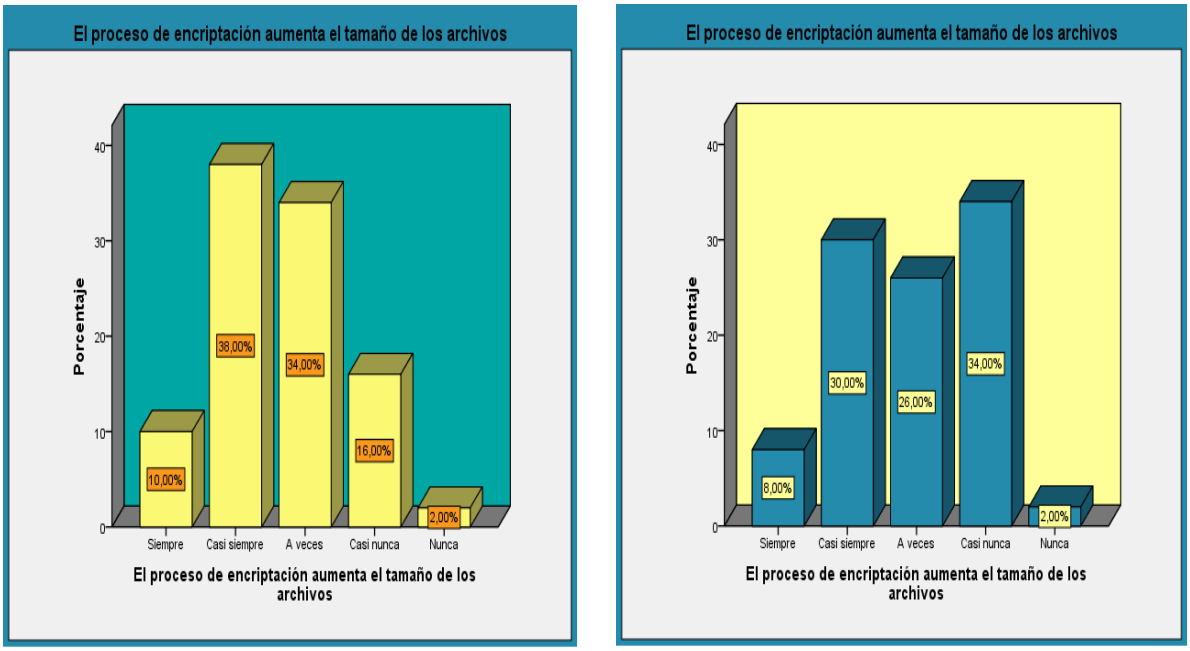
Análisis de los resultados: Del total de 43 encuestados el **82%** considera que todo dispositivo que se conecta a la red debe contar con una solución de seguridad criptográfica.

Análisis de los resultados: Del total de 43 encuestados el **88%** considera que todo dispositivo que se conecta a la red debe contar con una solución de seguridad criptográfica.

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **6%** con respecto a que los encuestados consideran que todo dispositivo que se conecta a la red debe contar con una solución de seguridad criptográfica; esto se debe a que la implementación del algoritmo cumple la función de proteger la información de los dispositivos que se conectan a la red.

19. Crees que el proceso de encriptación aumenta el tamaño de los archivos

Figura 62. Distribución porcentual efectos de la encriptación



Fuente: Elaboración propia

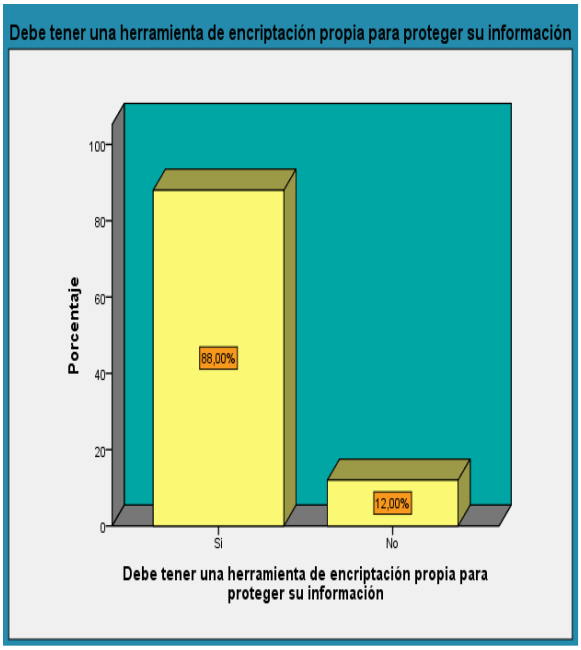
Análisis de los resultados: Del total de 43 encuestados el **38%** considera que el proceso de encriptación **casi siempre** aumenta el tamaño de los archivos

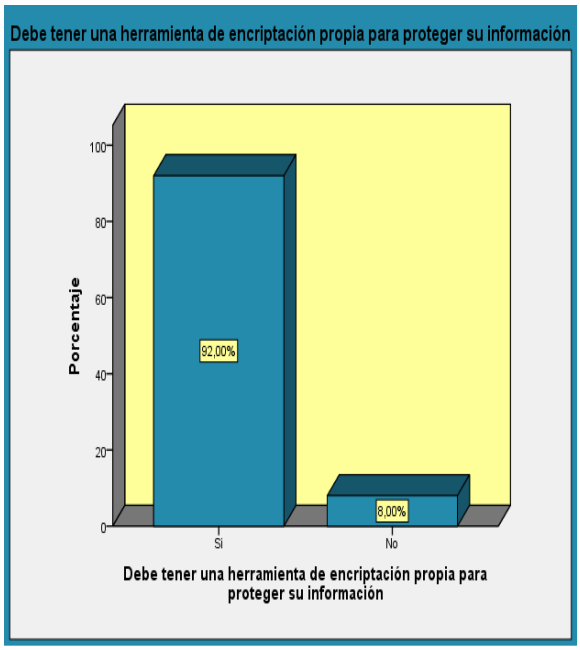
Análisis de los resultados: Del total de 43 encuestados el **30%** considera que el proceso de encriptación **casi siempre** aumenta el tamaño de los archivos

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **8%** con respecto a que los encuestados antes de la implementación del algoritmo consideraban que el proceso de encriptación **casi siempre** aumenta el tamaño de los archivos; pero se ha podido demostrar que después de la implementación del algoritmo el proceso de encriptación **casi nunca** aumenta el tamaño de los archivos.

20. Considera Ud. que se debe tener una herramienta de encriptación propia para proteger su información

Figura 63. Distribución porcentual uso de herramienta de encriptación propia





Fuente: Elaboración propia

Análisis de los resultados: Del total de 43 encuestados el **88%** considera que debe tener una herramienta de encriptación propia para proteger su información.

Análisis de los resultados: Del total de 43 encuestados el **92%** considera que debe tener una herramienta de encriptación propia para proteger su información

Se puede apreciar que al comparar los resultados antes y después de la aplicación del instrumento existe una variación del **4%** con respecto a que los encuestados consideran que deben tener una herramienta de encriptación propia para proteger su información; esto se debe a que la implementación del algoritmo propio ha permitido proteger mejor la información.

4.9 Prueba de hipótesis

Hipótesis 1

H0: La optimización del algoritmo Estándar de Encriptación Avanzada (AES) no incrementará la efectividad de la protección de la información.

H1: La optimización del algoritmo Estándar de Encriptación Avanzada (AES) incrementará la efectividad de la protección de la información.

Tabla 7. Prueba de rangos de Wilcoxon

Estadísticos de prueba[a]

	PostTest - PreTest
Z	-5,493[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

En esta tabla se muestran los rangos de Wilcoxon para la cantidad de información protegida con el uso de encriptación antes y después de la optimización del algoritmo.

De la tabla 7, se evaluó la significancia asintótica (bilateral), donde se observa que la significancia estadística es de 0.000 < 0.005, por lo que podemos afirmar que hay diferencias estadísticamente significativas entre las muestras relacionales (Pre-Test y Pos-Test), razón por la que se rechaza la hipótesis nula y se tiene que aceptar la hipótesis alterna (H1) donde indica que la implementación de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) incrementa la efectividad de la protección de la información.

Hipótesis 2

H0: La optimización e implementación del algoritmo Estándar de Encriptación Avanzada (AES) no aumentará el nivel de seguridad en la protección de la información.

H1: La optimización e implementación del algoritmo Estándar de Encriptación Avanzada (AES) aumentará el nivel de seguridad en la protección de la información.

Tabla 8. Prueba de rangos de Wilcoxon

Estadísticos de prueba[a]

	PosTest - PreTest
Z	-4,246[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

En esta tabla se muestran los rangos de Wilcoxon de la herramienta de encriptación utilizada para la protección de información protegida antes y después de la optimización del algoritmo.

De la tabla 8, se evaluó la significancia a sintótica (bilateral), donde se observa que la significancia estadística es <0.005, por lo que podemos afirmar que hay diferencias estadísticamente significativas entre las muestras relacionales (Pre-Test y Pos-Test), razón por la que se rechaza la hipótesis nula y se tiene que aceptar la hipótesis alterna (H1) donde indica que la implementación de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) aumentará el nivel de seguridad en la protección de la información.

4.10 Evaluación de la metodología de algoritmos estándar de Encriptación Prueba de hipótesis

Para evaluar la metodología se recurrió a tres expertos a fin de determinar la metodología pertinente para el desarrollo de la optimización del Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información, teniendo en cuenta los criterios respecto a cada metodología validada mediante la herramienta juicio de expertos (ver anexo 3). Asimismo, el resumen se puede evidencia en la siguiente tabla.

Tabla 9. Matriz de evaluación de las metodologías por los expertos

Expertos	Grados	AES	DES	T-DES
Blas Rebaza Maruja	Magister	27	21	18
Valenzuela Zegarra Anselmo	Magister	26	21	18
Cruz Tregear Luis	Ingeniero	26	24	18
Promedio		79	66	54

Fuente: Elaboración propia

Según la validación de expertos de la tabla 9, podemos determinar que la metodología escogida con mayor puntaje de 79 puntos es la AES de encriptación para la protección de la información.

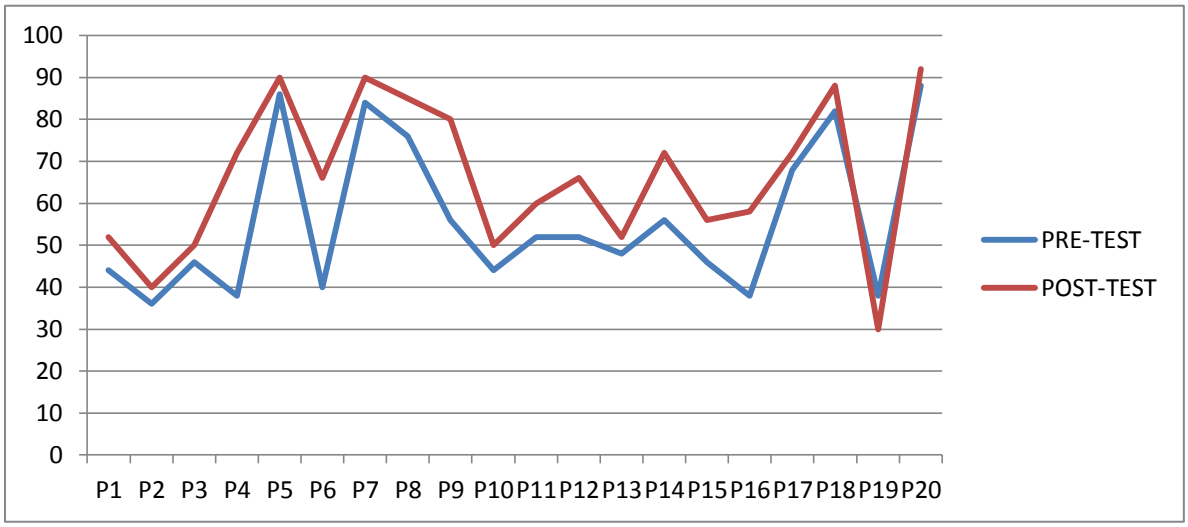
CAPÍTULO V

DISCUSIÓN DE LOS RESULTADOS

Los resultados de esta investigación son obtenidos al aplicar las técnicas con los instrumentos que se plantearon al inicio de este trabajo de investigación. Después de haber seguido un procedimiento sistemático usando Instrumentos de medición tipo encuesta a nuestra muestra obtenida de la población correspondiente a los Empleados de la empresa DIACSA, un total de 43 empleados (censado) la misma que se ha usado como muestra; Se realizó un cuestionario de 20 preguntas en dos etapas, una realizada antes de hacer la implementación de la optimización del algoritmo, y la segunda etapa se realizó después de la implementación de la optimización del algoritmo; estas preguntas están basadas en temas relacionados a obtener información de acuerdo a las variables y a los indicadores.

Para realizar la aplicación de los instrumentos se tuvo que hacer la implementación de la optimización del algoritmo de encriptación avanzada estándar a cada uno de equipos de cómputo de los empleados de la empresa DIACSA a los que se les dio instrucciones del empleo de dicho algoritmo para la protección de la información. Asimismo se capacito en temas relacionados encriptación y sus beneficios así como en temas relacionados a seguridad de la información.

Figura 64. Resultados Pre.Test y Post.Test



Fuente: Elaboración propia

Análisis de los resultados: Al hacer un análisis comparativo de los resultados obtenidos de la aplicación de los instrumentos se puede identificar que existe una variación significativa entre el Pres-test y el Post-test debido a que después de la implementación de nuestra optimización, y su

empleo existen indicadores que aumentan positivamente por ejemplo empleo y el nivel de conocimiento de la encriptación para la protección de la información y todo lo relacionado a la aplicación y cumplimiento de las políticas de seguridad de la información.

Para poder hacer esta implementación se hizo el análisis del algoritmo criptográfico AES para conocer sus fortalezas y debilidades hasta encontrar la manera de lograr su optimización y de esa manera lograr un algoritmo más seguro. Dentro de los cambios realizados para mejorar el algoritmo podemos mencionar que se tuvo que optimizar el programa del cifrado con en AES al momento de obtener los datos de la Caja S (S-BOXES) lográndose que sea más rápido debido a que la información que contiene la Caja S ya se encuentran definidos dentro del mismo programa y no tiene que hacer ningún cálculo matemático para su obtención algo que tomaría tiempo para lograr dicho calculo; también se hizo una variación del orden de la matriz del mixcolumns para darle mayor difusión al algoritmo obteniéndose resultados positivos en el cifrado y descifrado; por otro lado consideramos de gran importancia implementar un Generador de llaves Aleatorio dentro del algoritmo lo que le da un mayor nivel de seguridad además del tamaño de la llave que se use y la cantidad de rondas que se hayan implementado.

Con los resultados obtenidos de la aplicación de los instrumentos se pudo observar lo siguiente:

- Con la implementación de la optimización del algoritmo AES se incrementa la seguridad de la información.
- El aumento del nivel de seguridad se logró con la optimización del algoritmo
- Con la implementación de la optimización del algoritmo AES se incrementa la efectividad en la protección de la información.
- Se ha logrado aumentar los conocimientos de los de los empleados de la empresa DIACSA en temas relacionados a encriptación y medios de protección de la información
- Se ha podido comprobar que con la encriptación realmente ha mejorado la protección de la información.
- El algoritmo cumple la función de proteger la información de los dispositivos a los que se conectan a una red o dispositivos personales.
- Con la implementación del algoritmo se está protegiendo la información y se está cumpliendo las políticas de seguridad de la información establecidas

CONCLUSIONES

1. Se ha podido observar que al implementar la optimización del algoritmo AES se ha logrado aumentar los conocimientos de los de los empleados de la empresa DIACSA en temas relacionados a encriptación y medios de protección de la información porque han conocido el funcionamiento de un algoritmo de encriptación permitiendo de esa manera incentivarlos proteger la información y valorar la importancia del uso de herramientas de encriptación, por lo tanto después de esta investigación se ha podido comprobar la hipótesis general porque se ha logrado una **mejora en la protección** de la información.

2. Se ha podido comprobar que con la encriptación realmente ha mejorado la protección de la información debido a que la optimización del algoritmo cumple la función de proteger la información de los dispositivos a los que se conectan a una red o dispositivos personales porque al hacerse una optimización del algoritmo se ha hecho un algoritmo propio más fortalecido y funcional, que evita demoras por procesos de encriptación complejos, aumento del tamaño de archivo, etc. por lo tanto podemos comprobar una de las hipótesis especificas porque este nuevo algoritmo ha logrado un **aumentó en el nivel de seguridad** en la protección de la información.

3. Se ha podido comprobar una de las hipótesis especificas porque con la encriptación se **incrementa la efectividad** de la protección de la información debido a que con la implementación del algoritmo se está protegiendo la información y se está cumpliendo las políticas de seguridad de la información establecidas que consiste en el establecimiento de controles de acceso, uso de herramientas de protección de la información, nivel de cumplimiento de políticas de seguridad de información, etc.

RECOMENDACIONES

1. Se recomienda que para alcanzar una buena protección de la información se debe continuar capacitando al personal de empleados de la empresa DIACSA en temas relacionados a encriptación y medios de protección de la información porque con el conocimiento del funcionamiento de un algoritmo de encriptación, su importancia y empleo se podrá **mejorar la protección** de la información.

2. Se recomienda continuar revisando la optimización del algoritmo hasta obtener un algoritmo propio más fortalecido en diferentes partes del proceso de cifrado y descifrado para ser utilizado para proteger a todo tipo de dispositivos a los que se conecte y con este nuevo algoritmo se logre el **aumentó en el nivel de seguridad** en la protección de la información.

3. Se recomienda implementación de buenas políticas de seguridad de la información y una supervisión periódica del grado de cumplimiento de sus disposiciones debido a que se ha podido comprobar que con la encriptación se ha mejorado la protección de la información pero si se da cumplimiento efectivo de las políticas de seguridad de la información establecidas se obtendrá un **incremento de la efectividad** de la protección de la información.

4. Adicionalmente, es recomendable que los cambios que se hagan para obtener un algoritmo propio, una vez implementado en el algoritmo AES optimizado no sean de conocimiento público para mantener el grado y el nivel de seguridad que se le está dando.

REFERENCIAS BIBLIOGRAFICAS

1. Andina, Agencia Peruana de Noticias. https://andina.pe/agencia/. 14 de Junio de 2018. [Citado el: 12 de Marzo de 2019.] https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html.
2. POGGI, NICOLAS. Estadísticas de Seguridad Informática que Importan en el 2019. Buenos Aires : s.n., 2018.
3. Trayno, Vladlena. Ataque diferencial mediante inyección de un error en AES-128. España : s.n., 2016.
4. RAE. CRIPTOGRAFIA. España : s.n., 2018.
5. SIG, IEEE OC CyberSecurity. http://sites.ieee.org/ocs-cssig/?page_id=476. [En línea] 2016. [Citado el: 12 de febrero de 2019.]
6. wikipedia. https://es.wikipedia.org. [En línea] 16 de agosto de 2018. [Citado el: 10 de Febrero de 2019.] https://es.wikipedia.org/wiki/Algoritmo.
7. FAURA, Domingo. CRIPTOLOGIA: Criptografia y Criptoanalisis. Lima Peru : DESA S.A, 2004.
8. RAE. Real Academia de la Lengua Española. ESPAÑA : s.n., 2018.
9. wikipedia. https://es.wikipedia.org. [En línea] 8 de febrero de 2019. [Citado el: 11 de febrero de 2019.] https://es.wikipedia.org/wiki/Algoritmo.
10. Tecnología Educativa Revista CONAIC – ISSN: 2395-9061. Lic. Reyna García Belmont M. Gabriela Lotzin Rendón, Ing. Luis Cabrera Hernández. Del Consuelo Puente Pérez y Ing. Ofelia Verónica Méndez Lemus. Número 1, Mexico : s.n., Enero – Abril 2018, Vol. Volumen V.
11. Héctor Corrales Sánchez, Carlos Cilleruelo Rodríguez, Alejandro Cuevas Notario. Criptografía y Métodos de Cifrado. España : s.n., 2014.
12. CAPUÑAY Puican, Denys Ivan. Análisis Comparativo de Algoritmos Criptográficos para Redes Privadas Virtuales. Chiclayo - Peru : s.n., 2016.
13. FERNANDEZ Gonzalez, Hever - ICHPAS Gomez, Nerida - QUISPE Medina, James - SULCA Hermoza, Erick. Algortimo AES . Lima : s.n., 2015.
14. Johanna Beatriz MOYA Caza, Franklin Andrés ESCOBAR Erazo. Desarrollo de una Aplicación para Encriptar Información en la Transmisión de datos en un Aplicativo de Mensajeria Web. Quito : s.n., 2015.
15. Ojeda, Heber Gálvez. Análisis de algoritmos criptográficos en una red hibrida P2P. CHILE : s.n., 2014.
16. Facultad de Ingeniería, UNAM - Rubén Ramírez Cruz. https://criptografia.webnode.es. [En línea] 2015. [Citado el: 11 de febrero de 2019.] https://criptografia.webnode.es/algoritmos-asimetricos/.
17. TORRES, Juan Carlos Davila. "Análisis y Optimización del Algoritmo de Encriptación Rijndael el que se Basa el Estandar de Encriptacion Avanzada - AES. puno : s.n., 2017.
18. BACH. CORTÉZ Rodríguez, Amelia Ivon - BACH. SANTIAGO Cueva, Wilfredo Jhonatan. Plan de Seguridad Informática Basado en la Norma ISO 27002 para mejorar la gestión tecnológica. Trujillo : s.n., 2018.
19. NTP-ISO-27001. Sistema de Gestión de Seguridad de la Información . 2018.
20. RAE. Seguridad de la Informacion. ESPAÑA : s.n., 2018.
21. NTP-ISO/IEC17799. EDI. Tecnología de la información. 2ª Edición. LIMA : s.n., 2007.
22. NTP-ISO-27001. https://www.pmg-ssi.com/2018/12/iso-27001. [En línea] 20 de Noviembre de 2018. [Citado el: 13 de Febrero de 2019.] https://www.pmg-ssi.com/2018/12/iso-27001-en-que-se-basa-la-politica-de-seguridad-de-la-informacion/.
23. ISO/IEC 27000. Sistema de Gestión de Seguridad de la Información. 2014.

24. Santos Llanos, Daniel Elías. Establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la información, basado en la ISO/IEC 27001:2013. Lima: s.n., 2016.
25. PACHECO, Goyo Francisco Guzmán. Metodología para la seguridad de Tecnologías de Información y comunicaciones. Huancayo: s.n., 2015.
26. https://es.wikipedia.org/wiki/Cajas-S. [En línea] 11 de Enero de 2018. [Citado el: 10 de Marzo de 2019.]
27. API, Microsoft Programming reference for Windows. CryptGenRandom function. 2018.
28. Torre, Javier Martinez de la. Cifrado de clave privada: AES. 2015.

ANEXOS

ANEXO (1)

MATRIZ DE CONSISTENCIA
Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información

PROBLEMA	OBJETVO	HIPOTESIS	Variables	Indicadores	Metodología
Formulación del problema	**Objetivos**	**Hipótesis**			
Problema General ¿Cuál será la influencia de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información? **Problemas Específicos** ¿Cuál será el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para incrementar la efectividad de la protección de la información? ¿Cuál será el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para aumentar el nivel de seguridad en la protección de la información?	**Objetivo General** Implementar la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información. **Objetivos Específicos** Determinar cuál es el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para incrementar la efectividad de la protección de la información. Establecer cuál es el impacto de la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para aumentar el nivel de seguridad en la protección de la información.	**Hipótesis General** La optimización del algoritmo Estándar de Encriptación Avanzada (AES) mejorará la protección de la información **Hipótesis Específicas** La optimización del algoritmo Estándar de Encriptación Avanzada (AES) incrementará la efectividad de la protección de la información. La optimización del algoritmo Estándar de Encriptación Avanzada (AES) aumentará el nivel de seguridad en la protección de la información.	**Variable Independiente (X):** Algoritmo Estándar de Encriptación Avanzada (AES) **Variable Dependiente (Y):** La protección de la información **Dimensiones:** - Efectividad - Seguridad	**Efectividad** - Cantidad de información protegida - Políticas de seguridad establecidas - Frecuencia de uso de encriptación **Seguridad** - Herramientas de encriptación a usar - Nivel de conocimiento de herramientas de encriptación - Porcentaje cumplimiento de Políticas de seguridad establecidas	**Tipo de Investigación:** - Aplicada **Nivel de Investigación:** - Explicativo **Metodología de Desarrollo:** - Algoritmo Estándar de Encriptación Avanzada (AES) **Diseño de investigación:** - **Pre-**Experimental **Población:** - 43 empleados **Muestra**: - 43 empleados (censo) **Muestreo:** No aplica **Técnicas de Investigación y aplicación de instrumentos:** - Encuestas **Análisis e interpretación de datos:** - SPSS

ANEXO (2)

CUESTIONARIO

Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información

Objetivo: Implementar la optimización del algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información

INSTRUCCIONES: De las siguientes preguntas seleccionar una sola opción

Se agradece por su participación la cual es anónima y confidencial

1. Para Ud. la información que se procesa en el trabajo es lo más valioso que debe proteger con medios informáticos.

   Muy de acuerdo ☐ De acuerdo ☐ No sabe ☐ En desacuerdo ☐ Muy en desacuerdo ☐

2. Sabe Ud. que un ataque informático puede apropiarse de la totalidad de información, haciéndolo completamente inaccesible.

   Siempre ☐ Casi siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

3. Dentro de las medidas de seguridad que debe aplicar, considera que es importante el uso de algún medio informático para proteger la información de computadoras o base de datos.

   Muy importante ☐ Importante ☐ No sabe ☐ Poco importante ☐ No es importante ☐

4. Conoce algún programa informático para la protección de información de su computadora o base de datos.

   SI ☐ NO ☐

5. Ud. está de acuerdo que debe tener programas informáticos para proteger su información de su computadora o base de datos

   Muy de acuerdo ☐ De acuerdo ☐ No sabe ☐ En desacuerdo ☐ Muy en desacuerdo ☐

6. Dentro de su área de trabajo recibe capacitación para el empleo de una herramienta de protección de la información de su computadora o base de datos.

   Siempre ☐ Casi siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

7. Dentro de su área de trabajo han sido implementadas políticas de seguridad de la información.

   SI ☐ NO ☐

8. Existen controles de acceso para evitar perdida de información de las computadoras o base de datos.

   SI ☐ NO ☐

9. ¿Cuál es su nivel de conocimiento sobre la encriptación?

   Muy alto ☐ Alto ☐ Regular ☐ Bajo ☐ Muy bajo ☐

10. Sabe Ud. que un virus podría ingresar en tu computadora simplemente visitando una página de internet y llevarse tu información personal que no está protegida

Siempre ☐ Casi siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

11. En su área de trabajo se da cumplimiento a las políticas de seguridad establecidas para proteger la información.

Siempre ☐ Casi siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

12. Los controles de acceso a la información de las computadoras o base de datos son los adecuados para proteger su información.

Muy adecuado ☐ Adecuado ☐ No sabe ☐ Poco adecuado ☐ No es adecuado ☐

13. Cree Ud. que además de tener una buena política de copias de seguridad (backup), al encriptar la información más importante, conseguirás mantenerla a salvo.

Muy de acuerdo ☐ De acuerdo ☐ No sabe ☐ En desacuerdo ☐ Muy en desacuerdo ☐

14. Las políticas de seguridad implementadas realmente son efectivas para proteger su información.

Muy de acuerdo ☐ De acuerdo ☐ No sabe ☐ En desacuerdo ☐ Muy en desacuerdo ☐

15. Cuál es el grado de cumplimiento de las políticas de seguridad de la información establecidas en tu área de trabajo.

Muy alto ☐ Alto ☐ Regular ☐ Bajo ☐ Muy bajo ☐

16. Ha recibido capacitación sobre el uso de la encriptación para la protección de la información de las computadoras o base de datos.

SI ☐ NO ☐

17. Las soluciones de seguridad de información más adecuadas son las que se implementan usando la encriptación.

Muy de acuerdo ☐ De acuerdo ☐ No sabe ☐ En desacuerdo ☐ Muy en desacuerdo ☐

18. Cada dispositivo que se conecta a la red de tu área de trabajo debería contar con una solución de seguridad criptográfica apropiada

SI ☐ NO ☐

19. Crees que el proceso de encriptación aumenta el tamaño de los archivos

Siempre ☐ Casi siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

20. Considera Ud. que se debe tener una herramienta de encriptación propia para proteger su información

SI ☐ NO ☐

Fuente: Kelly Gabriela Bermúdez Molina y Edber Rafael Bailón Sánchez - Análisis En Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información - Guayaquil 2015

ANEXO (3)
EVALUACIÓN DE EXPERTOS - METODOLOGÍA DE DESARROLLO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO:

TÍTULO Y/O GRADO:
Doctor... ( ) Magister ( ) Ingeniero... ( ) Licenciado... ( ) Otros... ( )

Universidad que labora: Universidad Peruana los Andes

Fecha:
TÍTULO:

"Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información"

Autores: Simón Wilmer Mori Acero

Evaluación de Metodología de algoritmos Estándar de Encriptación

Mediante el empleo de la tabla de evaluación de expertos, Usted tiene opción de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones específicas al final de la tabla. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEMS	CRITERIOS	AES	DES	T-DES	OBSERVACIONES
1	Califique Ud. Como gestiona el trabajo en grupo las siguientes metodologías.				
2	Califique Ud. Como manejan la gestión de prioridades las siguientes metodologías.				
3	Califique Ud. Como manejan la orientación a la calidad las siguientes metodologías.				
4	Califique Ud. Como manejan el enfoque a usuarios las siguientes metodologías				
5	Califique Ud. Como manejan la documentación formal las siguientes metodologías.				
6	Califique Ud. Como utilizan los estándares de codificación las siguientes metodologías.				
	TOTAL				

FUENTE: Elaboración propia

Evaluar con la siguiente puntuación

1.- Muy Malo 2.- Malo 3.- Regular 4. Bueno 5. Muy bueno

Sugerencias:

_____

_____

_____
Firma del Experto

ANEXO (3)

EVALUACIÓN DE EXPERTOS - METODOLOGÍA DE DESARROLLO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Bias Reboza, Maruja

TÍTULO Y/O GRADO:

DOCTOR... ( ) Magister ... (✓) Ingeniero... ( ) Licenciado... ( ) Otros... ( )

Universidad que labora: Universidad Peruana los Andes

Fecha: 20/05/2019

TÍTULO:

"Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información"

Autores: Simón Wilmer Mori Acero

Evaluación de Metodología de algoritmos Estándar de Encriptación

Mediante la tabla de evaluación de expertos, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones específicas al final de la tabla. Asímismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEMS	CRITERIOS	AES	DES	T-DES	OBSERVACIONES
1	Califique Ud. Como gestiona el trabajo en grupo las siguientes metodologías.	5	3	4	
2	Califique Ud. Como manejan la gestión de prioridades las siguientes metodologías.	5	4	2	
3	Califique Ud. Como manejan la orientación a la calidad las siguientes metodologías.	4	4	3	
4	Califique Ud. Como manejan el enfoque a usuarios las siguientes metodologías	4	3	2	
5	Califique Ud. Como manejan la documentación formal las siguientes metodologías.	5	4	3	
6	Califique Ud. Como utilizan los estándares de codificación las siguientes metodologías.	4	3	4	
	TOTAL	27	21	18	

FUENTE: Elaboracion propia

Evaluar con la siguiente puntuación:

1.- Muy Malo 2.- Malo 3.- Regular 4. Bueno 5. Muy bueno

Sugerencias

_____

_____

Firma del Experto

Mg. Maruja Bias Reboza.

ANEXO (3)

EVALUACIÓN DE EXPERTOS - METODOLOGÍA DE DESARROLLO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: VALENWELA ZEGARRA, ANSELMO.

TÍTULO Y/O GRADO:

DOCTOR... ( ) Magister ... (X) Ingeniero... (X) Licenciado... ( ) Otros... ( )

Universidad que labora: Universidad Peruana los Andes

Fecha: 6/5/2019

TÍTULO:

"Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información"

Autores: Simón Wilmer Mori Acero

Evaluación de Metodología de algoritmos Estándar de Encriptación

Mediante la tabla de evaluación de expertos, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones específicas al final de la tabla. Asímismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEMS	CRITERIOS	AES	DES	T-DES	OBSERVACIONES
1	Califique Ud. Como gestiona el trabajo en grupo las siguientes metodologías.	5	4	3	
2	Califique Ud. Como manejan la gestión de prioridades las siguientes metodologías.	4	4	4	
3	Califique Ud. Como manejan la orientación a la calidad las siguientes metodologías.	3	4	2	
4	Califique Ud. Como manejan el enfoque a usuarios las siguientes metodologías	4	2	4	
5	Califique Ud. Como manejan la documentación formal las siguientes metodologías.	5	3	3	
6	Califique Ud. Como utilizan los estándares de codificación las siguientes metodologías.	5	4	2	
	TOTAL	26	21	18	

FUENTE: Elaboracion propia

Evaluar con la siguiente puntuación:

1.- Muy Malo 2.- Malo 3.- Regular 4. Bueno 5. Muy bueno

Sugerencias

Firma del Experto

ANEXO (3)

EVALUACIÓN DE EXPERTOS - METODOLOGÍA DE DESARROLLO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: CRUZ TREGEAR, LUIS HUMBERTO

TÍTULO Y/O GRADO:

DOCTOR... ( ) Magister ... ( ) Ingeniero... (X) Licenciado... ( ) Otros... ( )

Universidad que labora: Universidad Peruana los Andes

Fecha: 3/5/2019

TÍTULO:

"Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información"

Autores: Simón Wilmer Mori Acero

Evaluación de Metodología de algoritmos Estándar de Encriptación

Mediante la tabla de evaluación de expertos, Usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones específicas al final de la tabla. Asímismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEMS	CRITERIOS	AES	DES	T-DES	OBSERVACIONES
1	Califique Ud. Como gestiona el trabajo en grupo las siguientes metodologías.	4	4	3	
2	Califique Ud. Como manejan la gestión de prioridades las siguientes metodologías.	4	4	3	
3	Califique Ud. Como manejan la orientación a la calidad las siguientes metodologías.	5	4	3	
4	Califique Ud. Como manejan el enfoque a usuarios las siguientes metodologías	4	4	3	
5	Califique Ud. Como manejan la documentación formal las siguientes metodologías.	4	4	3	
6	Califique Ud. Como utilizan los estándares de codificación las siguientes metodologías.	5	4	3	
	TOTAL	26	24	18	

FUENTE: Elaboracion propia

Evaluar con la siguiente puntuación:

1.- Muy Malo 2.- Malo 3.- Regular 4. Bueno 5. Muy bueno

Sugerencias

Firma del Experto