FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Evaluación de la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

Autor:

Bach. Magallanes Carbajal Kenser

https://orcid.org/0000-0002-3269-0152

Asesor:

Mg. Tuesta Monteza Víctor Alexci

https://orcid.org/0000-0002-5913-990X

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel - Perú

2024

Aprobación del Jurado

Evaluación de la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana

_____

Bach. Magallanes Carbajal Kenser

Autor

_____

Dr. Tuesta Monteza Víctor Alexci

Asesor

_____ _____

Dr. Vásquez Leyva Oliver

Presidente de Jurado

Mg. Vidaurre Flores Miguel Angel

Secretario de Jurado

_____

Mg. Celis Bravo Percy Javier

Vocal de Jurado

Declaración jurada de originalidad

DECLARACIÓN JURADA DE ORIGINALIDAD

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

EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA

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

En virtud de lo antes mencionado, firma:

MAGALLANES CARBAJAL KENSER	DNI: 21869345	

Pimentel, 1 de marzo del 2024.

Dedicatoria

Este trabajo de investigación, está dedicado a mis seres amados, por su incondicional apoyo y aliento para concluir mis estudios de Ingeniería de Sistemas. En especial a mi padre Fernando Magallanes, pues me inspiró a esforzarme y a dar lo mejor de mí, para tener un futuro digno. Mi padre siempre me enseñó a soñar y a mirar el futuro con agrado, optimismo y así lograr mis metas a nivel profesional y personal.

Agradecimientos

Mi agradecimiento sincero desde lo más profundo de mi corazón a todas las personas que colaboraron en la realización de esta investigación y en especial a los que me alentaron a ser perseverante en los momentos difíciles, permitiéndome lograr el ansiado Título, que será muy preciado en mi vida profesional. También, gracias a Dios por poner en mi camino a un valioso ser humano que suma mucho en mi vida y por su apoyo incondicional.

A nuestro Profesor Ing. Heber Iván Mejía Cabrera, por sus sabias enseñanzas, paciencia, valía y entrega.

Índice

Índice de figuras

Índice de tablas

Índice de anexos

Resumen

En la actualidad el 60% de las empresas financieras del Perú, requieren de mayores recursos, capacidad técnica competente e infraestructura suficiente para implementar un sistema de encriptación que cumpla con altos niveles de seguridad. Por tal motivo, en esta investigación se evaluó 2 algoritmos de encriptación de datos, AES y 3DES con la finalidad de identificar el algoritmo más eficiente, accesible y que cumpla con los niveles adecuados de seguridad. Los algoritmos se implementaron con un lenguaje de programación de alto nivel PHP empleando el IDE XAMPP y se desplego en un servicio web administrado por CPANEL, se ejecutaron 10 encriptaciones calculando cada uno de los indicadores, en igualdad de condiciones. En rendimiento de cifrado AES obtuvo entre 79349638.10 y 5573227923.77 mientras que 3DES obtuvo entre 13256998.00 y 874527893.43, siendo así, AES logro mejor rendimiento de cifrado. En rendimiento de descifrado, AES obtuvo entre 63469558.83 y 6058449389.84 mientras que 3DES obtuvo entre 12516396.93 y 5139798302.58, siendo así, AES alcanzo mejor rendimiento de descifrado. En consumo de memoria RAM, AES obtuvo entre 0.000732 y 0.000709 mientras que 3DES obtuvo 0.000717, siendo así, AES obtuvo menor consumo de memoria RAM. En consumo de CPU, AES obtuvo entre 0.0001019 y 0.0000000 mientras que 3DES obtuvo entre 0.0012298 y 0.0000000, siendo así, AES obtuvo menor consumo de CPU. En integridad AES obtuvo 100% y 3DES obtuvo entre 100% y 99.99%, siendo así, AES supero en integridad a 3DES. En fortaleza AES obtuvo 100% mientras que 3DES obtuvo 83.3%, siendo así, AES es más fuerte que 3DES. Finalmente, el algoritmo AES para todas las mediciones cumple con la eficiencia criptográfica y seguridad de datos para una empresa financiera peruana.

Palabras Clave: clave criptográfica, criptografía, algoritmo AES, algoritmo 3DES, eficiencia, seguridad, empresa financiera peruana.

Abstract

Currently, 60% of financial companies in Peru require greater resources, competent technical capacity and sufficient infrastructure to implement an encryption system that meets high levels of security. For this reason, in this research, 2 data encryption algorithms were evaluated, AES and 3DES in order to identify the most efficient, accessible algorithm that meets the appropriate security levels. The algorithms were implemented with a high-level programming language PHP using the XAMPP IDE and deployed in a web service managed by CPANEL, 10 encryptions were executed calculating each of the indicators, under equal conditions. In encryption performance, AES obtained between 79349638.10 and 5573227923.77 while 3DES obtained between 13256998.00 and 874527893.43, thus, AES achieved better encryption performance. In decryption performance, AES obtained between 63469558.83 and 6058449389.84 while 3DES obtained between 12516396.93 and 5139798302.58, thus, AES achieved better decryption performance. In RAM memory consumption, AES obtained between 0.000732 and 0.000709 while 3DES obtained 0.000717, thus, AES obtained lower RAM memory consumption. In CPU consumption, AES obtained between 0.0001019 and 0.0000000 while 3DES obtained between 0.0012298 and 0.0000000, thus, AES obtained lower CPU consumption. In integrity, AES obtained 100% and 3DES obtained between 100% and 99.99%, thus, AES surpassed 3DES in integrity. In strength AES obtained 100% while 3DES obtained 83.3%, thus, AES is stronger than 3DES. Finally, the AES algorithm for all measurements meets cryptographic efficiency and data security for a Peruvian financial company.

Keywords: cryptographic key, cryptography, AES algorithm, 3DES algorithm, efficiency, security, financial company.

I. INTRODUCCIÓN

1.1. Realidad problemática

Es preciso comenzar diciendo que la criptografía está relacionada con el origen de la humanidad y con la sobrevivencia del hombre, debido a que no sólo la alimentación fue indispensable en esta etapa, sino también la comunicación, a su vez, con la comunicación nace la necesidad de ocultar o clasificar información importante y confidencial para conocimiento de ciertos miembros con exclusividad o con altos privilegios dentro de una comunidad.

Ahora bien, la finalidad de la criptografía en sus inicios era mantener una comunicación confidencial entre dos personas, agregándose ciertas reglas con la intención que la información sea incomprensible para el resto de personas. Así mismo, aproximadamente hace cuatro mil años atrás un hombre egipcio escribió la historia de una persona dando detalles inéditos y reservados utilizando jeroglíficos, la técnica de sustitución, y así se dio el inicio a la criptografía. [1]

De modo similar, el vocablo criptografía es definido por la real academia de la lengua española de la siguiente manera “El arte de escribir con clave secreta o de un modo enigmático”.

Bajo este contexto, la criptografía moderna comienza mientras se llevaba a cabo la segunda guerra mundial cuando Alan Turing con la colaboración de un grupo de expertos se desarrolló el proyecto ULTRA, que básicamente era descifrar mensajes del ejército alemán. Turing y su equipo crearon una máquina llamada ENIGMA para cifrar y descifrar información utilizando el cifrado Lorenz. Por otro lado, esta información recién fue expuesta en los años 70. [2]

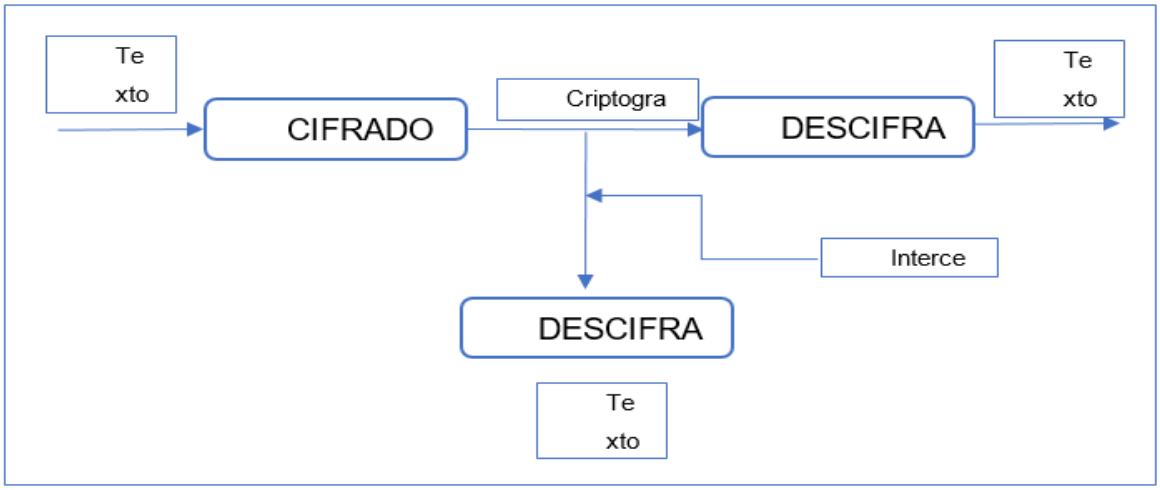
Actualmente, la criptografía es el estudio de técnicas matemáticas estrechamente

relacionados con los números primos y con los sistemas matemáticos hexadecimal, BCD y binario con el propósito primordial de mantener la precisión, coherencia, confidencialidad y privacidad de los paquetes o bloques de datos que se encuentran en las diferentes redes, para ello es necesario que existan llaves de encriptación y des-encriptación desde el inicio hasta el destino final con el objetivo de evitar los ataques en la información.

Por otra parte, el crecimiento exponencial del uso del internet por parte de los usuarios, ha llevado a la necesidad de proteger la información sensible o confidencial. Como sabemos, Internet nos permite intercambiar información y ejecutar una serie de operaciones comerciales como las transacciones financieras, actualmente estas operaciones circulan través de las redes, utilizando accesos en línea y de forma automática, es decir sin interacción presencial o física, y por ello se hace más fácil que pueda ser atacada, filtrada y malversada. Por esta razón, asegurar la información se hace imperativo y qué mejor a través de la criptografía que enmascara los mensajes. [1]

En el esquema siguiente de un procedimiento criptográfico de cifrado y descifrado, como se muestra en la siguiente gráfica.

Figura 1. Modelo de cifrado y descifrado. Fuente: Maiorano (2009).



Fuente: Elaboración propia

Dicho lo anterior, revisamos el análisis del año 2020 publicado por la OEA con la colaboración del BID cuyo título es “Ciberseguridad: Riesgos, avances y el camino a seguir en américa latina y el caribe”, exponiéndose que en los últimos años los ciberataques se han incrementado sobre todo en las entidades financieras de la región Latinoamérica, el incremento de las transacciones en línea a causa de pandemia que vivimos desde enero 2020 ha evidenciado bajos niveles de seguridad en muchos países de la región. Para ilustrar mejor, el indicador de fraudes en las operaciones bancarias ha aumentado en 7.8% comparado con las variaciones normales que mantiene del sector financiero, esto debido a la gran cantidad de usuarios inexpertos que descubren las bondades del internet o activan cuentas por primera vez, siendo el mayor número de usuarios los adultos mayores, estos nuevos usuarios con poco o casi nada de conocimiento en seguridad informática, incrementan el nivel de riesgo y se convierten en potenciales clientes de los atacantes. [3]

Del mismo modo, en el último año los usuarios que fueron atacados necesitaron tener conocimientos básicos en ciberseguridad con el objeto de evitar repetir ataques o estafas en línea según las estadísticas se ha incrementado de 20 a 100 los usuarios que buscan este tipo de información, por otra parte, otro grupo de usuarios son quienes ya tomaron conciencia del riesgo y desean aprender o profundizar el tema. [3]

Por otro lado, el Perú ha mostrado un lento avance en seguridad informática a nivel estratégico, sin embargo, a nivel normativo ha publicado varias leyes, pero en julio del 2017 recién la Ley N.º 30618 introduce el término de seguridad digital como “confianza en situaciones de un entorno totalmente digital, de cara a las amenazas frente a la infraestructura y capacidades nacionales, a través de la ciberseguridad y la gestión de riesgos en ciberdefensa, aumentando los objetivos del Estado”. [3]

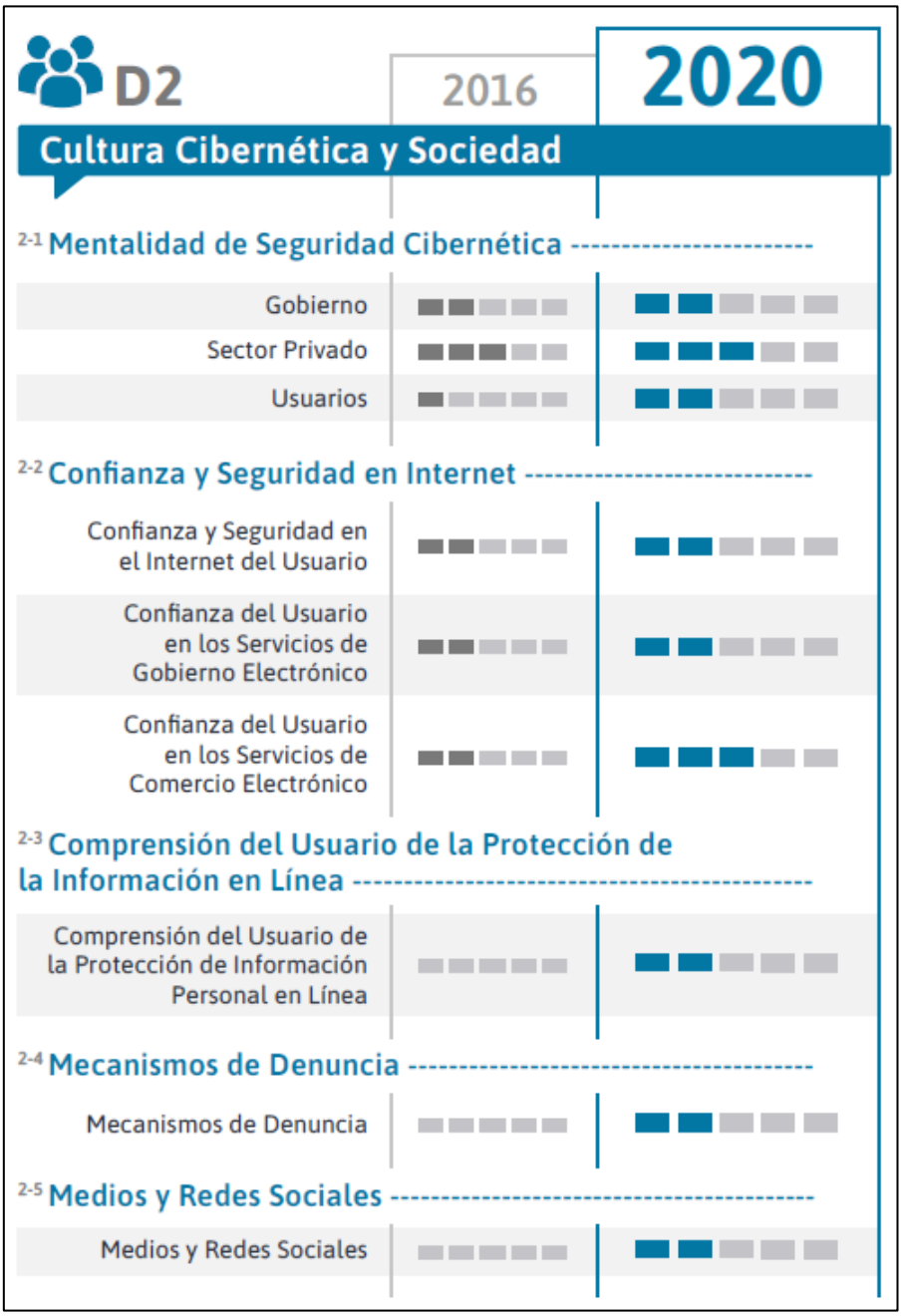
Al respecto, los siguientes cuadros comparativos a nivel Perú del año 2016 y el año 2020 de la política y estrategia de seguridad cibernética D1, así como de la Cultura cibernética

en la sociedad D2, se aprecia en el cuadro D1 un avance mínimo en manejo de crisis y redundancia de comunicaciones, mientras que el cuadro D2 presenta un avance mayor en lo referente al punto 2-3 entendimiento de los usuarios de salvaguardar la información en la redes, al punto 2-4 mecanismos o herramientas para poner denuncias y al punto 2-5 relacionado al uso de plataformas sociales.

Figura 2. Comparación del año 2016 y el 2020 respecto a las políticas y estrategias de seguridad informática en el Perú. Fuente: OEA (2020).

Fuente: OEA (2020).

Figura 3. Comparación del año 2016 y el 2020 respecto cultura cibernética y sociedad en el Perú. Fuente: OEA (2020).



Fuente: OEA (2020).

Ahora bien, en el siguiente cuadro comparativo a nivel Perú del año 2016 y el año 2020, en cuanto a la Formación, capacitación y habilidades de seguridad cibernética D3, Estándares, organizaciones y Tecnologías D5. Con respecto a las variables presentadas cuadro D3 se aprecia constante sin cambios para ambos años, situación opuesta que muestra

el cuadro D5 debido que se ha mejorado cuatro variables relacionadas con calidad, control y estándares de seguridad.

Figura 4. Comparación del año 2016 y el 2020 respecto a la Formación, capacitación y habilidades de seguridad cibernética en el Perú. Fuente: OEA (2020).

Fuente: OEA (2020).

Figura 5. Comparación del año 2016 y el 2020 respecto a los estándares organizaciones y tecnologías en el Perú. Fuente: (OEA, 2020).

Fuente: OEA (2020).

Prosiguiendo, en el siguiente cuadro comparativo a nivel Perú del año 2016 y el año 2020, con respecto a los Marcos legales y regulatorios D4. Este comparativo presenta un gran avance en cuanto a los marcos legales garantizando la información en distintos niveles

y avances en acuerdos para combatir delitos cibernéticos.

Figura 6. Comparación del año 2016 y el 2020 respecto a los marcos legales y regulatorios en el Perú. Fuente: OEA (2020).

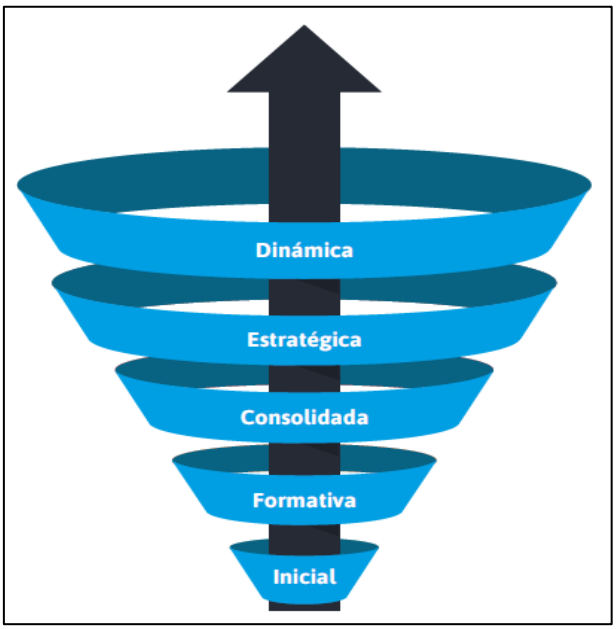
Fuente: OEA (2020).

Ahora bien, en relación a delitos cibernéticos se estima que para finales del 2021 los daños ascienden a varios billones de dólares americanos, para tener una idea de la magnitud esto podría equivaler al PBI de Japón que una de las principales potencias económicas, estas noticias son alarmantes, es por ello que el 50% de la población de la región desconfía de las operaciones en línea prefiriendo hacer sus compras de la forma tradicional, es decir, adquirir

bienes o servicios de manera presencial. Con la intención de conocer el crecimiento de la seguridad informática en los países latinoamericanos veamos el modelo de madurez en ciberseguridad elaborado por un grupo de especialistas de distintos países liderado por una conocida universidad del reino unido llegando al siguiente resultado [3].

a. Inicial: en este nivel no hay madurez de ningún tipo.
b. Formativa: en este nivel se ha comenzado a formular la iniciativa, pero aún está mal definida.
c. Consolidada: en este nivel se tiene indicadores instalados aun funcionando
d. Estratégica: en este nivel se está tomando decisiones respecto a los resultados de los indicadores
e. Dinámica: en este nivel hay mecanismos claros de alertas respecto a las amenazas, también hay métodos para cambiar los procedimientos y las estrategias.
f. A continuación, la representación gráfica de los niveles de madurez.

Figura 7. Nivel de madurez en ciberseguridad. Fuente: OEA (2020)



Fuente: OEA (2020)

Definitivamente, es importante la implementación de procedimientos y controles que permitan subir el nivel de seguridad, como por ejemplo aplicando algoritmos de encriptación para información confidencial o sensible.

Para mejor entendimiento, en los 2 últimos años durante la pandemia que actualmente vivimos en nuestro país, se han creado nuevas modalidades de robo cibernético como, por ejemplo, envió de mensajes de texto a los clientes que son titulares de cuentas bancarias del banco BBVA con la finalidad de mover dinero entre cuentas bancarias que los usuarios nunca han ejecutado. Las denuncias por estas transacciones fraudulentas rodean los S/ 2,500 soles por transacción [4]

Actualmente existen diversas soluciones de ingeniería en seguridad informática aplicando criptografía, pero hay una pregunta que siempre nos hacemos sobre todo en las empresas y los sectores que son propensos a recibir ataques ¿Cuándo un algoritmo de encriptación es seguro? y la respuesta en el sentido estricto es NUNCA. Pues no existe un indicador que determine la seguridad/no seguridad de un algoritmo de encriptación, sólo se puede estimar niveles de seguridad o elevar el grado de seguridad existente. A su vez, cuando los algoritmos de encriptación se han roto deberían quedar inutilizables, debido a que ha sido descrito por otro usuario no autorizado.

Dicho lo anterior, nuestro sistema bancario peruano como la banca comercial y de ahorros han implementado ciertas acciones para maximizar el nivel de confianza de las transacciones en línea de sus clientes, para ello han puesto a disposición distintas herramientas como por ejemplo certificados autorizados para firmas digitales con vigencia, tokens virtuales con reconocimiento facial, token con claves secretas y notificaciones confirmando compras en línea. Estas medidas han permitido reducir las pérdidas económicas que ocasionan los delitos cibernéticos.

Para tal efecto, la criptografía es el único método comprobado que ofrece protección

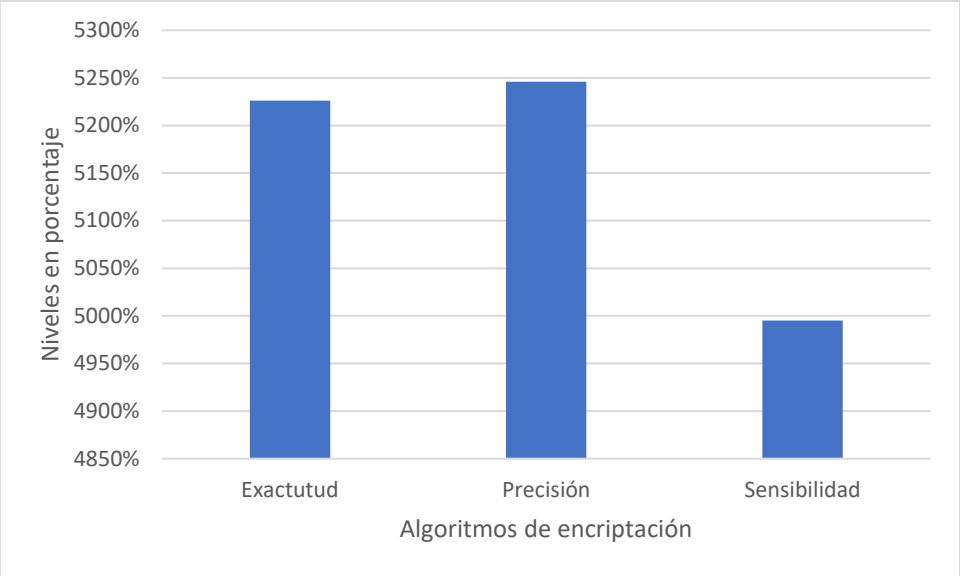
eficaz para los datos transaccionales que circulan o se ejecutan diariamente en línea, debido que garantiza altos niveles de seguridad, además de reforzar los niveles básicos de seguridad, permitiendo a ciertos sectores o empresas la posibilidad de crear, potencializar o implementar su propia metodología y estándar. [5]

Así mismo, debido al crecimiento de las operaciones bancarias realizadas en las redes y en parte, impulsado por la pandemia que estamos viviendo, la mayoría de los algoritmos criptográficos ya han sido rotos y muchos que actualmente se consideran seguros están próximo a ser descifrados, es por eso que muchos investigadores están llevando a cabo pruebas y desarrollos con base en la computación cuántica en combinación con procesadores TTA, RISC-V simulando protocolos y procedimientos cuánticos. [6]

Recientemente, una investigación sobre cómo mejorar un algoritmo criptográfico con la estenografía en imágenes llegó a la conclusión que la criptografía y la estenografía se complementan en gran medida debido que tienen como base la seguridad informática, es decir, una encripta los mensajes, pero la otra la oculta, por separado no ayuda mucho, sin embargo si se combina se incrementa en gran medida el nivel de seguridad del mensaje [7]

Denys Ivan Capuñay Puican [8] realizó una investigación sobre algoritmos criptográficos para redes privadas virtuales llegando a la conclusión que el algoritmo de encriptación AES sobresalió con respecto a 3DES y DES debido que AES fue mejor en cuanto a tiempo de envío, también fue superior para la encriptación de paquetes y finalmente en la encriptación de paquetes en número, el protocolo que utilizó fue IPSec con pruebas en redes virtuales de tipo VPN.

Figura 8. Evaluación por el número de paquetes generados.



Fuente: Capuñay (2016).

En efecto, la ingeniería ha llegado muy lejos en lo que respecta a investigaciones en criptografía, este año 2021 Vaibhavi L. en su investigación usó criptografía en la autenticación de usuarios por medio de señales cerebrales, es decir, el cerebro humano está formado por millones de células que a la vez se comunican mutuamente a través de las neuronas e impulsos magnéticos y hasta ahora ha sido imposible recolectar esta información de manera individual, sin embargo, en esta investigación logró una autenticación biométrica que recopila las ondas y señales del cerebro para luego con esta información crear nuevas claves criptográficas dependiendo del estados en que se encuentra el cerebro. Los resultados de esta investigación han revolucionado y generado interés en la comunidad científica, por lo que esta investigación continuará. [9]

Una investigación similar a la anterior, utilizó el ADN para generar claves criptográficas, esta propuesta permite mejorar las claves criptográficas intercambiando el algoritmo genético y el algoritmo Diffie-Helman. Concluyendo que se puede generar claves utilizando la secuencia de ADN, siendo el algoritmo genético indispensable para tal fin. [10]

Por consiguiente, la presente investigación se suma a las demás investigaciones ya existentes con en el propósito de mejorar la seguridad de las transacciones comerciales y financieras que se llevan a cabo a través de la red, buscando incrementar la seguridad en la región, muy a pesar de las políticas, leyes, reglamentaciones y estándares ya existentes, incluso a pesar, que algunas empresas han adoptado e implementado, los robos cibernéticos siguen en gran aumento, la responsabilidad no sólo recae en los usuarios finales, también en los comercios y las pymes que comparten la responsabilidad, y es ahí donde se deben implementar herramientas de seguridad en criptografía, sin embargo muchas veces estas no están al alcance de las pequeñas o microempresas por el alto costo de inversión que representan, sin embargo existen alternativas como algoritmos de encriptación de libre uso que requieren una evaluación previa antes de su implementación con el fin de garantizar el nivel de seguridad requerida. En esta investigación, tomaremos sólo 2 algoritmos de encriptación AES y 3DES y evaluaremos cuál de ellos cumple con los niveles de seguridad que una empresa de recursos limitados necesita en el Perú, se ha considerado estos algoritmos pues se utilizan en todo el mundo por su funcionamiento, capacidad de encriptación y fiabilidad, es decir, se encargan de cifrar texto y aceptan claves en las siguientes dimensiones 128, 192 y 256 bits. [11]

Respecto a esta problemática, se han desarrollado varias investigaciones a nivel internacional entre las cuales se tienen:

En [12] en Anhui, China, emprendió la investigación “Application of AES and DES Algorithms in File Management”. En los últimos años, con el vertiginoso avance de la tecnología informática y de redes, numerosas empresas e instituciones de renombre han progresivamente adoptado el uso de computadoras para sus actividades de oficina, y los documentos electrónicos han ido reemplazando paulatinamente a sus equivalentes en formato papel. Información crucial para las empresas, como los datos de los clientes, se almacenan en sistemas informáticos en forma de archivos electrónicos. Si bien la integración

de computadoras en los procesos de oficina ha brindado una serie de beneficios, como una mayor eficiencia y una utilización más eficaz de los recursos, también ha generado desafíos en términos de seguridad de la gestión de documentos electrónicos. Por ejemplo, el riesgo de filtración de información se ha incrementado significativamente, y el personal de oficina corre el riesgo de ocasionar daños irreversibles a los documentos electrónicos debido a errores en sus operaciones. Por esta razón, se abordó la situación actual en la gestión de seguridad de documentos electrónicos como contexto de investigación, y se logró proponer una solución para abordar esta problemática de manera efectiva mediante una estrategia que fusionó la teoría técnica de gestión de archivos con el algoritmo de cifrado AES, y que a su vez incorpora el principio teórico de gestión de archivos en conjunción con el algoritmo de cifrado DES. Este enfoque aprovecha las particularidades de la gestión de archivos para subsanar las deficiencias inherentes a los algoritmos AES y DES, con el objetivo de lograr un cifrado más eficaz y robusto, y de esta forma mejorar la resistencia ante intentos de descifrado. Los resultados obtenidos evidenciaron que, DES es mejor algoritmo en cuanto a cifrado obteniendo un +24.58% y en cuanto a descifrado obteniendo un +27.49%. Cuando se utilizan archivos de subida cifrados, el algoritmo de cifrado AES es ligeramente más rápido que el DES. Se concluyó que, desde el punto de vista de la experiencia del usuario, el mayor tiempo de carga debido al cifrado sigue siendo aceptable.

Mohamed Elhoseny [13], realizó una investigación en la India denominado “Hybrid optimization with cryptography encryption for medical image security in Internet of Things” by Faculty of Computers and Information, Mansoura University, Mansoura, Egypt, School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, India. Esta investigación presentó un modelo criptográfico estratégico innovador y optimizado para la seguridad de las imágenes médicas, debido a que toda la información de las historias clínicas se almacena en la nube. Para tal fin, se utilizó el equipo MATLAB 2016 con un procesador i5 y 4GB de RAM cuyos resultados de los pacientes se almacenaron en la nube para luego ser

descargados de manera encriptada y analizada descartando distorsiones, la muestra utilizada fueron escaneos del cerebro, glaucoma, pulmones y de células cancerígenas. Para la encriptación de las muestras se utilizaron los algoritmos AES y DES teniendo una variación de 0.5% de diferencia en tiempo de CPU consumido en la descarga de la nube con distorsión nula. Con respecto a la técnica se consideró algoritmo de cifrado híbrido mejorando el método, este es, de uso multinacional en cuanto a la decodificación y con ello siempre se obtiene el mensaje correcto, a la vez, el algoritmo uso poca memoria esto ocurrió porque la imprevisibilidad financiera fue en menor cantidad. Por otro lado, se evidenció que este procedimiento es inseguro pues no demostró impalpabilidad y se concluye que deben hacerse más investigaciones para elevar la seguridad de forma focalizada y buscando subir el nivel de integridad.

BahmanA. Sassani Sarrafpour [14], realizó una investigación en Nueva Zelanda denominado “Evaluating Encryption Algorithms for Sensitive Data Using Different Storage Devices” by Department of Computer Science, Unitec Institute of Technology, Auckland, New Zealand, Department of Computer Science, National University of Computer & Emerging Sciences, Islamabad, Pakistan, School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand. Esta investigación analizó la seguridad de la información confidencial utilizando algoritmos de encriptación en los dispositivos de almacenamiento como SSD, HDD y SSHD a través de una configuración experimental, para lograr este objetivo se implementó un ambiente de pruebas con los dispositivos de almacenamiento HDD, Seagate SSHD y Samsung 128 GB flash MLC SSD se comparó las variables de velocidad al escribir y leer en los medios de almacenamiento y en patrones diferentes de 4MB aleatoria, 4k y secuencial 4MB, las pruebas se llevaron a cabo hasta 10 veces y durante esta etapa el dispositivo HDD utilizó un archivo de 500GB, 16 de chache obteniendo una velocidad de 6 Gb/s max, mientras que para el dispositivo SSHD se utilizó un archivo de 1GB y 64 de caché obteniendo una velocidad de 600 MB/S max, para

ambos se utilizó una interfaz SATA III 6 Gb/s. Además los algoritmos utilizados fueron de cifrado simétrico en 3 dispositivos de almacenamiento HDD, SSHD y NAND MLC, en el caso de BestCrypt es un software de cifrado y TrueCrypt es un software cifrado de código abierto y a los 3 dispositivos se les aplicó los algoritmos de encriptación AES, Serpent y Twofish de 256 bits y se usó los software BestCrypt y TrueCrypt, dando como resultado los algoritmos AES, Serpent y Twofish de 256 bits tienen mejor rendimiento con HDD utilizando el software TrueCrypt mostrando un mejor rendimiento que BestCrypt. Sin embargo, BestCrypt tiene un mejor rendimiento con los algoritmos AES, Serpent y Twofish de 256 bits y el dispositivo SSHD y flash NAND MLC demostrando que AES y Twofish 256 bits siempre tiene un mejor rendimiento utilizando BestCrypt y TrueCrypt. Finalmente, el rendimiento varía dependiendo del dispositivo utilizado en combinación con los algoritmos de encriptación.

Franyelit María Suárez [15], realizó una investigación en Ecuador denominada "Seguridad para aplicaciones con múltiples usuarios" en Facultad de Ingeniería y Ciencias Aplicadas, Universidad de las Américas Quito, Ecuador. Este estudio analizó la protección de la información y datos sensibles en los sistemas de informáticos en un escenario de usuarios múltiples, es decir, un algoritmo asegura la privacidad de la información en aplicaciones web con usuarios múltiples o en sesiones de colaboración además demuestra que la encriptación no interfiere en el comportamiento de la aplicación, bloqueando usuarios sin permiso de acceso, así mismo los usuarios puede estar conectados modificando el documento compartido en forma simultánea. Esta investigación fue realizado con un algoritmo que a la vez usa las características de Chrome, también compatible con FireFox, en ambos casos la encriptación y la desencriptación se da por medio de un carácter a la vez dando como resultado que los datos se insertan antes de la construcción del documento mediante un encriptado de una overrideFunction, para esto, se utilizó Google Docs para iniciar con la carga de salida, un script sobrescribiendo XMLHttpRequest.send, carga de entrada XMLHttpRequest.open descifra el contenido inicial, posteriormente, la carga de salida válida

la llave e incrusta un código JavaScript este código redefine el XMLHttpRequest.send, este nuevo método aplica a todo XMLHttpRequest siendo ejecutado cuando llame a XMLHttpRequest.send, que permitió acceder a la información de salida dando como consecuencia la visualización y modificación antes de enviarse a XMLHttpRequest.prototype.realSend, luego la información de salida fue enviada temporalmente a la ventana de modificación o edición. En conclusión, la encriptación de la información en el terminal del cliente respecto a las aplicaciones web a través de la sustitución polialfabético, encriptar y descifrar información sin interferir en la aplicación web, permitió obtener privacidad tanto para el servidor como para el cliente. Adicionalmente, este algoritmo puede aplicarse a los siguientes navegadores Chrome, Firefox, Mandrake, Ubuntu y Fedora incluso llega a extenderse a Linux y Cluster. En lo concerniente al costo de implementación de seguridad, este fue muy alto, siendo contrario a lo recomendado para este tipo de industria, es decir, la implementación de metas específicas, realizables y alcanzables para lograr el costo beneficio esperado.

Jia Xu [16], realizó una investigación en Singapur denominada “Strong leakage-resilient encryption: enhancing data confidentiality by hiding partial ciphertext by Singapore University of Technology and Design. Este estudio buscó obtener un cifrado de información con niveles de seguridad aceptables que sea capaz de enfrentar los ataques de caballo de Troya, amenaza que siempre ha buscado las vulnerabilidades en la información. Así pues, se evaluó tres escenarios i) formulaciones de encriptación AES, RSA, ii) encriptación resistente a fugas y iii) el esquema ocultando parciales. En la primera formulación de encriptación AES, RSA y en las siguientes cuatro evaluaciones se obtuvieron diferentes resultados que se explican a continuación; para la consulta: ¿Puede el adversario acceder a la clave de descifrado k?, el resultado fue No, sin embargo para la consulta: ¿Puede el adversario acceder al texto cifrado (Ctx0, Ctx1)?, el resultado fue Full Access, para la definición de seguridad el resultado fue Seguridad semántica, y para herramientas y metodologías el

resultado fue Computación distinguible. En la segunda formulación para encriptación resistente a fugas los resultados fueron; para la consulta: ¿Puede el adversario acceder a la clave de descifrado k? el resultado fue Acceso parcial acotado y controlado, para la consulta: ¿Puede el adversario acceder al texto cifrado (Ctx0, Ctx1)? el resultado fue Full Access, para la definición de seguridad el resultado fue adoptar ORACLE consultas y para herramientas y metodologías el resultado fue extractor aleatorio. Finalmente, la tercera formulación denominada esquema ocultando parciales obtuvo para la consulta: ¿Puede el adversario acceder a la clave de descifrado k? un resultado de acceso parcial no limitado, para la consulta: ¿Puede el adversario acceder al texto cifrado (Ctx0, Ctx1)? el resultado fue Full Access para Ctx0, pero limitado para Ctx1, para definición de seguridad el resultado fue evitar fugas y para herramientas y metodologías el resultado fue inapropiado. En conclusión, se logró construir un esquema tan seguro bajo una configuración de fugas fuertes.

Benavides Eduardo [17], desarrolló una investigación en Ecuador titulada "Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura" en la Escuela Politécnica Nacional, Universidad de las Fuerzas Armadas ESPE. El presente estudio analiza cómo evitar que las personas no autorizadas obtengan información de manera inadecuada, con el fin de evitar que causen daño a las personas y a la industria, Esta investigación ha utilizado la técnica creada por Barbara Kitchenham para la verificación estructural de la literatura, el cual consta de cuatro pasos consecutivos: i) búsqueda general, ii) selección de los artículos relevantes, iii) extracción de datos y iv) resultados localizados, dando como solución el uso adecuado de buenas prácticas de seguridad, como por ejemplo detectar correos sospechosos, identificar llamadas telefónicas, reconocer a las personas aplicando frecuentemente políticas de certificación de cuentas. Además, hay sitios web como Phishtank, Anti-Phishig Work Group (APWG), Anti-Phishig Work Group (APWG), Corpora entre otros de mucha utilidad que sirven de ayuda para evitar la ingeniería social. Esta investigación fue un precedente para otros investigadores

permitiendo tener una base para continuar profundizando y publicando resultados. Estos últimos años, los catálogos negros o blancos no fueron suficientes o precisos para detectar ataques conocidos como Phishing. En conclusión, los ataques actuales o recientes contra las empresas y el público usuario en la ciudad de Quito tienen una característica común con respecto los web site engañosos, este hallazgo permitió tener un abanico de probabilidades para detectar si una página web es fraudulenta o no, en ese sentido, los vectores de ataques encontrados fueron para la detección de correos falsificados, detección de cuentas de redes sociales falsas, detección de apropiación ilegal y detección de malware o virus de tipo caballos de Troya.

Daniel F. Santos [18], realizó una investigación en Colombia, titulada “Encryption Algorithm for Color Images Based on Chaotic Systems” en Facultad de Ingeniería de la Universidad Distrital Francisco José de Caldas. Este estudio evalúa cómo evitar que personas no acreditadas tengan acceso a información confidencial con la intención de prevenir riesgos o pérdidas económicas que afectan a la sociedad. En ese sentido, se propone un algoritmo de tipo simétrico utilizando para el intercambio el método caótico llamado “Cat de Arnold” y para la difusión el método “hiper caótico de Chen” o también el método denominado “hiper caótico de Lorenz”. Con respecto a la implementación se ha apostado por abreviar los tiempos ejecutados mediante programación paralela a través de la librería de hilos denominado “POSIX de Linux pthread.lib” cuyo grado de eficacia aproximado obtenido fue del 17%, es decir, con 4 hilos se logró disminuir el lapso de tiempo de cumplimiento del algoritmo debido que 1 hilo se demora 0.189131 segundos, con 8 hilos 0.163825 y con 16 hilos demora 0.164549, así mismo, luego de ejecutar el algoritmo se genera la clave de desencriptación que permite recuperar la imagen. Finalmente, este estudio aprovecha las cualidades o particularidades de los modelos dinámicos caóticos para consolidar el algoritmo, para ocultar las imágenes originales y para la posterior recuperación, en consecuencia, este artículo es comparable con otros artículos dado que la eficacia del algoritmo fue buena.

Omar Javier Solano Rodríguez [19], realizó una investigación en Colombia que tiene por título “The information system and computer security mechanisms in the SMEs” cuyo problema está centrado en la carencia de estándares y controles suficientes para enfrentar frontalmente los ataques cibernéticos en las Pymes, la metodología usada fue la recolección de datos y medición de variables que dio como resultado que las pymes de la ciudad de Cali en Colombia son conscientes de la importancia de implementar un diseño de controles de la información y que es prioritario que los usuarios finales participen de ese diseño. Por otro lado, recomendó la adaptación de modelos de controles existentes que otorgan niveles de garantía, es decir, controles ya validados y/o implementados, siendo así, las herramientas tecnológicas y los estándares de controles existentes que necesariamente deberían adoptar las pymes, son por ejemplo COBIT, ISO, norma ISO27001, ISO27002, algoritmos de encriptación que elevan el grado de garantía de la seguridad de la información. Así también se tomaron encuestas siendo una de las preguntas más resaltante ¿La empresa invierte en seguridad informática a través de capacitaciones para sus colaboradores? Las posibles respuestas por parte de los entrevistados era SI, NO y NO SABE, dando como resultado 50 frecuentemente respondió SI, 56 frecuentemente respondió NO y 1.0 frecuentemente respondió NO SABE, dando un total de 107, también en porcentaje, 460.7 en porcentaje respondió que SI, 52.3 en porcentaje respondió que NO y 00.9 en porcentaje respondió que NO SABE, también en porcentaje válido, 460.7 en porcentaje valido respondió que SI, 52.3 en porcentaje válido respondió que NO y 00.9 en porcentaje válido respondió que NO SABE, esto dio lo siguientes acumulados, para los que respondieron SI 460.7, para que los que respondieron que NO 99.1 y para los que respondieron NO SABE 100, los acumulados en Frecuencia 107, los acumulados en porcentaje 100 y por último en porcentaje válido fueron 100. Finalmente, se concluye que los sectores empresariales están dispuestos a invertir, potenciar y actualizar su tecnología reduciendo así el riesgo tecnológico y el riego humano por errores involuntarios, considerando que todas las empresas tienen acceso a las herramientas y a los beneficios que estos nos brindan, como buenas prácticas, estándares y

herramientas como COBIT, ISO27001, además se necesita implementar planes de trabajo alineados a la realidad, adecuar la infraestructura tecnológica y vincularlo a la estrategia del negocio con el objetivo de potenciar la seguridad de la información.

Luis Cáceres Álvarez [20], realizó una investigación en Chile, titulada “Desarrollo de un sistema que simula protocolo de criptografía de tipo cuántica E91 en un ambiente distribuido” en la Escuela Universitaria de Ingeniería Industrial, Informática y Sistemas de la Universidad de Tarapacá. En esta investigación se llevó a cabo la simulación del protocolo E91 en la aplicación de 3 casos. En el primer caso se trabajó con tres computadoras conectadas a una red wifi con 8 bits lográndose 1,7 bits y 5,3 de tiempo total con 6,3 de bits perdido, con 16 bits se logró 3,7 bits y 7,3 de tiempo total con 12,3 de bits perdido, con 32 bits se alcanzó 9,0 bits y 11,2 de tiempo total con 23,0 de bits perdido, con 64 bits se obtuvo 15,3 bits, 22,2 de tiempo total y 48,7 de bits perdido, con 128 bits se obtuvo 27,0 bits, 41,3 de tiempo total y 101,0 de bits perdido, con 256 bits se obtuvo 58,0 bits, 84,9 de tiempo total y 198,0 de bits perdido, con 542 bits se obtuvo 114,0 bits, 171,8 de tiempo total y 398,0 de bits perdido, con 1024 bits se obtuvo 233,7 bits, 341,4 de tiempo total y 790,3 de bits perdido, finalmente con 2048 bits se obtuvo 443,3 bits, 726,4 de tiempo total y 1604,7 de bits perdido. En el segundo caso, también se utilizó tres computadoras pero esta vez conectadas con un switch y cableado físico con 8 bits lográndose para 1,0 bits, 2,5 de tiempo total y 7,0 de bits perdido, con 16 bits se obtuvo 2,7 bits, 4,9 de tiempo total y 13,3 de bits perdido, con 32 bits se obtuvo 5,3 bits, 9,8 de tiempo total y 26,7 de bits perdido, con 64 bits se obtuvo 14,0 bits, 19,5 de tiempo total y 50,0 de bits perdido, con 128 bits se obtuvo 29,0 bits, 38,8 de tiempo total y 99,0 de bits perdido, con 256 bits se obtuvo 59,3 bits, 79,0 de tiempo total y 196,7 de bits perdido, con 512 bits se obtuvo 111,0 bits, 155,5 de tiempo total y 401,0 de bits perdido, con 1024 bits se obtuvo 229,0 bits, 310,4 de tiempo total y 795,0 de bits perdido, con 2048 bits se obtuvo 462,0 bits, 619,4 de tiempo total y 1586,0 de bits perdido. Por último, en el tercer caso otra vez se emplearon tres computadoras pero conectadas a una red diferente y

luego se conectó a una red con un switch central de 16 puertos con 8 bits alcanzando para 1,3 bits, 2,7 de tiempo total y 6,7 de bits perdido, con 16 bits se obtuvo 4,3 bits, 6,1 de tiempo total y 11,7 de bits perdido, con 32 bits se obtuvo 7,7 bits, 11,0 de tiempo total y 24,3 de bits perdido, con 64 bits se obtuvo 14,3 bits, 19,8 de tiempo total y 49,7 de bits perdido, con 128 bits se obtuvo 30,3 bits, 41,5 de tiempo total y 97,7 de bits perdido, con 256 bits se obtuvo 63,0 bits, 79,0 de tiempo total y 193.0 de bits perdido, con 512 bits se obtuvo 112,0 bits, 157,9 de tiempo total y 400,0 de bits perdido, con 1024 bits se obtuvo 224,7 bits, 315,4 de tiempo total y 799,3 de bits perdido, con 2048 bits se obtuvo 453,3 bits, 630,8 de tiempo total y 1594,7 de bits perdido. En conclusión, con el uso continuo de equipos convencionales se logró simular el protocolo E91, considerando además que esta investigación fue para fines estrictamente académicos dejó las bases para que otros investigadores sigan experimentando pero esta vez utilizando computadoras cuánticas con encriptado de información de forma cuántica usando E91 que permita perder el 70% de bits aproximadamente, lo resaltante de esta investigación es que con este protocolo se obtiene la clave final sin que las partículas sean compartidas por el usuario, asimismo, el comportamiento de este protocolo dio mejor resultado con 128 bits con un tiempo de ejecución es de 40 segundos aproximadamente, considerar que el tiempo aumentará a medida que se incrementa el tamaño de la clave.

Latif AKCAY [6], realizó una investigación en Turquía, titulado “Comparison of RISC-V and transport triggered architectures for a postquantum cryptography application” by Department of Electronics and Communication Engineering, Faculty of Electrical and Electronics Engineering, İstanbul Technical University, Turkey. Este estudio cotejo procesadores TTA y ROSC-V utilizando el algoritmo NTRU dando como resultado que los TTA logran mejor rendimiento en cuanto al consumo de energía y recursos utilizados durante las pruebas, es decir, si los buses paralelos aumentaban los recursos del procesador TTA también aumentaban. Sin embargo, los resultados se consideraron conforme ratificándose

que los procesadores TTA fueron muy buena opción para los algoritmos NTRU. Con respecto, a los procesadores RISC-V se afirmó que es una buena opción siempre que se aplique el rediseño adecuado y la técnica apropiada, lográndose una ventaja sobre el resto de procesadores, los logros de la comparación de los 8 procesadores fueron para el procesador RV32I un alto consumo de 15.763 muy por encima de los demás procesadores, para el procesador RV32IMC, tuvo un alto consumo de 0.219 siendo muy por encima de los demás procesadores, para el procesador RV32IMC, tuvo un alto consumo de 0.224 muy por encima de los demás procesadores, además un alto consumo de recursos de 7521 muy por encima de los demás procesadores, para el procesador TTA-P1, tuvo un alto consumo de 0.238 sobre los demás procesadores, por otro lado los procesador TTA-P2, TTA-P3, TTA-P4, TTA-P5 tuvieron los mejores rendimientos superando a los procesadores RV32. En resumen, se necesita continuar con otras Investigaciones para determinar cuál es la arquitectura de un procesador con mayor eficiencia para el algoritmo NTRU con el objetivo de reducir los ataques de la computación cuántica.

Carlos Roberto Sampedro Guamán [21], realizó una investigación en Ecuador, que lleva como título “Percepción de seguridad de la información en las pequeñas y medianas empresas en santo domingo” en la Universidad regional Autónoma de los Andes, Santo Domingo, Ecuador, Universidad regional Autónoma de los Andes, Ambato, Ecuador. Esta investigación, busca mantener e incrementar la confidencialidad, así como la integridad y la disponibilidad de la información en las Pymes con observación científica, considerándose una población 106 empresas de las cuales 73 eran pequeñas empresas y 33 medianas empresas con un nivel de confianza del 98% para la evaluación de los lineamientos o normas de seguridad de la información a través del cuestionario. Siendo la pregunta base si tenían estas políticas de seguridad que garanticen niveles razonables de confidencialidad, integridad y disponibilidad y los encuestados que marcaron que SI para políticas de seguridad fue 66, para confidencialidad 33, para integridad 88, para disponibilidad 88, mientras otros

respondieron que NO para políticas de seguridad en 33, para confidencialidad en 11, para integridad en 0, para disponibilidad en 0, otro grupo indicó que desconoce las políticas de seguridad en 0, para confidencialidad en 0, para integridad en 11, para disponibilidad en 11, también otro grupo respondió que parcialmente para políticas de seguridad en 22, para confidencialidad en 55, para integridad en 0, para disponibilidad en 0. En conclusión, las Pymes mayormente tienen documentos con objetivos definidos, políticas de seguridad, métricas, sin embargo tienen la cultura de realizar pruebas de continuidad de negocio en donde los procedimientos y protocolos se verifican, es decir, revisan el antes, durante y el después, con el fin de adoptar medidas de ajuste o gestionar cambios en caso sea necesario, sin embargo, la confidencialidad, la integridad y la disponibilidad muchas veces no están incluidas en sus políticas de seguridad, casi siempre no tienen políticas preventivas sólo acciones reactivas, convirtiéndose en práctica común y repetitiva en las Pymes.

En cuanto a la justificación e importancia de estudio, este proyecto de investigación, se sustentó en la existencia de diversas herramientas de encriptación que facilitan el trabajo de las empresas o entidades de distintos sectores que requieren este tipo de servicio, empero, estas son desarrolladas y/o fabricadas dejando de lado a las pequeñas empresas del sector financiero, debido que muchas veces no disponen de los recursos suficientes para adquirir infraestructura de alto costo, siendo el precio una característica del cual dependerá el éxito o fracaso de dicho proyecto.

Los resultados obtenidos de este proyecto de investigación, permite colaborar con las pequeñas empresas del sector financiero, con respecto a la mejora de la seguridad de la información sensible y confidencial que gestionan, implementando encriptación a bajo costo con un alto nivel de calidad y desempeño. Asimismo, este proyecto contribuirá con otros trabajos de investigación, a través de la discusión de los resultados obtenidos y la posibilidad de reformular los algoritmos de encriptación.

1.2. Formulación del problema

¿Cuál es el algoritmo de criptografía más eficiente para cumplir con los niveles adecuados de seguridad de datos de una empresa financiera peruana?

1.3. Hipótesis

El algoritmo de criptografía AES es el más eficiente para cumplir con los niveles adecuados de seguridad de datos de una empresa financiera peruana.

1.4. Objetivos

1.4.1. Objetivo general.

Evaluar la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana.

1.4.2. Objetivos específicos.

a. Definir los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana.

b. Analizar los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras.

c. Desarrollar en lenguaje de programación sistema que permita la comparación de los algoritmos de criptografía considerando los indicadores propuestos.

d. Plantear recomendaciones que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos.

1.5. Teorías relacionadas al tema

1.5.1. Criptografía

Los algoritmos son funciones matemáticas aplicadas en la encriptación y la desencriptación de datos, esto se traduce en una función que recibe un parámetro para encriptarla y/o desencriptarla. Por otro lado, debo mencionar que también existen las funciones hashing, esto genera números aleatorios.

1.5.2. Matemáticas involucradas

Consiste en estudiar la cantidad de información que se encuentran en el mensaje y las llaves, el mensaje se encripta por medio de un número medio de bits de información.

a) Algoritmos de criptografía simétrica

Algoritmos DES y 3DES

En inglés Data Encryption Standard (DES) fue creado con la colaboración de la multinacional IBM, de la Oficina de Estándares y el Departamento de Comercio en los Estados Unidos en los años de 1977.

Actualmente, este algoritmo es el más estudiado y utilizado por las escuelas de

educación superior e industrias como por las pymes, cajas de ahorro y crédito y bancos.

El algoritmo DES se basa fundamentalmente en la confusión y difusión mediante permutaciones de texto de entrada utilizando las llaves, realizándose por 16 veces.

Cabe recalcar que la misma llave y algoritmo se utilizan para el cifrado y el descifrado de la información con una longitud para la llave de 56 bits.

Por otro lado, el algoritmo 3DES está basado en el algoritmo DES, pero ejecutando el proceso 3 veces. [22]

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \infty f[R_{i-1}, K_i]$$

Algoritmos AES

En inglés Advanced Encryption Standard (AES) fue creado con el propósito de reemplazar al DES, consiste en una encriptación por bloques, actualmente es un estándar en los Estados Unidos.

Fue desarrollado en Estados Unidos por Joan Daemen y Vincent Rijmen en el año 2001 y publicado por el ANSI organismo nacional de estándares de ese país.

AES básicamente utiliza una estructura de bucle que permite realizar repetidamente reordenamientos de datos e información o también llamadas permutaciones. Las repeticiones o bucles reemplazan una parte de los datos de entrada.

Este algoritmo permite un mayor rango de tamaños de bloques y un mayor rango de tamaño de longitud de llaves, también requiere un tamaño fijo de 128 bits de longitud y para las llaves necesita 128,192 o 256 bits para ello debe cumplir la regla de ser múltiplo de 32

bits.

$$p = 0$$

Si el bit menos significativo de b es 1 entonces:

$$p = p \; \theta \; a$$

Se realiza una copia de resguardo de a, luego

$$a = a \ll 1$$

Si la copia de a, en su bit más importante, tenía un 1:

$$b = b \gg 1$$

Termina el ciclo de ocho interacciones, p contendrá el valor resultante del producto entre a y b.

Algoritmos IDEA

En inglés International Data Encryption Algorithm (IDEA), fue publicado por los especialistas en Criptología Xuejia Lai y James L. Massey en el año 1991 en la ciudad de Zúrich.

Este algoritmo pretendía reemplazar al algoritmo DES, este algoritmo trabaja sobre bloques de 64 bits

IDEA fue desarrollado para el uso no comercial, es decir, era un algoritmo libre, posteriormente fue patentado y vendido en el año 2011. Actualmente está licenciado mundialmente por MediaCrypt. Este algoritmo nació con la versión de PGP.

Este algoritmo utiliza 128 bits que a su vez se subdividen en ocho sub llaves de 16 bits comenzando la primera ronda, luego la llave será rotada hacia la izquierda en 25 bits y se volverá a dividir en ocho sub llaves, donde las primeras cuatro serán usadas en la segunda ronda y las cuatro llaves restantes se utilizarán en la tercera ronda. [1]

A continuación, lo mencionado:

1. Multiplicación X1 con la primera sub-llave.

2. Sumatoria X2 con la segunda sub-llave.

3. Sumatoria X3 con la tercera sub-llave.

4. Multiplicación X4 con la cuarta sub-llave.

5. Efectuar XOR entre los resultados de los puntos 1 y 3.

6. Efectuar XOR entre los resultados de los puntos 2 y 4.

7. Multiplicación del resultado del punto 5 con la quinta sub-llave.

8. Sumatoria del resultado de los puntos 6 y 7.

9. Multiplicación del resultado del punto 8 con la sexta sub-llave.

10. Sumatoria del resultado de los puntos 7 y 8.

11. Efectuar XOR entre los resultados de los puntos 1 y 9

12. Efectuar XOR entre los resultados de los puntos 3 y 9

13. Efectuar XOR entre los resultados de los puntos 2 y 10

14. Efectuar XOR entre los resultados de los puntos 4 y 10

Los cuatro sub bloques resultantes de los puntos 11 y 14 se conectan con las rondas de salida, por último, terminada las cuatro rondas tendremos una ronda con cuatro primeros movimientos como salida.

1. Multiplicación X1 y la primera sub-llave

2. Sumatoria X2 y la segunda sub-llave

3. Sumatoria X3 y la tercera sub-llave

4. Multiplicación X4 y la cuarta sub-llave

Algoritmos MD5

El algoritmo hashing MD5 criptográfico es una versión con mejoras respecto a su antecesor MD4, las siglas en inglés MD significa Message Digest y en español resumen de mensajes. Posteriormente, en una reunión un grupo de investigadores resolvió que el algoritmo estaba libre de problemas críticos.

Este algoritmo en la entrada procesa bloques con 512 bits de longitud, distribuido a la vez en 16 sub bloques con 32 bits para la salida, ejecuta una serie de 32 bits por cuatro que uniéndose forman 128 bits de longitud. El paso siguiente seria inicializar y asignar valor a cuatro variables de 32 bits, llamadas variables de encadenamiento, con valores fijos.

A = 0x01234567

B = 0x89abcdef

C = 0xfedcba98

D = 0x76543210

Son cuatro las funciones de tipo no lineales referidas, pero solamente una de ellas se utiliza en las cuatro rondas y a su vez en 16 ocasiones, tal como se muestra, en cada vuelta se combina de manera diferente, los tres parámetros o variables entre a, b, c y d. teniendo en cuanta que el símbolo ® corresponde a la operación XOR, ^a AND, v a OR y ¬a NOT. [1]

F(X,Y,Z)=(X^Y) v ((¬x) ^Z)

G(X,Y,Z)=(X^Z) v (Y ^(¬Y))

H(X,Y,Z)=X®Z®Y

I(X,Y,Z)=Y® (X v (¬Z))

Finalmente, luego de las cuatro vueltas de 16 pasos cada una a, b, c y d estas son sumadas en A, B, C y D, seguido del bloque de entrada. Al finalizar el último bloque dará como resultado una unión o concatenación de A, B, C y D.

Algoritmos SHA

El instituto de Estándares y Tecnología (NITS) en conjunto con la Agencia Nacional de seguridad (NSA) diseñaron el algoritmo SHA conocido así por las siglas Secure Hash Algorithm.

Este algoritmo fue desarrollado para utilizarlo en el estándar Digital Signature Standard (DSS), este estándar implementó algoritmos de firma digital llamados DSA.

SHA-1, genera un hash de encriptación de 160 bits y actualmente es la más popular en el registro de shecksums para la integridad de archivos, cumpliendo el fin con el que fue desarrollado, es decir, para usarlos en firmas digitales.

Este algoritmo es muy similar al algoritmo MD5, sin embargo, una gran diferencia es

que SHA-1 utiliza 5 variables de 32 bits a diferencia de MD5 que solo utiliza 4; produciendo una longitud de 160 bits. [1].

A=0x67452301

B=0xabcbebca

C=0x987bbcac

D=0x01234567

E=0xc2c5c2c5

b) Algoritmos de criptografía asimétrica

Algoritmos RSA

Este algoritmo o protocolo creado por los matemáticos Ron Rivest, Adi Shamir y Leonard Adlleman, su nombre RSA fácilmente se deduce que deriva de las siglas de los nombres de los creadores. Este algoritmo fue publicado en el año 1997, hasta el momento existe incertidumbre que sea seguro, pero tampoco se ha demostrado que no lo sea. Sin embargo, esto indica que estamos ante un algoritmo confiable y con cierta importancia para la industria.

En la actualidad es el algoritmo más utilizado, pues está considerado como uno de los más seguros para la encriptación, este algoritmo utiliza llaves de 1024 bits de longitud.

RSA basa su seguridad en factoriales de grandes números, se calculan dos números primos para obtener las llaves públicas y privadas, estos dos dígitos están entre los primeros 200 números en algunos casos se incluyen números más grandes.

Se establece que:

$$n = pq$$

Donde e será elegida aleatoriamente

$$ed \equiv mod\ (p-1)(q-1)$$

$$d = e^{-1}\ mod\ \big((p-1)(q-q)\big)$$

Para la des-encriptación:

$$m_1 = c_i^d\ mod\ n$$

Algoritmos ElGamal

Este algoritmo fue desarrollado por Taher Elgamal en el año 1984, el autor se basó en algoritmos anteriores a este, este esquema puede utilizarse en la encriptación y desencriptación de firmas digitales en documentos electrónicos.

Actualmente está implementado en software libre como GNU y versiones actuales de PGP.

Este algoritmo basa su seguridad en campos finitos diferenciándose así de los algoritmos anteriormente mencionados. [18]

La generación de la llave pública se produce cuando se une un número p con dos números, al mismo tiempo los valores g y x deben ser inferiores a p, siendo la fórmula como se indica a continuación.

$$y = g^x\ mod\ p$$

En efecto, la llave pública estará conformada por y, g y p donde x es una llave privada.

De manera que, para la firma de un mensaje se asigna un número aleatorio k que será el número relativo a p – 1, a continuación, el cálculo.

$$a = g^x \, mod \, p$$

Entonces debemos obtener b de la siguiente fórmula:

$$M = (xa + kb) mod (p - 1)$$

Luego la firma será a y b, en el caso de k se mantendrá oculto.

$$y^a a^b \, mod \, p = g^M \, mod \, p$$

En consecuencia, para encriptar M que simboliza el mensaje protegido, debemos aplicar la siguiente fórmula para obtener k

$$a = g^k \, mod \, p$$

Y

$$b = y^k M \, mod \, p$$

Finalmente, a y b serán el texto encriptado.

Algoritmos DSA

DSA es una variante del algoritmo ElGammal y Schnorr. Este algoritmo fue desarrollado en el año 1991 por David Kravitz, colaborador del organismo nacional de inteligencia y seguridad en Estados Unidos, este algoritmo inicialmente fue llamado DSS (Digital Signature Standard), posteriormente fue propuesto por NIST cambiando el nombre

del algoritmo a DSA (Digital Signature Algorithm.

En el desarrollo de este algoritmo se necesita p que representa a un valor primo con un tamaño de 512 hasta 1024 bits recomendable usar 2048 bits de manera que la longitud sea múltiplo de 64 a su vez, q corresponde a un número de 160 bits de longitud que debe ser factor primo de p – 1 y G será h(p-1)/q mod p y h será un número menor a p – 1 tal que h(p-1)/q mod p sea mayor que 1 y x será menor que q, en tanto que Y será igual a gx mod p.

La fórmula que obtenemos es:

$$r = \left(g^k \bmod p\right) \bmod q$$

Y

$$s = \left(k^1(H(m) + xr)\right) \bmod q$$

A continuación, la verificación.

$$w = s^{-1} \bmod q$$

$$u_1 = (H(m) * w) \bmod q$$

$$u_2 = (rw) \bmod q$$

$$v = \left((g^{u1} * y^{u2}) \bmod p\right) \bmod q$$

El resultado si v será igual a r, entonces la firma es válida y confirmada.

Descripción del pseudocódigo para AES

AES es un algoritmo que procesa texto en bloques y están en claro de 128 bits con clave estándar de 128, 192 y 256 bits, utilizó una matriz de 4 * 4, cuyás 16 celdas que van

cambiando de valor con los procesos de encriptación que se van ejecutando, utilizando técnicas de sustitución, permutación y en algunos casos operaciones polinómicas [23].

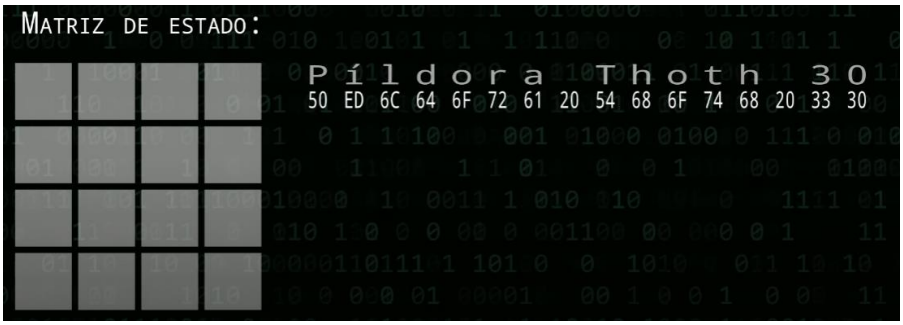
En AES las operaciones de encriptación se realizaron en la matriz y con texto de 32 bits pues se escriben en orden comenzando de arriba hacia abajo, así como de izquierda a derecha.

Figura 9. Matriz de estado, donde se incluirán los datos a encriptar.

Fuente: [24].

Los datos se transportan de forma lineal mostrando el valor en claro para cada hexadecimal, en este caso la frase que se está encriptando es “PildoraThoth 30”.

Figura 10. Matriz de estado, donde se incluirán los datos a encriptar.



Fuente: [24].

Luego de transportarse la matriz queda sólo con los valores hexadecimales quedando de la siguiente manera.

Figura 11. Matriz de estado, donde se incluirán los datos a encriptar.

Fuente: [24].

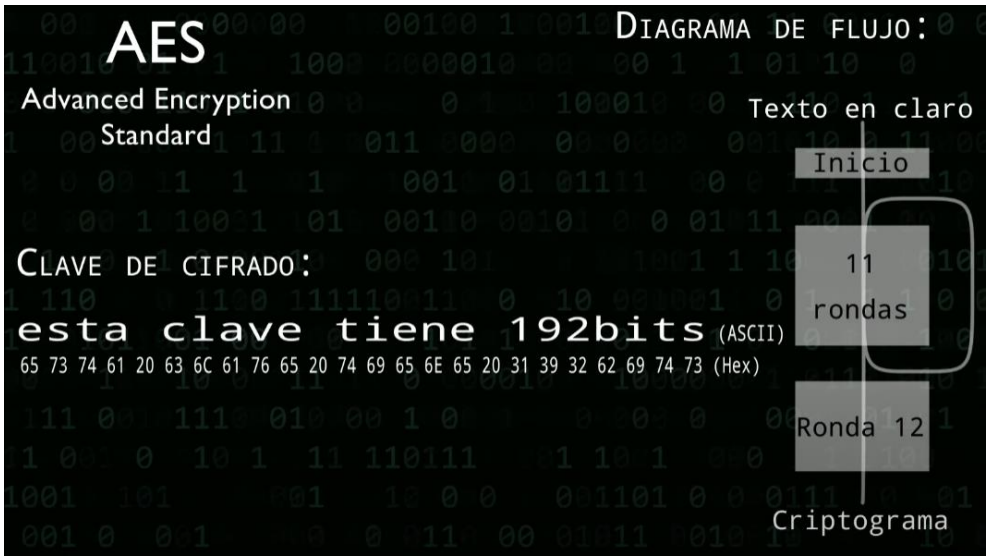
Cuando se utiliza una clave de 128 bits el proceso de cifrado ejecutará 9 vueltas en el flujo del algoritmo.

Figura 12. Diagrama de flujo AES con una clave de 128bits en formato ASCII.

Fuente: [24].

Para una clave de 192 bits el algoritmo realizará 12 vueltas en el flujo del algoritmo.

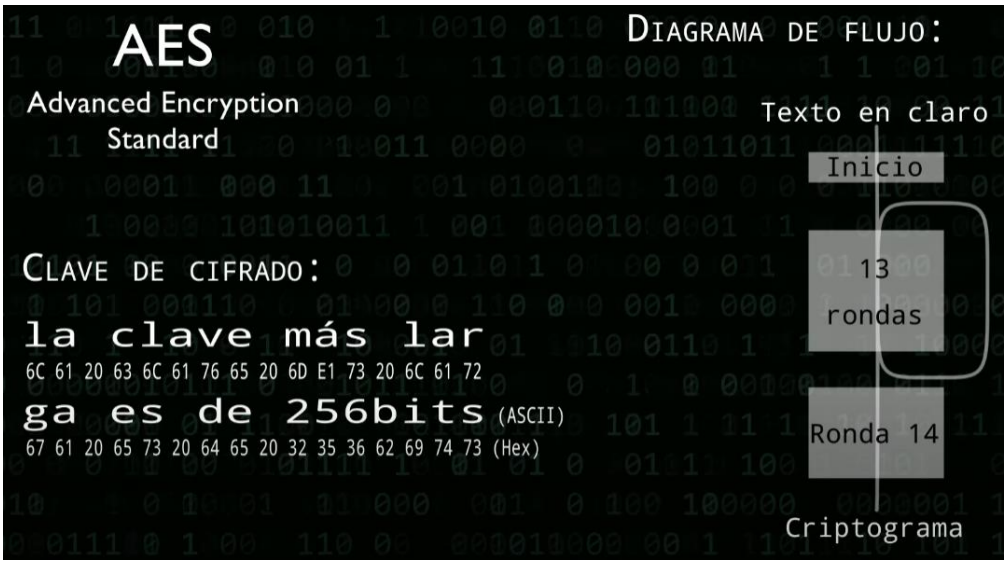
Figura 13. Diagrama de flujo AES.



Fuente: [24].

Para encriptar una clave de 256 bits se requiere de 14 vueltas en el flujo del algoritmo.

Figura 14. Diagrama de flujo AES.



Fuente: [24].

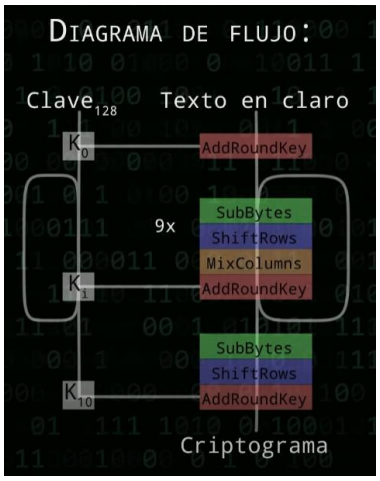
La clave maestra genera una llave para cada una de las vueltas que dará el algoritmo.

Cifrando información

El cifrado AES inicia con la suma de OR exclusiva del mensaje y la clave, a continuación, para una clave de tamaño de bloque de 128 bits se generan 10 claves que se utilizaran una en cada vuelta y el algoritmo ejecutara cuatro operaciones: Primero, de la matriz toma un byte y lo sustituye mediante el uso de una tabla. Segundo, se permutan las filas comienzan a rotas, sin embargo, la primera fila no rota, pero segunda fila rota solo un byte, la tercera fila incrementa una fila, es decir, rotan dos bytes, por último, la cuarta fila también incrementa una fila más, es decir, rotan 3 bytes. Tercero, en este paso se multiplica una a una las columnas de la matriz con un polinomio. Cuarto, se ejecuta la sumatoria de OR Exclusiva de la clave de cada vuelta con los valores de la matriz de estado, todo esto durante 9 vueltas. [23]

Por último, se repiten las operaciones de sustitución, permutación y suma OR Exclusiva, dando como resultado una matriz de estado con 16 bytes que contiene el criptograma cifrado, que sería el primer bloque texto en claro. Tal como se muestra en la siguiente figura.

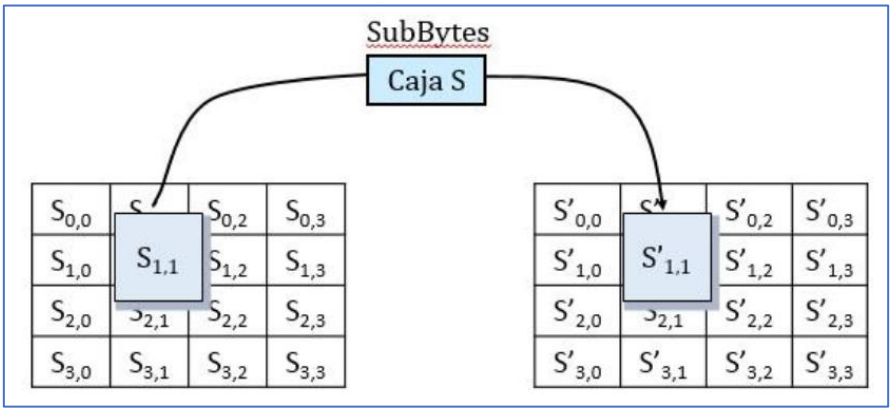
Figura 15. Diagrama de flujo AES.



Fuente: [24].

En esta operación se toma un byte de la matriz y lo sustituye mediante el uso de una tabla

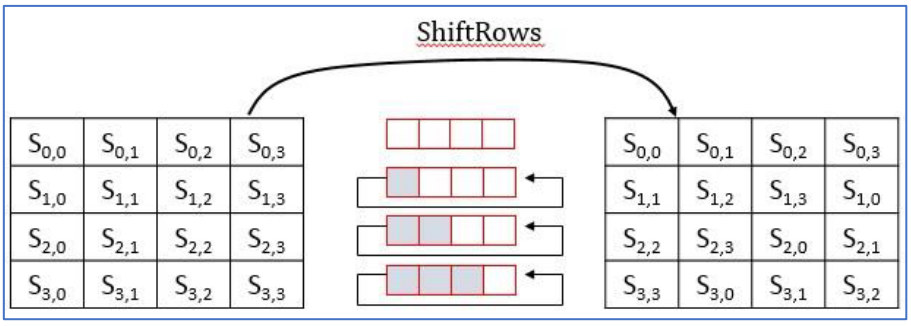
Figura 16. Diagrama de flujo AES.



Fuente: [23].

En esta operación se permutan las filas es decir comienzan a rotas, sin embargo, la primera fila no rota, pero segunda fila rota solo un byte, la tercera fila incrementa una fila es decir rotan dos bytes, por último, la cuarta fila también incrementa una fila más es decir rotan 3 bytes.

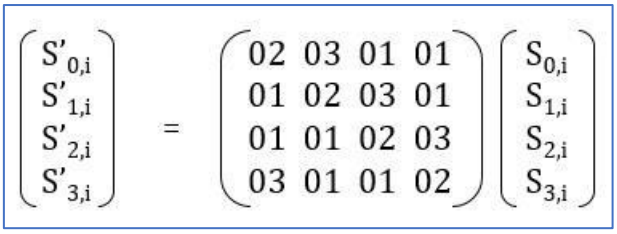
Figura 17. Diagrama de flujo AES.



Fuente: [23].

Siendo una operación más compleja pues se multiplica una a una las columnas de la matriz con un polinomio

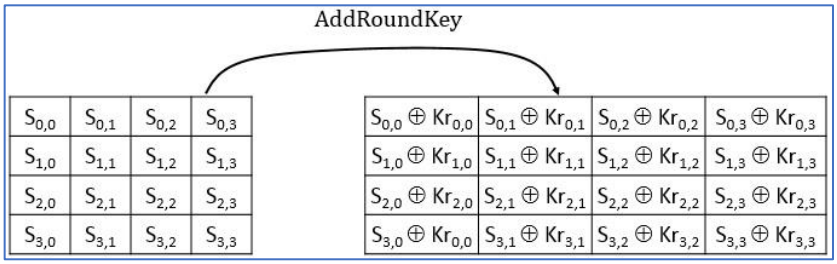
Figura 18. Diagrama de flujo AES.



Fuente: [23].

Esta operación se ejecuta la sumatoria de OR Exclusiva de la clave de cada vuelta con los valores de la matriz de estado.

Figura 19. Diagrama de flujo AES.

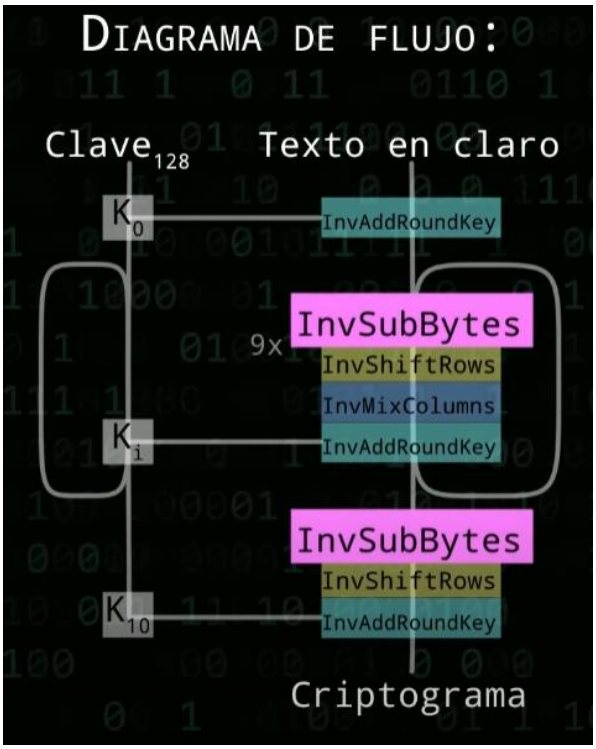


Fuente: [23].

Des-cifrado

En este caso el algoritmo dará vueltas en sentido contrario y se utilizarán las funciones necesarias para este proceso.

Figura 20. Diagrama de flujo AES.

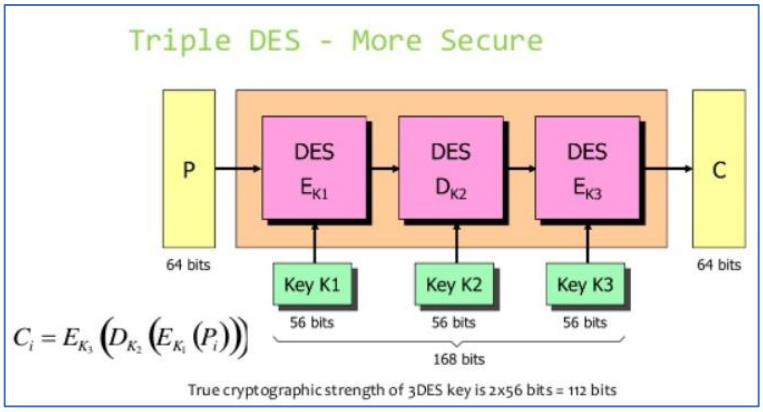


Fuente: [24].

Descripción del pseudocódigo para 3DES

3DES es un algoritmo para cifrar la información de un texto para posteriormente convertirse en un texto cifrado mediante una serie de pasos ya establecidos. Por otro lado, es un elemento de tres factores de informaciones, es decir el DES ejecutado 3 veces para fortalecer la seguridad [25]

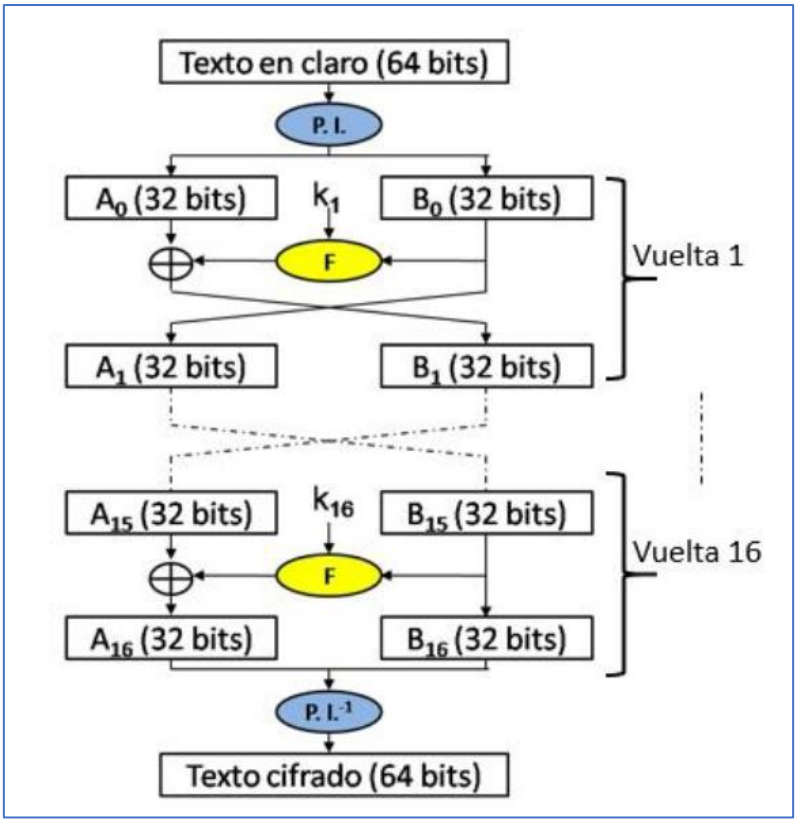
Figura 21. Diagrama de flujo 3DES ejecutando 3 veces DES.



Fuente: [24].

DES cifra bloques de 64 bits con una clave de 64 bits pero que se ve reducida 56 al eliminar el octavo bit de cada byte que se usa para control de paridad, por cada bloque de texto realiza 16 vueltas usando claves diferentes generadas a partir de la clave principal, divide el bloque de texto en dos mitades de 32 bits cada una y solo una de esas mitad es la mezcla con la clave correspondiente a esa vuelta a la siguiente vuelta intercambia los bloques obtenidos y repite el mismo procedimiento hasta la vuelta número 16 en que ya general criptograma de 64 bits del primer bloque de texto.

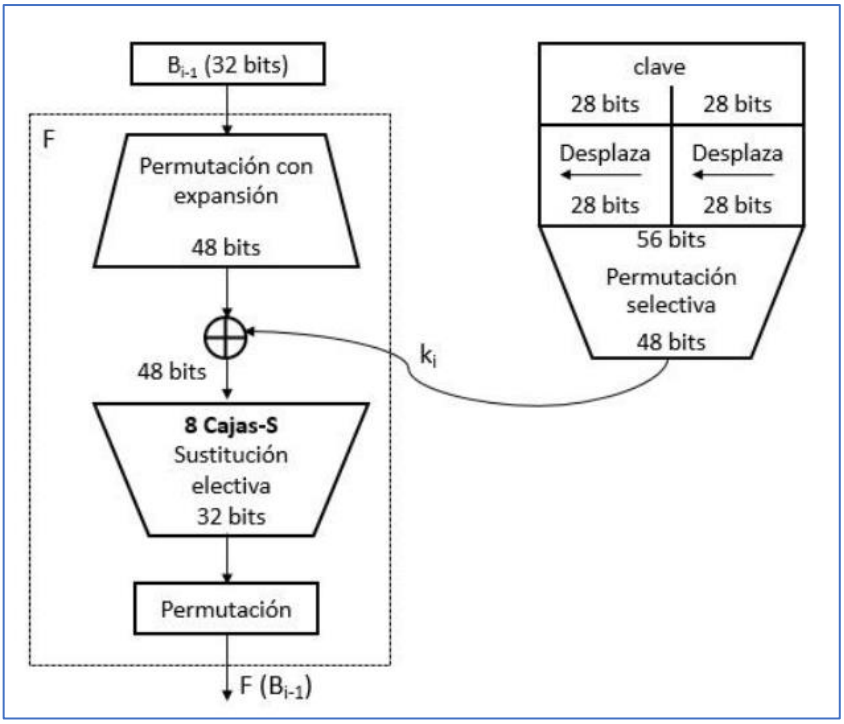
Figura 22. Diagrama de flujo 3DES.



Fuente: [23].

Cómo durante el cifrado las claves de cada una de las 16 vueltas se obtienen aplicando desplazamientos de bits a la izquierda las claves de descifrados se calculan realizando los mismos desplazamientos, pero ahora hacia la derecha y se descifra haciendo desde la vuelta 16 hasta la vuelta 1.

Figura 23. Diagrama de flujo 3DES.



Fuente: [23].

Las misteriosas cajas S

Aunque muchos escritos sobre este tema y la existencia de una posible puerta trasera en el algoritmo, lo cierto es que dichas cajas no tienen nada de misterioso, es decir, se trata de la fase más importante del algoritmo donde se sustituyen cadenas de 48 bits, que, a su vez, son el resultado de una operación entre bits de bloque de texto y bits de una clave de vuelta por cadenas de 32 bits.

Será muy fácil obtener esos 32 bits de salida pero resultará computacionalmente muy difícil hacer lo contrario ya que romper el algoritmo a partir de las cajas implica realizar 2 ^ 256 intentos en tanto que aplicando, fuerza bruta directamente al criptograma dicho trabajo significa solo 2 ^ 56 intentos, en la figura se muestra el funcionamiento de una caja

s en donde los extremos de la cadena de 6 bit de entrada indicar una fila en dicha caja y los cuatro bits interiores indican la columna del contenido de la celda, siendo un número de 4 bits y al ser ocho las cajas S la salida será 32 bits.

Algoritmo de encriptación AES

La encriptación AES se desarrolló en el lenguaje de programación PHP, la implementación completa se muestra en punto 3.3.3 de este documento.

El desarrollo cuenta con una función openssl_encrypt que se encarga de encriptar de la información, su vez utilizar librerías propias del PHP, que tienen la lógica para la encriptación AES.

Algoritmo de encriptación 3DES

La encriptación 3DES se desarrolló en el lenguaje de programación PHP, la implementación completa se muestra en el 3.3.3 de este documento.

El desarrollo cuenta con una función openssl_encrypt que se encarga de encriptar de la información, que a su vez utilizar librerías propias del PHP, que tienen la lógica para la encriptación 3DES

II. MATERIALES Y MÉTODO

2.1. Tipo y Diseño de Investigación

En [26] se reveló que, “las investigaciones aplicadas se centran en la aplicabilidad práctica de conocimientos adquiridos para la resolución de problemáticas específicas, en diversas ciencias tales como, verbigracia, ciencias tecnológicas, ciencias de la computación, ciencias de ingeniería, ciencias sociales o cualquier otro tipo de disciplina”.

Respecto al tipo, esta investigación fue tecnológica aplicada ya que, se enfocó en el abordaje a una problemática del mundo real de la ingeniería de sistemas, más específicamente alineado a la seguridad de la información, aplicando métodos para la evaluación de los algoritmos de criptografía en términos de eficiencia y de la confidencialidad, integridad y disponibilidad de los datos de documentos de carácter privado en una empresa financiera peruana.

En [26] se reveló que, “las investigaciones cuasi experimentales comparten ciertas similitudes con el diseño experimental, pero no necesariamente termina por cumplir con la totalidad de criterios de control experimentales rigurosos, sino que, de manera parcial ejecuta experimentos para analizar resultados y llegar a conclusiones”.

Respecto al diseño, esta investigación fue cuasi experimental ya que, se enfocó en experimentos de manera uniforme para los algoritmos de criptografía, pero no para la totalidad de ellos, sino que se ejecutó de manera parcial a la población de estudio, además de ello, la muestra no fue seleccionada de manera aleatoria sino por conveniencia.

Finalmente, esta investigación también fue de enfoque cuantitativa, pues permitió recolectar, examinar y analizar datos de manera numérica, llevando a tener mayor claridad y visibilidad de la información. Además, estos tipos de investigación son eficaces para realizar predicciones y comprobaciones relacionadas [27].

2.2. Variables, Operacionalización

Variable Independiente:

Algoritmos de criptografía

Según Hamouda [28] los algoritmos de criptografía son “procedimientos matemáticos diseñados para codificar y decodificar información de manera segura, garantizando la confidencialidad, la integridad y la disponibilidad de los datos durante su transmisión o almacenamiento. Estos algoritmos emplean técnicas avanzadas para transformar el documento de texto en un documento cifrado, utilizando claves únicas que solo el emisor y el receptor conocen. Su objetivo principal es proteger la información sensible frente a accesos no autorizados, asegurando que solo las partes autorizadas puedan acceder a los datos en su forma original”.

Variable dependiente:

Seguridad de datos en una empresa financiera peruana

Según Ahmed al. [29] se refiere al “conjunto de medidas, políticas y procedimientos implementados para proteger la confidencialidad, integridad y disponibilidad de la información financiera sensible en el entorno corporativo. Esto implica la utilización de algoritmos criptográficos avanzados para cifrar datos sensibles, garantizando que solo las partes autorizadas puedan acceder a ellos. Además, incluye la aplicación de controles de acceso, la monitorización activa de la red, la detección de intrusiones y la gestión de riesgos para prevenir y mitigar posibles amenazas cibernéticas que puedan comprometer la seguridad de los datos financieros de la empresa”.

Tabla I.

Operacionalización de la Variable Independiente

Variable de estudio	**Definición conceptual**	**Definición operacional**	**Dimensiones**	**Indicadores**	**Ítems**	**Instrumento**	**Valores finales**	**Tipo de variable**	**Escala de medición**
Variable Independiente Algoritmos de criptografía	Los algoritmos se utilizan en la criptografía con el propósito de garantizar la seguridad de los datos confidenciales durante su transmisión o almacenamiento	Procesos matemáticos esenciales para cifrar y descifrar los datos, esto implica la claridad y precisión de los algoritmos y operaciones matemáticas involucradas en el proceso	Eficiencia del algoritmo	Rendimiento de cifrado	$R_c = \frac{Tamaño\ del\ archivo\ (bytes)}{Tiempo\ de\ encriptación\ (s)}$	Bitácora de resultados	Kb/s	Numérico	Intervalo
				Rendimiento de descifrado	$R_d = \frac{Tamaño\ del\ archivo\ (bytes)}{Tiempo\ de\ desencriptación\ (s)}$		Kb/s	Numérico	Intervalo
			Consumo de recursos del algoritmo	Consumo de RAM	$C_r = \frac{M_t - M_u}{M_t}$	Registro electrónico	%	Numérico	Intervalo
				Consumo de CPU	$C_{cpu} = \frac{T_{cpu}}{N_{cpu}}$				

Fuente. Adaptado de [30].

Tabla II.

Operacionalización de la Variable Dependiente

Variable de estudio	**Definición conceptual**	**Definición operacional**	**Dimensiones**	**Indicadores**	**Ítems**	**Instrumento**	**Valores finales**	**Tipo de variable**	**Escala de medición**
Variable dependiente: Seguridad de datos en una empresa financiera peruana	La seguridad de datos se basa en el uso de técnicas y herramientas criptográficas para garantizar la confidencialidad, integridad y disponibilidad de la información	Medidas de gestión de claves y autenticación para asegurar que solo los usuarios autorizados puedan acceder a la información de documentos privados	Seguridad de la información de los datos	Integridad	$I = \frac{(N_{tb})}{(N_{bnm})} * 100\%$	Bitácora de resultado Guías de observación	Se expresa como un porcentaje al multiplicar el resultado por 100%	Numérico	Intervalo
				Fortaleza del algoritmo	$F_a = \frac{\sum K_p}{n}$	Matriz de Kerckhoffs	%	Numérico	Intervalo

Fuente. Adaptado de [30].

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

Población

Se ha considerado, 8 algoritmos de encriptación para la población de este trabajo de investigación, los mismos se encuentran distribuidas en las categorías simétrica y asimétrica, cada una de estas categorías contiene un gran número de algoritmos de encriptación, también conocido en el argot informático como código abierto.

Tabla III.

Población de estudio

#	CATEGORÍAS	ALGORITMOS DE ENCRIPTACIÓN
1		3DES
2		AES
3	Criptografía simétrica	IDEA
4		MD5
5		SHA
6		RSA
7	Criptografía asimétrica	EIGamal
8		DSA

Nota. Lista de algoritmos de encriptación. Fuente: Elaboración propia.

Muestra

La presente investigación ha utilizado el muestreo no probabilístico, dado que la

muestra no depende de algo probable, a su vez, tomando en cuenta el criterio de mayor reputación han elegido por conveniencia los algoritmos AES y 3DES, Además, se consideraron los indicadores de rendimiento de cifrado, rendimiento de descifrado, consumo de memoria RAM, consumo de CPU, integridad y fortaleza.

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

Técnicas e Instrumentos

Instrumentos mecánicos o electrónicos:

Este instrumento nos permite realizar una investigación analizando diferentes problemas, dando un abanico de resultados que facilitaran el análisis y la evaluación, con el objetivo de conocer qué algoritmo cumple con los niveles de seguridad de datos.

Ficha de registro electrónico:

Es un instrumento que permite la recolección de los datos obtenidos por indicadores, proporcionando resultados y teniendo en cuenta que las métricas de esta investigación son el rendimiento y seguridad. Por ejemplo, métricas de rendimiento, integridad y fortaleza, así pues, se utilizaron formatos de registro de matriz de confusión, también las métricas de consumo de CPU, Memoria y promedio de tiempo de respuesta que corresponde a esta investigación.

2.5. Procedimiento de análisis de datos

Concerniente a la variable independiente fueron empleadas las siguientes fórmulas

estadísticas alineadas a los indicadores siguientes:

a. Rendimiento de cifrado.

La velocidad de encriptación de un algoritmo R_c está asociada con el rendimiento de cifrado, que indica la rapidez con la que el algoritmo realiza la tarea de encriptación.

$$R_c = \frac{Tamaño\ del\ archivo\ (bytes)}{Tiempo\ de\ encriptación\ (s)}$$

R_c = Rendimiento de cifrado

b. Rendimiento de descifrado.

La velocidad de desencriptación de un algoritmo (R_d) está vinculada al rendimiento de descifrado, lo cual indica la rapidez con la que el algoritmo realiza la tarea de desencriptación.

$$R_d = \frac{Tamaño\ del\ archivo\ (bytes)}{Tiempo\ de\ desencriptación\ (s)}$$

R_d = Rendimiento de descifrado

Concerniente a la variable dependiente fueron empleadas las siguientes fórmulas estadísticas alineadas a los indicadores siguientes:

a. Integridad

Se expresa como un porcentaje al multiplicar el resultado por 100%. Este porcentaje indica que la integridad aumenta a medida que mayor sea el número de bits modificados (NBM) y disminuye a medida que se modifican menos bits durante la transmisión o el

almacenamiento, teniendo la siguiente fórmula:

$$I = \frac{(N_{tb})}{(N_{bnm})} * 100\%$$

I = Integridad

N_{tb} = Número total de bits en los datos originales sin encriptar.

N_{bnm} = Número de bits no modificados.

b. Fortaleza del algoritmo

La fortaleza del algoritmo F_a se relaciona con el cumplimiento que tiene el algoritmo evaluado en concordancia con los seis (06) Principios Criptográficos de Kerckhoffs.

$$F_a = \frac{\sum K_p}{n}$$

F_a = Fortaleza del algoritmo

K_p = Algoritmos que sí cumplen con los Principios de Kerckhoffs que evalúan la seguridad de la información del envío en texto plano

n = Número total de los principios de Kerckhoffs

2.6. Criterios éticos

a. Confidencialidad: toda la información utilizada en esta investigación, utiliza información de la organización en donde se solicitó el permiso para dicho fin, se mantendrá protegida en todo momento evitando divulgaciones.

b. Originalidad: Esta investigación respeta los derechos de autor, prevaleciendo la

autenticidad, incluyendo citas y referencias en todo el documento de la investigación, evitando de esta manera el plagio.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

3.1.1. Resultados de la Variable Independiente “Algoritmos de criptografía”

La seguridad de los datos financieros es de suma importancia en cualquier sector, y especialmente crítica en el ámbito de las Administradoras de Fondos de Pensiones (AFP) en el Perú. En este contexto, la elección del algoritmo de cifrado adecuado desempeña un papel crucial para garantizar la confidencialidad y la integridad de la información sensible.

En esta sección, se analizó el rendimiento de cifrado, el rendimiento de descifrado, el consumo de recursos de memoria RAM y CPU de dos (02) de los algoritmos de cifrado simétrico más ampliamente utilizados: AES y 3DES. El enfoque se centró en evaluar cómo estos algoritmos manejan diez (10) archivos con datos de una empresa financiera peruana del sector de las AFP. Dichos archivos analizados se encuentran especificados en los anexos de esta investigación.

Mediante una evaluación meticulosa, se analizaron Las métricas identificadas en la operacionalización de variables, considerando ambos algoritmos: AES y 3DES. El propósito fue proporcionar una perspectiva fundamentada que ayude a las AFP peruanas a tomar decisiones informadas sobre la elección del algoritmo de cifrado más adecuado.

3.1.1.1. Indicador “Rendimiento de cifrado”

Con el propósito de lograr la evaluación del Indicador “Rendimiento de Cifrado (R_c)” se ejecutaron los cifrados de diez (10) archivos conteniendo datos de una empresa financiera peruana, los cuales permitieron realizar las pruebas, reflejándose los resultados en la siguiente tabla:

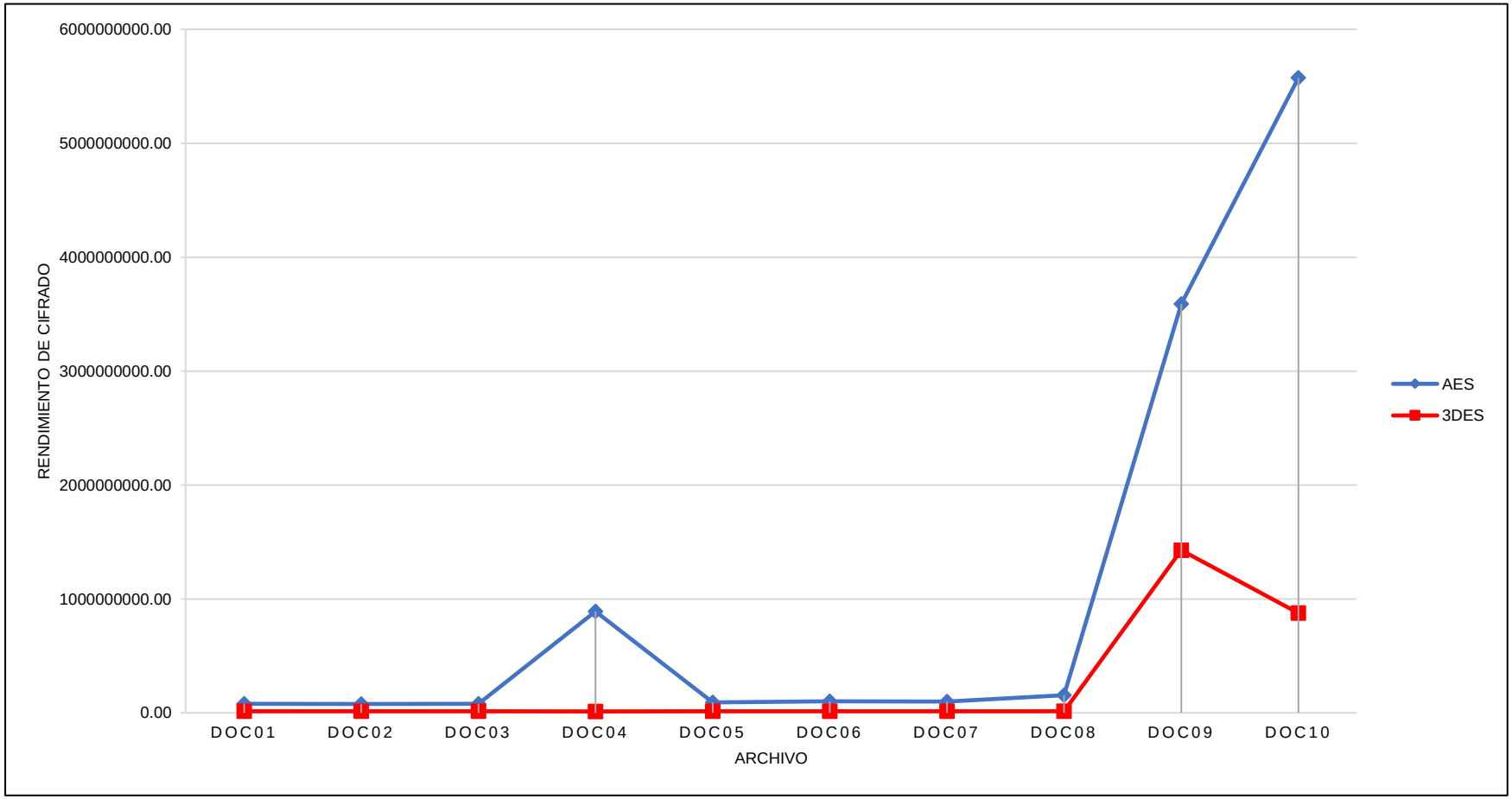
Tabla IV.

Resultados del Indicador “Rendimiento de Cifrado”

Características			Algoritmo			
			AES		3DES	
Archivo	Tamaño del archivo (kB)	Tamaño del archivo (bytes)	Tiempo de cifrado (s)	R_c	Tiempo de cifrado (s)	R_c
Doc01	162.00	165,593.00	0.00208687782287600	79349638.10	0.01249098777771000	13256998.00
Doc02	242.00	247,588.00	0.00318503379821780	77734810.90	0.01748704910278300	14158363.63
Doc03	364.00	372,736.00	0.00467896461486820	79662068.57	0.02620887756347700	14221746.01
Doc04	617.00	630,866.00	0.00070953369140625	889127616.69	0.04980611801147500	12666435.88
Doc05	786.00	804,384.00	0.00888490676879880	90533758.08	0.05579304695129400	14417280.36
Doc06	1064.00	1,089,216.00	0.01062190055847200	102544360.49	0.07606697082519500	14319171.49
Doc07	1074.00	1,099,281.00	0.01097290420532200	100181408.63	0.08040404319763200	13671961.71
Doc08	1507.00	1,543,145.00	0.01004592323303200	153609077.45	0.10410213470459000	14823375.18
Doc09	2591.00	2,652,738.00	0.00073909759521484	3589157936.89	0.00185806846618652	1427685819.05
Doc10	2781.00	2,847,535.00	0.00051093101501465	5573227923.77	0.00325608253479000	874527893.43

Fuente: Elaboración propia.

Figura 24. Resultados del Indicador “Rendimiento de Cifrado”.



Fuente: Elaboración propia.

Según la Tabla IV y Figura 19 para el rendimiento de cifrado existe una diversidad en la complejidad y cantidad de datos en cada documento. En cuanto al tiempo de cifrado, se proporcionan los tiempos de cifrado en segundos para cada archivo y algoritmo. Se puede observar que, en general, los tiempos de cifrado de AES son mucho más cortos que los de 3DES. Asimismo, puede distinguirse que, el rendimiento de cifrado de AES es significativamente mejor que el de 3DES, especialmente cuando el tamaño del archivo es grande. Aunque AES es generalmente más rápido que 3DES para cifrar archivos de tamaño moderado, la eficiencia relativa de cada algoritmo puede depender del tamaño y la complejidad del archivo. Finalmente, es evidente que, el tiempo de cifrado de AES aumenta de manera significativa con el tamaño del archivo, mientras que el de 3DES también aumenta, pero en menor medida. Esto sugiere que la escalabilidad de AES puede ser un factor a considerar al cifrar archivos muy grandes.

En resumen, estos datos proporcionan información valiosa sobre el rendimiento de los algoritmos AES y 3DES en términos de rendimiento de cifrado para una variedad de tamaños de archivo, específicamente para los diez (10) archivos analizados. Dependiendo de las necesidades específicas de seguridad y rendimiento de la empresa financiera, se podría optar por uno u otro algoritmo en función de estos resultados y otras consideraciones adicionales.

3.1.1.2. Indicador “Rendimiento de descifrado”

Con el propósito de lograr la evaluación del Indicador “Rendimiento de Descifrado R_d se ejecutaron los cifrados de diez (10) archivos conteniendo datos de una empresa financiera peruana, los cuales permitieron realizar las pruebas, reflejándose los resultados en la siguiente tabla:

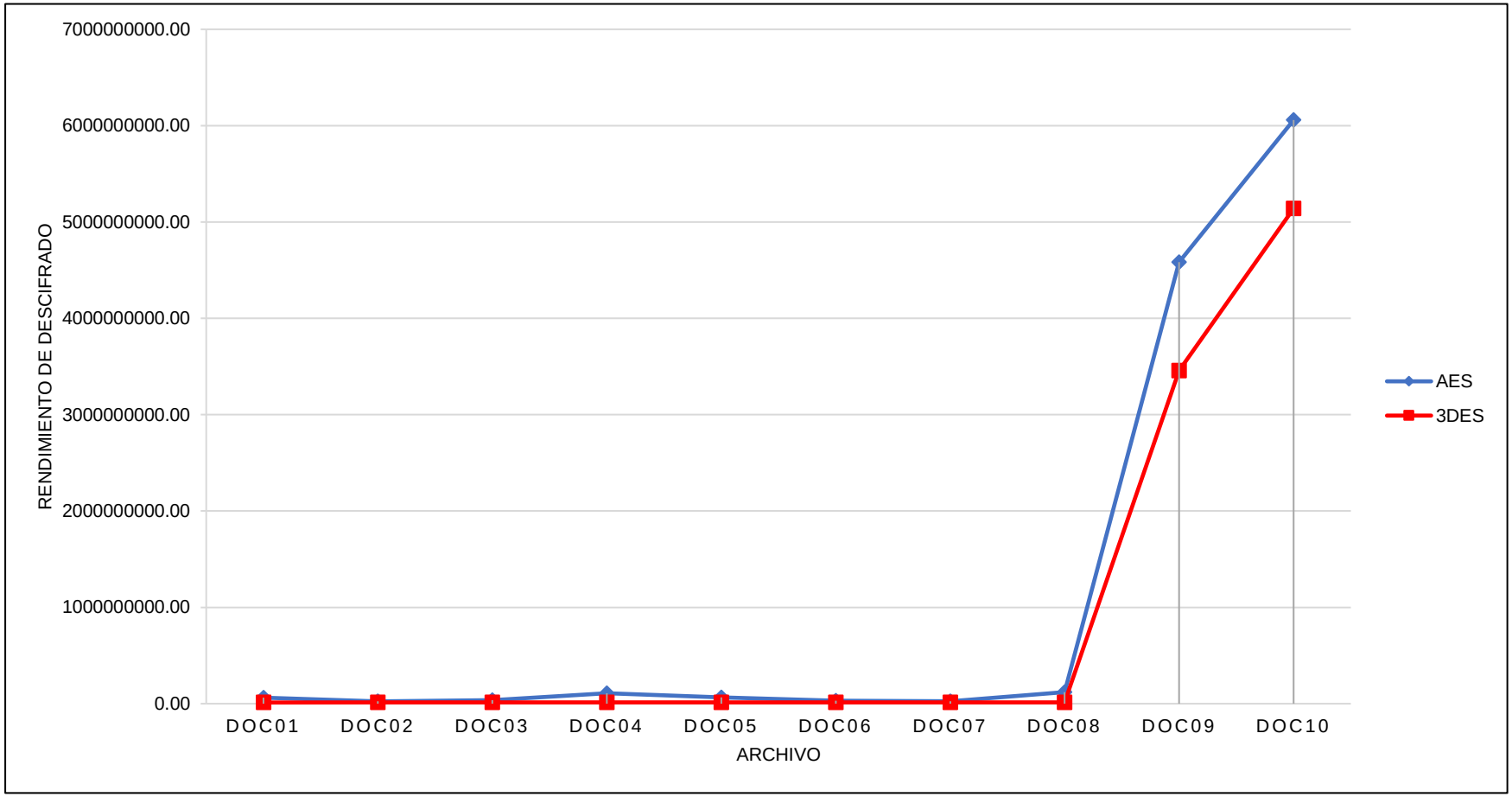
Tabla V.

Resultados del indicador “Rendimiento de Descifrado”

Características			Algoritmo			
			AES		3DES	
Archivo	Tamaño del archivo (kB)	Tamaño del archivo (bytes)	Tiempo de descifrado (s)	R_d	Tiempo de descifrado (s)	R_d
Doc01	162.00	165,593.00	0.00260901451110840	63469558.83	0.01323008537292500	12516396.93
Doc02	242.00	247,588.00	0.01019007034301800	24296986.35	0.01870203018188500	13238562.74
Doc03	364.00	372,736.00	0.01016506958007800	36668317.62	0.02684998512268100	13882167.84
Doc04	617.00	630,866.00	0.00575709342956540	109580643.03	0.04910492897033700	12847305.01
Doc05	786.00	804,384.00	0.01228210258483900	65492369.44	0.05697107315063500	14119165.32
Doc06	1064.00	1,089,216.00	0.03438901329040500	31673371.69	0.07749104499816900	14056024.15
Doc07	1074.00	1,099,281.00	0.04104012107849100	26785520.39	0.08609008789062500	12768961.29
Doc08	1507.00	1,543,145.00	0.01278515625000000	120698172.93	0.11635398864746000	13262501.94
Doc09	2591.00	2,652,738.00	0.00057888031005859	4582532785.98	0.00076712837219238	3458010544.47
Doc10	2781.00	2,847,535.00	0.00047001052856445	6058449389.84	0.00055401687622070	5139798302.58

Fuente: Elaboración propia.

Figura 25. Resultados del Indicador “Rendimiento de Descifrado”.



Fuente: Elaboración propia.

Según la Tabla V y Figura 25 para el rendimiento de descifrado existe una diversidad en la complejidad y cantidad de datos en cada documento. Se proporcionan los tiempos de descifrado en segundos para cada archivo y algoritmo. Se puede observar que, al igual que en el cifrado, en general, los tiempos de descifrado de AES son más cortos que los de 3DES. Asimismo, puede distinguirse que, el rendimiento de descifrado de AES es significativamente mejor que el de 3DES, especialmente cuando el tamaño del archivo es grande. Aunque AES es generalmente más rápido que 3DES para descifrar archivos de tamaño moderado, la eficiencia relativa de cada algoritmo puede depender del tamaño y la complejidad del archivo. Finalmente, es evidente que, los tiempos de descifrado de AES son más cortos que los de 3DES. Al igual que en el cifrado, se puede observar que el tiempo de descifrado de AES aumenta de manera significativa con el tamaño del archivo, mientras que el de 3DES también aumenta, pero en menor medida. Esto sugiere que la escalabilidad de AES puede ser un factor a considerar al descifrar archivos muy grandes.

En resumen, estos datos proporcionan información valiosa sobre el rendimiento de los algoritmos AES y 3DES en términos de tiempo de descifrado para una variedad de tamaños de archivo. Dependiendo de las necesidades específicas de seguridad y rendimiento de la empresa financiera, se podría optar por uno u otro algoritmo en función de estos resultados y otras consideraciones adicionales.

3.1.1.3. Indicadores “Consumo de RAM” y “Consumo de CPU”

Con el propósito de lograr la evaluación de los indicadores “Consumo de RAM” y “Consumo de CPU” se ejecutaron los cifrados de diez (10) archivos conteniendo datos de una empresa financiera peruana, los cuales permitieron realizar las pruebas, reflejándose los resultados en la siguiente tabla:

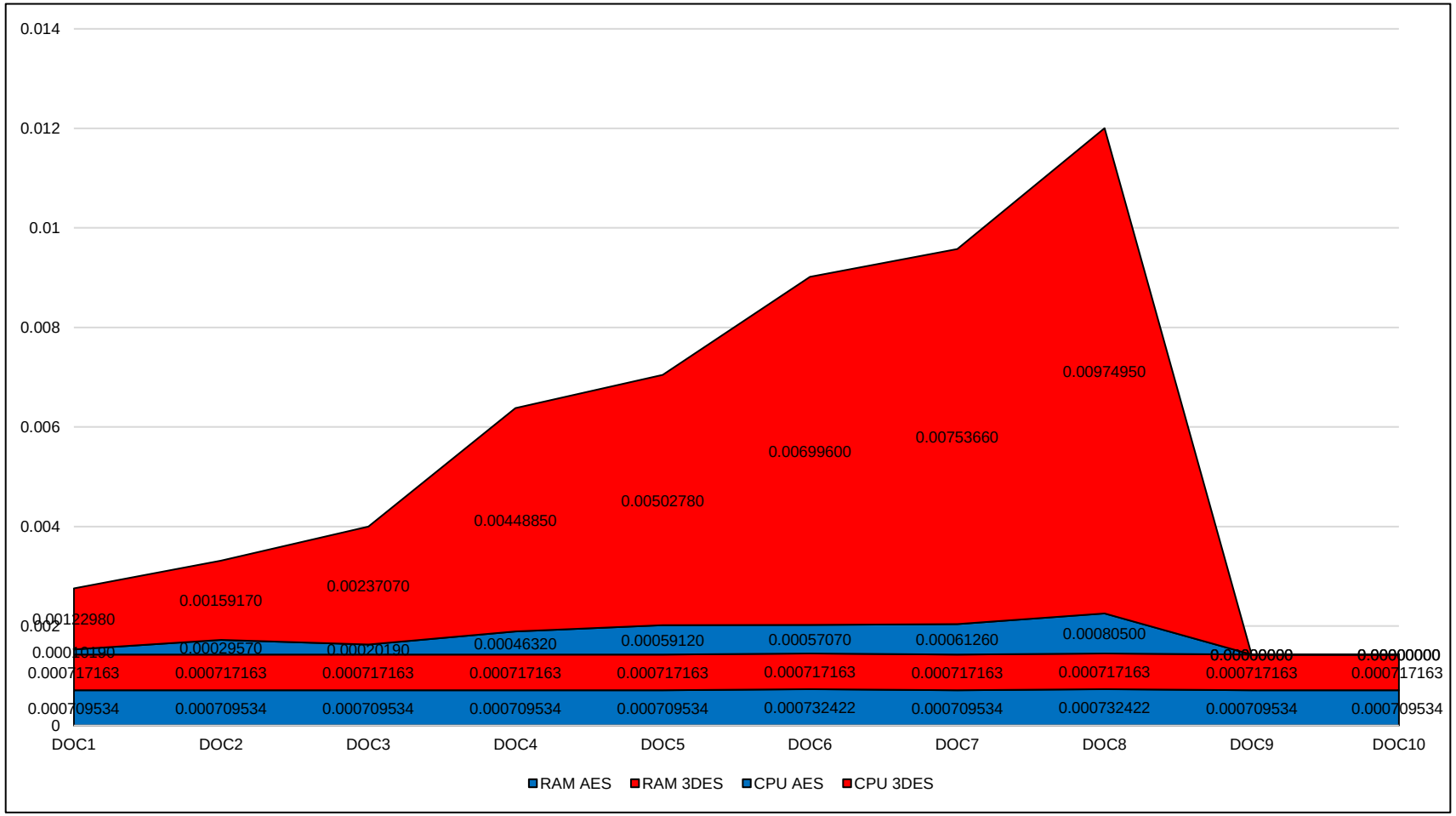
Tabla VI.

Resultados de los indicadores “Consumo de RAM” y “Consumo de CPU”

Características			Algoritmo			
			AES		3DES	
Archivo	Tamaño del archivo (kB)	Tamaño del archivo encriptado (bytes)	Consumo RAM	Consumo CPU	Consumo RAM	Consumo CPU
Doc01	162.00	165,593.00	0.00070953369140625000	0.0001019	0.00071716308593750000	0.0012298
Doc02	242.00	247,588.00	0.00070953369140625000	0.0002957	0.00071716308593750000	0.0015917
Doc03	364.00	372,736.00	0.00070953369140625000	0.0002019	0.00071716308593750000	0.0023707
Doc04	617.00	630,866.00	0.00070953369140625000	0.0004632	0.00071716308593750000	0.0044885
Doc05	786.00	804,384.00	0.00070953369140625000	0.0005912	0.00071716308593750000	0.0050278
Doc06	1064.00	1,089,216.00	0.00073242187500000000	0.0005707	0.00071716308593750000	0.0069960
Doc07	1074.00	1,099,281.00	0.00070953369140625000	0.0006126	0.00071716308593750000	0.0075366
Doc08	1507.00	1,543,145.00	0.00073242187500000000	0.0008050	0.00071716308593750000	0.0097495
Doc09	2591.00	2,652,738.00	0.00070953369140625000	0.0000000	0.00071716308593750000	0.0000000
Doc10	2781.00	2,847,535.00	0.00070953369140625000	0.0000000	0.00071716308593750000	0.0000000

Fuente: Elaboración propia.

Figura 26. Resultados de los indicadores “Consumo de RAM” y “Consumo de CPU”.



Fuente: Elaboración propia.

Según la Tabla VI y Figura 26, se presentan el tamaño de cada archivo en kilobytes (kB) y el tamaño del archivo encriptado en bytes para cada documento, así como también muestra el consumo de RAM y el consumo de CPU para el proceso de encriptado utilizando los algoritmos AES y 3DES. Se puede observar que, los tamaños de archivo encriptado varían dependiendo del tamaño del archivo original y el algoritmo de criptografía utilizado.

En este caso, se proporciona el tamaño del archivo encriptado en bytes después de aplicar cada algoritmo de cifrado. Se proporcionan los valores de consumo de RAM y CPU en relación con el proceso de encriptado para cada documento y algoritmo. Estos valores indican la cantidad de recursos del sistema que se utilizan durante el proceso de encriptado. Se observa que, en general, el consumo de RAM y CPU es bajo para ambos algoritmos y varía ligeramente entre los diferentes documentos, siendo AES el que obtiene un menor consumo de recursos, tanto en CPU, como en RAM.

Tanto AES como 3DES muestran un bajo consumo de recursos de RAM y CPU durante el proceso de encriptado, lo que sugiere una eficiencia en el uso de recursos del sistema. Sin embargo, es importante tener en cuenta que el consumo de recursos puede variar dependiendo del tamaño y la complejidad del archivo.

Para los documentos más grandes (Doc09 y Doc10), el consumo de CPU es cero. Esto podría ser un artefacto de cómo se están registrando los datos o podría indicar que el proceso de encriptado se detuvo o no se realizó correctamente para esos documentos.

En resumen, estos datos proporcionan información sobre el consumo de recursos de RAM y CPU durante el proceso de encriptado utilizando los algoritmos AES y 3DES para una variedad de tamaños de archivo. Esto puede ser útil para evaluar el impacto en el rendimiento del sistema al implementar cada algoritmo de cifrado.

3.1.2. Resultados de la Variable Dependiente “Seguridad de datos en una empresa financiera peruana”

3.1.2.1. Indicador “Integridad”

Dentro de la triada de la seguridad de la información, la integridad es esencial en la criptografía ya que, sin ella, los atacantes podrían lograr la modificación de los datos en reposo o en tránsito, de manera que, podrían verse comprometidas dichas informaciones. Para ello, se ejecutaron diversas evaluaciones con propósitos de evidenciar la integridad de los documentos de las empresas financieras peruanas, considerando los algoritmos de criptografía AES y 3DES, donde N_{bnm} hace referencia a aquella cantidad de bits no modificados y donde N_{tb} hace referencia al número total de bits en los datos originales sin encriptar.

Por esta razón, a manera de comprobar la integridad se ejecutó un análisis de diez (10) documentos conteniendo datos confidenciales de la empresa financiera peruana caso de estudio. Vale mencionar que, la totalidad de documentos fueron de tamaños distintos para poder ejecutar el análisis de manera más profunda.

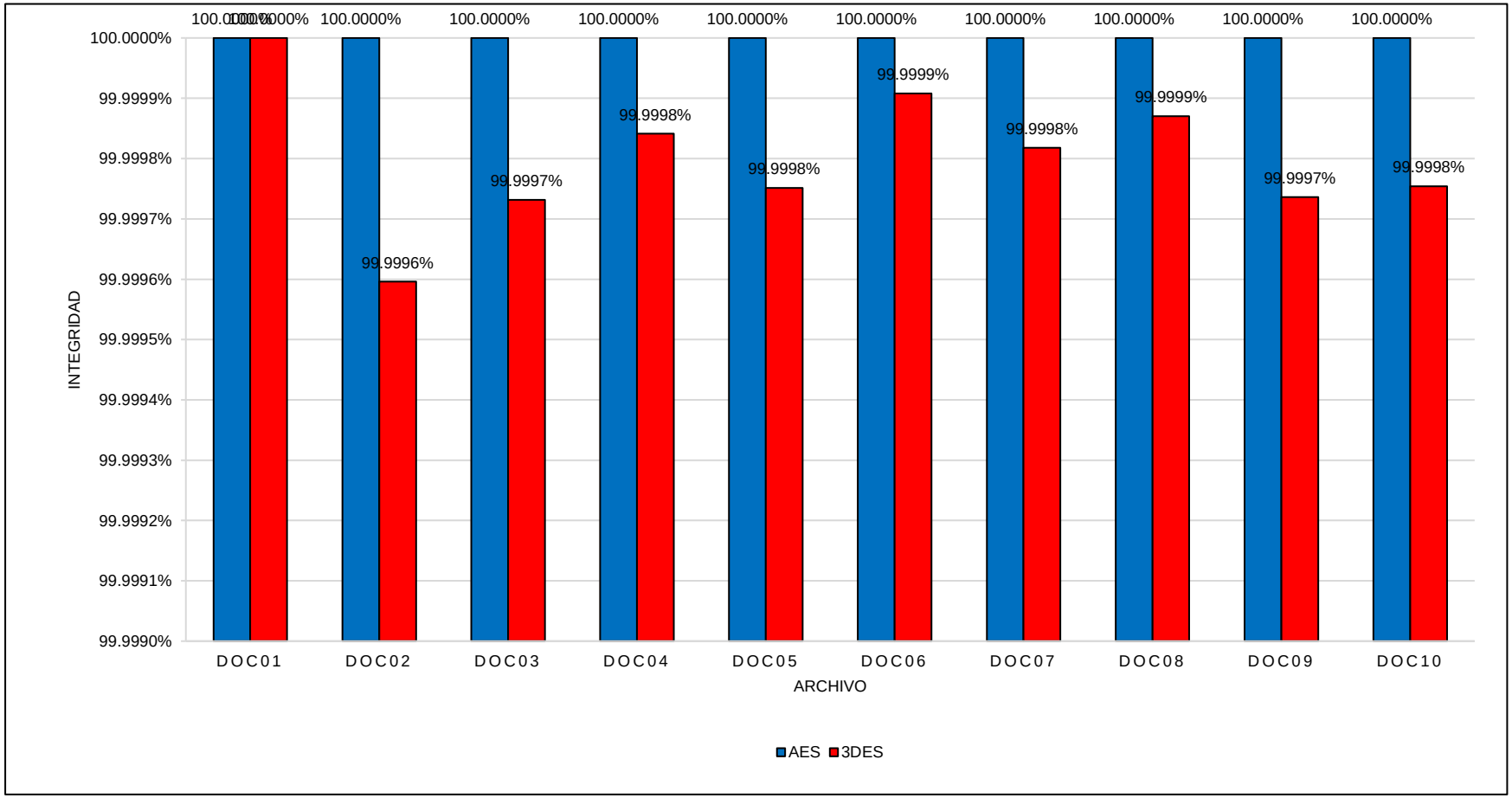
Tabla VII.

Resultados del indicador “Integridad”

Características			Algoritmo			
			AES		3DES	
Archivo	Tamaño del archivo (kB)	Tamaño del archivo encriptado (bytes)	Tamaño del archivo desencriptado (bytes)	Integridad	Tamaño del archivo desencriptado (bytes)	Integridad
Doc01	162.00	165,593.00	165,593.00	100.0000%	165,593.00	100.0000%
Doc02	242.00	247,588.00	247,588.00	100.0000%	247,587.00	99.9996%
Doc03	364.00	372,736.00	372,736.00	100.0000%	372,735.00	99.9997%
Doc04	617.00	630,866.00	630,866.00	100.0000%	630,865.00	99.9998%
Doc05	786.00	804,384.00	804,384.00	100.0000%	804,382.00	99.9998%
Doc06	1064.00	1,089,216.00	1,089,216.00	100.0000%	1,089,215.00	99.9999%
Doc07	1074.00	1,099,281.00	1,099,281.00	100.0000%	1,099,279.00	99.9998%
Doc08	1507.00	1,543,145.00	1,543,145.00	100.0000%	1,543,143.00	99.9999%
Doc09	2591.00	2,652,738.00	2,652,738.00	100.0000%	2,652,731.00	99.9997%
Doc10	2781.00	2,847,535.00	2,847,535.00	100.0000%	2,847,528.00	99.9998%

Fuente: Elaboración propia.

Figura 27. Resultados del indicador “Integridad”.



Fuente: Elaboración propia.

Según la Tabla VII y Figura 27 que presentan el tamaño del archivo original en kilobytes (kB), el tamaño del archivo encriptado en bytes, el tamaño del archivo desencriptado en bytes y la integridad del archivo después de cada proceso (en porcentaje) puede evidenciarse que, después del proceso de encriptado y desencriptado, se evalúa la integridad del archivo comparando el tamaño del archivo desencriptado con el tamaño del archivo original. La integridad del archivo se expresa como un porcentaje, donde 100% indica que el tamaño del archivo desencriptado es idéntico al tamaño del archivo original.

Para todos los documentos evaluados, tanto con AES como con 3DES, la integridad del archivo es prácticamente del 100%. Esto indica que el proceso de encriptado y desencriptado no ha alterado el contenido de los archivos y que el proceso ha sido exitoso en preservar la integridad de los datos, sin embargo, si se lleva a un análisis más micro, puede observarse que AES tiene la ventaja al obtener ese 100% de integridad, mientras que 3DES un 99.9998% de integridad. Aunque la integridad se mantiene en un nivel del 100%, se observan pequeñas diferencias en el tamaño del archivo desencriptado en comparación con el tamaño del archivo original. Estas variaciones son mínimas y pueden deberse a factores como la forma en que se manejan los metadatos o la estructura del archivo durante el proceso de encriptado y desencriptado.

En resumen, estos datos muestran que tanto AES como 3DES son efectivos para preservar la integridad de los archivos durante el proceso de encriptado y desencriptado. Los resultados consistentes y la integridad cercanas al 100% indican que los algoritmos de cifrado han realizado su función correctamente, garantizando que los archivos desencriptados sean idénticos a los originales en términos de contenido y tamaño, pero que, sin embargo, AES destaca por su 100% de integridad al límite.

3.1.2.2. Indicador “Fortaleza del algoritmo”

La fortaleza del algoritmo es un aspecto crucial en la evaluación de la eficiencia de los métodos criptográficos utilizados para proteger los datos sensibles de una empresa financiera. Este indicador se refiere al grado en que un algoritmo de cifrado cumple con los seis principios criptográficos establecidos por el renombrado criptógrafo neerlandés Auguste Kerckhoffs. Estos principios proporcionan un marco riguroso para evaluar la seguridad, la manejabilidad y la eficiencia de los algoritmos.

Para fundamentar este análisis, se ha tomado como referencia la obra de Petitcolas [31]. Este recurso proporcionó una comprensión profunda y actualizada de los principios de Kerckhoffs y su aplicación en la evaluación de algoritmos criptográficos.

En esta sección, se presenta un análisis detallado de los algoritmos AES y 3DES, seleccionados para este estudio. Se examino el grado de cumplimiento de cada algoritmo con los principios de Kerckhoffs, ofreciendo una visión comparativa de su eficacia para garantizar la seguridad de los datos en una empresa financiera peruana. Este análisis es fundamental para determinar cuál de estos algoritmos proporciona una mejor protección y eficiencia operativa en el contexto de las necesidades específicas del sector financiero.

La fortaleza del algoritmo se encuentra asociada con el nivel de cumplimiento que tiene el algoritmo a evaluar de acuerdo con los seis (06) Principios. Por tanto, a continuación, se ejecuta el análisis respectivo de los algoritmos de criptografía seleccionados para este estudio, los algoritmos AES y 3DES:

Tabla VIII.

Resultados del indicador “Fortaleza del algoritmo”

N°	Principio	AES	Puntaje	3DES	Puntaje
1	“El sistema debe ser, si no matemáticamente indescifrable, al menos no susceptible de desciframiento en la práctica” [31].	AES utiliza un diseño moderno y seguro, con bloques de 128 bits y claves de 128, 192 o 256 bits, lo que lo hace altamente seguro contra ataques actuales.	10	3DES es más antiguo y utiliza una longitud de clave efectiva de 112 bits, lo que lo hace menos seguro ante ataques de fuerza bruta.	8
2	“El sistema no debe requerir que sea secreto, y debe poder caer en manos del enemigo sin inconvenientes” [31].	AES es un estándar abierto y su seguridad se basa en la longitud de la clave y no en la confidencialidad del algoritmo.	10	3DES también es un estándar abierto, pero debido a su antigüedad, es más susceptible a análisis y posibles vulnerabilidades.	8
3	“La clave debe poder ser comunicada y recordada sin necesidad de notas escritas, y cambiarse fácilmente” [31].	AES permite el uso de claves de varias longitudes (128, 192, 256 bits), proporcionando flexibilidad y facilidad para recordar y cambiar claves.	9	3DES utiliza una clave triple de 56 bits (en tres claves diferentes), lo que puede ser más complicado de manejar y recordar.	8

4	“El sistema debe ser aplicable a la correspondencia telegráfica” [31].	AES es eficiente y rápido, adecuado para sistemas modernos de telecomunicaciones y transmisión de datos.	9	3DES es más lento debido a su triple cifrado, lo que puede afectar el rendimiento en sistemas modernos.	7
5	“El aparato debe ser portátil y funcionar sin necesidad de una gran cantidad de individuos” [31].	AES puede implementarse fácilmente en hardware y software con alta eficiencia.	9	3DES también puede ser implementado en hardware y software, pero con menor eficiencia.	8
6	“El sistema debe ser fácil de usar, requiriendo poca habilidad o entrenamiento” [31].	AES es fácil de implementar y usar en diversas aplicaciones, con un excelente balance entre seguridad y rendimiento.	10	3DES es más complejo debido a su triple cifrado, lo que puede requerir más esfuerzo en la implementación y uso.	8
Puntaje de cumplimiento		57/60		47/60	
F_a		**95.00%**		**78.33%**	

Fuente: Elaboración propia.

Como bien se mencionaba previamente, los principios de Kerckhoffs establecidos por el criptógrafo Auguste Kerckhoffs en el siglo XIX, son esenciales para evaluar la solidez y seguridad de los algoritmos criptográficos. Estos principios resaltan que la seguridad de un sistema criptográfico no debería depender del secreto del algoritmo en sí, sino más bien de la seguridad de la clave.

Para este informe en específico, estos principios permitieron comparar la verdadera fortaleza de ambos algoritmos por varias razones importantes, tales como, verbigracia, transparencia, enfoque en la clave, resistencia a ataques y adaptabilidad.

Para una empresa financiera peruana, la seguridad de los datos es de suma importancia debido a la sensibilidad de la información manejada. Al comparar los algoritmos de cifrado AES y 3DES siguiendo los principios de Kerckhoffs, se puede observar que ambos algoritmos tienen sus fortalezas y debilidades, pero AES se destaca como la opción superior.

La transparencia del sistema también es fundamental. Tanto AES como 3DES son estándares abiertos, pero la antigüedad de 3DES lo hace más susceptible a vulnerabilidades descubiertas con el tiempo. AES, con su diseño más reciente, asegura que la seguridad no dependa de la confidencialidad del algoritmo, logrando una puntuación de 10, mientras que 3DES obtiene 8.

La facilidad para recordar y cambiar las claves es otro factor crítico en un entorno financiero. AES, con sus opciones de clave más manejables, facilita esta tarea y recibe una puntuación de 9. Por otro lado, la complejidad de las claves de 3DES lo hace menos práctico, obteniendo una puntuación de 8.

La eficiencia y velocidad del algoritmo también son esenciales para las transacciones financieras que requieren procesamiento rápido. AES es más rápido y eficiente que 3DES, lo que lo hace ideal para aplicaciones modernas, obteniendo una puntuación de 9 frente a los 7

de 3DES, que puede ralentizarse debido a su triple cifrado.

En términos de implementación, AES puede ser fácilmente adaptado tanto en hardware como en software con alta eficiencia, logrando una puntuación de 9. 3DES, aunque también puede ser implementado en ambos, no es tan eficiente, alcanzando solo 8 puntos.

Finalmente, la facilidad de uso es vital para asegurar que el personal de TI pueda manejar el sistema sin necesidad de entrenamiento extenso. AES es más simple de implementar y usar, con una puntuación de 10, mientras que 3DES, debido a su complejidad adicional, obtiene 8.

3.2. Discusión

Respecto al objetivo específico, establecer los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana, se seleccionaron dichos algoritmos mediante una revisión sistemática de la literatura considerando las etapas propuestas por Kitchenham & Charters mediante la cual establecieron a AES y 3DES como los algoritmos de criptografía más ampliamente reconocidos y utilizados por su seguridad y eficiencia. Según esta literatura revisada, ambos algoritmos son relevantes porque han sido sometidos a rigurosas pruebas de seguridad por parte de expertos en criptografía y han resistido ataques durante muchos años, destacando ambos, en particular, porque son estándares de facto para el cifrado de datos sensibles y ha sido adoptado por el gobierno de los Estados Unidos para proteger información clasificada. En cuanto a la eficiencia que se pudo distinguir en estos estudios, tanto AES como 3DES son algoritmos eficientes en términos de rendimiento, lo que significa que pueden cifrar y descifrar datos de manera rápida y sin consumir demasiados recursos computacionales. Esto es crucial en entornos financieros donde se manejan grandes volúmenes de datos y se requiere un procesamiento rápido.

Estos resultados concuerdan con los obtenidos por, Wang [12] quien abordó la situación actual en la gestión de seguridad de documentos electrónicos como contexto de investigación, y se logró proponer una solución para abordar esta problemática de manera efectiva mediante una estrategia que fusionó la teoría técnica de gestión de archivos con el algoritmo de cifrado AES, y que a su vez incorpora el principio teórico de gestión de archivos en conjunción con el algoritmo de cifrado DES. Este enfoque aprovecha las particularidades de la gestión de archivos para subsanar las deficiencias inherentes a los algoritmos AES y DES, con el objetivo de lograr un cifrado más eficaz y robusto, y de esta forma mejorar la resistencia ante intentos de descifrado. Los resultados obtenidos evidenciaron que, DES es mejor algoritmo en cuanto a cifrado obteniendo un +24.58% y en cuanto a descifrado obteniendo un +27.49%. Cuando se utilizan archivos de subida cifrados, el algoritmo de cifrado AES es ligeramente más rápido que el DES. Se concluyó que, desde el punto de vista de la experiencia del usuario, el mayor tiempo de carga debido al cifrado sigue siendo aceptable.

Respecto al objetivo específico, analizar los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras, se analizaron los principales ataques, los cuales fueron previamente seleccionados mediante una búsqueda de artículos en las bases de datos en las cuales también se investigaron los algoritmos más relevantes, de manera que se seleccionaron ocho (08) ataques. Esta metodología de búsqueda fue sólida, ya que permitió identificar y priorizar los ataques más significativos y pertinentes para el contexto de seguridad de datos en empresas financieras. Los ocho ataques mencionados abarcan una amplia gama de técnicas de ataque, desde ataques clásicos como Fuerza Bruta y Diccionario hasta ataques más sofisticados como Criptoanálisis y Ataque de Canal Lateral. Esta diversidad es esencial, ya que refleja la realidad de las amenazas a las que se enfrentan las empresas financieras en el entorno actual de ciberseguridad. Además de examinar los ataques, se menciona que se investigaron los algoritmos de cifrado más relevantes. Esto es

crucial, ya que los algoritmos de cifrado son la primera línea de defensa contra muchos de estos ataques. Al comprender los algoritmos más utilizados y sus vulnerabilidades potenciales, las empresas financieras pueden tomar decisiones informadas sobre qué medidas de seguridad implementar.

Estos resultados son muy parecidos a los obtenidos por Lozano & Guerrero [30] quienes tuvieron un objetivo de investigación muy parecido pues también seleccionaron los algoritmos criptográficos más relevantes se centraban en garantizar la seguridad de los datos durante el envío a través de internet. Este objetivo implicaba identificar y evaluar los algoritmos de cifrado más adecuados para proteger la información sensible que se transmite en forma de texto plano por la red. En resumen, el objetivo específico de selección de algoritmos criptográficos más relevantes busca encontrar las herramientas de cifrado más efectivas que puedan garantizar la confidencialidad e integridad de los datos durante su transmisión por internet. Esto implica evaluar varios algoritmos criptográficos y seleccionar aquellos que sean más seguros y adecuados para proteger la información frente a posibles ataques cibernéticos, por lo que como resultado final seleccionaron un total de once (11) ataques criptográficos.

Respecto al objetivo específico, desarrollar en lenguaje de programación los algoritmos de criptografía para el cifrado de datos de un texto plano en documentos privados de una empresa financiera peruana. Los algoritmos fueron desarrollados en lenguaje PHP, así como su integración en un sistema web denominado Sfile para cifrar datos de un texto plano en documentos privados de una empresa financiera peruana fue trascendental para comprender la eficacia y la relevancia de esta implementación. El hecho de haber desarrollado los algoritmos de cifrado AES y 3DES en PHP es un paso crucial hacia la protección de los datos sensibles de la empresa financiera. Esto demuestra un compromiso con la seguridad de la información y proporciona una solución interna para cifrar datos de manera efectiva. El uso de AES y 3DES para el cifrado de datos es una elección sólida, ya

que ambos son algoritmos bien establecidos y ampliamente utilizados en el campo de la criptografía. AES, en particular, es considerado uno de los estándares de cifrado más seguros y eficientes disponibles. El alojamiento de los algoritmos en un sistema web denominado Sfile proporciona una plataforma conveniente y accesible para cifrar documentos privados de la empresa financiera. Esto facilita su uso por parte del personal de la empresa y garantiza que el cifrado de datos sea una parte integral de los procesos operativos. Al implementar algoritmos de cifrado en un sistema interno, la empresa financiera demuestra su compromiso con el cumplimiento normativo y la protección de la información confidencial de sus clientes. Esto es especialmente importante en el contexto actual de crecientes amenazas cibernéticas y regulaciones estrictas en materia de privacidad de datos.

Estos resultados concuerdan con los obtenidos por Wang [12] quien desarrolló un sistema de gestión de archivos facilitando enormemente la gestión de archivos del usuario para que así puedan encriptarlos y desencriptarlos mediante los algoritmos AES y 3DES. Este autor, primeramente, diseñó la arquitectura del sistema de gestión de archivos, incluyendo en ello determinar cómo se almacenarán y organizarán los archivos, así como qué funcionalidades y características tendrá el sistema. Luego procedió a implementar los algoritmos de cifrado AES y DES en el sistema, escribiendo el código necesario para encriptar y desencriptar archivos utilizando estos algoritmos, empleando para ello bibliotecas como PyCrypto o cryptography para implementar AES y DES. Una vez que los implementó, los integró en el sistema de gestión de archivos. Esto implica modificar el flujo de trabajo del sistema para que los archivos se encripten automáticamente cuando se cargan en el sistema y se desencripten cuando se solicitan.

Respecto al objetivo específico, plantear recomendaciones que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos. La investigación realizada proporciona una visión detallada de la implementación y funcionamiento de los algoritmos AES y 3DES en el contexto específico de una empresa

financiera peruana, Profuturo AFP. La aplicación de estos algoritmos se considera una medida crucial para garantizar la seguridad de los datos sensibles manejados por la AFP, especialmente en un entorno donde la integridad de la información financiera es de suma importancia. Las recomendaciones planteadas son fundamentales para mejorar aún más la seguridad de los datos en dicha compañía financiera peruana. La implementación de algoritmos criptográficos actualizados y seguros, como AES, y la utilización de claves sólidas y complejas son pasos clave para fortalecer la protección de la información confidencial. Además, la gestión integral de claves y el monitoreo continuo del sistema de cifrado son aspectos esenciales para garantizar su eficacia a lo largo del tiempo. En cuanto al uso de 3DES, se recomienda limitarlo y considerar su migración hacia algoritmos más seguros como AES. Sin embargo, mientras se planifica esta transición, se sugiere implementar la triple encriptación (EEE) para aumentar la seguridad del cifrado. Es crucial establecer un sólido sistema de gestión de claves para 3DES y considerar alternativas más seguras en el largo plazo. Además, se destacó la importancia de cumplir con las regulaciones y normativas de seguridad de datos, así como de realizar auditorías periódicas para evaluar la efectividad de las medidas implementadas. La capacitación y concientización del personal sobre las mejores prácticas de seguridad cibernética son aspectos clave para promover una cultura organizacional centrada en la protección de la información. En resumen, las recomendaciones planteadas proporcionan un marco integral para mejorar la seguridad de los datos en Profuturo AFP, asegurando así la seguridad de la información financiera de sus afiliados y pensionistas, fortaleciendo no solo la protección de los datos sensibles de la empresa, sino también mantener la confianza y la reputación en el mercado financiero.

Estos resultados obtenidos se contraponen con los obtenidos por Bahman et al. [14] quien, aunque su trabajo "Evaluating Encryption Algorithms for Sensitive Data Using Different Storage Devices" proporciona una evaluación detallada de varios algoritmos de cifrado en diferentes dispositivos de almacenamiento, carece de una parte crucial en la investigación: la

propuesta de recomendaciones basadas en los resultados obtenidos. La ausencia de estas recomendaciones limita significativamente la utilidad práctica del estudio y deja a los lectores sin una guía clara sobre cómo aplicar los hallazgos en entornos reales para mejorar la seguridad de los datos sensibles. La falta de recomendaciones puede ser una oportunidad perdida para traducir los resultados de la investigación en acciones concretas que las organizaciones pueden tomar para mejorar su seguridad de datos. Estas recomendaciones podrían incluir sugerencias sobre qué algoritmos de cifrado son más adecuados para diferentes tipos de datos o dispositivos de almacenamiento, cómo configurar adecuadamente los parámetros de seguridad, cómo gestionar y proteger las claves de cifrado, entre otros aspectos relevantes para la implementación efectiva de la seguridad de datos. Además, la inclusión de recomendaciones habría enriquecido la discusión y la relevancia práctica del estudio, mostrando a los lectores cómo pueden utilizar los resultados para fortalecer sus prácticas de seguridad de datos y proteger la información sensible de manera más efectiva. Sin estas recomendaciones, el impacto y la aplicabilidad del trabajo pueden verse comprometidos, limitando su valor para la comunidad de seguridad de la información y las organizaciones que buscan mejorar su postura de seguridad.

3.3. Aporte de la investigación

3.3.1 Definir los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana.

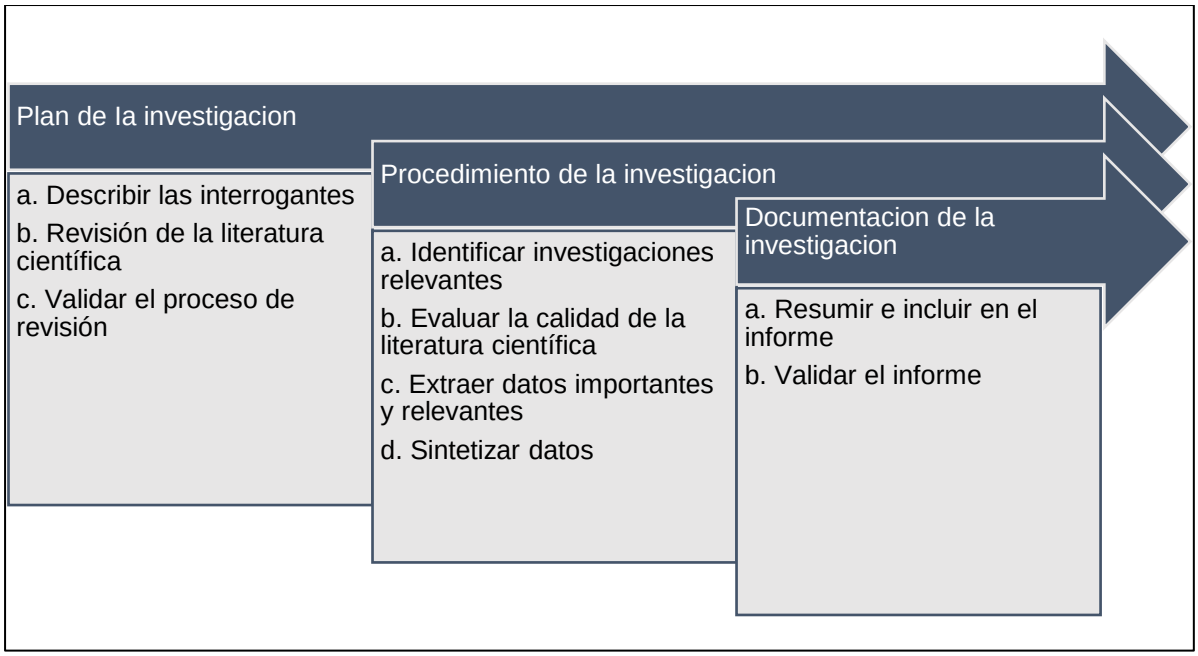
Proceso de selección de algoritmos de encriptación

Esta investigación aporta ampliando los datos existentes sobre los algoritmos de criptografía de manera que puedan utilizarse en una empresa financiera peruana. Asimismo, se identificó en primer lugar los algoritmos de criptografía para luego seleccionarlos, y durante el proceso de la investigación se realizó una revisión de la literatura científica siguiendo los métodos propuestos por Mohamed Elhoseny [13], Bahman A. Sassani Sarrafpour [14] y Jia Xu [16], que tiene 3 pasos, los cuales son; plan, procedimiento y documentación. Como resultado de este trabajo tenemos 2 algoritmos 3DES y AES.

Entre los documentos encontrados destacó el trabajo del señor Luis Cáceres Álvarez quien desarrolló un simulador que ejecuta algoritmos de criptografía cuántica llamado E91, en este sistema se probó algoritmos AES a través de una interfaz llamada Módulo Descifrador y concluye que la tecnología actual de criptografía como RSA, DES y AES se volverán obsoletas cuando la computación cuántica se vuelvan una realidad.

La revisión de la literatura fue en 3 fases, es decir, el plan, el procedimiento y la documentación de la investigación, como se aprecia en la siguiente figura:

Figura 28. Fases ejecutadas para la revisión de la literatura.



Fuente: Elaboración propia.

Plan de la investigación:

a) Describir las interrogantes
b) Revisión de la literatura científica
c) Validar el proceso de revisión

Procedimiento de investigación:

a) Identificar investigaciones relevantes
b) Evaluar la calidad de la literatura científica encontrada
c) Extraer datos importantes y relevantes
d) Sintetizar datos

Documentación de la investigación:

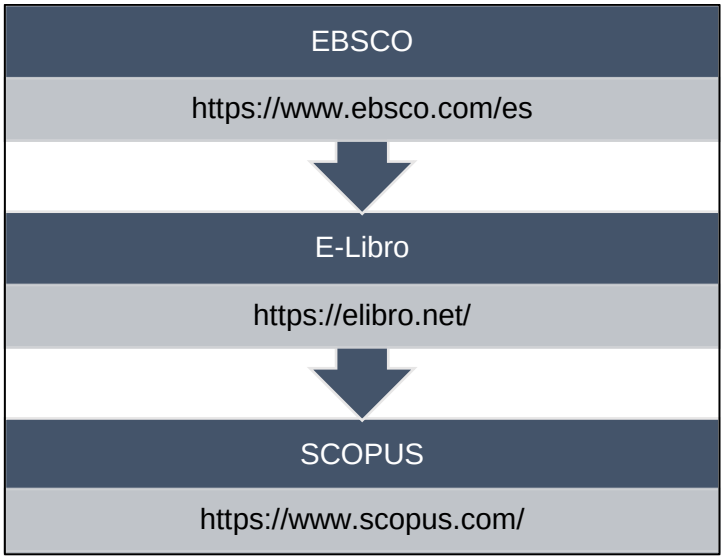
a) Resumir e incluir en el informe

b) Validar el informe

En primer lugar, se planteó interrogantes de investigación que conducen el proceso de búsqueda de la literatura, basado en las preguntas se estableció la región.

El proceso de análisis de la literatura científica fue realizado mediante el uso de la estructura Population, Intervention, Comparison, Outcome, Context (PICOP), las investigaciones fueron extraídas de las bases de datos EBSCO, E-Libro y SCOPUS.

Figura 29. Bases de datos científicas empleadas.



Fuente: Elaboración propia.

Con las bases de datos listas para la búsqueda de información, se procedió a la ejecución de la búsqueda mediante la siguiente cadena:

Figura 30. Cadena de búsqueda empleada para el análisis de artículos.

("evaluation of cryptographic algorithms" AND "comparison of cryptographic algorithms" AND "analysis of cryptographic algorithms")

Fuente: Elaboración propia.

De todas las investigaciones encontradas sólo se revisó las que fueron publicadas en los 5 últimos años (2015 – 2020), cuyo contenido era encriptación de información. Los bases seleccionados pertenecen al campus de la USS, por tal motivo son confiables.

Con respecto, al proceso de selección de las investigaciones, sólo se revisó las publicaciones en idioma inglés pues son de mayor reputación, tienen mayor detalle y mejores resultados, de esta manera, el total de las investigaciones escogidas fueron 15 y organizados por resultados.

Figura 31. Fases de la revisión de la literatura.

Fuente: Elaboración propia.

Para garantizar la veracidad de la literatura científica encontrada, se plantearon 3 preguntas, en referencia al material bibliográfico, algoritmos más utilizados, patrones de encriptación y técnicas de encriptación:

a. ¿Cuánto material bibliográfico relacionado a los algoritmos de encriptación se ha publicado entre los años 2014 a 2021?

Las investigaciones relacionadas para AES y 3DES fueron 1 para el 2014, ninguno para el 2015, 1 para el 2016, ninguno para el 2017, 1 para el 2018, 1 para el 2019, 5 para el 2020 y 1 para el 2021.

Tabla IX.

Publicaciones de algoritmos AES y 3DES agrupado por año

N°	Algoritmo	Año	Investigación
1	AES, 3DES	2014	Luis Cáceres Álvarez [20]
2	AES, 3DES	2015	
3	AES, 3DES	2016	Omar Javier Solano Rodríguez [19]
4	AES, 3DES	2017	
5	AES, 3DES	2018	Mohamed Elhoseny [13]
6	AES, 3DES	2019	Carlos Roberto Sampedro Guamán [21]
			BahmanA. Sassani Sarrafpour [14]
			Franyelit María Suárez [15]
7	AES, 3DES	2020	Benavides Eduardo [17]
			Daniel F. Santos [18]
			Jia Xu [16]
8	AES, 3DES	2021	Latif AKCAY [6]

Nota. Lista de algoritmos agrupados por año y algoritmos. Fuente: Elaboración propia.

b. ¿Cuáles son los algoritmos de encriptación más utilizados?

En 15 investigaciones se mencionan el uso de 3DES y el AES, en 7 se mencionan el uso del algoritmo IDEA, en 6 investigaciones se mencionan el uso de MD5, en 5 se mencionan el uso de SHA, en 8 se mencionan el uso de RSA, en 5 se mencionan el uso de ElGamal y por último y no menos importante, en 4 se menciona el uso de DSA.

Tabla X.

Publicaciones referidas a los algoritmos de criptografía más utilizados

N°	Algoritmos de criptografía	Veces utilizados
1	3DES	15
2	AES	15
3	IDEA	7
4	MD5	6
5	SHA	5
6	RSA	8
7	EIGamal	5
8	DSA	4

Nota. Lista de algoritmos más utilizados. Fuente: Elaboración propia.

Por otro lado, los algoritmos criptográficos más utilizados por las empresas públicas y privadas. Se encontró publicaciones en sitios web de las empresas mismas, en donde mencionan el uso de los algoritmos AES y 3DES, también se evidencia que son los más utilizados, las publicaciones encontradas son de empresas importantes como Bancos, AFP y Universidades, que tuvieron la necesidad de implementar el uso de algoritmos de criptografía para encriptar información confidencial. Las publicaciones fueron seleccionados de entre las empresas más representativas que tienen altos niveles de seguridad y protocolos de comunicación seguras y que antes de implementar herramientas de seguridad las evalúan de manera exhaustiva.

Estas publicaciones en su mayoría son de las páginas webs oficiales de cada empresa respectivamente. En la tabla siguiente se listan los países donde encontraron las publicaciones, las entidades, el tipo de entidad, estatal o privada y el año de publicación.

Tabla XI.

Publicaciones de algoritmos más utilizados por las empresas públicas y privadas

PAIS	TIPO	ENTIDAD	AÑO
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [32]	2009
Argentina	ENTIDAD ESTATAL EXTRANJERO	Poder judicial provincia del Neuquén [33]	2012
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [34]	2015

Perú	EMPRESA ESTATAL	Banco de la nación [35]	2016
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [36]	2018
Argentina	ENTIDAD ESTATAL EXTRANJERO	Banco central de la república argentina [37]	2019
República dominicana	ENTIDAD ESTATAL EXTRANJERO	Superintendencia de bancos de la republica dominicana [38]	2019
México	ENTIDAD ESTATAL EXTRANJERO	Poder judicial tribunal superior del estado de Yucatán [39]	2020
Uruguay	ENTIDAD ESTATAL EXTRANJERO	Banco de la república oriental del Uruguay [40]	2020
Perú	ENTIDAD ESTATAL NACIONAL	Municipalidad distrital de tambo grande [41]	2020
Colombia	EMPRESA EXTRANJERA	La previsora s.a. compañía de seguros [42]	2021
México	ENTIDAD ESTATAL EXTRANJERO	Poder judicial del estado de Yucatán [43]	2021

Perú	ENTIDAD ESTATAL NACIONAL	Banco central de reserva del Perú [44]	2021
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia nacional de aduanas y de administración tributaria [45]	2021
Estados unidos	EMPRESA EXTRANJERA	Amazon web service (aws) [46]	2022
México	ENTIDAD ESTATAL EXTRANJERO	Universidad autónoma del estado de hidalgo [47]	2022
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [48]	2022
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [49]	2022
España	EMPRESA EXTRANJERA	Rtve corporación radio televisión española s.a. [50]	2023
Argentina	ENTIDAD ESTATAL EXTRANJERO	Provincia santa fe caja de jubilaciones y pensiones [51]	2023
Perú	ENTIDAD ESTATAL NACIONAL	Banco central de reserva del Perú [52]	2023

Perú	ENTIDAD ESTATAL NACIONAL	Banco central de reserva del Perú [53]	2023
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [54]	2023
Perú	ENTIDAD ESTATAL NACIONAL	Banco central de reserva del Perú [55]	2024
Perú	ENTIDAD ESTATAL NACIONAL	Superintendencia de banca, seguros y AFP [56]	2024

Fuente: Elaboración propia.

Por otro lado, en el contexto de la seguridad de datos de las empresas privadas y estatales importantes han considerado el uso de algoritmos criptográficos robustos y de mayor reputación, como AES y 3DES, justamente para garantizar y salvaguardar la integridad y confidencialidad de la información. Por ejemplo, en el Informe nº 027-2009-gti y el Anexo 1 se especifica la necesidad de estándares AES - 3DES para los servicios de Mcafee y Checkpoint, subrayando la importancia de estos algoritmos en la protección contra vulnerabilidades cibernéticas. Así mismo en licitaciones como nº 03/12 - expte. Nº 18677 y la Licitación pública nº 009/2015-sbs para el desarrollo este proyecto se solicitó el uso del algoritmo criptográfico AES esto para asegurar y garantizar que todas las conexiones sean confiables y seguras además que los sistemas electrónicos mantengan niveles altos de calidad. Por otro lado, el uso de AES y 3DES ha sido solicitado para la encriptación de voz en la telefonía IP, tal como se describe en la Adjudicación simplificada nº 027/2018-sbs.

Esto evidencia cómo los algoritmos de encriptación AES y 3DES son necesarios para

cumplir con los estándares de seguridad y protección de datos en muchas plataformas y servicios críticos en el sector público y privado. La implementación de estos algoritmos de encriptación no solo asegura la confidencialidad de los datos y la información que se envía y se almacenada, sino que también garantiza y asegura la integridad de las transacciones y fortalece ante los posibles ataques y amenazas cibernéticas que pudieran aparecer.

En la siguiente tabla se muestra la lista de publicaciones, indicando el país, el detalle de la publicación, el documento, el tipo y el uso de AES y 3DES.

Tabla XIII.

Publicaciones de algoritmos más utilizados por las empresas públicas y privadas

PAIS	DETALLE	DOCUMENTO	TIPO	AES	3DES
Perú	Para la seguridad de datos en los servicios Mcafee y Checkpoint se demandó emplear estándares aes - 3des	Informe nº 027-2009-gti	ENTIDAD ESTATAL NACIONAL	X	X
Argentina	Para conexiones confiables inalámbricas Odu radwin rw-2000 c-series demandó aes	Licitación pública nº 03/12 - expte. Nº 18677	ENTIDAD ESTATAL EXTRANJERO	X	
Perú	Para los sistemas electrónicos para seguridad de locales SBS se solicitó equipos con aes como recurso criptográfico confiable	Licitación pública nº 009/2015-sbs (primera convocatoria)	ENTIDAD ESTATAL NACIONAL	X	

Perú	Para la grabación de la huella digital en operaciones de pago de programas sociales se solicitó uso algoritmo seguro aes - 3des	Informe técnico previo de evaluación de software n° 001/2470	EMPRESA ESTATAL	X	X
Perú	Para los servicios de voz de telefonía IP se demandaron encriptado de extremo a extremo usando aes	Adjudicación simplificada nº 027/2018-sbs	ENTIDAD ESTATAL NACIONAL	X	
Argentina	Para fortalecer los enlaces de comunicaciones redes LAN y sistema demandó uso aes - 3des	Licitación pública n° xx/19 expediente N° 718/16/19	ENTIDAD ESTATAL EXTRANJERO	X	X
República dominicana	Para asegurar plataforma firewall contra vulnerabilidades tecnológicas, con respecto al VPN IPSEC se demandó aes - 3des	Licitación pública no. Sib-lpn-002/2019	ENTIDAD ESTATAL EXTRANJERO	X	X
México	Para conmutadores de datos se solicitó aes - 3des para cumplir con los niveles de confianza requeridos	Licitación pública número “podjudtsj-ca 13/2020”	ENTIDAD ESTATAL EXTRANJERO	X	X

Uruguay	Para garantizar la confidencialidad en identificadores token digitales y físicas se demandó uso de algoritmo aes - 3des	Expediente ee2020/51/02289	ENTIDAD ESTATAL EXTRANJERO	X	X
Perú	Para la prestación del VPN IPSEC se demandó aes para asegurar la comunicación vía internet	Resolución gerencial N° 208-2020-mdt-gm - términos de referencia	ENTIDAD ESTATAL NACIONAL	X	
Colombia	Con el propósito de fortalecer la seguridad informática solicito conservar algoritmos acreditados como aes - 3des	Invitación abierta no. 005 – 2021	EMPRESA EXTRANJERA	X	X
México	Con el fin de garantizar la seguridad de información en Checkpoint demandó uso de aes - 3des para redes virtuales VPN	Licitación pública número podjudcj 14/2021	ENTIDAD ESTATAL EXTRANJERO	X	X
Perú	Para cajas seguras HSM que garantizan el servicio crucial	Informe nº 0155-2021-gti220-n	ENTIDAD ESTATAL NACIONAL		X

	lbtr y continuidad del software six/tcl indicó que usa 3des				
Perú	Sunat como parte de la transformación digital demandó software de llaves y encriptado a fin con aes - 3des	Lpi n° 005-2021-sunat/bid	ENTIDAD ESTATAL NACIONAL	X	X
Estados unidos	El servicio AWS propone uso aes - 3des como algoritmos autorizados y confiables	Guía prescriptiva mejores prácticas y funciones de cifrado para servicios de AWS	EMPRESA EXTRANJERA	X	X
México	Para conmutadores SWITCH 24 y 48 puertos se solicitó cifrado mejorado super seguro aes	Licitación pública nacional uaeh-lp-n11-2022	ENTIDAD ESTATAL EXTRANJERO	X	
Perú	Para servicios Cloud de licencia vía SAAS se demandó uso de algoritmos aes - 3des, los cuales fueron aceptados y validados por la industria	Concurso público Nº 009/2022-sbs	ENTIDAD ESTATAL NACIONAL	X	X

Perú	Sistema IBM ASPERA cumple la seguridad con el uso algoritmo aes para transferir archivos finales vía SUCAVE y mesa de partes virtual	Informe Nº 00065-2022-gti	ENTIDAD ESTATAL NACIONAL	X	
España	En el rubro de parámetros inalámbricos para el sistema de transmisión de video demandó nada menos que encriptación aes	Pliego de condiciones técnicas expediente s-03898-2023	EMPRESA EXTRANJERA	X	
Argentina	Para resguardar el software robots de procesamiento automatizado (RPA) demandó utilizar aes	Licitación privada n° 02 / 23 expediente n° 15120-0159117-7	ENTIDAD ESTATAL EXTRANJERO	X	
Perú	Para aumentar el nivel de veracidad del sistema LBTR con las cajas de seguridad six/tcl demandó cifrado aes - 3des	Informe nº 0063-2023-gti220-n	ENTIDAD ESTATAL NACIONAL	X	X
Perú	En la homologación de licencias para software six/tcl se solicitó incorporar aes - 3des	Informe nº 0068-2023-gti220-n	ENTIDAD ESTATAL NACIONAL	X	X

	para mayor fiabilidad de las transferencias bancarias				
Perú	Para servicios Cloud se demandó algoritmos aes - 3des los cuales fueron aceptados y validados por la industria	Adjudicación simplificada n° 47-2023-sbs	ENTIDAD ESTATAL NACIONAL	X	X
Perú	En la renovación de la versión del software six/tcl incorporo aes para las cajas seguras HSM	Informe nº 0208-2024gti220-n	ENTIDAD ESTATAL NACIONAL	X	
Perú	Para proteger los correos electrónicos y correos SAAS se demandó cifrado aes	Adjudicación simplificada n° 002-2024-sbs (primera convocatoria)	ENTIDAD ESTATAL NACIONAL	X	

Fuente: Elaboración propia.

El siguiente cuadro muestra cuantas veces se utiliza AES y 3DES por tipo de entidades, se evidencia que en total 25 veces fuero utilizados, sin embargo, solo 3DES fue utilizado 1 vez por una entidad estatal nacional, AES fue utilizado 6 veces en una entidad estatal, 1 vez por una empresa extranjera y 3 veces en una entidad estatal extranjera, en total 10 veces para AES, finalmente 1 vez fue utilizada por una empresa estatal, 6 veces por una entidad estatal nacional, 2 veces por una empresa extranjera, 5 veces por una entidad estatal extranjera, en total 14 veces.

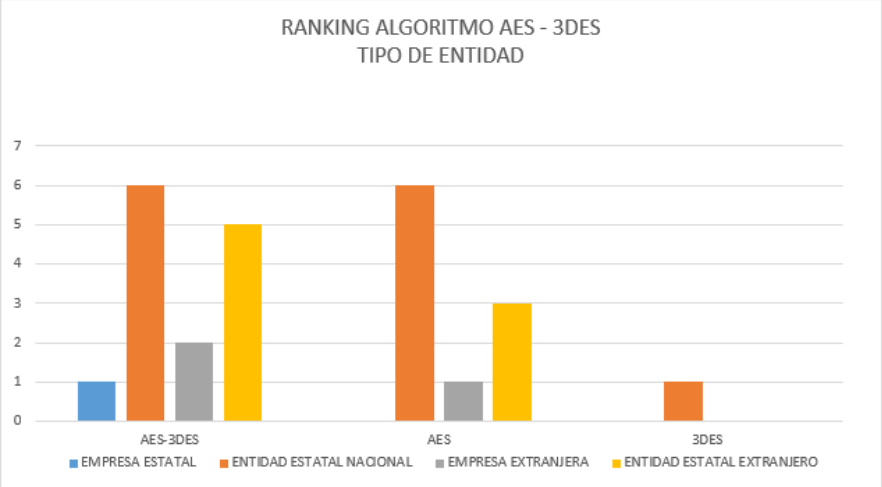
Figura 32. Cuadro de resumen del uso de AES – 3DES por tipo de entidades

	AES-3DES	AES	3DES
EMPRESA ESTATAL	1		
ENTIDAD ESTATAL NACIONAL	6	6	1
EMPRESA EXTRANJERA	2	1	
ENTIDAD ESTATAL EXTRANJERO	5	3	
	14	10	1

Fuente: Elaboración propia.

La siguiente imagen es la representación de la lista del cuadro de resumen del uso de AES – 3DES por tipo de entidades, en esta grafica se evidencia que hay mayor publicaciones web para entidades estatales nacionales para AES.

Figura 33. Diagrama de resumen del uso de AES – 3DES por tipo de entidades



Fuente: Elaboración propia.

El siguiente cuadro muestra las publicaciones encontradas por años y por algoritmo de encriptación.

Figura 34. Cuadro de resumen del uso de AES – 3DES por año de publicación

	AES-3DES	AES	3DES
2009	1		
2012		1	
2015		1	
2016	1		
2018		1	
2019	2		
2020	2	1	
2021	3		1
2022	2	2	
2023	3	2	
2024		2	
	14	10	1

Fuente: Elaboración propia.

La siguiente grafica muestra el resumen del uso de AES – 3DES por año de publicación, en este se evidencia que las publicaciones se concentran entre los años 2019 y el año 2023

Figura 35. Diagrama de resumen del uso de AES – 3DES por año de publicación

Fuente: Elaboración propia.

Según el análisis ejecutado en la tabla anterior, puede, de manera cualitativa, identificarse que, el algoritmo AES tiene mejores características para el cumplimiento de los niveles de seguridad de datos de una empresa financiera peruana.

c. ¿Qué método, técnica, se utilizan para la encriptación de la información?

Para el método de encriptación simétrico se encontró 4 algoritmos, para el asimétrico se encontraron 4 algoritmos y para mixto se encontraron 2 algoritmos.

Tabla XIII.

Publicaciones de algoritmos y sus métodos de ejecución

N°	Método de encriptación	Cantidad	Algoritmos empleados
1	SIMÉTRICO	4	3DES AES IDEA MD5
2	ASIMÉTRICO	4	SHA RSA ELGamal DSA
3	MIXTO	2	RSA DSA

Nota: Lista de algoritmos y métodos. Fuente: Elaboración propia.

Se identificó las investigaciones más relevantes gracias a la estructura PICOP, pues

responden a las preguntas planteadas, de manera que en su contenido tenían algoritmos, protocolos, métodos y técnicas de encriptación.

A continuación, la lista de los criterios de Exclusión e Inclusión, estos criterios se aplicaron sobre el resumen, desarrollo y conclusiones.

Respecto a los Criterios de Exclusión se tuvieron los siguientes:

- E1 - Estudios que contienen conclusiones poco precisas.
- E2 - Estudios que no abordan las técnicas actuales de encriptación
- E3 - Estudios no publicados desde 2014 hasta 2021
- E4 - Estudios publicados en idioma español.

La tabla siguiente muestra el resultado de las investigaciones que se descartó dado que cumplían con los criterios de exclusión.

Tabla XIV.

Listado de publicaciones excluidas

N°	Referencia	E1	E2	E3	E4
1	Mohamed Elhoseny [13]				
2	BahmanA. Sassani Sarrafpour [14]				
3	Franyelit María Suárez [15]				

4	Jia Xu [16]				
5	Benavides Eduardo [17]				
6	Daniel F. Santos [18]				
7	Omar Javier Solano Rodríguez [19]				
8	Luis Cáceres Álvarez [20]				
9	Latif AKCAY [6]				
10	Carlos Roberto Sampedro Guamán [21]				
11	Angelina Espejel, Mariko Nakano y Héctor Pérez(2012)	X	X	X	X
12	Yran Marrero Travieso (2003)	X	X	X	X
13	Renan Correa Detomini(2011)	X	X	X	X
14	Santos, Daniel F (2020)	X	X	X	X
15	Rubén D. Nieto, Alvaro Bernai(2013)	X	X	X	X

Nota. Exclusión de trabajos de investigación. Fuente: Elaboración propia.

Respecto a los criterios de inclusión se tuvieron los siguientes:

- I1 - Estudios que contienen conclusiones precisas.
- I2 - Estudios que abordan las técnicas actuales de encriptación
- I3 - Estudios publicados desde 2014 hasta 2021
- I4 - Estudios publicados en idioma inglés

La siguiente tabla muestras las investigaciones utilizadas para realizar este trabajo, los cuales cumplían con los criterios de inclusión.

Tabla XV.

Listado de publicaciones incluidas

N°	Referencia	I1	I2	I3	I4
1	Mohamed Elhoseny [13]	X	X	X	X
2	BahmanA. Sassani Sarrafpour [14]	X	X	X	X
3	Franyelit María Suárez [15]	X	X	X	X
4	Jia Xu [16]	X	X	X	X
5	Benavides Eduardo [17]	X	X	X	X
6	Daniel F. Santos [18]	X	X	X	X
7	Omar Javier Solano Rodríguez [19]	X	X	X	X

8	Luis Cáceres Álvarez [20]	X	X	X	X
9	Latif AKCAY [6]	X	X	X	X
10	Carlos Roberto Sampedro Guamán [21]	X	X	X	X
11	Angelina Espejel, Mariko Nakano y Héctor Pérez (2012)				
12	Yran Marrero Travieso (2003)				
13	Renan Correa Detomini(2011)				
14	Santos, Daniel F (2020)				
15	Rubén D. Nieto, Alvaro Bernai(2013)				

Nota. Trabajos de investigación incluidos. Fuente: Elaboración propia.

Posteriormente a la identificación de los 10 artículos científicos que servirían para los antecedentes de esta investigación, y que son algoritmos de criptografía que pretenden cumplir con los niveles de seguridad de datos, se procedió a seleccionarlos con propósitos de evaluarlos. A partir de las métricas encontradas en los artículos científicos, se pudieron evidenciar los siguientes resultados:

Tabla XVI.

Comparación de algoritmos según la literatura científica

Tamaño (MB)	Algoritmo	T-Cifrado	T-Descifrado
64	AES	1.159.563	1.078.016
64	ARC2	9.952.153	9.563.221
64	Blowfish	2.760.837	2.780.431
64	CAST	9.126.131	9.135.119
64	3DES	1.231.014	1.230.503

Fuente: Elaboración propia.

Según la tabla anterior, son AES y 3DES los que tienen mejor rendimiento en cifrado y descifrado, habiéndose ejecutado los experimentos con un mensaje de 64MB. Sin embargo, aún existía una brecha en cuanto a una visión general de cómo se comparan los cinco (05) algoritmos criptográficos en diferentes aspectos clave. Por tanto, para ello, esta investigación ejecutó una búsqueda asociada a estos algoritmos encontrados en la literatura científica. Para ello se fundamentó en el estudio ejecutado en [57].

Este estudio, presentó un análisis exhaustivo y comparativo de cinco algoritmos criptográficos clave: DES, 3DES, AES, RSA y Blowfish, que justamente coinciden con los algoritmos seleccionados en esta investigación. La evaluación abarcó aspectos cruciales como la seguridad, la eficiencia y su aplicabilidad en diferentes contextos.

Tabla XVII.

Algoritmos de criptografía de mayor usanza según Patil.

N°	Algoritmo	Descripción
1	DES	“Introducido en los años 70, fue uno de los primeros algoritmos de cifrado simétrico ampliamente utilizado. Utiliza una clave de 56 bits, que en la actualidad se considera insuficiente debido a los avances tecnológicos que facilitan los ataques de fuerza bruta. Aunque DES ha sido esencial en la historia de la criptografía, su seguridad limitada ha impulsado la necesidad de desarrollar alternativas más seguras” [57]
2	3DES	“Se creó para mejorar la seguridad de DES aplicando el algoritmo tres veces consecutivas. Esta técnica incrementa significativamente la seguridad, pero también reduce la eficiencia, ya que el proceso de cifrado y descifrado se vuelve más lento comparado con otros algoritmos más modernos” [57].
3	AES	“Fue desarrollado para reemplazar a DES y 3DES, ofreciendo claves de 128, 192 y 256 bits, lo que proporciona un nivel de seguridad mucho mayor. AES destaca por su eficiencia y rapidez, convirtiéndose en el estándar de cifrado simétrico preferido en diversas aplicaciones, desde la protección de datos personales hasta la seguridad en redes corporativas” [57].
4	RSA	“Es un algoritmo de cifrado asimétrico ampliamente utilizado en situaciones que requieren alta seguridad, como el intercambio de claves

		y las firmas digitales. RSA se basa en la dificultad de factorizar números grandes, proporcionando una fuerte seguridad. No obstante, es menos eficiente en términos de velocidad y uso de recursos en comparación con los algoritmos simétricos” [57].
5	Blowfish	“Diseñado como una alternativa más segura y eficiente a DES, permite el uso de claves de longitud variable (hasta 448 bits), adaptándose a distintos niveles de seguridad. Blowfish es conocido por su alta velocidad y efectividad en aplicaciones que requieren cifrado rápido y seguro” [57].

Nota. Fuente, adaptado de [57].

Una vez conceptualizados los cinco (05) algoritmos de criptografía seleccionados, a saber, DES, 3DES, AES, RSA y Blowfish, se procedió a la elección de los parámetros de evaluación adecuados. Estos parámetros fueron cruciales para medir y comparar la efectividad y eficiencia de cada algoritmo. En este caso, se seleccionaron cinco (05) parámetros específicos, algunos de los cuales se mencionan en el informe según la **¡Error! No se encuentra el origen de la referencia.**: tiempo de cifrado, tiempo de descifrado, memoria utilizada, efecto avalancha y entropía. Estos criterios permitieron una evaluación integral de los algoritmos, proporcionando una visión clara de su desempeño en diferentes aspectos críticos para su implementación en diversas aplicaciones.

Tabla XVIII.

Algoritmos de criptografía de mayor usanza según Patil et al.

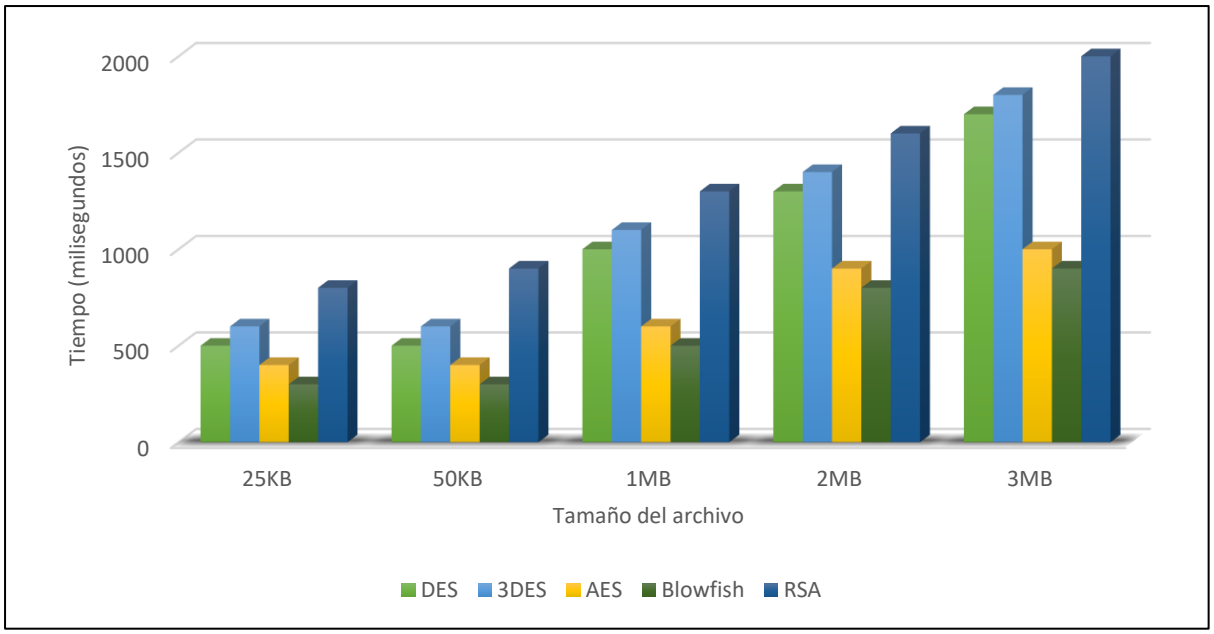
Parámetro	**Descripción**	**Importancia en Criptografía**	**Impacto en la Eficiencia**	**Ejemplo en Instituciones Financieras**

Tiempo de Cifrado	El tiempo que tarda un algoritmo en convertir el texto plano en texto cifrado.	Determina la velocidad del algoritmo, crucial para aplicaciones en tiempo real.	Algoritmos más rápidos son preferidos para sistemas con grandes volúmenes de datos.	Cifrado de transacciones bancarias en línea.
Tiempo de Descifrado	El tiempo que tarda un algoritmo en convertir el texto cifrado de vuelta a texto plano.	Similar al tiempo de cifrado, es vital para aplicaciones donde el descifrado rápido es esencial.	Afecta la eficiencia en la recuperación de datos.	Acceso rápido a datos cifrados de clientes en bases de datos.
Memoria Utilizada	La cantidad de memoria que un algoritmo consume durante el proceso de cifrado y descifrado.	Importante para dispositivos con recursos limitados como teléfonos móviles y dispositivos IoT	Algoritmos con menor uso de memoria son más adecuados para entornos con limitaciones de hardware.	Cifrado en cajeros automáticos y dispositivos de punto de venta.
Efecto Avalancha	La propiedad de un algoritmo donde un pequeño cambio en el texto plano resulta en un cambio significativo en el texto cifrado.	Garantiza la seguridad al hacer difícil predecir cambios en el texto cifrado basados en cambios mínimos en el texto plano.	Algoritmos con un fuerte efecto avalancha son considerados más seguros.	Protección de datos sensibles contra alteraciones.
Entropía	Una medida de la aleatoriedad en el texto cifrado.	Alta entropía indica un mayor nivel de seguridad, haciendo difícil predecir patrones en el texto cifrado.	Afecta la resistencia contra ataques de criptoanálisis.	Generación de contraseñas y claves de cifrado seguras.

Nota. Fuente, adaptado de [57].

Los parámetros revelados en la tabla anterior proporcionan una base sólida para evaluar y comparar la eficiencia de los algoritmos de criptografía en el contexto de las instituciones financieras peruanas, permitiendo una elección informada según las necesidades específicas de seguridad y rendimiento en este sector. A continuación, se tienen:

Figura 36. Tiempo cifrado vs tamaño de archivo para DES, 3DES, AES, Blowfish y RSA.



Nota. Fuente, adaptado de [57].

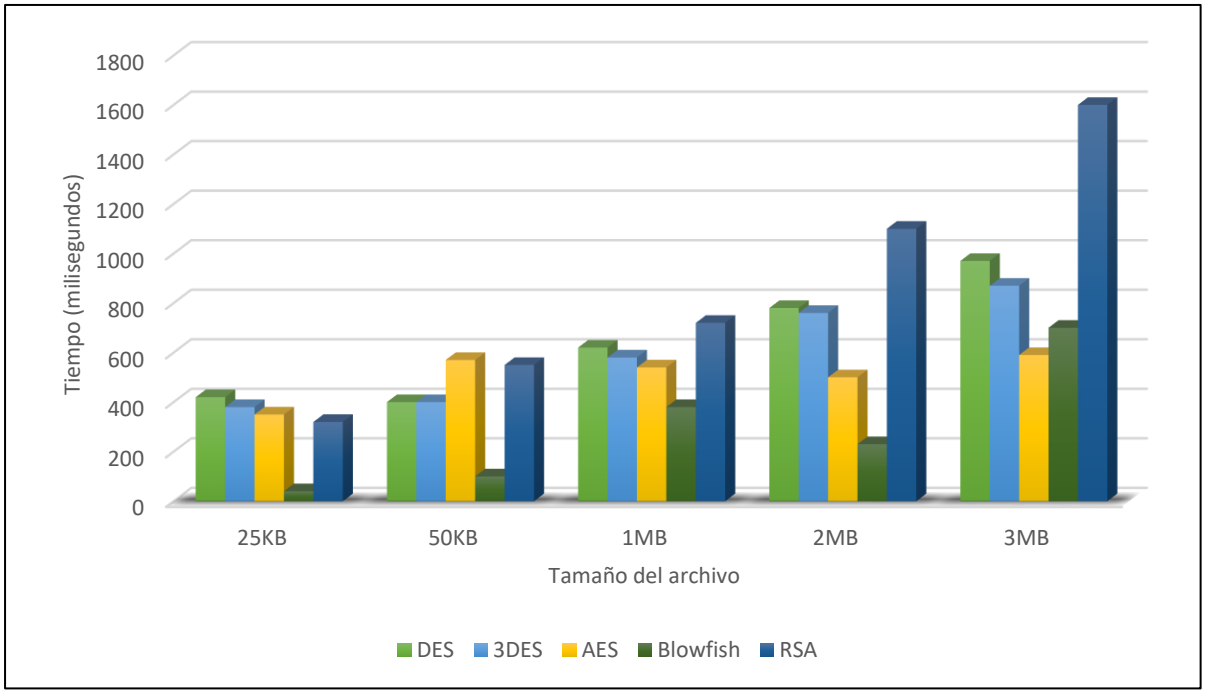
El gráfico previo ilustra el tiempo de cifrado en milisegundos frente a diferentes tamaños de archivo para cinco algoritmos de cifrado: DES, 3DES, AES, Blowfish y RSA. Este análisis se centra en evaluar la eficiencia de estos algoritmos, lo cual es crucial para garantizar niveles óptimos de seguridad de datos en una empresa financiera peruana.

Respecto a la eficiencia de cifrado, AES y Blowfish son los algoritmos más eficientes, mostrando tiempos de cifrado consistentemente bajos; DES y 3DES tienen tiempos de cifrado

más altos, con 3DES siendo notablemente más lento debido a su estructura más compleja y; RSA es el algoritmo más lento, lo cual es esperado debido a la naturaleza computacionalmente intensiva del cifrado asimétrico.

En el contexto de una empresa financiera peruana como es el caso de esta investigación, la elección del algoritmo de cifrado debe equilibrar eficiencia y seguridad. AES y 3DES ofrecen una excelente combinación de ambos factores, haciéndolos ideales para la protección de datos sensibles en operaciones diarias. RSA, debido a su alta seguridad, pero menor eficiencia, puede ser reservado para aplicaciones críticas donde la seguridad de la clave pública es primordial. Este análisis demuestra que una comprensión clara de las características de cada algoritmo es esencial para diseñar una estrategia de cifrado efectiva que cumpla con los niveles de seguridad requeridos en el sector financiero.

Figura 37. Tiempo descifrado vs tamaño de archivo para DES, 3DES, AES, Blowfish y RSA



Nota. Fuente, adaptado de [57].

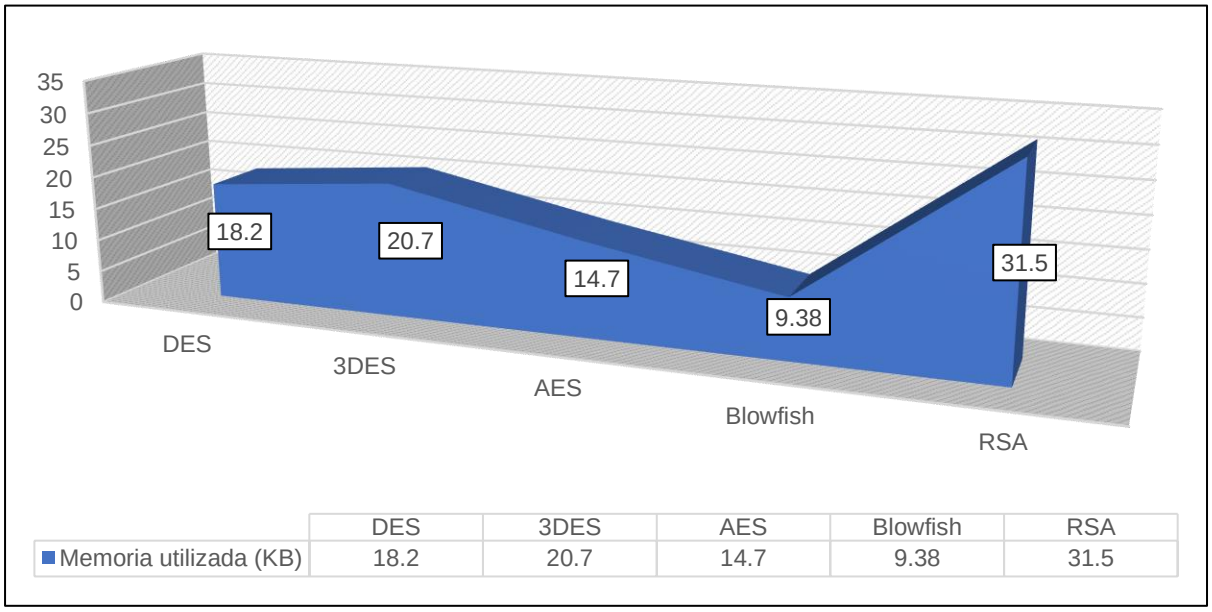
El gráfico previo ilustra el tiempo de descifrado en milisegundos frente a diferentes tamaños de archivo para cinco algoritmos de cifrado: DES, 3DES, AES, Blowfish y RSA. Este análisis se centra en evaluar la eficiencia de estos algoritmos, lo cual es crucial para garantizar niveles óptimos de seguridad de datos en una empresa financiera peruana.

Respecto a la eficiencia de descifrado, AES y Blowfish son los algoritmos más eficientes, mostrando tiempos de descifrado consistentemente bajos en comparación con otros algoritmos, lo que los hace ideales para aplicaciones que requieren alta velocidad y eficiencia; Aunque tienen tiempos de descifrado más altos, DES muestra un aumento significativo con tamaños de archivo más grandes, mientras que 3DES, debido a su estructura más compleja, es notablemente más lento pero ofrece mayor seguridad en comparación con DES y; RSA es el algoritmo más lento, lo cual es esperado debido a la naturaleza computacionalmente intensiva del cifrado asimétrico, haciéndolo menos adecuado para el cifrado de grandes volúmenes de datos pero útil para la protección de claves.

En el contexto de una empresa financiera peruana como es el caso de esta investigación, la elección del algoritmo de cifrado debe equilibrar eficiencia y seguridad. AES y Blowfish ofrecen una excelente combinación de eficiencia y seguridad, haciéndolos ideales para la protección de datos sensibles en operaciones diarias. AES, en particular, es ampliamente adoptado por su robustez y rapidez. 3DES a pesar de ser más lento, puede ser adecuado para aplicaciones que requieren niveles adicionales de seguridad. RSA, debido a su alta seguridad, pero menor eficiencia, puede ser reservado para aplicaciones críticas donde la seguridad de la clave pública es primordial, como en el intercambio de claves o la protección de certificados digitales.

Este análisis demuestra que una comprensión clara de las características de cada algoritmo es esencial para diseñar una estrategia de cifrado efectiva que cumpla con los niveles de seguridad requeridos en el sector financiero.

Figura 38. Memoria utilizada para DES, 3DES, AES, Blowfish y RSA.



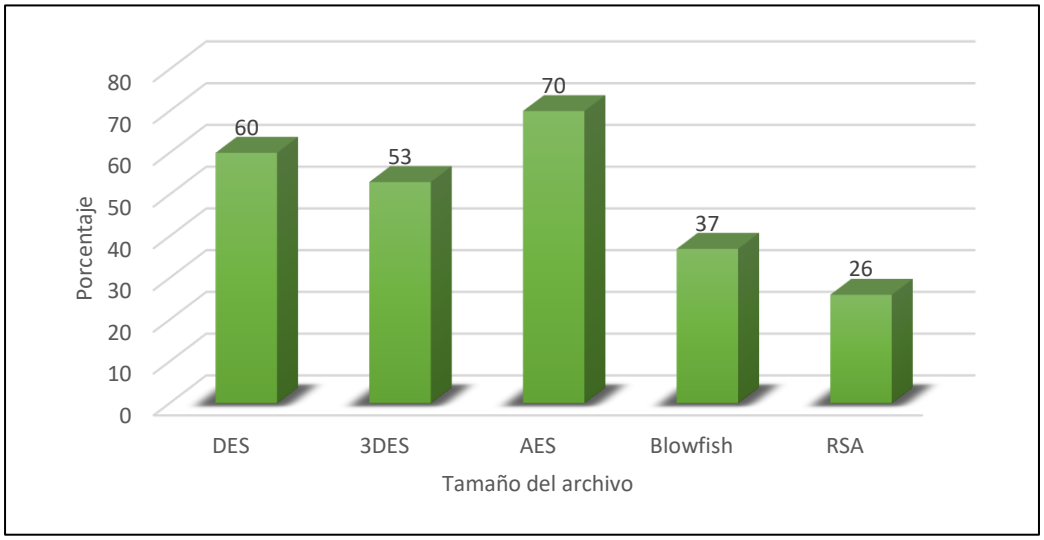
Nota. Fuente, adaptado de [57].

El gráfico previo ilustra la memoria utilizada en KB frente a diferentes tamaños de archivo para cinco algoritmos de cifrado: DES, 3DES, AES, Blowfish y RSA. El algoritmo DES (18.2 KB) consume una cantidad moderada de memoria y aunque no es el más eficiente en términos de uso de memoria, su consumo no es excesivo; 3DES (20.7 KB) tiene un consumo de memoria ligeramente mayor que DES debido a su proceso de cifrado triple, lo que incrementa la seguridad pero también, el uso de recursos; AES (14.7 KB) muestra un uso de memoria relativamente bajo en comparación con DES y 3DES, esto, combinado con su alta eficiencia de descifrado, lo hace una opción muy atractiva; Blowfish (9.38 KB) es el algoritmo que menos memoria utiliza entre los cinco, este bajo consumo de memoria, junto con sus buenos tiempos de descifrado, lo convierte en una opción altamente eficiente para aplicaciones con limitaciones de recursos y; RSA (31.5 KB) utiliza la mayor cantidad de memoria, lo cual es consistente con su naturaleza de cifrado asimétrico que requiere más recursos computacionales. Esto lo hace menos adecuado para aplicaciones que requieren la

gestión de grandes volúmenes de datos en tiempo real.

En el contexto de una empresa financiera peruana, donde la eficiencia y la seguridad son cruciales, el análisis del uso de memoria de estos algoritmos es fundamental para una implementación exitosa. AES y Blowfish son los algoritmos más eficientes en términos de uso de memoria y tiempo de descifrado. AES, con su combinación de baja utilización de memoria y alta seguridad, es ideal para transacciones diarias y protección de datos sensibles. Blowfish, con el menor uso de memoria, es especialmente útil en sistemas con recursos limitados. DES y 3DES, aunque consumen más memoria que AES y Blowfish, siguen siendo opciones viables en entornos donde se requiere un equilibrio entre seguridad y eficiencia. Sin embargo, el uso de 3DES puede justificarse en aplicaciones que necesitan un nivel adicional de seguridad. RSA: Dado su alto consumo de memoria y su menor eficiencia en descifrado, RSA debería ser reservado para aplicaciones específicas que requieren una alta seguridad en el intercambio de claves y certificados, en lugar de ser utilizado para el cifrado de grandes volúmenes de datos.

Figura 39. Efecto avalancha para DES, 3DES, AES, Blowfish y RSA.



Nota. Fuente, adaptado de [57].

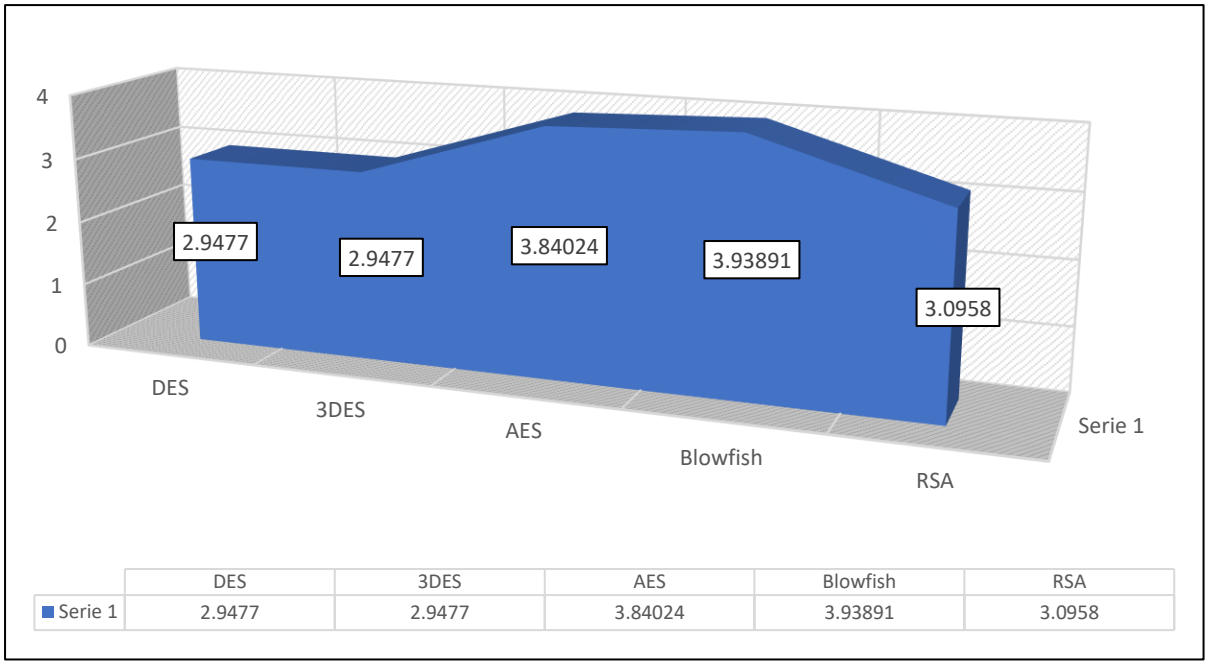
El gráfico previo ilustra el efecto avalancha para cinco algoritmos de cifrado: DES, 3DES, AES, Blowfish y RSA. El efecto avalancha mide el porcentaje de bits modificados en la salida cuando un solo bit de entrada se altera, lo cual es una característica deseada en un buen algoritmo de cifrado para asegurar que pequeñas modificaciones en los datos de entrada resulten en grandes cambios en la salida cifrada, dificultando así el criptoanálisis.

DES tiene un buen efecto avalancha, con un 60% de los bits de salida cambiando cuando se altera un solo bit de entrada. Esto indica una buena difusión, aunque no es el mejor entre los algoritmos evaluados; 3DES (53%), aunque es más seguro que DES debido a su triple aplicación, muestra un efecto avalancha ligeramente inferior al de DES. Esto podría ser debido a su estructura más compleja que, aunque aumenta la seguridad, puede tener implicaciones en la difusión de cambios en los bits; AES (70%) presenta el mejor efecto avalancha indicando que, tiene una excelente capacidad para difundir cambios en la entrada a través de la salida, haciendo más difícil cualquier intento de criptoanálisis diferencial. Blowfish (70%) también muestra un fuerte efecto avalancha, lo que demuestra su capacidad para difundir eficazmente los cambios en la entrada. Esto lo hace una opción robusta para el cifrado de datos y; RSA (40%) muestra el menor efecto avalancha. Dado que RSA es un algoritmo de cifrado asimétrico y se utiliza principalmente para la encriptación de pequeñas cantidades de datos (como claves), este resultado es consistente con su diseño y propósito, que no se centra en la difusión de cambios en la entrada de manera tan eficiente como los algoritmos simétricos.

La evaluación del efecto avalancha muestra que AES y Blowfish son los algoritmos más adecuados para garantizar la seguridad de los datos en una empresa financiera, debido a su alta capacidad de difusión de cambios en la entrada. DES y 3DES, aunque menos eficientes en este aspecto, aún pueden ser considerados para aplicaciones específicas. RSA, con su menor efecto avalancha, debe ser reservado para funciones críticas de gestión de claves y autenticación, donde su seguridad y eficiencia en el cifrado asimétrico son más

relevantes.

Figura 40. Entropía para DES, 3DES, AES, Blowfish y RSA.



Nota. Fuente, adaptado de [57].

El gráfico previo ilustra la entropía de cinco algoritmos de cifrado: DES, 3DES, AES, Blowfish y RSA. La entropía es una medida de la impredecibilidad o el desorden en los datos cifrados; una alta entropía indica un mayor nivel de seguridad, dificultando la predicción o descompresión de los datos cifrados.

DES (2.9477) presenta una entropía relativamente baja comparada con los otros algoritmos. Esto sugiere un menor nivel de impredecibilidad, lo que podría hacerlo más vulnerable a ataques criptoanalíticos. 3DES (2.9477) tiene la misma entropía que DES, a pesar de ser más complejo y seguro. Esto indica que la impredecibilidad de 3DES no mejora respecto a DES, aunque ofrece mayor resistencia a ciertos tipos de ataques; AES (3.84024) muestra una alta entropía, indicando un alto nivel de desorden y seguridad en sus datos

cifrados. Esta característica, junto con su eficiencia, lo convierte en una opción robusta y confiable para la protección de datos; Blowfish (3.93891) tiene la mayor entropía entre los algoritmos analizados, sugiriendo que es el más impredecible y, por ende, uno de los más seguros en términos de resistencia a ataques. Su alta entropía, combinada con bajo uso de memoria y alta eficiencia de cifrado, lo hace muy adecuado para aplicaciones críticas; RSA (3.0958) presenta una entropía moderada, lo cual es consistente con su uso en cifrado asimétrico. Aunque su entropía no es tan alta como la de AES o Blowfish, sigue siendo significativa para la seguridad de claves y autenticación.

Finalmente, y en base a los resultados obtenidos, se procedió a ejecutar un ranking para ver cuáles eran los dos mejores algoritmos de criptografía con mejores prestaciones para proceder a evaluarlos en base a eficiencia de manera que se pueda cumplir con los niveles de seguridad de datos de una empresa financiera peruana:

Tabla XIX.

Ranking de algoritmos de criptografía seleccionados.

N°	Algoritmo	Tiempo de Cifrado	Tiempo de Descifrado	Memoria Utilizada	Efecto Avalancha	Entropía	Puntuación Total	% Total
1	AES	10/10	10/10	8/10	10/10	9/10	47/50	94.00%
2	3DES	10/10	10/10	8/10	9/10	9/10	46/50	92.00%
2	Blowfish	7/10	7/10	6/10	8/10	5/10	33/50	66.00%
5	DES	6/10	6/10	7/10	6/10	5/10	30/50	60.00%
4	RSA	5/10	5/10	4/10	4/10	6/10	24/50	24.75%

Nota. Fuente, adaptado de [57].

De la tabla anterior, por una parte, se desprende que, AES es el algoritmo que sobresale en esta evaluación con una puntuación total de 47/50 (94.00%). Este algoritmo muestra una notable eficiencia en términos de tiempo de cifrado y descifrado, ambos con una puntuación de 10 sobre 10, lo que lo convierte en una opción extremadamente rápida. En cuanto a la memoria utilizada, AES presenta un uso moderadamente bajo, con una puntuación de 8 sobre 10. Además, AES destaca significativamente en el efecto avalancha, con una puntuación perfecta de 10 sobre 10, lo que indica una excelente difusión de cambios en los datos de entrada. Finalmente, su entropía, que mide el nivel de aleatoriedad en los datos cifrados, es alta, con una puntuación de 9 sobre 10. Estas características hacen de AES una opción robusta y confiable para una amplia gama de aplicaciones, particularmente en el contexto de una empresa financiera que requiere alta seguridad y eficiencia.

Por otra parte, se desprende que, 3DES logra una puntuación total de 46/50 (92%), destacándose por su alta eficiencia y seguridad. Este algoritmo muestra una notable eficiencia en términos de tiempo de cifrado y descifrado, ambos con una puntuación de 10 sobre 10, lo que lo convierte en una opción extremadamente rápida. En cuanto a la memoria utilizada, 3DES presenta un uso moderadamente bajo, con una puntuación de 8 sobre 10. Además, 3DES tiene un excelente efecto avalancha y una alta entropía, ambos con puntuaciones de 9 sobre 10, lo que indica una gran difusión de cambios y alta aleatoriedad en los datos cifrados. Estas características hacen que 3DES sea una opción robusta para aplicaciones críticas, aunque AES se mantiene como una opción preferida por su equilibrio global entre rendimiento y seguridad.

Posteriormente a ello, y antes de desarrollar los algoritmos de encriptación, se ejecutó una comparativa entre ambos algoritmos seleccionados, AES y 3DES, con propósitos de identificarlos previamente, considerando algunas características importantes y los indicadores de la operacionalización de las variables, pero de manera cualitativa según datos analizados de la literatura científica:

Tabla XX.

Comparativa de algoritmos de criptografía a implementar

Característica	**AES**	**3DES**
Tipo de Algoritmo	Simétrico	Simétrico
Longitud de Clave	128, 192, o 256 bits	168 bits
Tamaño de Bloque	128 bits	64 bits
Estructura de Clave	Estructura de clave única, pero dependiendo del tamaño de la clave, utiliza un número fijo de rondas y transformaciones de clave	Estructura de clave triple, donde se aplica el algoritmo DES tres veces, utilizando tres claves diferentes.
Rondas	10 rondas (128 bits de clave), 12 rondas (192 bits de clave), 14 rondas (256 bits de clave)	48 rondas (16 rondas por cada una de las tres aplicaciones de DES)
Tipo de Ronda	Rondas de sustitución-permutación	Rondas de permutación-substitución
Autor/Estándar	AES fue adoptado por el Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU. como estándar en 2001.	3DES es una extensión del estándar de cifrado de datos (DES) desarrollado por IBM en la década de 1970, con su uso más amplio estandarizado por ANSI y luego NIST.
Implementación	Ampliamente implementado y aceptado como el estándar de cifrado de facto en todo el mundo	Utilizado en sistemas heredados y en entornos donde se requiere compatibilidad con versiones anteriores de DES.

Desempeño	Más rápido que 3DES	Más lento que AES
Flexibilidad	Mayor flexibilidad en términos de longitud de clave y tamaño de bloque.	Limitada flexibilidad debido a la longitud fija de la clave y tamaño de bloque.
Escalabilidad	Escalable para aplicaciones que requieren altos niveles de seguridad.	Limitada escalabilidad debido a su desempeño inferior en comparación con AES y su estructura repetitiva.
Velocidad de Procesamiento	Más rápido en comparación con 3DES.	Más lento en comparación con AES.
Rendimiento de Cifrado	Eficiente y rápido para cifrar grandes volúmenes de datos.	Adecuado para cifrar volúmenes moderados de datos debido a su velocidad más lenta.
Rendimiento de Descifrado	Eficiente y rápido para descifrar datos cifrados.	Adecuado para descifrar volúmenes moderados de datos, aunque más lento que AES.
Consumo de Recursos	Requiere menos recursos en comparación con 3DES debido a su eficiencia y velocidad.	Requiere más recursos en comparación con AES debido a su estructura repetitiva y procesamiento más lento.
Confidencialidad	Ofrece un alto nivel de confidencialidad para datos protegidos.	Ofrece un nivel moderado de confidencialidad, aunque menos seguro que AES debido a su estructura repetitiva.
Integridad	Proporciona integridad de datos adecuada para garantizar que los datos no hayan sido alterados.	Proporciona integridad de datos adecuada, aunque menos seguro que AES debido a su estructura repetitiva.

Disponibilidad	Ampliamente disponible y compatible con la mayoría de los sistemas y plataformas.	Disponible pero menos utilizado en comparación con AES debido a su desempeño inferior y limitaciones de seguridad. Puede estar menos disponible en sistemas modernos y nuevas implementaciones debido a su obsolescencia gradual.
Fortaleza según Principios de Kerckhoffs	Resistente a los ataques criptográficos conocidos. Sigue el principio de Kerckhoffs: la seguridad del algoritmo no debe depender del secreto del algoritmo, sino solo de la clave.	Aunque 3DES es más lento y menos seguro que AES, sigue siendo resistente a los ataques criptográficos, pero no tan seguro como AES debido a su clave más corta y estructura repetitiva. Sigue el principio de Kerckhoffs, pero su seguridad se ve afectada por su clave más corta y estructura repetitiva.
Autor/Estándar	AES fue adoptado por el Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU. como estándar en 2001.	3DES es una extensión del estándar de cifrado de datos (DES) desarrollado por IBM en la década de 1970, con su uso más amplio estandarizado por ANSI y luego NIST.

Nota. Los datos obtenidos han sido de un análisis según la literatura obtenida. Fuente: Elaboración propia.

Según el análisis ejecutado en la tabla anterior, puede, de manera cualitativa, identificarse que, el algoritmo AES tiene mejores características para el cumplimiento de los niveles de seguridad de datos de una empresa financiera peruana.

3.3.2 Analizar los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras.

Posteriormente al establecimiento de los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana, se desarrolló una revisión de artículos científicos que lograrán identificar los ataques de criptografía que vulneran ambos algoritmos seleccionados previamente: AES y 3DES. Para ello se siguió el siguiente flujo:

Figura 41. Diagrama de pasos ejecutados para seleccionar ataques criptográficos

Fuente: Elaboración propia.

Como resultado de esa revisión sistemática de la literatura, se identificaron ocho (08) ataques que vulneran dichos algoritmos y los cuales, se especifican a continuación:

Tabla XXI.

Resumen de ataques de criptografía según literatura

N°	Ataque		Descripción
	Nombre original	Transcripción al español	
1	Brute Force Attack	Ataque de Fuerza Bruta	Intentos repetidos de descifrar datos mediante la prueba de todas las posibles combinaciones de claves. “Es un término utilizado para describir un tipo de ataque donde se prueban todas las combinaciones posibles de claves hasta encontrar la correcta” [58].
2	Dictionary Attack	Ataque de Diccionario	Se utiliza una lista de palabras comunes para intentar descifrar una contraseña o clave de cifrado. “Este tipo de ataque implica el uso de una lista de palabras comunes para intentar descifrar una contraseña o clave de cifrado” [59].
3	Man-in-the-Middle Attack	Ataque de Hombre en el Medio	Un atacante intercepta la comunicación entre dos partes y puede alterar o leer la información transmitida. Es un tipo de ataque en el que un tercero intercepta la comunicación entre dos partes y puede manipular o leer la información transmitida [60].
4	Meet-in-the-Middle Attack	Ataque por encuentro a medio camino	Un tercero interpone la comunicación entre dos partes y puede alterar o leer la información transmitida. “Este término describe un tipo de ataque en el que un tercero se interpone en la comunicación entre dos partes y puede modificar o acceder a la información transmitida” [61].

5	Known Plaintext Attack	Ataque de Texto Claro Conocido	Un atacante conoce parte del texto cifrado y utiliza este conocimiento para deducir la clave de cifrado. “Este tipo de ataque implica que un atacante tiene acceso a una parte del texto cifrado y utiliza esa información para intentar descifrar el resto de los datos o deducir la clave de cifrado” [62].
6	Substitution Attack	Ataque de Reemplazo	Un atacante sustituye el cifrado por otro, generalmente más débil, para facilitar su descifrado. “Este tipo de ataque implica que un atacante cambia el método de cifrado por otro más débil con el fin de hacer más fácil el proceso de descifrado o manipulación de la información protegida” [63].
7	Cryptanalysis Attack	Ataque de Criptoanálisis	Se analizan los patrones y propiedades matemáticas del algoritmo de cifrado para encontrar debilidades. “Se refiere al proceso de examinar los patrones y las propiedades matemáticas del algoritmo de cifrado con el fin de detectar vulnerabilidades que puedan ser utilizadas para descifrar la información cifrada” [64].
8	Side-Channel Attack	Ataque de Canal Lateral	Se explotan las fugas de información, como la energía, el tiempo o el sonido, durante el proceso de cifrado. “Este tipo de ataque implica la explotación de información indirecta, como el consumo de energía o el tiempo de respuesta, durante el proceso de cifrado para obtener información sobre los datos protegidos o la clave secreta” [65].

Nota. Los algoritmos de criptografía mencionados han sido recopilados de la revisión de la literatura. Fuente: Elaboración propia.

Asimismo, se detallaron las vulnerabilidades que atacan cada uno de estos ataques identificados, pudiendo ser estos, la gestión de contraseñas, las palabras claves comunes, la intercepción de mensajes, la manipulación de los datos, etcétera.

Tabla XXII.

Comparativa de algoritmos de criptografía a implementar

N°	Ataque criptográfico	Origen	Vulnerabilidad atacada	Autor del artículo encontrado
1	Brute Force Attack	Desarrollo en la comunidad de seguridad informática	Gestión de contraseñas	[58]
2	Dictionary Attack	Desarrollo en la comunidad de seguridad informática	Contraseñas, palabras clave comunes	[59]
3	Man-in-the-Middle Attack	Terminología establecida en seguridad informática	Intercepción de mensajes, manipulación de datos	[60]
4	Meet-in-the-Middle Attack	Terminología establecida en criptografía	Diversas, dependiendo del método de cifrado utilizado	[61]
5	Known Plaintext Attack	Terminología establecida en seguridad informática	Confidencialidad de datos	[62]
6	Substitution Attack	Terminología establecida en seguridad informática	Integridad de datos	[63]
7	Cryptanalysis Attack	Terminología establecida en criptografía	Diversas, dependiendo de las debilidades del algoritmo	[64]

8	Side-Channel Attack	Terminología establecida en criptografía y seguridad	Confidencialidad, integridad, disponibilidad de datos	[65]

Nota. Información recolectada mediante una revisión sistemática de la literatura. Fuente: Elaboración propia.

Como puede distinguirse en los resultados de la literatura científica, los ataques de criptografía representan acciones maliciosas dirigidas a comprometer la integridad de los sistemas criptográficos, con el propósito de aprovechar debilidades y obtener entrada no permitida a datos confidenciales, tal y como sucede en el sector financiero peruano.

La seguridad en el ámbito de la criptografía requiere una comprensión exhaustiva de las diversas amenazas que plantean diversos tipos de ataques. Desde la persistencia incansable de los ataques de fuerza bruta hasta las manipulaciones más sutiles de los ataques de canales laterales, cada uno de los ocho (08) tipos de ataques criptográficos encontrados en la literatura demanda un análisis detallado por separado. La defensa contra estas amenazas no solo implica la adopción de algoritmos de criptografía robustos, sino también la implementación de medidas preventivas como una gestión de claves segura y actualizaciones continuas del sistema. Con el avance de la tecnología, la efectividad de las defensas criptográficas depende de mantenerse al tanto de las amenazas en constante evolución, asegurando así la confidencialidad, integridad y disponibilidad de la información sensible en un entorno digital interconectado y en constante cambio, tal y como es el sector financiero peruano.

En base a ello, a continuación, se brinda un análisis comparativo según la literatura científica acerca de estos ataques criptográficos en el sector financiero mundial:

Tabla XXIII.

Comparativa de ataques de criptografía según literatura

N°	Ataque criptográfico	Descripción	Objetivo	Complejidad	Detectabilidad	Eficiencia frente a Algoritmos Criptográficos Actuales	Requerimientos	Defensas	Ejemplo de aplicación en el sector financiero
1	Brute Force Attack	Intenta descifrar datos probando todas las posibles combinaciones de claves.	Clave de cifrado	Alta	Alta	Baja	Poder computacional elevado, tiempo extenso	Implementar bloqueos automáticos después de varios intentos fallidos, utilizar contraseñas fuertes y multifactoriales.	Acceso no autorizado a una cuenta con una contraseña débil.
2	Dictionary Attack	Utiliza listas de palabras comunes para intentar descifrar contraseñas o claves de cifrado.	Clave de cifrado	Media	Alta	Media	Acceso a una lista de contraseñas comunes	Implementar políticas de bloqueo después de intentos fallidos, uso de autenticación de dos factores, y educación sobre contraseñas seguras.	Intento de descifrar una contraseña utilizando "password" o "123456".
3	Man-in-the-Middle Attack	Un atacante intercepta y manipula la comunicación entre dos partes, accediendo potencialmente a información confidencial.	Integridad de la comunicación	Alta	Media	Baja	Capacidad para interceptar y manipular comunicaciones	Uso de protocolos de seguridad como HTTPS, uso de certificados SSL/TLS, y monitoreo continuo de la red en busca de actividad sospechosa.	Un atacante intercepta y modifica transacciones financieras en línea entre un cliente y un banco con propósitos de obtener beneficio personal.
4	Meet-in-the-Middle Attack	Divide el proceso de cifrado en dos partes y utiliza una tabla de búsqueda para	Algoritmo de cifrado	Alta	Baja	Baja	Conocimiento del algoritmo de cifrado, recursos	Implementar algoritmos de cifrado más robustos, utilizar claves más largas y complejas,	Descifrar una comunicación cifrada mediante la búsqueda de coincidencias

		descifrar eficientemente los datos.					computacionales significativos	y cifrar tanto el texto claro como el texto cifrado.	entre el texto cifrado y el texto claro conocido.
5	Known Plaintext Attack	El atacante conoce parte del texto cifrado y utiliza este conocimiento para deducir la clave de cifrado.	Clave de cifrado	Media	Baja	Baja	Acceso al texto cifrado y al texto claro conocido	Implementar algoritmos de cifrado más seguros y complejos, y realizar un cifrado completo de los datos.	Un atacante conoce una parte del mensaje cifrado y puede deducir la clave utilizada a partir de partes conocidas del texto cifrado.
6	Substitution Attack	Reemplaza el cifrado con otro más débil, facilitando así su descifrado.	Algoritmo de cifrado	Baja	Baja	Baja	Acceso a sistemas de seguridad para realizar reemplazo	Implementar sistemas de detección de intrusiones, realizar auditorías de seguridad periódicas, y mantener actualizaciones de seguridad.	Reemplazo de un algoritmo de cifrado fuerte por uno más débil en un sistema de seguridad.
7	Cryptanalysis Attack	Analiza patrones y propiedades matemáticas del algoritmo de cifrado para encontrar debilidades y obtener información sobre la clave.	Algoritmo de cifrado	Alta	Baja	Alta	Conocimiento profundo de matemáticas y algoritmos	Implementar algoritmos de cifrado más resistentes y complejos, y realizar evaluaciones de seguridad regulares.	Desarrollo de técnicas matemáticas para romper un algoritmo de cifrado.
8	Side-Channel Atack	Explota las fugas de información durante el proceso de cifrado, como la energía, el tiempo o el sonido, para obtener información sobre la clave o los datos cifrados.	Implementación de cifrado	Alta	Baja	Alta	Acceso físico al dispositivo y capacidades de monitoreo	Implementar técnicas de contramedidas físicas, utilizar algoritmos de cifrados resistentes a ataques de canal lateral, y aislar el dispositivo de posibles fuentes de fuga de información.	Utilización de información lateral, como la energía consumida por un dispositivo, para inferir datos confidenciales a partir de fugas de información

Nota. Análisis basado en la revisión sistemática de la literatura. Fuente: Elaboración propia.

3.3.3 Desarrollar en lenguaje de programación sistema que permita la comparación de los algoritmos de criptografía considerando los indicadores propuestos.

En el ámbito de la seguridad de datos financieros, surge una tarea esencial: evaluar algoritmos de criptografía para salvaguardar la información confidencial contenida en los documentos empresariales de una importante institución financiera peruana del sector AFP. Para ello, fue necesario establecer el contexto en el que se desarrollarían dichas pruebas.

Ante esta situación, se definió emplear documentos, en formatos Word y PDF, albergando datos sensibles que requieren una protección impenetrable. Por tanto, se plantea la necesidad de realizar pruebas rigurosas con el objetivo de garantizar que los algoritmos seleccionados, AES y 3DES, cumplan con los más rigurosos estándares de seguridad, asegurando así la protección óptima de los activos más valiosos de la empresa: sus datos. Este proceso de evaluación no solo se enfocó en el rendimiento de cifrado, rendimiento de descifrado, consumo de recursos, la integridad y la fortaleza del algoritmo mismo, los cuales son aspectos importantes para mantener la confianza de los clientes y cumplir con las regulaciones financieras vigentes en el país.

Se completaron las implementaciones de los algoritmos AES y 3DES conforme a sus especificaciones individuales. Para este propósito, se empleó el lenguaje de programación PHP. Cada algoritmo se llevó a cabo siguiendo las directrices teóricas expuestas en la investigación.

La aplicación se desarrolló utilizando la herramienta XAMPP, que es el entorno de desarrollo PHP más popular, es una distribución de Apache gratuita y fácil de instalar y usar, contiene MariaDB, PHP y Perl, esta herramienta es de código abierto.

La aplicación se montó sobre un host en internet administrador por CPANEL.

Tabla XXIV.

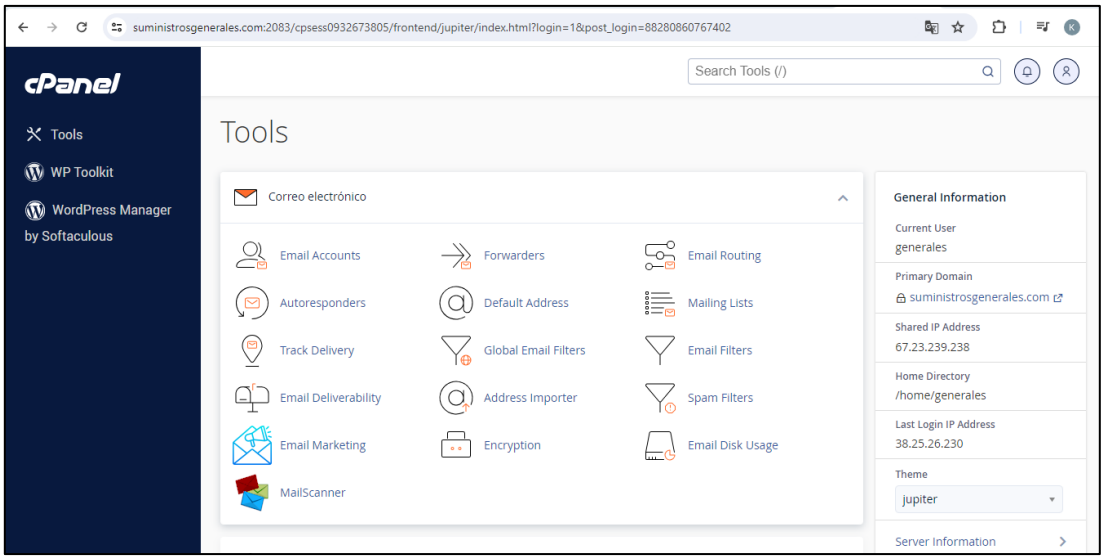
Configuración del domino en donde se desplego la aplicación

Primary Domain suministrosgenerales.com
Shared IP Address67.23.239.238
Home Directory/home/generales
Last Login IP Address38.25.26.230

Fuente: Cpanel – dominio suministros generales

El dominio se llama suministrosgenerales.com este dominio permite desplegar aplicaciones en lenguaje PHP y base de datos MySql, a continuación, se evidencia la página principal de configuración del dominio. Que se caracteriza por su gestión simple de sitios web y servidores, fácil e intuitivo, es una herramienta potente, permite configurar servidores hiperescaladores basados en la nube, incluye correo electrónico, seguridad, copias de seguridad, soporte técnico 24 horas al día los 7 días a la semana.

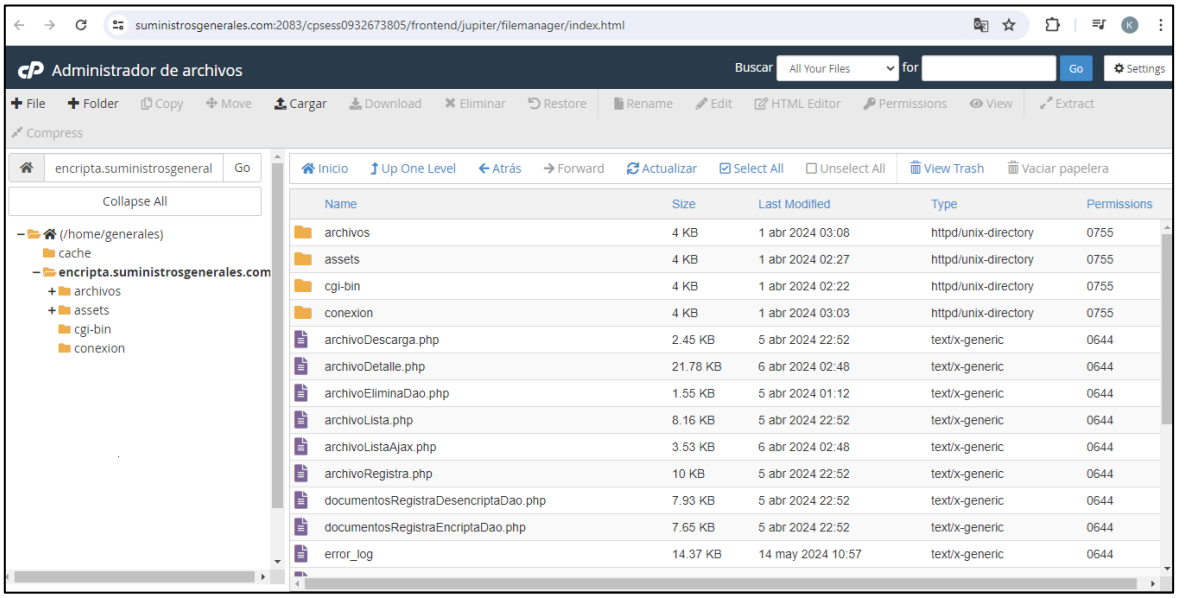
Figura 42. Panel de control del dominio de despliegue.



Fuente: Cpanel – dominio suministros generales.

Directorio raíz de la aplicación desplegada, lista de archivos de la aplicación en el dominio.

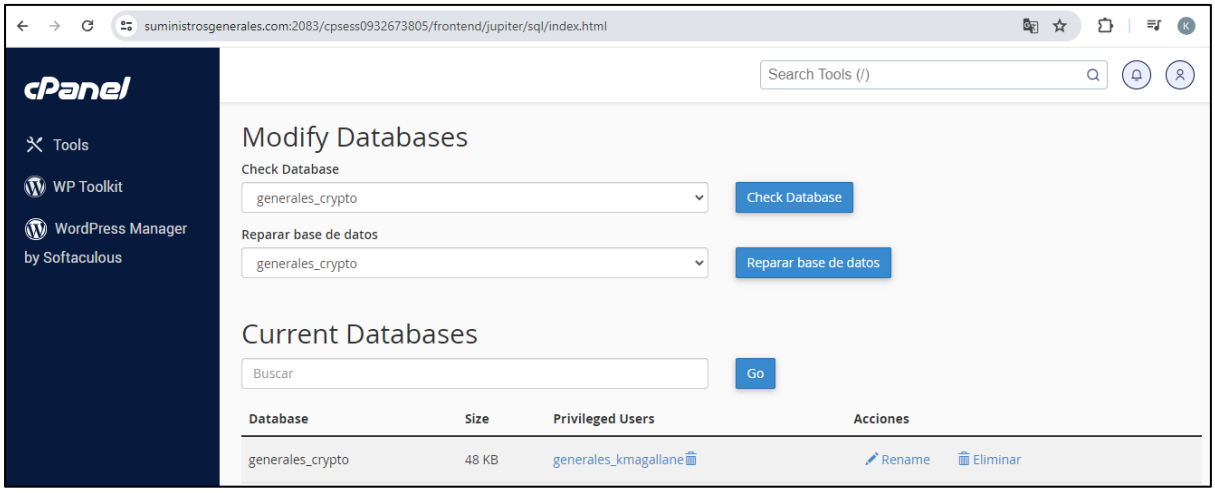
Figura 43. Panel de control del dominio de despliegue.



Fuente: Cpanel – dominio suministros generales.

A continuación de muestra una imagen con la configuración del usuario que conecta la aplicación con la base de datos.

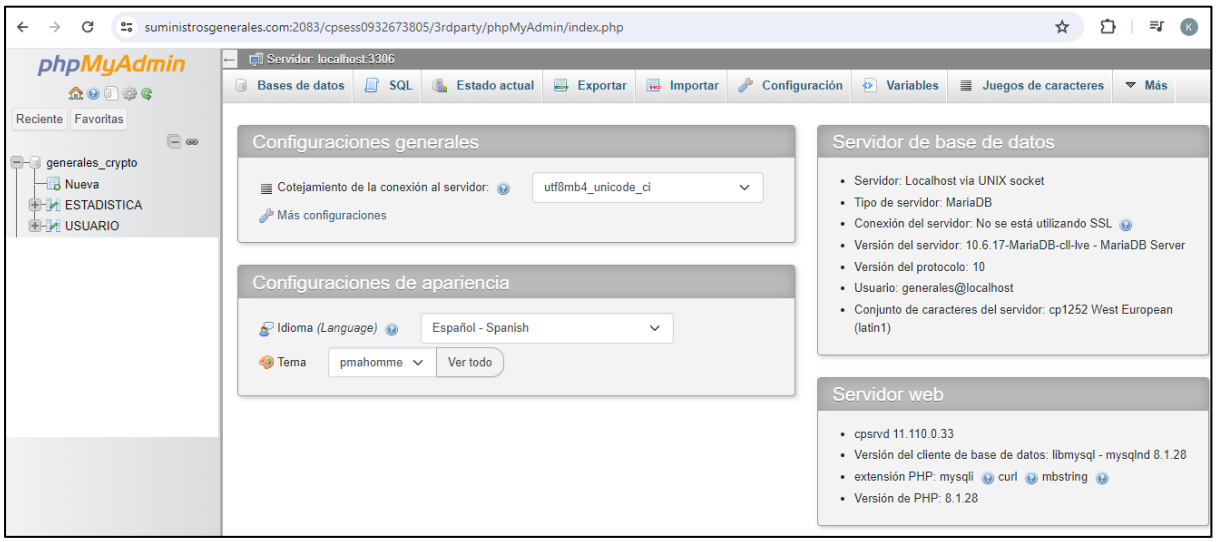
Figura 44. Configuración del usuario de conexión a la base de datos.



Fuente: Cpanel – dominio suministros generales.

La imagen muestra la configuración del servidor de la base de datos MySql y el servidor web, así mismo la base de datos CRYPTO y los objetos de base de datos como tablas.

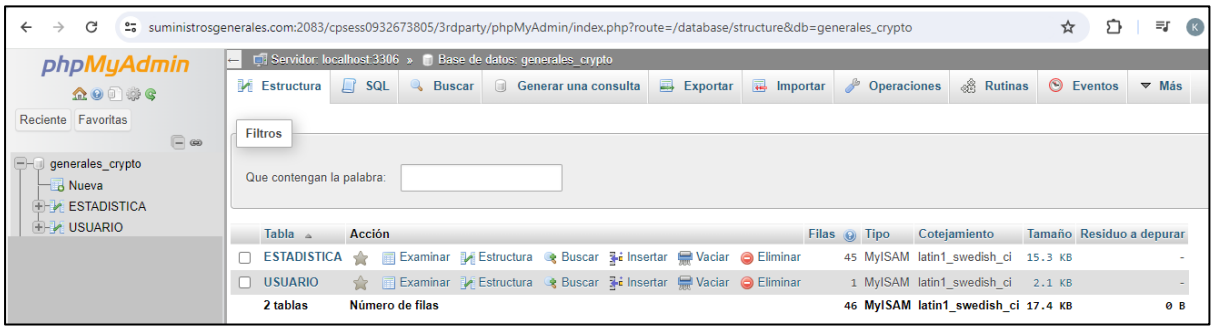
Figura 45. Configuración de Base de datos.



Fuente: Cpanel – dominio suministros generales

Lista de tablas que almacena información de usuario de acceso a la aplicación y la tabla estadística que almacena información de la encriptación y la desencriptación de los archivos.

Figura 46. Lista de tablas.



Fuente: Cpanel – dominio suministros generales.

Diccionario de datos de la tabla Usuario.

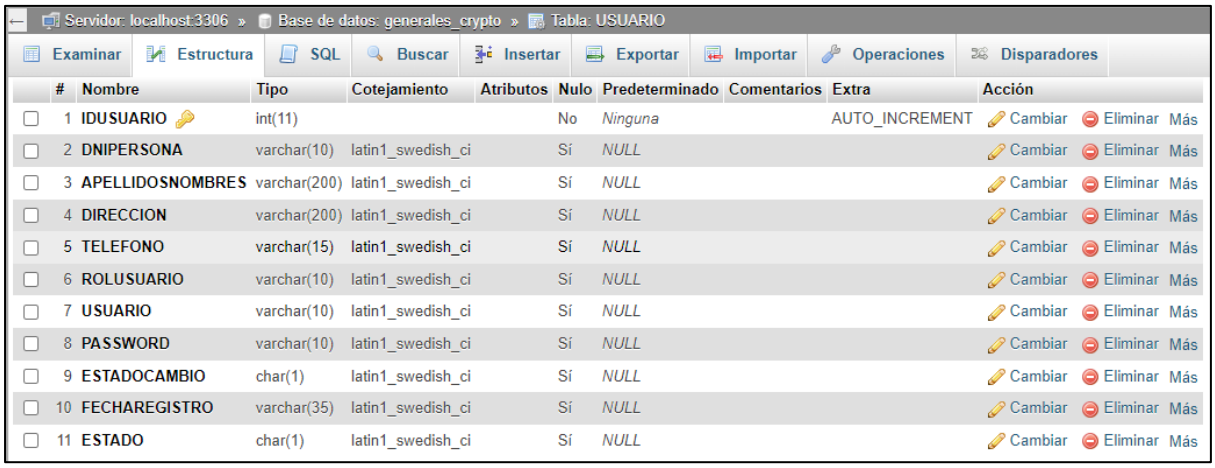
Tabla XXV.

Diccionario de la tabla Usuario

#	ATRIBUTOS	DESCRIPCION
1	IDUSUARIO	Identificación del usuario
2	DNIPERSONA	Documento nacional de identificación
3	APELLIDOSNOMBRES	Apellidos y nombres del usuario
4	DIRECCION	Dirección del usuario
5	TELEFONO	Teléfono del usuario
6	ROLUSUARIO	Rol de usuario
7	USUARIO	Nombre de usuario
8	PASSWORD	Clave de acceso
9	ESTADOCAMBIO	Estado de cambio de clave primera vez
10	FECHAREGISTRO	Fecha de registro de usuario
11	ESTADO	Estado del registro del usuario

Fuente: Elaboración propia.

Figura 47. Tabla Usuario.



#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Comentarios	Extra	Acción
1	IDUSUARIO	int(11)			No	*Ninguna*		AUTO_INCREMENT	Cambiar Eliminar Más
2	DNIPERSONA	varchar(10)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
3	APELLIDOSNOMBRES	varchar(200)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
4	DIRECCION	varchar(200)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
5	TELEFONO	varchar(15)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
6	ROLUSUARIO	varchar(10)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
7	USUARIO	varchar(10)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
8	PASSWORD	varchar(10)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
9	ESTADOCAMBIO	char(1)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
10	FECHAREGISTRO	varchar(35)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más
11	ESTADO	char(1)	latin1_swedish_ci		Sí	*NULL*			Cambiar Eliminar Más

Fuente: Cpanel – dominio suministros generales

Diccionario de la tabla Estadística.

Tabla XXVI.

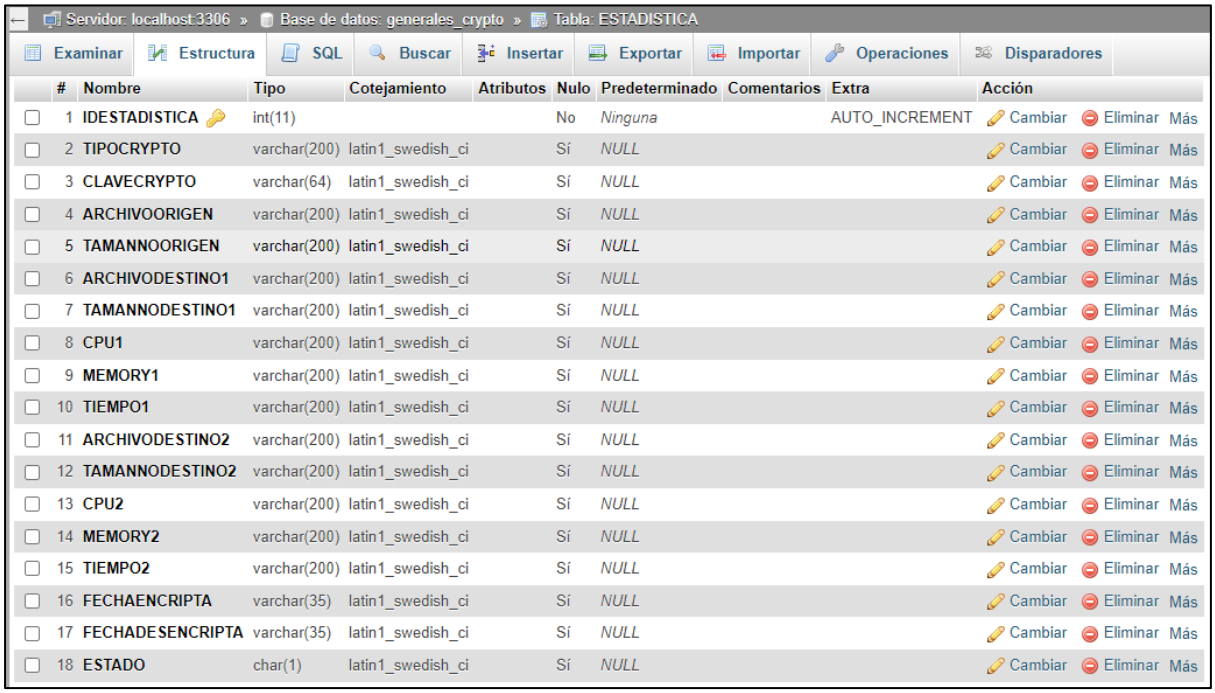
Diccionario de la tabla Estadística

#	ATRIBUTOS	DESCRIPCION
1	IDESTADISTICA	Identificación de registros de encriptación
2	TIPOCRYPTO	Tipo de encriptación AES o 3DES
3	CLAVECRYPTO	Clave de encriptación y desencriptación
4	ARCHIVOORIGEN	Archivo origen
5	TAMANNOORIGEN	Tamaño del archivo origen
6	ARCHIVODESTINO1	Archivo encriptado
7	TAMANNODESTINO1	Tamaño de archivo encriptado
8	CPU1	Consumo de CPU encriptado
9	MEMORY1	Consumo de memoria encriptado
10	TIEMPO1	Tiempo de ejecución encriptado
11	ARCHIVODESTINO2	Archivo desencriptado
12	TAMANNODESTINO2	Tamaño de archivo desencriptado
13	CPU2	Consumo de CPU desencriptado
14	MEMORY2	Consumo de memoria desencriptado
15	TIEMPO2	Tiempo de ejecución desencriptado

16	FECHAENCRIPTA	Fecha de registro encriptación
17	FECHADESENCRIPTA	Fecha de registro desencriptación
18	ESTADO	Estado de registro

Fuente: Elaboración propia.

Figura 48. Tabla Estadística



Fuente: Cpanel – dominio suministros generales

A continuación, se presentan las especificaciones detalladas necesarias para la ejecución del programa desarrollado. Cada aspecto relevante para el funcionamiento del software fue abordado minuciosamente, desde los requisitos técnicos hasta las consideraciones de seguridad y eficiencia:

Tabla XXVII.

Especificaciones del contenido para la ejecución del programa

Código	**Descripción**	**Función**

$clave = $CLAVECRYPTO;	Variable que almacena la clave	Esta clave sirve para encriptar y desencriptar

$archivoNombre1 = $_FILES["miarchivo"]["name"][$key];
$archivoNombre2 = $_FILES["miarchivo"]["name"][$key];
$pos = strlen($archivoNombre2)-strpos($archivoNombre2,".");
$archivoNombre2 = substr($archivoNombre1,
$archivoSize = 0,strlen($archivoNombre1)-$pos);$_FILES["miarchivo"]["size"][$key];
$guardado = $_FILES["miarchivo"]["tmp_name"][$key];
$texto = "Ecriptacion AES.";
$rutaAes = 'archivos/aaes/'.$archivoNombre1;
$rutaAes1 = 'archivos/aaes1/'.$archivoNombre2.'_e.aes';
move_uploaded_file($guardado,$rutaAes);
$clave = $txtClave;
$iv = '1234567890123456';
encryptFileAES($rutaAes,$rutaAes1,$clave,$iv);
	Variables, función que encripta archivos, luego es guardado en un directorio del disco	Encriptar

$archivoNombre1 = $ARCHIVOORIGEN; $archivoNombre2 = $ARCHIVOORIGEN; $pos = strlen($archivoNombre2)-strpos($archivoNombre2,"."); $archivoNombre2 = substr($archivoNombre1,0,strlen($archivoNombre1)-$pos); $archivoExtencion = substr($archivoNombre1,strpos($archivoNombre1,".")+1); $texto = "Ecriptacion AES."; $rutaAes = 'archivos/aaes/'.$archivoNombre1;	Variables, función que desencripta archivos, luego es guardado en un directorio del disco	Desencriptar

$rutaAes1 = 'archivos/aaes1/'.$archivoNombre2.'_e.aes';
$rutaAes2 = 'archivos/aaes2/'.$archivoNombre2.'_d.'.$archivoExtencion;
move_uploaded_file($guardado,$rutaAes);
$clave = $CLAVECRYPTO;
$iv = '1234567890123456';
 	
decryptFileAES($rutaAes1,$rutaAes2,$clave,$iv);		

Fuente: Elaboración propia.

Asimismo, se muestran los indicadores a evaluar con los algoritmos implementados:

Tabla XXVIII.

Indicadores a evaluar con los algoritmos implementados

Código	**Descripción**	**Función**
$tiempo_ejecucion2 = ($tiempo_fin - $tiempo_inicio);	Esta línea de código registra el tiempo de finalización de la encriptación	Encriptación en segundos
$tiempo_ejecucion2 = ($tiempo_fin - $tiempo_inicio);	Esta línea de código registrar el tiempo de finalización de la encriptación	Desencriptación en segundos

$start = getrusage(); // CPU - INICIO
 	
$memoriaAntes = memory_get_usage(); // MEMORIA - INICIO
 	
$tiempo_inicio = microtime(true); // TIEMPO - INICIO
 	
encryptFileAES($rutaAes,$rutaAes1,$clave,$iv);
 	
$tiempo_fin = microtime(true); // TIEMPO - FIN
 	
$memoriaDespues = memory_get_usage(); // MEMORIA - FIN
 	
$end = getrusage(); // CPU - FIN
	Obtención de consumo de memoria, CPU y tiempo de ejecución	Rendimiento de encriptado

$start = getrusage(); // CPU - INICIO
$memoriaAntes = memory_get_usage(); // MEMORIA - INICIO
$tiempo_inicio = microtime(true); // TIEMPO - INICIO
decryptFile3DES($ruta3Des1, $ruta3Des2, $clave);
$tiempo_fin = microtime(true); // TIEMPO - FIN
$memoriaDespues = memory_get_usage(); // MEMORIA - FIN
$end = getrusage(); // CPU - FIN
	Obtención de consumo de memoria, CPU y tiempo de ejecución	Rendimiento de desencriptado

$archivoSize = $_FILES["miarchivo"]["size"][$key];	La función filesize recupera el tamaño del archivo al encriptar	Esta variable almacena el tamaño del archivo original (bytes)
$archivoSize2 = filesize($rutaAes2);	La función filesize recupera el tamaño del archivo al desencriptar	Esta variable almacena el tamaño del archivo original (bytes)

Fuente: Elaboración propia.

A continuación, se presenta un análisis detallado de la implementación del algoritmo AES como parte de la evaluación de la eficiencia de los algoritmos de criptografía. Se proporciona una descripción de la implementación, incluyendo su código, descripción y función. Los resultados obtenidos se presentan en forma de tabla, lo que permitirá una comparación clara y objetiva con otros algoritmos evaluados en el estudio:

Tabla XXIX.

Implementación del algoritmo AES

Algoritmo criptográfico AES		
Código	**Descripción**	**Función**
function encryptFileAES($input_file, $output_file, $key,$iv){	Esta función recibe como parámetro el archivo y la llave de encriptación.	Encriptar

$contenido_original = file_get_contents($input_file);
 	
$contenido_encriptado = openssl_encrypt($contenido_original, 'aes-256-cbc', $key, 0, $iv);
 	
file_put_contents($output_file, $contenido_encriptado);
 	
}		

function decryptFileAES($input_file, $output_file, $key,$iv){
$contenido_encriptado = file_get_contents($input_file);
$contenido_desencriptado = openssl_decrypt($contenido_encriptado, 'aes-256-cbc', $key, 0, $iv);
file_put_contents($output_file, $contenido_desencriptado);
}
	Esta función recibe como parámetros el archivo cifrado y la llave.	Desencripta

Fuente: Elaboración propia.

A continuación, se presenta un análisis detallado de la implementación del algoritmo 3DES como parte de la evaluación de la eficiencia de los algoritmos de criptografía. Se proporciona una descripción de la implementación, incluyendo su código, descripción y función. Los resultados obtenidos se presentan en forma de tabla, lo que permitirá una comparación clara y objetiva con otros algoritmos evaluados en el estudio:

Tabla XXX.

Implementación del algoritmo 3DES

Algoritmo criptográfico 3DES		
Código	**Descripción**	**Función**
function encryptFile3DES($input_file, $output_file, $key) { $input_data = file_get_contents($input_file); $iv = openssl_random_pseudo_bytes(8);	Esta función recibe como parámetro el archivo y la llave de encriptación.	Encriptar

$encrypted_data = openssl_encrypt($input_data, 'des-ede3-cbc', $key, OPENSSL_RAW_DATA, $iv);
 	
file_put_contents($output_file, $iv . $encrypted_data);
 	
}		

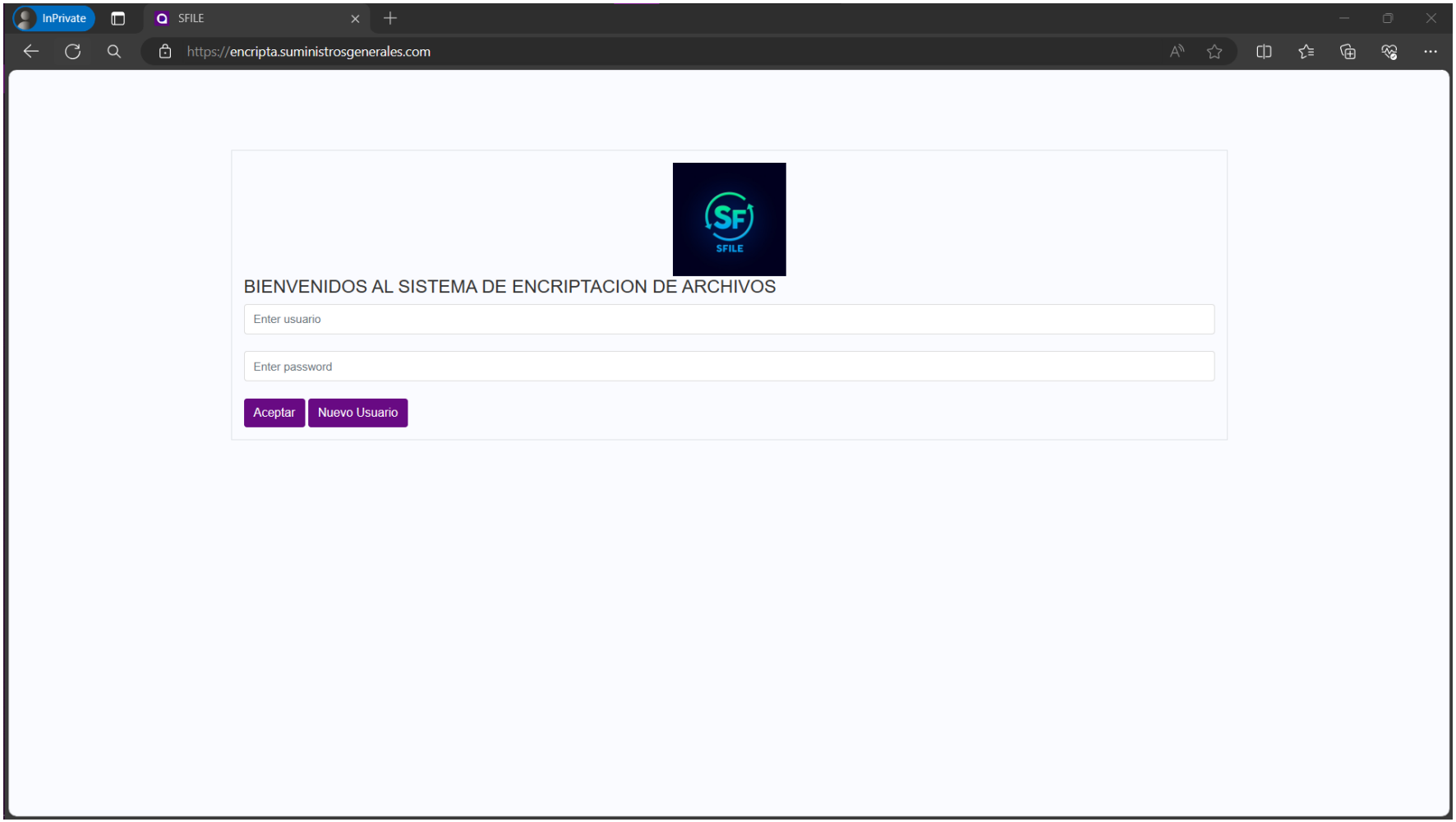
function decryptFile3DES($input_file, $output_file, $key) {
$input_data = file_get_contents($input_file);
$iv = substr($input_data, 0, 8);
$encrypted_data = substr($input_data, 8);
$decrypted_data = openssl_decrypt($encrypted_data, 'des-ede3-cbc', $key, OPENSSL_RAW_DATA, $iv);
file_put_contents($output_file, $decrypted_data);
}
	Esta función recibe como parámetros el archivo cifrado y la llave.	Desencripta

Fuente: Elaboración propia.

Luego de desarrollados los algoritmos AES y 3DES, se procedió al desarrollo del sistema de cifrado. El sistema se denominó Sfile, el cual tuvo la funcionalidad de poder funcionar con ambos algoritmos de criptografía elegidos en pasos previos.

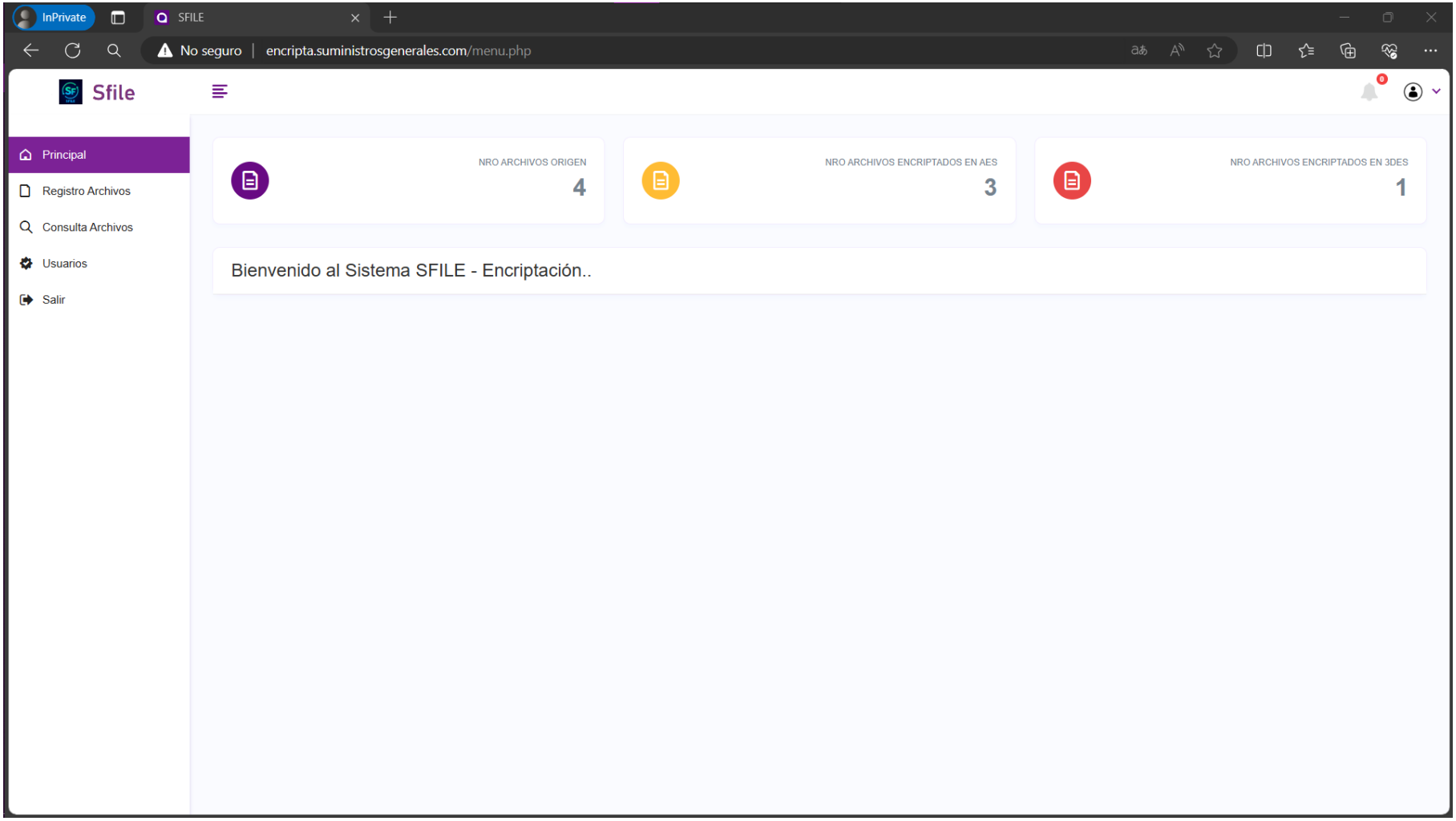
En la interfaz principal se visualizan las siguientes opciones:

Figura 49. Interfaz de logeo al sistema SFILE, encriptación y desencriptación.



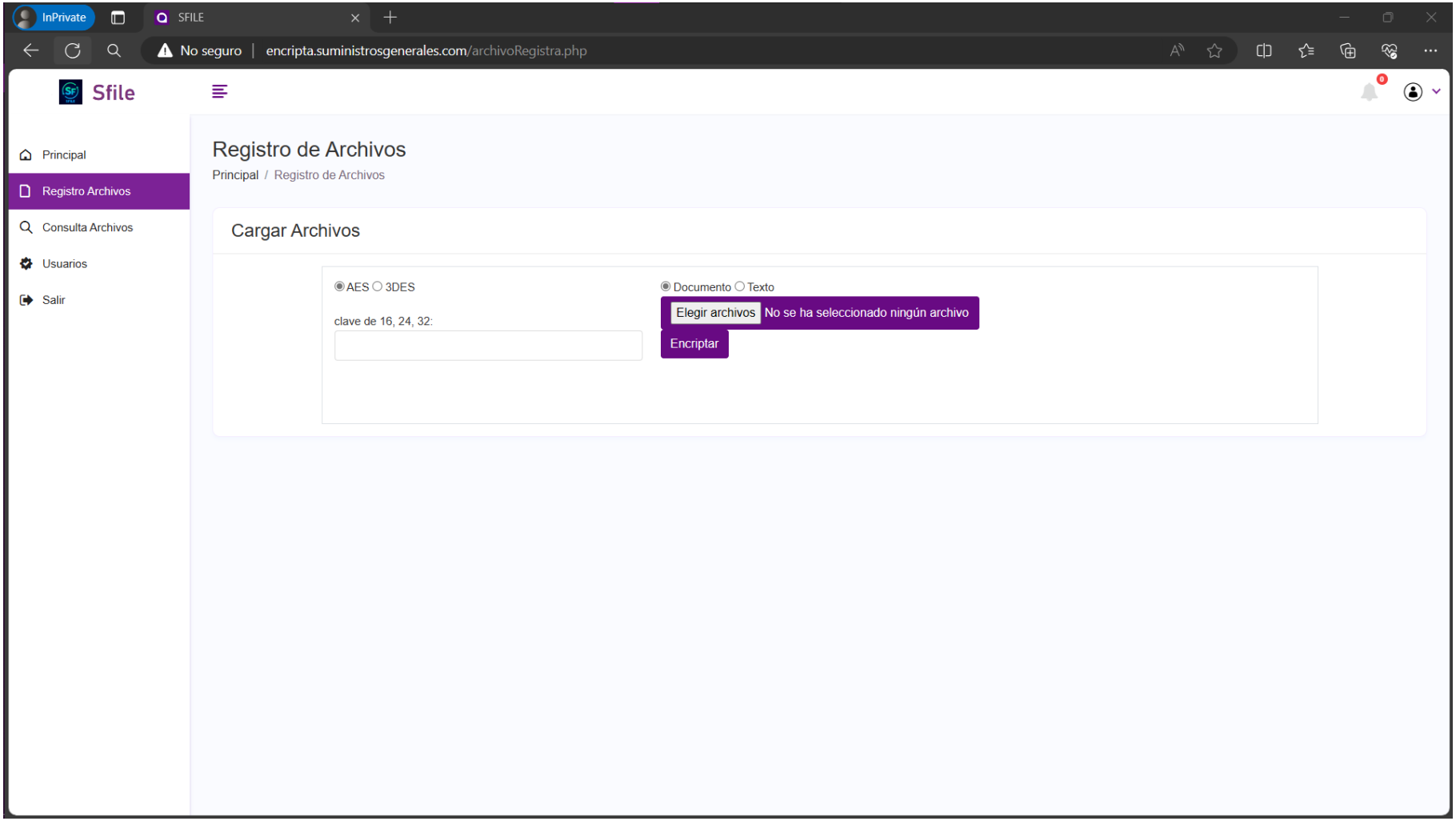
Fuente: Elaboración propia.

Figura 50. Interfaz principal del sistema, menú de opciones y estadístico.



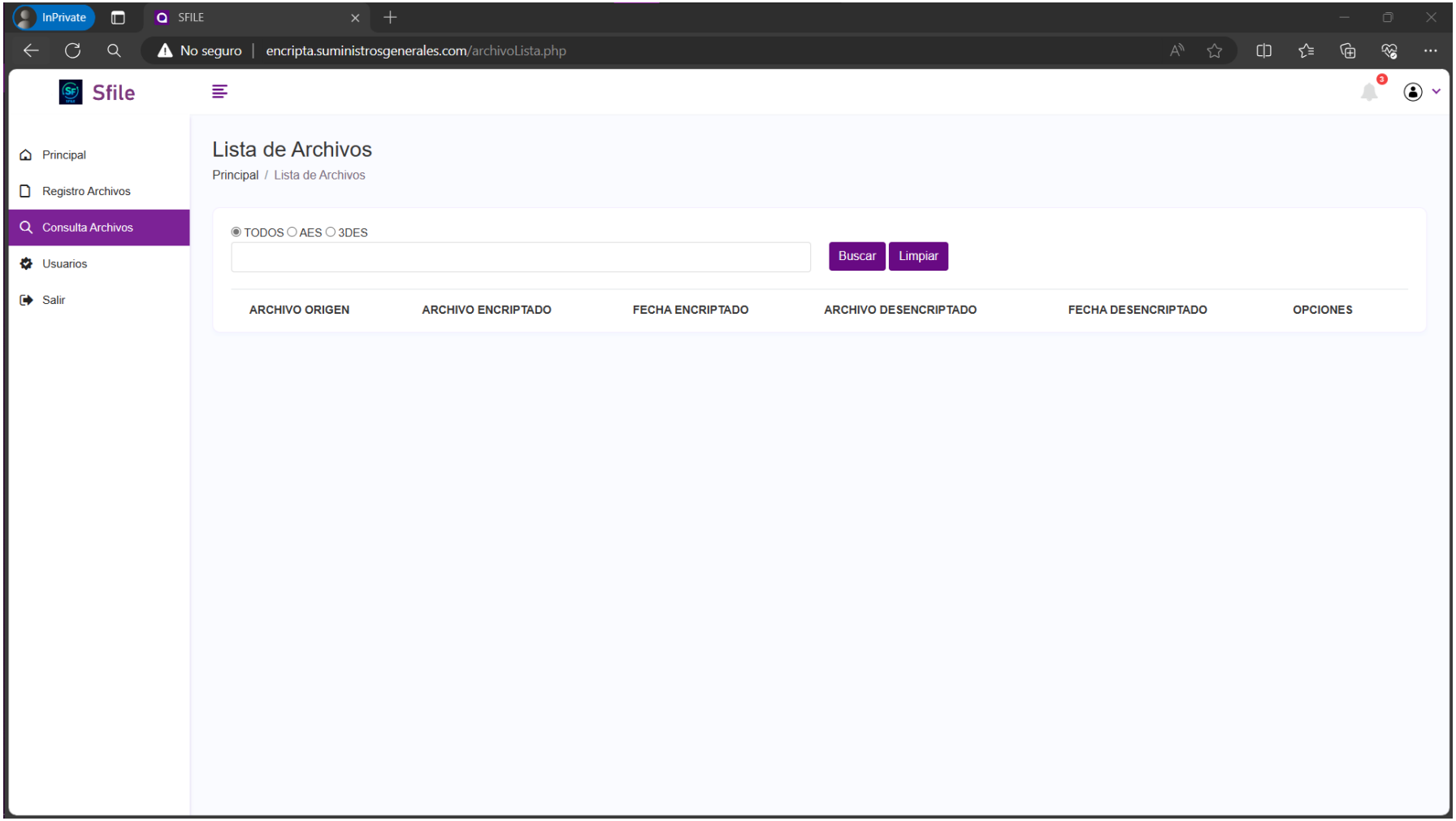
Fuente: Elaboración propia.

Figura 51. Interfaz de registro de archivos en el sistema Sfile.



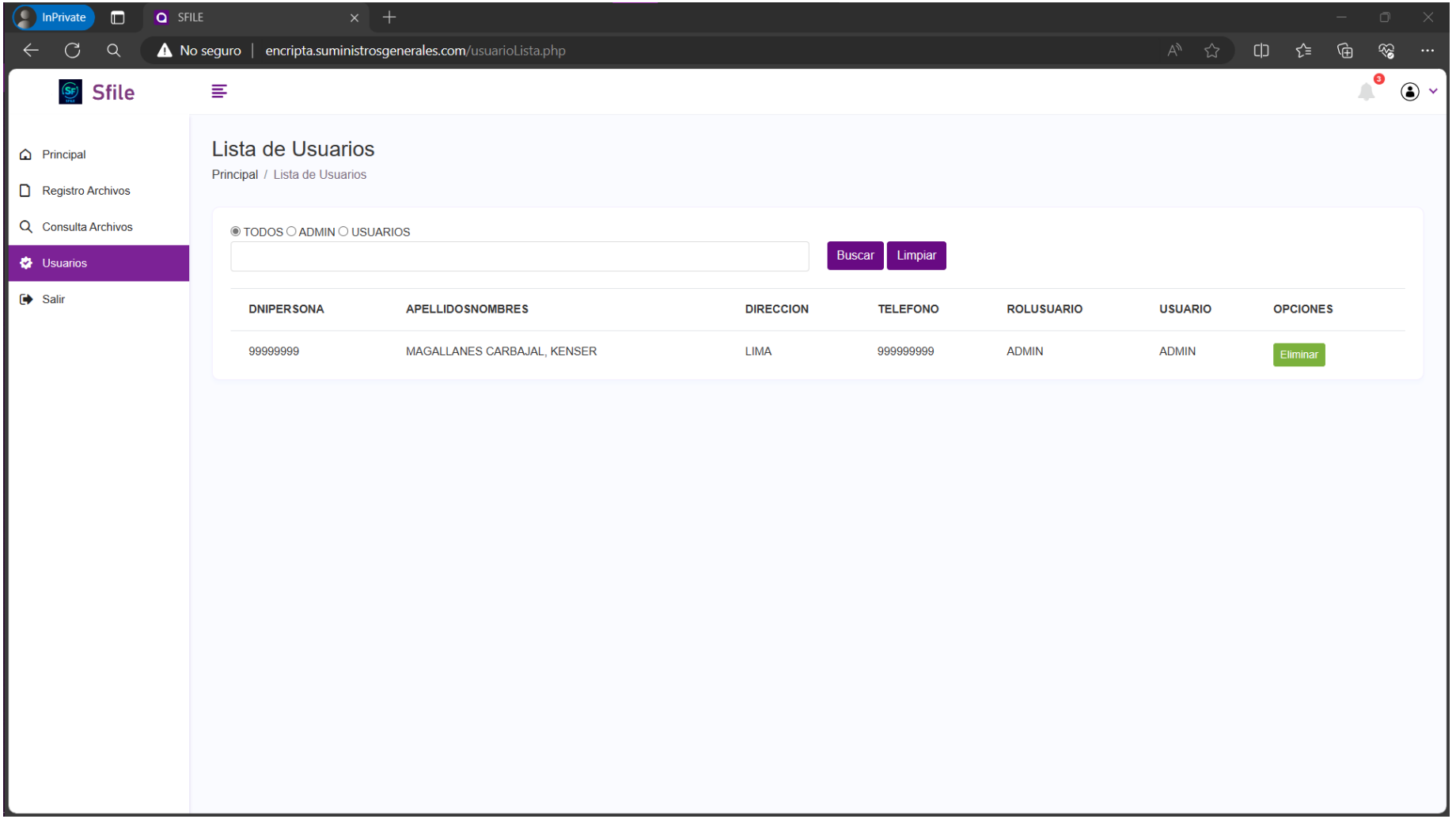
Fuente: Elaboración propia.

Figura 52. Interfaz de lista de archivos en el sistema Sfile.



Fuente: Elaboración propia.

Figura 53. Interfaz de lista de usuarios en el sistema Sfile.



Fuente: Elaboración propia.

3.3.4 Plantear recomendaciones que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos.

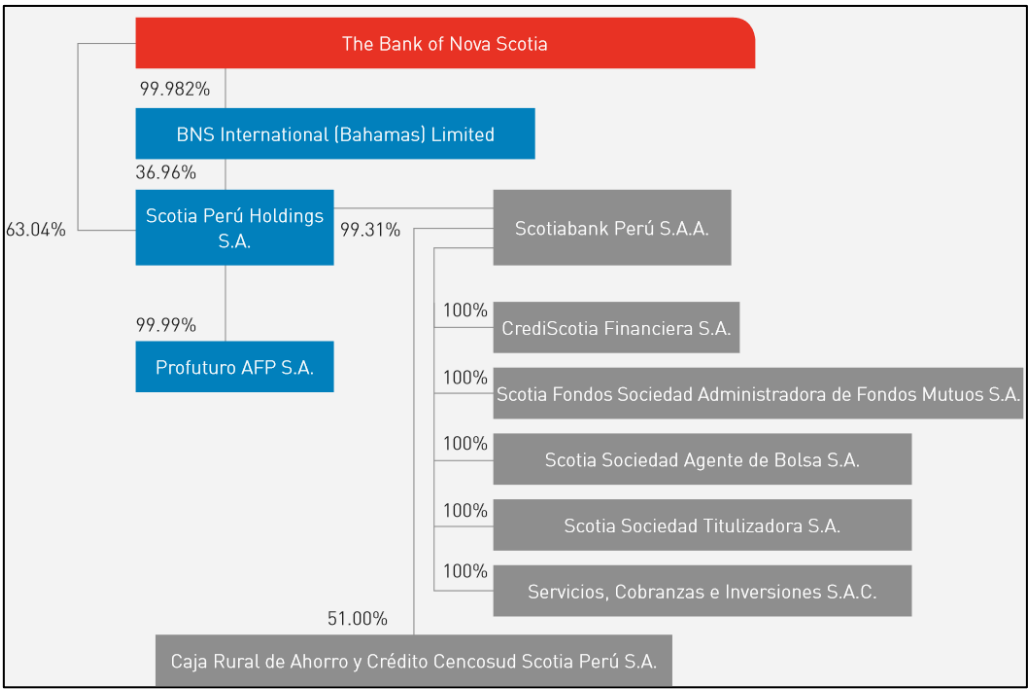
Respecto a la institución caso de estudio, se consideró para la ejecución de las pruebas, documentación pública perteneciente a la empresa PROFUTURO AFP, subsidiaria del grupo canadiense Scotiabank, que, a su vez, conforma el sistema financiero nacional.

Figura 54. Logo de PROFUTURO AFP.

Fuente: Profuturo AFP

Profuturo AFP es una administradora de pensiones peruana especializada en gestionar fondos de jubilación, el cual está avalado por The Bank of Nova Scotia, una institución bancaria multinacional con presencia global. Profuturo AFP ofrece distintos servicios de gestión de fondos obligatorios y voluntarios, tanto para individuos como para empresas, brindando un paquete completo de asesoramiento y soluciones de inversión personalizadas para garantizar el crecimiento financiero de los ahorros de sus clientes que aportará bienestar durante la jubilación. La sinergia con Scotiabank proporciona a Profuturo AFP acceso a una amplia gama de recursos y experiencia en el sector financiero, fortaleciendo su posición dentro del mercado de fondos de pensiones en el Perú.

Figura 55. Diagrama del grupo económico Scotiabank en el Perú [66].

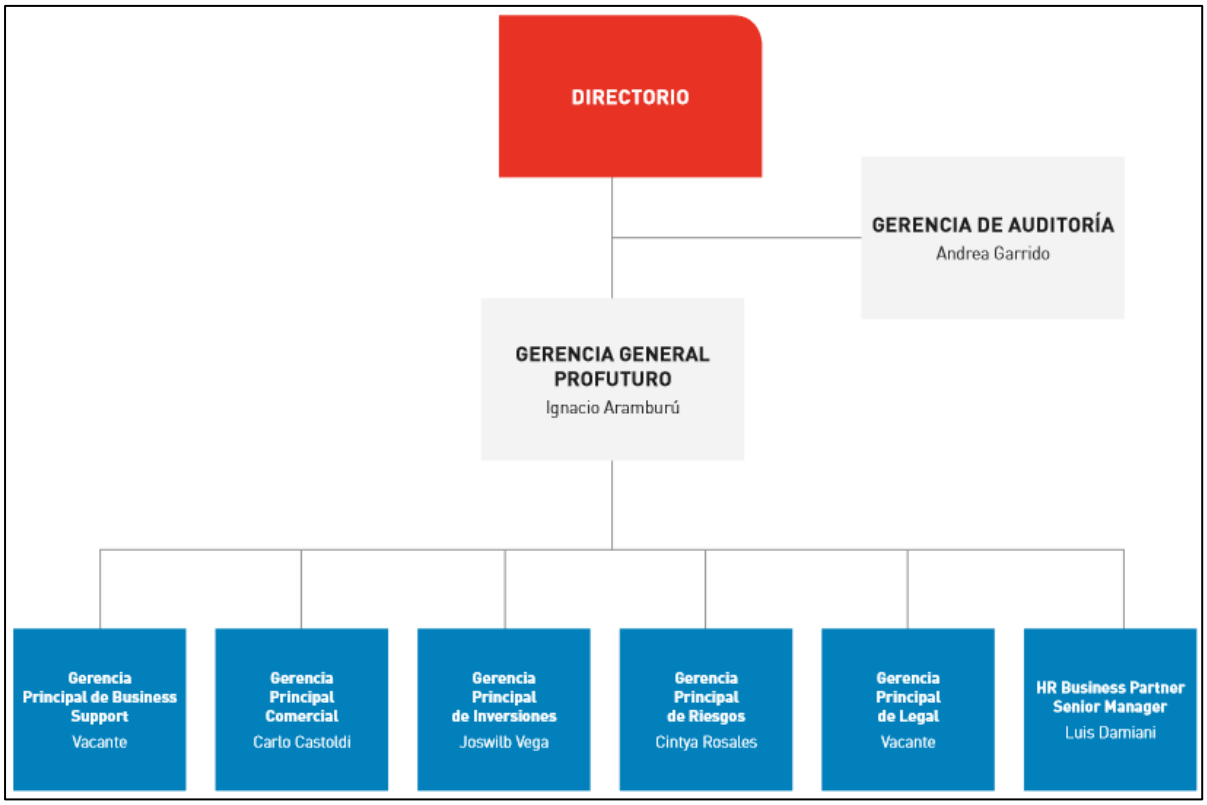


Fuente: Profuturo AFP

Por otro lado, la estructura organizativa de la AFP refleja una jerarquía clara y funcional diseñada para gestionar eficazmente sus operaciones y servicios. La alta dirección está encabezada por un director general, quien supervisa las funciones estratégicas y la toma de decisiones clave. A su vez, la dirección se apoya en diferentes áreas como finanzas, operaciones, recursos humanos y tecnología, cada una liderada por un gerente o director especializado en su respectivo campo. Estos gerentes, a su vez, supervisan equipos dedicados a funciones específicas dentro de cada área, garantizando así una distribución efectiva de responsabilidades y tareas.

En resumen, el organigrama de Profuturo AFP en Perú presenta una disposición organizativa sólida y bien definida que facilita la coordinación y el cumplimiento de los objetivos institucionales.

Figura 56. Organigrama general de Profuturo AFP [66].



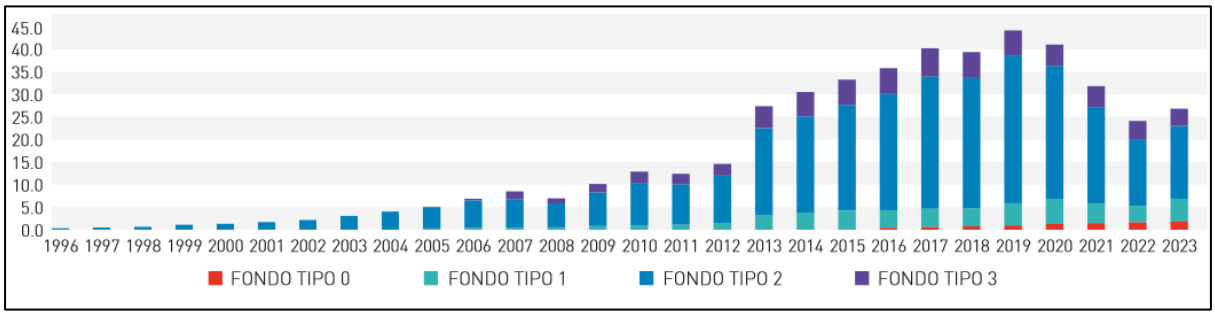
Fuente: Profuturo AFP

Durante el período comprendido entre 1996 y 2023, los fondos administrados por Profuturo AFP han experimentado variaciones y desempeños diversos, reflejando las condiciones del mercado financiero y económico en el Perú y a nivel global. Se observan fluctuaciones en los rendimientos de los fondos, influenciadas por factores como la volatilidad del mercado, los cambios en las políticas económicas y las tendencias macroeconómicas. A lo largo de estos años, Profuturo AFP ha implementado estrategias de gestión de inversiones diseñadas para maximizar el rendimiento y proteger los intereses de sus afiliados. Sin embargo, es importante tener en cuenta que el rendimiento pasado no garantiza resultados futuros, y que la inversión en fondos siempre está sujeta a los riesgos inherentes de los acontecimientos diarios que presentan los mercados especializados.

A continuación, se muestra de manera gráfica la evolución continua de los Fondos

administrados por Profuturo AFP:

Figura 57. Fondos administrados por Profuturo AFP, según tipo de fondo [66].

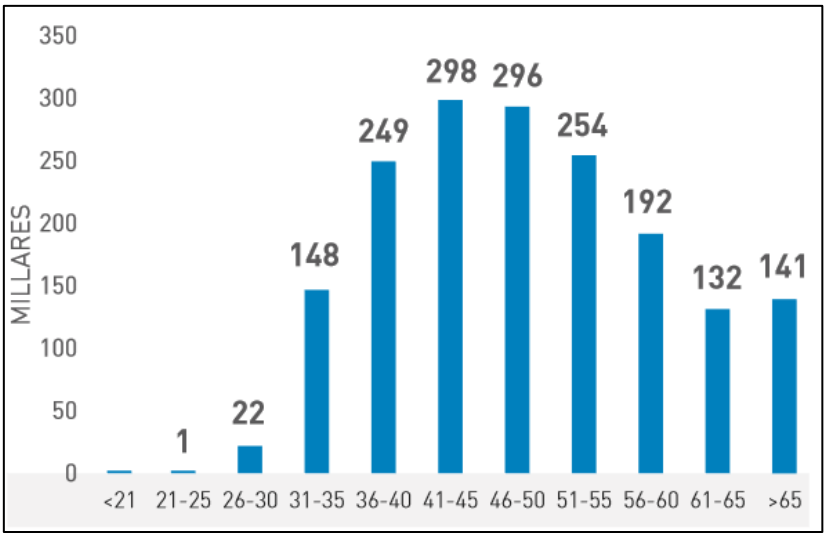


Fuente: Profuturo AFP

(miles de millones de soles)

Respecto a los afiliados de PROFUTURO AFP, durante el año 2023, se ha observado un aumento significativo en el número de afiliados, llegando a cerrar dicho año en 1’732,304 clientes, lo que sugiere una tendencia positiva en cuanto a la preferencia de los trabajadores por esta empresa financiera peruana para la gestión de sus fondos de pensiones, tal y como puede visualizarse en la siguiente imagen:

Figura 58. Afiliados activos por rango de edad [66].



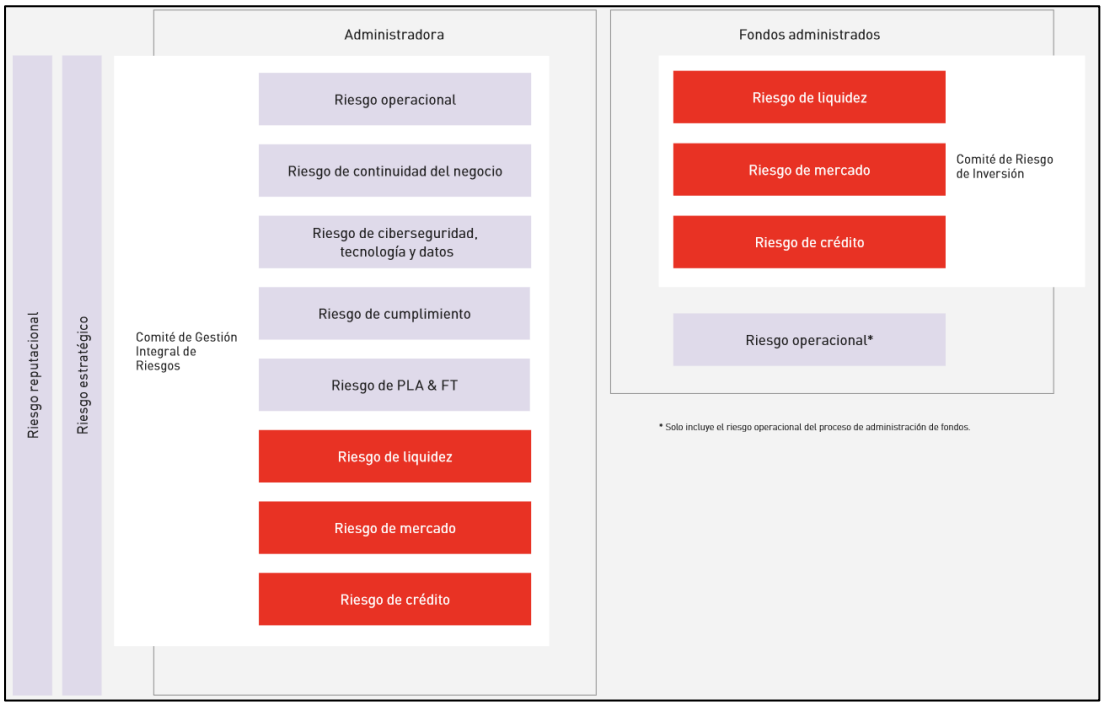
Fuente: Profuturo AFP

(en miles)

Este incremento en la cantidad de afiliados puede atribuirse a diversos factores, como la confianza en la reputación y solidez financiera de Profuturo AFP, así como a las estrategias efectivas de marketing y promoción implementadas por la institución para atraer a nuevos clientes. Además, es posible que cambios en las regulaciones gubernamentales o mejoras en los beneficios y servicios ofrecidos por Profuturo AFP hayan influido en esta tendencia afirmativa en la afiliación durante el año 2023. Esta información refleja una dinámica relevante en el sector de las administradoras de fondos de pensiones en el Perú, en la cual, PROFUTURO AFP ha tenido un alza al nivel de los años.

Respecto a su gestión del riesgo, Profuturo AFP la caracteriza por un enfoque integral y proactivo orientado a identificar, evaluar y mitigar los riesgos inherentes a sus operaciones y actividades, los cual se refleja en la siguiente lamina:

Figura 59. Gestión de riesgos en PROFUTURO AFP [66].



Fuente: Profuturo AFP

Esta empresa peruana del sistema financiero implementa un conjunto de políticas, procesos y controles diseñados para anticipar y responder eficazmente a los riesgos financieros, operativos, legales y reputacionales que podrían afectar su estabilidad y cumplimiento de objetivos. A través de la implementación de herramientas de análisis de riesgos, la realización de evaluaciones periódicas y la participación activa de los diferentes niveles organizativos, Profuturo AFP busca garantizar una gestión rigurosa y efectiva de los riesgos, promoviendo así la protección de los intereses de sus afiliados y el cumplimiento de las regulaciones aplicables en el sector financiero. Este enfoque refleja el compromiso de Profuturo AFP con la prudencia y la transparencia en la gestión de sus operaciones, contribuyendo a la generación de valor sostenible y la confianza de sus stakeholders en el largo plazo.

Ahora bien, específicamente en el ámbito de la gestión de riesgos, Profuturo AFP se dedica esfuerzos para recortar el riesgo asociado con la ciberseguridad, la tecnología y los datos de manera diligente y dinámica. Siendo así, se implementa una serie de medidas y controles diseñados para proteger sus sistemas de información y salvaguardar la confidencialidad, integridad y disponibilidad de los datos de sus clientes. Esto implica la adopción de TI avanzadas de seguridad, como firewalls y sistemas de detección de intrusiones, así como la realización de pruebas regulares de seguridad y evaluaciones de vulnerabilidad para identificar y mitigar posibles riesgos. Además, Profuturo AFP brinda capacitación enfocada y concientización a su personal sobre las mejores prácticas de seguridad cibernética y promueve una cultura organizativa centrada en la protección de la información y la prevención de amenazas cibernéticas. Estas medidas son fundamentales para garantizar la confianza de los clientes y mantener la integridad de los sistemas de información en un entorno digital cada vez más complejo y dinámico.

En base a los resultados obtenidos, se plantean las siguientes recomendaciones generales:

a. Implementación de Algoritmos Criptográficos: Se sugiere emplear algoritmos criptográficos resistentes y eficientes, como AES (Estándar de Cifrado Avanzado) y 3DES (Estándar de Cifrado de Datos Triple), para salvaguardar la confidencialidad de los datos sensibles manejados.
b. Selección del Algoritmo Adecuado: Es importante evaluar las características y eficacia de cada algoritmo criptográfico en función de los requerimientos de seguridad y las capacidades tecnológicas requeridos. Aspectos como la velocidad de procesamiento, el consumo de recursos y la resistencia a diversos tipos de ataques deben ser considerados.
c. Gestión de Claves: Se debe establecer un robusto sistema de gestión de claves para asegurar la seguridad y la integridad de las claves de cifrado utilizadas por los algoritmos AES y 3DES. Esto incluye la generación, distribución, almacenamiento y rotación periódica de las claves de manera segura.
d. Actualizaciones de Seguridad: Se recomienda mantenerse informado sobre las últimas recomendaciones y prácticas de seguridad de la información, así como aplicar las actualizaciones y parches de seguridad pertinentes para los algoritmos criptográficos empleados. Esto garantizará la mitigación de posibles vulnerabilidades y la adaptación a nuevas amenazas.
e. Auditorías de Seguridad: Se aconseja llevar a cabo auditorías regulares de seguridad para evaluar la efectividad de las medidas de protección implementadas. Esto incluye revisar la configuración de los algoritmos criptográficos, la gestión de claves y el cumplimiento de las políticas de seguridad de datos.
f. Capacitación y Concientización: Es fundamental proporcionar capacitación y concientización periódicas a todo el personal en grupos focalizados sobre la importancia de la seguridad de la información, así como sobre el adecuado uso y manejo de los datos sensibles y los sistemas de cifrado.

g. Cumplimiento Normativo: Se debe asegurar el cumplimiento de todas las regulaciones y normativas pertinentes en materia de seguridad de datos, tanto a nivel nacional como internacional, para garantizar una adecuada protección de la información confidencial de los afiliados y pensionistas.

Por una parte, a continuación, se muestran recomendaciones enfocadas específicamente en la eficiencia de los algoritmos de criptografía AES, para que se logre el propósito de cumplir con los niveles de seguridad de datos de una empresa financiera peruana como la AFP caso de estudio:

Tabla XXXI.

Recomendaciones para el cumplimiento de los niveles de seguridad de datos AES

N°	Característica	Descripción
1	Implementación de Versiones Actualizadas	Se recomienda adoptar las versiones más recientes y seguras de AES, como AES-256, para asegurar la protección óptima de los datos confidenciales manejados.
2	Uso de Claves Altamente Seguras	Es esencial emplear claves largas y complejas con AES para resistir eficazmente intentos de acceso no autorizado y ataques de criptoanálisis.
3	Selección del Modo de Operación Adecuado	Se debe elegir cuidadosamente el modo de operación más adecuado para AES, considerando los estándares de seguridad y los requisitos específicos de las operaciones financieras de entrada y salida.
4	Gestión Integral de Claves	Implementar un sólido 5sistema de gestión de claves que abarque desde la generación segura hasta la rotación periódica, asegurando la confidencialidad de la información financiera sensible.

5	Monitoreo Permanente	Es crucial realizar un seguimiento continuo de la implementación de AES para detectar y mitigar cualquier riesgo potencial de seguridad en las operaciones.

Fuente: Elaboración propia.

Por otra parte, a continuación, se muestran recomendaciones enfocadas específicamente en la eficiencia de los algoritmos de criptografía 3DES, para que se logre el propósito de cumplir con los niveles de seguridad de datos de una empresa financiera peruana como la AFP caso de estudio:

Tabla XXXII.

Recomendaciones para el cumplimiento de los niveles de seguridad de datos 3DES

N°	Característica	Descripción
1	Uso Limitado y Migración	Dado que 3DES se considera menos seguro en comparación con AES, se sugiere limitar su uso a casos donde sea estrictamente necesario, mientras se planifica una migración hacia algoritmos más seguros como AES.
2	Implementación de Triple Encriptación	Si se requiere seguir utilizando 3DES temporalmente, se recomienda implementar el modo de triple encriptación (EEE) para aumentar la seguridad y la resistencia contra ataques.
3	Gestión de Claves Rigurosa	Al igual que con AES, se debe establecer un sistema de gestión de claves riguroso para 3DES, garantizando la generación segura, distribución, almacenamiento y rotación adecuada de las claves.
4	Consideración de Alternativas	Se debe explorar y evaluar alternativas más seguras a 3DES, como algoritmos de cifrado simétrico modernos y eficientes, para garantizar una protección óptima de los datos sensibles.
5	Plan de Migración	Se recomienda la instrucción mediante un plan de migración claro y detallado para pasar de 3DES a algoritmos más

	seguros, tales como AES según los resultados obtenidos en esta investigación, como parte de una estrategia integral de mejora de la seguridad criptográfica.

Fuente: Elaboración propia.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Se concluye que el algoritmo AES para todas las mediciones cumple con la eficiencia criptográfica y seguridad de datos para una empresa financiera peruana.

Se establecieron los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana, buscando información en las bases de datos, artículos, publicaciones de investigaciones y revistas, identificándose un total de ocho algoritmos criptográficos existentes para dicho fin, los cuales, AES y 3DES se identificó que tienen las mejores valoraciones respecto a indicadores como rendimiento, consumo de memoria RAM, consumo de CPU, integridad y fortaleza.

Se analizaron los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras.

Se desarrollaron en lenguaje de programación PHP un sistema que utiliza las librerías de criptografía propios del lenguaje, empleando el entorno de desarrollo XAMPP, para el cifrado de documentos privados de una empresa financiera peruana, esto nos permitió observar cómo es que variaban las mediciones o resultados de los indicadores en los algoritmos AES y 3DES por cada documento.

Se plantearon recomendaciones enfocadas específicamente en la eficiencia de los algoritmos de criptografía AES y 3DES que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos.

4.2. Recomendaciones

Para seleccionar algoritmos de encriptación con mejores desempeños, se recomienda revisar investigaciones en idioma inglés y que no sean menores de 6 años.

El algoritmo AES tiene mejor desempeño en encriptación de paquetes con paquetes de 128 bits y claves de 256 bits, teniendo mejor rendimiento respecto al 3DES

Las investigaciones con mejor precisión, en idioma inglés deben buscarse en las siguientes bases de datos: EBSCOhost, Business Source Complete y DynaMed.

En las siguientes bases de datos Base de datos SCOPUS, IOP Science, Base de datos Eureka y Base de datos Web of Science, se encontró investigaciones poco precisas y en idioma español. Por lo tanto, se recomienda no buscar en estas bases de datos.

Las ejecuciones de los algoritmos de encriptación tanto de AES como para 3DES, se recomienda utilizar una red con conexión WIFI y una computadora personal con sistema operativo Windows 10, 64 bits, disco Sólido 256 GB, 8 GB de memoria RAM y un procesador Intel(R) Core (TM) i7-1075 H CPU 2.60GHz, de esta manera se obtendrá los resultados muy similares a lo expuesto en este documento.

REFERENCIAS

[1] A. Maiorano, «Técnicas de desarrollo para profesionales,» Aggentina, Alfaomega Grupon Editor, Buenos aires, Mexico, Santiago de chile, 2009.

[2] C. P. ·. J. Pelzl, «Understanding Cryptography,» Library of Congress Control Number: 2009940447, Springer Heidelberg Dordrecht London New York, 2010.

[3] B. OEA, «Reporte Ciberseguridad 2020,» OEA, BID, Publicado en Internet, 2020.

[4] D. Expreso, «Denuncian incremento de robos cibernéticos,» Lima, 2021.

[5] M. Abu-Faraj, «A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography,» Academic Editors: Alexander, Department of Computer Information Systems, The University of Jordan, Aqaba 77110, Jordan, 24 March 2022.

[6] B. O. Latif AKCAY, «Comparison of RISC-V and transport triggered architectures for a postquantum cryptography application,» Faculty of Electrical and Electronics Engineering, Faculty of Electrical and Electronics Engineering,, California, CA, USA, 2021.

[7] A. S. C. B. Pablo Martí Méndez Naranjo, «Propuesta de mejora de un algoritmo criptográfico con la combinación de la esteganografía en imágenes,» Universidad Nacional de Chimborazo, Ecuador, 2017.

[8] A. M. G. M. J. E. V. V. Denys Ivan Capuñay Puican, «Análisis comparativo de algoritmos criptográficos para redes privadas virtuales,» Rev. Ingeniería: Ciencia, Tecnología e Innovación VOL 3/N° 2 – ISSN 2313-1926/Setiembre 2016, Lambayeque. Perú., 2016.

[9] V. B. Vaibhavi Lakhani, «User authentication and cryptography using brain signals – a systematic review,» Gujarat Technological University, Department of Computer Engineering G H Patel College of Engg. & Tech., 2021.

[10] R. R. E. Vidhya, «Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Hellman Key Exchange Algorithm,» Department of Computer Science Periyar University Tamilnadu, Salem, India, University Tamilnadu, Salem, India, 2020.

[11] R. S. S. N. L. A. P. A. V. Ritu Shaktawat, «A Hybrid Technique of Combining AES Algorithm with Block Permutation for Image Encryption,» 5Department of Computer Science, Mohanlal Sukhadia University, Udaipur, India, Udaipur, India, 2020.

[12] Y. Wang, «Application of AES and DES Algorithms in File Management,» de *Journal of Physics: Conference Series, Volume 2037, 2021 International Conference on Artificial Intelligence and Information Technology (ICAIIT 2021)*, Pekín, 2021.

[13] K. S. S. K. L. A. M. N. A. Mohamed Elhoseny, «Hybrid optimization with cryptography encryption for medical image,» The Natural Computing

Applications Forum 2018, Faculty of Computers and Information, Mansoura University, 2018.

[14] M. A. N. J. ,. A. N. a. F. M. BahmanA. Sassani Sarrafpour, «Evaluating Encryption Algorithms for Sensitive Data Using Different Storage Devices,» Copyright © 2020 Bahman A. Sassani, New Zealand, 2020.

[15] O. C. F. C. L. C. L. D. R. Franyelit María Suárez, «Seguridad para aplicaciones con múltiples usuarios,» 15th Iberian Conference on Information Systems and Technologies (CISTI), Ecuador, 2020.

[16] J. Z. Jia Xu, «Strong leakage-resilient encryption: enhancing data confidentiality,» Springer-Verlag GmbH Germany, part of Springer Nature 2020, Singapore University of Technology and Design, Singapore, Singapore, 2020.

[17] F. W. S. S. Benavides Eduardo, «Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura,» Escuela Politécnica Nacional, Universidad de las Fuerzas Armadas, Ecuador, 2020.

[18] I. A. B. C. A. S. P. Daniel F. Santos, «Encryption Algorithm for Color Images Based on Chaotic Systems,» Facultad de Ingeniería Universidad Distrital Francisco José de Caldas, Colombia, 2020.

[19] O. J. S. Rodríguez, «El sistema de información y los mecanismos de seguridad informática en la pyme,» Universidad del Valle, Colombia, 2016.

[20] R. F. P. P. C. C. Luis Cáceres Álvarez, «Desarrollo de un simulador para el protocolo de criptografía cuántica E91 en un ambiente distribuido,» Revista chilena de ingeniería, vol. 23 Nº 2, 2015, Escuela Universitaria de Ingeniería Industrial, Informática y Sistemas. Universidad de Tarapacá, 2014.

[21] S. A. M. V. D. P. P. R. F. A. Carlos Roberto Sampedro Guamán, «Percepción de seguridad de la información en las pequeñas y medianas empresas en santo domingo,» Universidad regional Autónoma de los Andes, Santo Domingo, Ecuador, Santo Domingo, Ecuador, 2019.

[22] L. H. E. A. M. M. F. M. V. J. M. M. Amparo Fuster Sabater, «Criptografia, proteccion de datos y aplicaciones para estudiantes y profesionales,» Alfaomega Grupo Editor, S.A. de C.V., Ciudad de Mexico, 2012.

[23] J. R. Aguirre, «Cómo cifrar con el algoritmo AES,» Marzo 2015. [En línea]. Available: http://www.criptored.upm.es/thoth/material/texto/pildora030.pdf.

[24] A. Bukowski, «Proyecto Thoth - Pildoras Informativas,» 23 Abril 2014. [En línea]. Available: http://www.criptored.upm.es/thoth/index.php#.

[25] B. Xing, «Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor,» under exclusive licence to Springer

Science+Business Media, LLC, part of Springer Nature 2021, College of Information Science and Engineering, Ocean University of China, Qingdao 266100, China, 4 March 2020.

[26] C. Espinoza, Metodología de la Investigación Tecnológica: Pensando en Sistemas, Segunda ed., Huancayo: Universidad Nacional del Centro, 2014.

[27] Alvira M, Perspectiva cualitativa / perspectiva cuantitativa en la metodología sociológica, México. México: Mc Graw Hill, 2002.

[28] B. Hamouda, «Comparative study of different cryptographic algorithms,» *Journal of Information Security,* vol. 11, nº 3, pp. 138-148, 2020.

[29] A. Ahmed, H. Paruchuri, S. Vadlamudi y A. Ganapathy, «Cryptography in Financial Markets: potential channels for future financial stability,» *Academy of Accounting and Financial Studies Journal,* vol. 25, nº 4, pp. 1-9, 2021.

[30] E. Guerrero y K. Lozano, «Evaluación de algoritmos criptográficos para mejorar la seguridad de la información en el envío de texto plano por internet,» Universidad Señor de Sipán, Pimentel, 2023.

[31] F. Petitcolas, «Kerckhoffs' principle,» de *Encyclopedia of Cryptography, Security and Privacy*, Berlín, Springer, 2023, pp. 1-2.

[32] sbs.gob.pe, «INFORME Nº 027-2009-GTI,» 2019. [En línea]. Available: https://www.sbs.gob.pe/Portals /0/jer/inftecesano2009

/Informe_Adquisici%C3 %B3n%20de% 20licencias%20de %20software% 20endpoints.pdf.

[33] L. P. N. 0. -. E. N. 18677, «PODER JUDICIAL,» 2012. [En línea]. Available: http://200.70.33.130/images2/AdmGen/licitaciones /vigentes/2012/PCGPu%2003-12.pdf.

[34] SBS, «LICITACIÓN PÚBLICA Nº 009/2015-SBS (Primera Convocatoria),» 2015. [En línea]. Available: https://www.sbs.gob.pe/Portals /0/jer/baseliscano2015 /20160105_LP-009-2015-SBS.pdf.

[35] I. T. P. D. E. D. S. N. 001/2470, «BANCO DE LA NACION,» [En línea]. Available: https://www.bn.com.pe /transparenciabn/informes /2016/informe-tecnico -lectores-biometricos -04042016.pdf.

[36] A. S. N. 027/2018-SBS, «SBS,» 2018. [En línea]. Available: https://www.sbs.gob.pe/Portals/0/jer/ BASELISCANO2018/AS_N _027-2018-SBS-1.pdf.

[37] L. P. N. X. E. N. 718/16/19, «BANCO CENTRAL DE RESERVA,» 2018. [En línea]. Available: https://www.bcra.gob.ar /Pdfs/Institucional /Servicio-enlaces-MPLS.pdf.

[38] L. P. N. SIB-LPN-002/2019, «SUPERINTENDENCIA DE BANCOS,» 2019. [En línea]. Available: https://sb.gob.do/media /oomfwdk3/tdr-para-

la- adquisicion-y-contratacion-de-bienes-y- servicios-de-tecnologia- para-la-superintendencia -de-bancos.pdf.

[39] L. P. N.-C. 13/2020”, «PODER JUDICIAL,» 2020. [En línea]. Available: https://tsjyuc.gob.mx/licitaciones/2020/ PODJUDTSJ13-2020/AnexoTecnico 13-2020.pdf.

[40] B. REPUBLICA, «EXPEDIENTE EE2020/51/02289,» 2020. [En línea]. Available: https://www.comprasestatales.gub.uy /Pliegos/pliego_829912.pdf.

[41] M. D. T. GRANDE, «RESOLUCIÓN GERENCIAL N° 208-2020-MDT-GM - Términos de referencia,» 2020. [En línea]. Available: https://munitambogrande.gob.pe/uploads /Resolucion/2020/A6927_9107_11122020.pdf.

[42] P. SEGUROS, «INVITACIÓN ABIERTA No. 005 – 2021,» 2021. [En línea]. Available: https://previsora.gov.co /documents/20121/49790 /005_2021_pliegoCondiciones.pdf/ d4b48254-d03d- dedb-9675-c89108ab4cc5?t= 1670016007941.

[43] P. JUDICIAL, «LICITACIÓN PÚBLICA NÚMERO PODJUDCJ 14/2021,» 2021. [En línea]. Available: https://www.cjyuc.gob.mx/licitaciones /2021/PODJUDCJ14-2021/ ANEXO_TECNICO.pdf.

[44] B. C. D. RESERVA, «INFORME Nº 0155-2021-GTI220-N,» 2021. [En línea]. Available: https://www.bcrp.gob.pe/docs/Transparencia /Licitacion/2021/informe-0155-2021 -gti220-n.pdf.

[45] SUNAT, «LPI N° 005-2021-SUNAT/BID,» 2021. [En línea]. Available: https://view.officeapps.live. com/op/view.aspx? src=https%3A%2F%2Fwww. sunat.gob.pe %2Fcuentassunat% 2Fadquisiciones%2FcontratosBID%2FllamadoLicita% 2Fli4725%2F2021%2Fdoc-lp-005-2021 .docx&wdOrigin=BROWSELINK.

[46] A. G. prescriptiva, «GUIA PRESCRIPTIVA Mejores prácticas y funciones de cifrado para Servicios de AWS,» [En línea]. Available: https://docs.aws.amazon.com/ es_es/prescriptive-guidance /latest/encryption-best-practices/ encryption-best-practices.pdf.

[47] U. A. d. E. d. Hidalgo, «LICITACIÓN PÚBLICA NACIONAL UAEH-LP-N11-2022,» 2022. [En línea]. Available: https://www.uaeh.edu.mx/convocatorias/2342/index.html.

[48] SBS.GOB.PE, «CONCURSO PÚBLICO Nº 009/2022-SBS,» 2022. [En línea]. Available: https://www.sbs.gob.pe/Portals/0 /jer/BASELISCANO2022 /CP%20N%20009-2022-SBS.pdf.

[49] SBS.GOB.PE, «INFORME Nº 00065-2022-GTI,» 2022. [En línea]. Available: https://www.sbs.gob.pe/Portals/0/jer/INFTECSAO2022 /INFORME%20N%2000065%20-%202022%20 -% 20GTI-PRI.pdf.

[50] M. D. TRABAJO, «PLIEGO DE CONDICIONES TÉCNICAS Expediente S-03898-2023,» 2023. [En línea]. Available: https://www.google.com.pe/url?sa=t&rct=j&q= &esrc=s&source=web&cd=&ved=2ahUKEwi8kM2X -d-GAxWWO7kGHUiIB_gQFnoECBMQAQ&url =https%3A%2F%2Flicitaciones.rtve.es%2Flicitacion% 2Fdocumento%3FnumExpediente %3DS-03898-2023%26idDoc%3DR0369470&usg.

[51] M. D. TRABAJO, «LICITACIÓN PRIVADA N° 02 / 23 EXPEDIENTE N° 15120-0159117-7,» 2023. [En línea]. Available: https://www.google.com.pe/url?sa=t&rct=j&q =&esrc=s&source=web&cd=&ved=2ahUKEwis4YW1-9-G AxVZKbkGHa5pBcgQFnoECA4QAQ&url=https%3A%2 F%2Fwww.santafe .gob.ar%2Fgestionesdecompras %2Fdescargar.ph.

[52] B. C. D. RESERVA, «INFORME Nº 0063-2023-GTI220-N,» 2023. [En línea]. Available: https://www.bcrp.gob.pe/docs/ Transparencia/Licitacion/2023 /informe-0063-2023-gti220-n.pdf.

[53] B. C. D. RESERVA, «INFORME Nº 0068-2023-GTI220-N,» 2023. [En línea]. Available: https://www.bcrp.gob.pe/docs/ Transparencia/informes /2023/memorando-0082-2023-adm 110-n.pdf.

[54] SBS, «ADJUDICACIÓN SIMPLIFICADA N° 47-2023-SBS,» 2023. [En línea]. Available:

https://www.sbs.gob.pe/Portals/0/jer/BASELISCANO2023
/AS_47_2023_SBS_2daconv.pdf.

[55] B. C. D. RESERVA, «INFORME Nº 0208-2024GTI220-N,» 2024. [En línea]. Available: https://www.bcrp.gob.pe/docs/Transparencia /Licitacion/2024/informe-0208-2024- gti220-n.pdf.

[56] SBS, «ADJUDICACIÓN SIMPLIFICADA N° 002-2024-SBS (Primera Convocatoria),» 2024. [En línea]. Available: https://www.sbs.gob.pe/Portals/0 /jer/BASELISCANO2024 /Bases%20AS%20002-2024%20s.pdf.

[57] P. Patil, P. Narayankar, D. Narayan y S. Meena, «A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,» *Procedia Computer Science,* vol. 78, nº 1, pp. 617-624, 2016.

[58] P. Revenkov, A. Berdyugin y P. Makeev, «Research on Brute Force and Black Box Attacks on ATMs,» de *CEUR Workshop Proceedings. Selected Papers of XI International Scientific and Technical Conference on Secure Information Technologies (BIT 2021)*, Moscú, 2021.

[59] J. Aumasson, Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographer, Primera ed., San Francisco: No Starch Press, 2021.

[60] A. Mallik, «Man-in-the-middle-attack: Understanding in simple words,» *Jurnal Pendidikan Teknologi Informasi,* vol. 2, nº 2, pp. 109-134, 2019.

[61] A. Kar y S. Dey, «Cryptography in the banking industry,» *Frontiers,* vol. 1, nº 1, pp. 1-7, 2012.

[62] P. S. R. T. K. &. A. N. Kanaga Priya, «Various Attacks on the Implementation of Cryptographic Algorithms,» de *Homomorphic Encryption for Financial Cryptography: Recent Inventions and Challenges*, Cham, 2023.

[63] M. Rahman, T. Akter y A. Rahman, «Development of cryptography-based secure messaging system,» *Journal of Telecommunications Systems & Management,* vol. 5, nº 3, pp. 1-6, 2016.

[64] N. Mathur, G. Mitawa y P. Mathur, «A review on cryptography attacks and cyber security,» *International Journal of Advance Research and Innovative Ideas in Education(IJARIIE),* vol. 5, nº 2, pp. 1610-1615, 2019.

[65] Q. Phan, L. Bang, C. Pasareanu, P. Malacaria y T. Bultan, «Synthesis of adaptive side-channel attacks,» de *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, Santa Bárbara, 328-342.

[66] Profuturo AFP, «Memoria Anual 2023,» Grupo Scotiabank, Lima, 2024.

[67] R. S. S. N. L. A. P. A. V. Ritu Shaktawat, «A Hybrid Technique of Combining AES Algorithm with Block Permutation for Image Encryption,» Department of Computer Science, Mohanlal Sukhadia University, Udaipur, India 2Department of Computer Science, College of Technology, Udaipur, India, 2020.

[68] G. K. V. T. V. K. Nina Sinyagina, «Developing an Application for Researching the RSA Algorithm Behavior on a Multithread Platform,» South-West University - Neofit Rilski, South-West University - Neofit Rilski, 2020.

[69] S. H. M. Vahid Rashtchi, «Strengthened of AES Encryption Algorithms within New Logic Topology,» Department of Electrical and Computer Engineering, Zanjan University, Zanjan, Iran, Zanjan, Iran, 2018.

[70] E. J. a. T. H. Herbert Siregar, «Analysis of Attacks on Mail Disposition Systems Secured by Digital Signatures Equipped with AES and RSA Algorithms,» Departemen Pendidikan Ilmu Komputer, Universitas Pendidikan Indonesia, Jl. Dr. Setiabudi,, Bandung 40154, Indonesia, 2018.

[71] J. Gong, «Plaintext recovery attack on 3DES algorithm with different byte keys,» School of Data and Computer Science, Guangdong Peizheng College, Guangzhou, China Guangzhou, 2020.

[72] E. Guerrero y K. Lozano, «Evaluación de algoritmos criptográficos para mejorar la seguridad de la información en el envío de texto plano por internet,» Universidad Señor de Sipán, Pimentel, 2023.

[73] W. Sandoval, «Comparación de algoritmos de segmentación de imágenes digitales de plantas de arroz en ambientes no controlados,» Universidad Señor de Sipán, Pimentel, 2023.

ANEXOS

Anexo 1. Resolución de aprobación del proyecto de investigación

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

VISTO:
El Acta de reunión N°1305-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N°0227-2021/FIAU-IS-USS de fecha 19 de mayo de 2021, y;

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

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

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

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerdan aprobar los temas de las Tesis a cargo de los estudiantes del curso de Investigación I que se detallan en el anexo de la presente Resolución.

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

SE RESUELVE:

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

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

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

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

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

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

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

ANEXO

N°	AUTOR (ES)	TEMA DE TESIS
1	RIMARACHIN ESCRIBANO NERI RUT NIÑO MORENO NAJHELY YAMILETT	EVALUACIÓN DE TÉCNICAS DE CIFRADO PARA EL INTERCAMBIO DE DATOS DE INTERNET DE LAS COSAS EN EL ÁMBITO DE LA SALUD
2	GUEVARA CHAMBERGO JHON DENNIS BOBADILLA CAMPOS ROLANDO MARTIN	DESARROLLO DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN MARCOS INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA
3	CIEZA CELIS JESUS ABELARDO OJEDA ROMERO ANTHONNY JHONATAN	EVALUACIÓN DEL DESEMPEÑO DE LOS ESQUEMAS DE SEGURIDAD DE RED PARA COMBATIR VULNERABILIDADES EN REDES INALÁMBRICAS BASADAS EN EL PROTOCOLO WPA2
4	MENDOZA FERRÉ ESPERANZA NATALY CABRERA SANCHEZ KEVIN ALONSO	COMPARACIÓN DEL RENDIMIENTO DE TECNOLOGÍAS DE VIRTUALIZACIÓN PARA EL DESPLIEGUE DE APLICACIONES CON ARQUITECTURA DE MICROSERVICIOS
5	TEMOCHE GOMEZ LENNIN BILLEY	DESARROLLO DE UN MÉTODO PARA DETECTAR CON EFICIENCIA LAS VULNERABILIDADES INFORMÁTICAS DE ATAQUE CROSS-SITE SCRIPTING UTILIZANDO TÉCNICAS DE APRENDIZAJE AUTOMÁTICO
6	CASTRO MEDINA MIGUEL ANGEL	IMPLEMENTACIÓN DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO
7	MURO ESPINOZA JUAN JOSE	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UN INSTITUTO SUPERIOR PEDAGÓGICO PERUANO
8	DIAZ ZAVALA ROXANA KARINA FRIAS VASQUEZ LADY	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA UNIDAD DE GESTIÓN EDUCATIVA PERUANA
9	CARRASCO BORDA APARICIO	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE POR LICENCIA PARA UNA MYPE DE SERVICIOS DE TI BASADO EN ISO/IEC 29110
10	OTERO MORALES JAVIER LIZARDO AQUINO SOSA NOELIA STEPHANY	DESARROLLO DE UN MODELO DE PROCESOS BASADO EN NORMAS DE PEQUEÑAS ORGANIZACIONES PARA MEJORAR LA CONSTRUCCIÓN DE SOFTWARE EN UN ÁREA DE DESARROLLO DE GOBIERNO MUNICIPAL
11	CALDERON YNOÑAN PAMELA DEL CARMEN PRIETO NEIRA FRANCK ALBERSON	DESARROLLO DE UN MÉTODO BAJO EL ENFOQUE ÁGIL EN ENTORNOS DE EXPERIENCIA DE USUARIO UI/UX PARA ASEGURAR LA USABILIDAD WEB
12	FLORES TINEO HUGO GALVANI DOLORIER POMA RONY RAUL	EVALUACIÓN DE LA USABILIDAD EN ENTORNOS VIRTUALES DE APRENDIZAJE PARA USUARIOS DE LAS ZONAS RURALES DEL PERÚ UTILIZANDO LA NORMA ISO/IEC 25010
13	CHANCAFE CASTRO JULIO JOEL	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE PARA UNA MUNICIPALIDAD BASADO EN ISO/IEC 29110
14	SALAZAR DAVILA GIANFRANCO STEVEN	COMPARACIÓN DE TÉCNICAS DE VALIDACIÓN DE REQUISITOS DE SOFTWARE PARA MEDIR LA INFLUENCIA EN EL ÉXITO DE LOS PROYECTOS DE DESARROLLO EN PEQUEÑAS EMPRESAS PERUANAS
15	RIOJA MESIA CHARLES SEGUNDO FERNANDEZ RIOJA JUAN NICANOR	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE INCIDENCIAS BASADO EN ITIL PARA MEJORAR EL SERVICIO DE TI EN UNA MUNICIPALIDAD DISTRITAL DE LA REGIÓN LAMBAYEQUE
16	ALFARO PAJARES JUAN PEDRO	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA EMPRESA CONSTRUCTORA PERUANA
17	MONSALVE FERNANDEZ LENIN ESTALIN	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SERVICIOS DE TI BASADO EN ITIL PARA MEJORAR LA GESTIÓN DE LOS SERVICIOS DE LA DIRECCIÓN DE TECNOLOGÍA DE UN GOBIERNO REGIONAL PERUANO
18	PEREZ CAMPOS DE QUIROZ BETTY MAGALY	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA MICRO EMPRESA PERUANA DESARROLLADORA DE SOFTWARE
19	MONTJOY PITA BRUNO	DESARROLLO DE UN SISTEMA DE RECOMENDACIÓN AUTOMÁTICA PARA EL TRATAMIENTO DE LAS PLAGAS EN CULTIVOS DE ARROZ DE LAS VARIEDADES QUE SE PRODUCEN EN LA REGIÓN LAMBAYEQUE
20	CRUZ FLORES JOSE ANTONIO CHAVEZ ANGULO GERMAN NEPTALI	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADO EN METODOLOGÍA ÁGIL PARA ALINEAR LAS TECNOLOGÍAS DE INFORMACIÓN CON LOS OBJETIVOS DE NEGOCIO DE UN ESTABLECIMIENTO PERUANO DE SALUD BUCAL

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

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

N°	AUTOR (ES)	TEMA DE TESIS
21	PISFIL CORONADO JOSE LUIS FELIPE	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADA EN METODOLOGÍA ÁGIL PARA ALINEAR TI CON LOS PROCESOS DE NEGOCIO EN UNA EMPRESA CONSTRUCTORA PERUANA DE OBRAS CIVILES
22	ABAD HERRERA JOHNNY RENSO TEPE ESPINOZA LUIS RAMON	IMPLEMENTACIÓN DE ITIL V4 PARA MEJORAR LOS SERVICIOS DE TI EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE UNA UNIDAD DE GESTIÓN EDUCATIVA LOCAL PERUANO
23	URRUTIA VASQUEZ MIGUEL JULCA ROJAS ALEX ROGELIO	DESARROLLO DE UN MÉTODO DE IDENTIFICACIÓN AUTOMÁTICA DE ATAQUES SPOOFING DE ENVENENAMIENTO ARP EN LA SUPLANTACIÓN DE IDENTIDAD EN REDES LAN
24	SANCHEZ CELADA ERLIN FERNANDEZ ROMAN ISMAEL	COMPARACIÓN DE ARQUITECTURAS DE IDS HÍBRIDO PARA LA IDENTIFICACIÓN DE ATAQUES DE DOS EN LOS SERVIDORES WEB DE UNA MUNICIPALIDAD PROVINCIAL PERUANA
25	PERALES CHAVEZ JEFFERSON ADRIAN	IMPLEMENTACIÓN DE UN MODELO DE ARQUITECTURA DE INDUSTRIA 4.0 PARA MEJORAR LA INTEROPERABILIDAD ENTRE SISTEMAS DE UNA EMPRESA PERUANA
26	MAGALLANES CARBAJAL KENSER	EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA
27	RACCHUMI LECCA JESÚS MANUEL	DESARROLLO DE UN MIDDLEWARE PARA MEJORAR LA COMUNICACIÓN ENTRE DOS INTERFACES DE LMS Y CRM EN EL PROCESO DE REGISTRO Y EMISIÓN DE CREDENCIALES DE USUARIOS
28	CASTRO QUESQUEN JAIME ELTON	COMPARACIÓN DE ALGORITMOS DE CIFRADO DE DATOS EN EL ASEGURAMIENTO DE VIDEO LLAMADA SOBRE REDES IP
29	PEREZ DIAZ NEILER WILTER CHINCHAY MALDONADO JORGE OBED	IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA
30	MOSCOSO PAREDES ANIBAL	DISEÑO DE UN MODELO DE ARQUITECTURA DE SEGURIDAD DE BAJO COSTO PARA REFORZAR LA SEGURIDAD DE LA RED DEL HOGAR ANTE ATAQUES INFORMÁTICOS
31	MARTINEZ CUMPA JORGE JOSE	EVALUACIÓN DE FACTIBILIDAD DE USO DE TECNOLOGÍA WIRELESS 5GHZ PARA PROPORCIONAR SERVICIOS DE COMUNICACIÓN INALÁMBRICA EN LOS CENTROS POBLADOS RURALES DE LA REGIÓN LAMBAYEQUE
32	CAMPOS BARRERA SANDRO PAUL PASTOR OLIVA CESAR AUGUSTO	IMPLEMENTACIÓN DE UN MÉTODO DE CLASIFICACIÓN PARA DETECTAR LA DESERCIÓN DE ESTUDIANTES DE LA CARRERA DE INGENIERÍA DE INDUSTRIAS ALIMENTARIAS DE UNA UNIVERSIDAD NACIONAL PERUANA BASADO EN APRENDIZAJE DE MAQUINA
33	PICON VASQUEZ ANGEL GABRIEL CESPEDES SALAZAR JUAN CARLOS	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA BASADA EN TÉCNICAS ESTADÍSTICAS Y DE MACHINE LEARNING PARA CLASIFICAR A LOS POSTULANTES DE ACUERDO AL PERFIL DE TRABAJO DE UN CALL CENTER
34	MIÑANO SANCHEZ CARLOS JOHNY	COMPARACIÓN DE TÉCNICAS DE MINERÍA DE DATOS PARA DESCUBRIR INFORMACIÓN RELEVANTE DE VENTAS DE UNA MYPE COMERCIAL
35	MARTOS PAREDES JOEL HAROLD VILLAZON SOSA JAIR AUGUSTO	IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADO EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S
36	QUISPE PUEMAPE LUIS ALONSO	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001:2014 EN UNA EMPRESA PERUANA DE TELECOMUNICACIONES
37	CHUCO AGUILAR GERSON RAUL	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27001 PARA MEJORAR EL NIVEL DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN UNA EMPRESA CONSTRUCTORA DE OBRAS CIVILES
38	CAJUSOL ROJAS JOSE DEL CARMEN	IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA LA PLANIFICACIÓN Y MONITOREO DE RUTAS DE RECOJO DE RESIDUOS SÓLIDOS DE UN MUNICIPIO DE LA REGIÓN LAMBAYEQUE
39	VALLEJOS RAMOS FERNANDO RAFAEL	DESARROLLO DE UN MÉTODO DE OPTIMIZACIÓN DE USO DE TELA EN EL PROCESO DE ELABORACIÓN DE PRENDAS TEXTILES DE MICROEMPRESAS PERUANAS
40	REQUEJO NAVARRO JERSONS EXFRANSHER	EVALUACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR SEGURIDAD EN UNA RED PRIVADA VIRTUAL

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

Ampliación de vigencia

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0785-2023/FIAU-USS

Pimentel, 18 de diciembre de 2023

VISTO:
El Acta de reunión N°01412-2023 del Comité de investigación de la INGENIERÍA DE SISTEMAS remitida mediante vía oficio N° 0296-2023/FIAU-IS-USS de fecha 15 de diciembre de 2023, y;

CONSIDERANDO:

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

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

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

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

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó ampliar la vigencia de tesis, de la línea de investigación de CIENCIAS DE LA INFORMACIÓN COMO HERRAMIENTAS MULTIDISCIPLINARES Y ESTRATÉGICAS EN EL CONTEXTO INDUSTRIAL Y DE ORGANIZACIONES, a cargo de los estudiantes y /o egresados del Programa de estudios INGENIERÍA DE SISTEMAS, hasta la fecha que indica la presente resolución.

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

SE RESUELVE:

ARTÍCULO 1: APROBAR, Ampliación de vigencia de tesis a cargo de los estudiantes y /o egresados del Programa de estudios de **INGENIERÍA DE SISTEMAS que** se detallan en el anexo de la presente Resolución.

ARTÍCULO 2: DEJAR SIN **EFECTO**, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0785-2023/FIAU-USS

Pimentel, 18 de diciembre de 2023

ANEXO

AMPIACION DE VIGENCIA DE TESIS

	APELLIDOS	TESIS	AMPLIACION DE VIGENCIA
1	MAGALLANES CARBAJAL KENSER	RESOLUCION **0445-2021/FIAU-USS** Evaluación de la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana	**Se amplía hasta el 27/05/2024.**

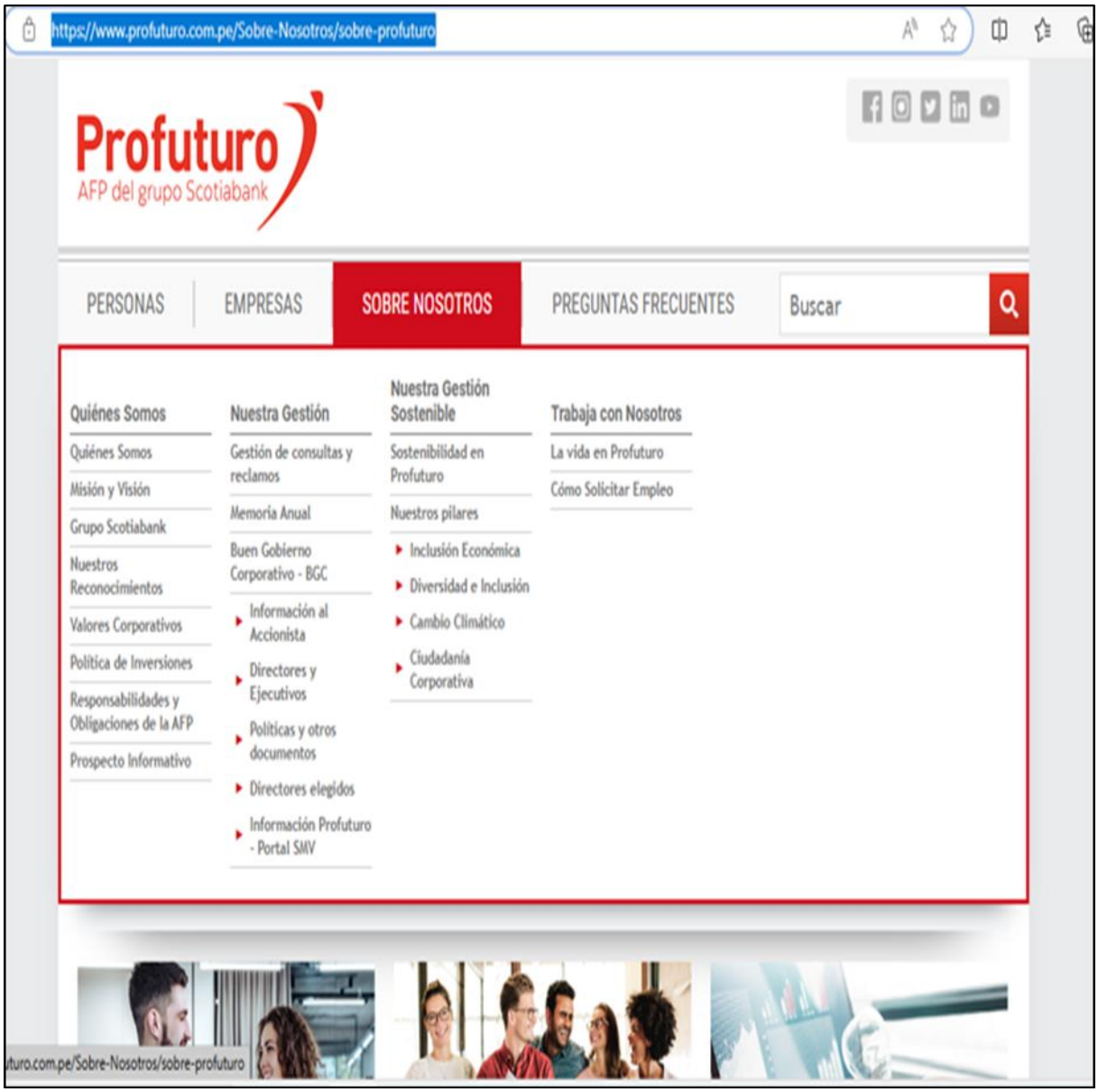
REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Víctor Alexci Tuesta Monteza
Decano (E) / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Dr. Halyn Alvarez Vásquez
Secretario Académico Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

Anexo 2. Recolección de datos privados y publicados por Profuturo AFP



https://www.profuturo.com.pe/Sobre-Nosotros/sobre-profuturo

Anexo 3. Declaración jurada de originalidad

Universidad Señor de Sipán

DECLARACIÓN JURADA DE ORIGINALIDAD

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

EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA

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

En virtud de lo antes mencionado, firma:

MAGALLANES CARBAJAL KENSER	DNI: 21869345	

Pimentel, 1 de marzo del 2024.

Anexo 4. Acta de aprobación del asesor

USS	DIRECTIVA PARA EL DESARROLLO DE LOS CURSOS DE INVESTIGACIÓN Y TRABAJOS CONDUCENTES A TÍTULOS PROFESIONALES PREGRADO	Código:	PP2-DI.03
		Versión:	04
		Fecha:	06/11/2023
		Hoja:	1 de 140

USS Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **Mg. Tuesta Monteza Víctor Alexci**. quien suscribe como asesor designado mediante Resolución de Facultad N° **0785-2023/FIAU-USS, N°0445-2021/FIAU-USS**, del proyecto de investigación titulado **Evaluación de la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana**, desarrollado por el(los) estudiante(s): **Kenser Magallanes Carbajal**, del programa de estudios de **INGENIERÍA DE SISTEMAS**, acredito haber revisado, y declaro expedito para que continue con el trámite pertinentes.

En virtud de lo antes mencionado, firman:

Mg. Tuesta Monteza Víctor Alexci.	DNI: 42322721	

Pimentel, 20 de mayo del 2024

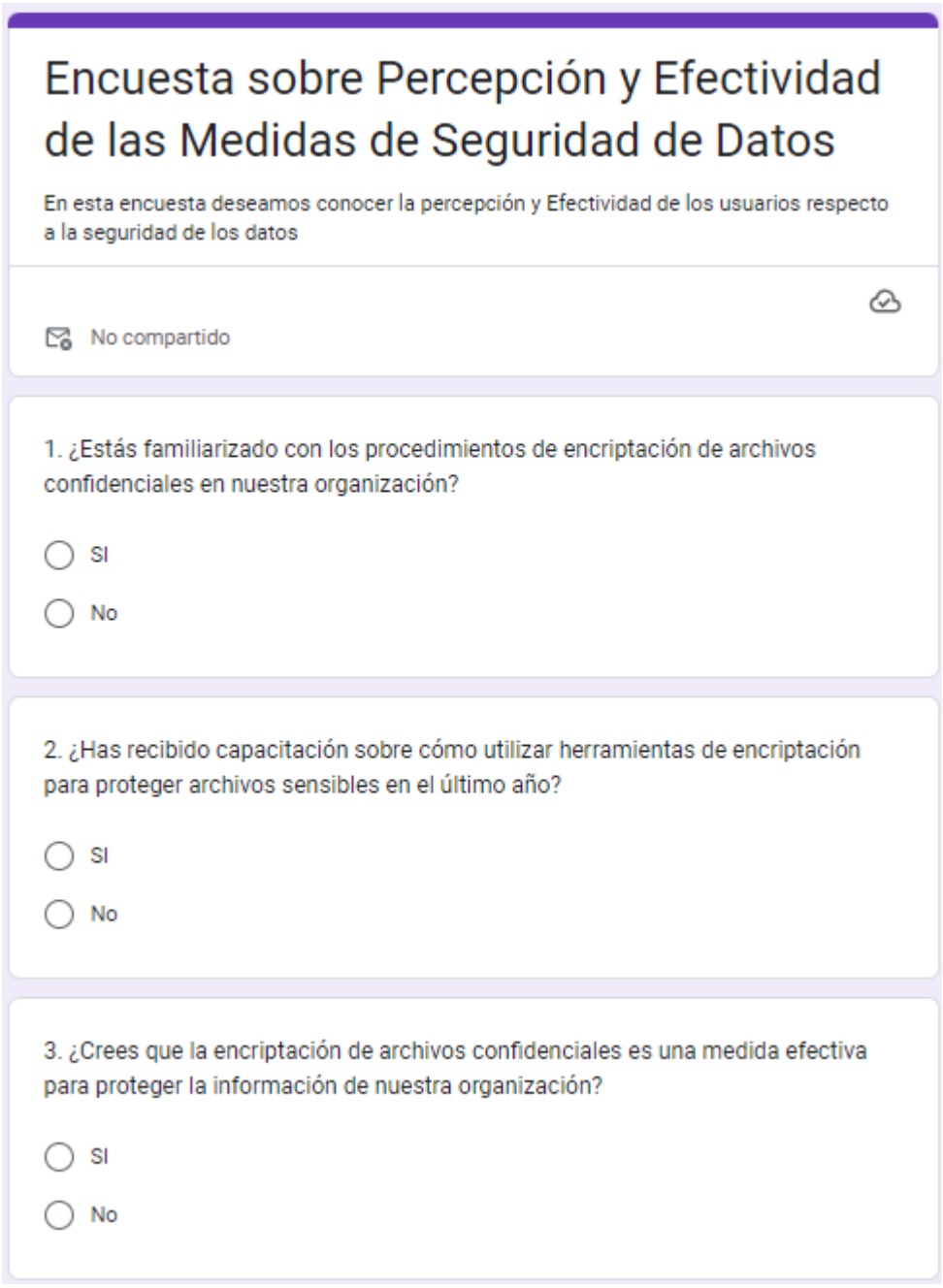
Anexo 5. Matriz de consistencia

MATRIZ DE CONSISTENCIA LOGICA DE PROYECTO DE INVESTIGACION – ENFOQUE METODOLOGICO

Titulo	EVALUACION DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFIA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA						
Tipo de investigación	**Problema**	**Variables**	**Indicadores**	**Población**	**Muestra**	**Método de recolección de datos**	**Técnicas de procesamiento de datos**
Tecnológica Aplicada	¿Cuál es el algoritmo de criptografía más eficiente para cumplir con los niveles adecuados de seguridad de datos de una empresa financiera peruana?	**Variable Independiente:** Algoritmos de criptografía **Variable dependiente:** Seguridad de datos en una empresa financiera peruana	**Eficiencia del algoritmo:** - Rendimiento de cifrado - Rendimiento de descifrado **Consumo de recursos del algoritmo:** - Consumo de RAM - Consumo de CPU **Seguridad de la información de los datos:** - Integridad - Fortaleza del algoritmo	Se ha considerado, 8 algoritmos de encriptación para la población de este trabajo de investigación, los mismos se encuentran distribuidas en las categorías simétrica y asimétrica, cada una de estas categorías contiene un gran número de algoritmos de encriptación, también conocido en el argot informático como código abierto.	La presente investigación ha utilizado el muestreo no probabilístico, dado que la muestra no depende de algo probable, a su vez, tomando en cuenta el criterio de mayor reputación han elegido por conveniencia los algoritmos AES y 3DES	Registros electrónicos. Bibliografías.	Análisis electrónicos. Estadísticos.
Diseño de investigación	**Hipótesis**	**Objetivo General**	**Objetivo especifico**	**Método propuesto y desarrollo**		**Resultado preliminar**	
cuasi experimental	El algoritmo de criptografía AES es el más eficiente para cumplir con los niveles adecuados de seguridad de datos de una empresa financiera peruana.	Evaluar la eficiencia de los algoritmos de criptografía para cumplir con los niveles de seguridad de datos de una empresa financiera peruana.	**OBJ 01.** Definir los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana. **OBJ 02.** Analizar los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras. **OBJ 03.** Desarrollar en lenguaje de programación los algoritmos de criptografía para el cifrado de datos de un texto plano en documentos privados de una empresa financiera peruana. **OBJ 04.** Plantear recomendaciones que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos.	1. Definir los algoritmos de criptografía más relevantes para cumplir con los niveles de seguridad de datos de una empresa financiera peruana. 1.1. En la literatura científica se adoptaron las directrices para la revisión sistemática que propusieron Kitchenham & Charters con el propósito de seleccionar los algoritmos criptográficos. 2. Analizar los principales ataques de criptografía que vulneran la seguridad de datos en empresas financieras. 2.1. Se revisaron los artículos que pusieron en manifiesto dichos ataques para cada uno de los algoritmos AES y 3DES. 3. Desarrollar en lenguaje de programación los algoritmos de criptografía para el cifrado de datos de un texto plano en documentos privados de una empresa financiera peruana. 3.1. Se llevo a cabo la implementación de los algoritmos AES y 3DES, para ello se utilizo el lenguaje de programación PHP. 4. Plantear recomendaciones que permitan el cumplimiento de los niveles de seguridad de datos en base a los resultados obtenidos. 4.1. Se realizan recomendaciones para documentar el cumplimiento de seguridad.		Encriptación de datos y seguridad de la información	

Anexo 6. Cuestionario SUS (System Usability Scale)

Figura 60. Encuesta sobre Percepción y Efectividad de las Medidas de Seguridad de Datos



Encuesta sobre Percepción y Efectividad de las Medidas de Seguridad de Datos

En esta encuesta deseamos conocer la percepción y Efectividad de los usuarios respecto a la seguridad de los datos

No compartido

1. ¿Estás familiarizado con los procedimientos de encriptación de archivos confidenciales en nuestra organización?

- SI
- No

2. ¿Has recibido capacitación sobre cómo utilizar herramientas de encriptación para proteger archivos sensibles en el último año?

- SI
- No

3. ¿Crees que la encriptación de archivos confidenciales es una medida efectiva para proteger la información de nuestra organización?

- SI
- No

4. ¿Has experimentado dificultades al intentar acceder a archivos encriptados debido a restricciones de acceso?

- ◯ Siempre
- ◯ A veces
- ◯ Nunca

5. ¿Estás al tanto de las políticas de gestión de claves de encriptación en nuestra organización?

- ◯ SI
- ◯ No

6. ¿Consideras que se realiza un seguimiento adecuado de los archivos encriptados y las claves correspondientes?

- ◯ Siempre
- ◯ A veces
- ◯ Nunca

7. ¿Te sientes seguro de que los archivos encriptados están protegidos de manera adecuada en caso de una posible violación de seguridad?

- ◯ Siempre
- ◯ A veces
- ◯ Nunca

8. ¿Estás al tanto de las regulaciones y estándares relacionados con la encriptación de datos que deben cumplirse en nuestra organización?

- ◯ SI
- ◯ No

9. ¿Cómo evaluarías la eficacia de las herramientas de encriptación utilizadas en nuestra organización en términos de seguridad y facilidad de uso?

	1	2	3	4	5	
Muy mala	◯	◯	◯	◯	◯	Muy buena

10. ¿Tienes alguna sugerencia para mejorar la implementación o el uso de la encriptación de archivos confidenciales en nuestra organización?

Tu respuesta

Enviar Borrar formulario

Anexo 7. Formato T1

UNIVERSIDAD SEÑOR DE SIPÁN

FORMATO Nº T1-VRI-USS AUTORIZACIÓN DEL AUTOR (ES)
(LICENCIA DE USO)

Pimentel, 1 de marzo del 2024

Señores
Vicerrectorado de Investigación
Universidad Señor de Sipán
Presente.-

El suscrito:
MAGALLANES CARBAJAL KENSER con DNI 21869345.

En calidad de autor exclusivo de la investigación titulada: EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA, presentada y aprobada en el año 2024 como requisito para optar el título de Ingeniero de Sistemas, de la Facultad de Ingeniería, Arquitectura y Urbanismo, Programa Académico de INGENIERÍA DE SISTEMAS, por medio del presente escrito autorizo al Vicerrectorado de investigación de la Universidad Señor de Sipán para que, en desarrollo de la presente licencia de uso total, pueda ejercer sobre mi trabajo y muestre al mundo la producción intelectual de la Universidad representado en este trabajo de grado, a través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios pueden consultar el contenido de este trabajo de grado a través del Repositorio Institucional en el portal web del Repositorio Institucional – http://repositorio.uss.edu.pe, así como de las redes de información del país y del exterior.
- Se permite la consulta, reproducción parcial, total o cambio de formato con fines de conservación, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de investigación y a su autor.

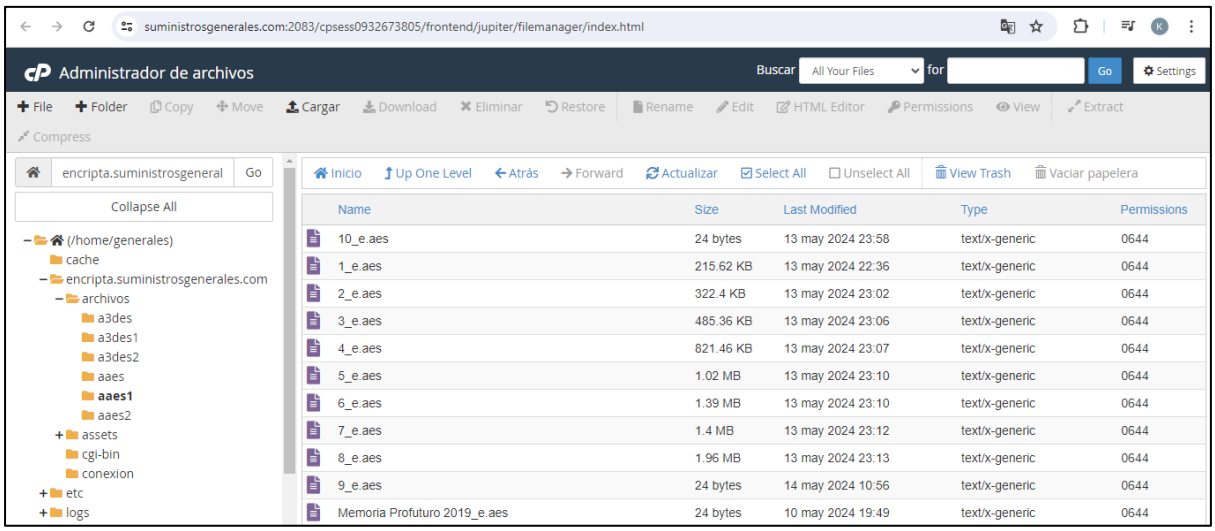
De conformidad con la ley sobre el derecho de autor decreto legislativo N° 822. En efecto, la Universidad Señor de Sipán está en la obligación de respetar los derechos de autor, para lo cual tomará las medidas correspondientes para garantizar su observancia.

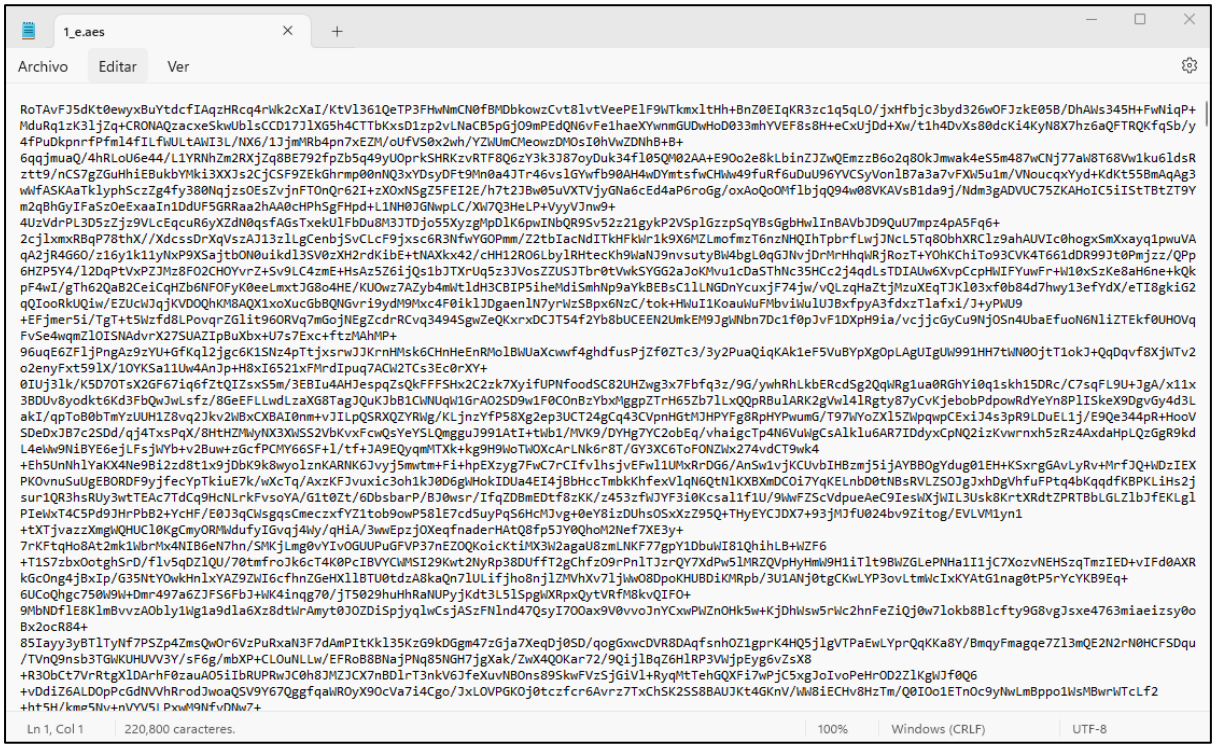
Los usuarios pueden consultar el contenido de este trabajo de grado a través del Repositorio Institucional en el portal Web del repositorio institucional -http://repositorio.uss.edu.pe, así como de las redes de información del país y del exterior.

APELLIDOS Y NOMBRES	NÚMERO DE DOCUMENTO DE IDENTIDAD	FIRMA
MAGALLANES CARBAJAL KENSER	21869345	

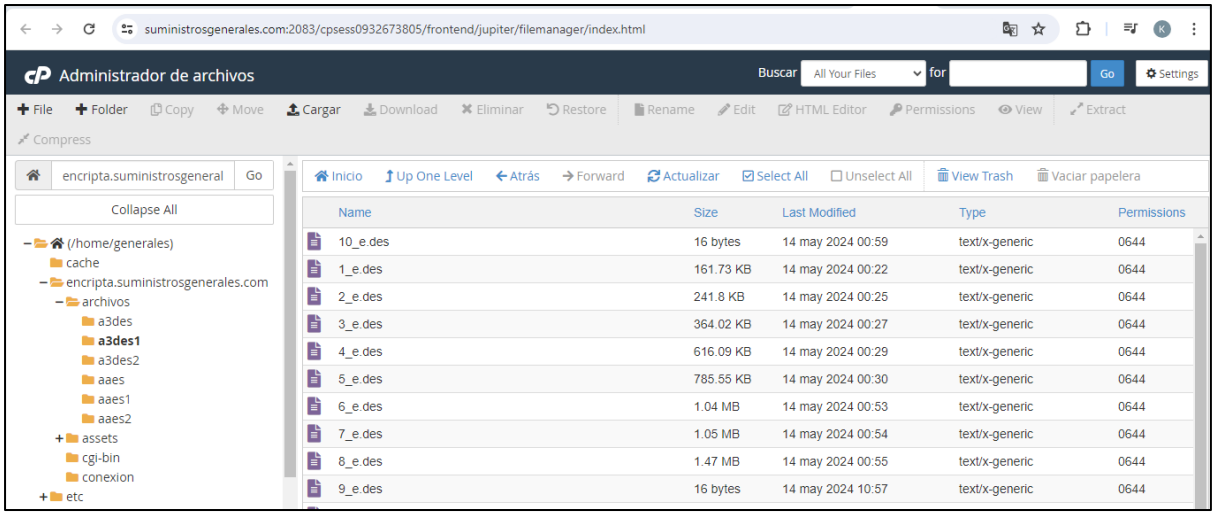
Anexo 8. Evidencias fotográficas Encriptación AES y 3DES

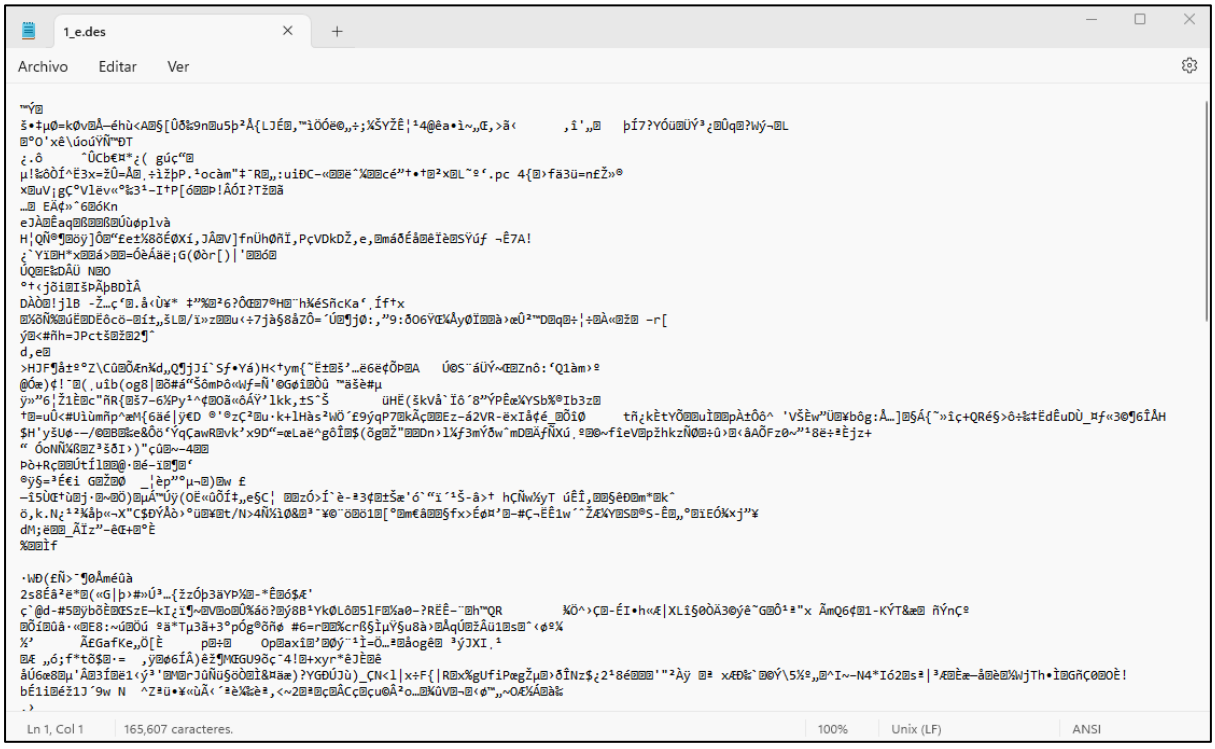
Archivos encriptado en AES





Archivos encriptado en 3DES





REPORTE SOBRE EL CUMPLIMIENTO DEL CODIGO DE BUEN GOBIERNO CORPORATIVO PARA LAS SOCIEDADES PERUANAS (10150)

Denominación:

PROFUTURO AFP

Ejercicio: 2023

Página Web: https://www.profuturo.com.pe/

Denominación o razón social de la empresa revisora: (1)

RPJ AFP004

(1) Solo es aplicable en el caso en que la información contenida en el presente informe haya sido revisada por alguna empresa especializada (por ejemplo: sociedad de auditoría o empresa de consultoría).

Firmado Digitalmente por:
JOSWILB VEGA UGARTE
Fecha: 22/03/2024 06:35:05 p.m.

"Reglamento del Comité de Auditoría Interna"

Código	CG-AU-013	**Macroproceso**	Control de Gestión
Versión	Versión 15	**Proceso**	Auditoría Interna
Propietario	Gerente de Auditoría Interna		
Deroga a	Versión 14		

Niveles de Aprobación	**Elaborador**	**Revisor**	**Aprobador**
	Gerente de Auditoría Interna	Gerente de Legal	Gerente de Auditoria Interna

Historial de Cambios			
Versión	**Fecha de Aprobación**	**Fecha de Vigencia**	**Motivo del Cambio**
13	26.11.2021	26.11.2021	Adecuación a las modificaciones del Título IV contenidas en la Resolución SBS N°01657-2021
14	22.08.2022	22.08.2022	Cambio a formato nuevo Reorganización del documento Cambio en la función de Secretario del Comité Precisión de términos en las funciones
15	26.02.2024	26.02.2024	Actualización sobre las funciones del Comité

ProFuturo AFP

Información trimestral al 31 de Diciembre de 2023

NOTAS A LOS ESTADOS FINANCIEROS

1. Actividad Económica

La administradora de fondos de pensiones Profuturo AFP fue constituida el 17 de mayo de 1993 con el objetivo de administrar un fondo de pensiones y otorgar prestaciones de jubilación, invalidez, sobrevivencia y gastos de sepelio a sus afiliados en los términos y modalidades que establece el Decreto Ley 25897 y las normas reglamentarias, modificatorias y sustitutorias que regulan el Sistema Privado de Pensiones. Su oficina principal está ubicada en Andrés Reyes 489, San Isidro, Lima y cuenta con 7 agencias en las principales ciudades del país, incluida la agencia en la capital.

A partir de diciembre de 2005, se amplió la gestión para administrar tres fondos de pensiones, diferenciados por el nivel de perfil de riesgo de sus respectivas carteras de inversiones y a partir de abril de 2016 la SBS estableció la puesta a disposición de un fondo adicional (Fondo 0).

Con fecha 23 de abril de 2013 PROFUTURO adquirió el 50% de las acciones representativas del capital social de AFP Horizonte S.A por miles S/. 668 458. En dicha operación simultáneamente, AFP Integra S.A. adquirió el otro 50% de las acciones representativas del capital social de AFP Horizonte. Para tal efecto, y en observancia de las autorizaciones conferidas por la Superintendencia de Banca, Seguros y AFP ("SBS"), AFP Horizonte, PROFUTURO y AFP Integra iniciaron un procedimiento ante la SBS por medio del cual, dentro de un plazo de seis meses se aprobaría una operación "Escisión-Fusión".

Mediante Resolución SBS N° 4747-2013 se aprobó la escisión del bloque patrimonial de AFP Horizonte a favor de Profuturo AFP y la fusión del remanente a favor de AFP Integra con la consiguiente extinción de AFP Horizonte. Mediante Resolución SBS N° 5071-2013 se precisó que, la fecha de entrada en vigencia de la escisión - fusión para efectos societarios era el 31/08/2013, mientras que para efectos operativos la fecha de separación, transferencia y fusión de los fondos administrados por la AFP era el 29/08/2013.

Con fecha 20 de mayo del 2014 se inscribió en la Partida Electrónica N° 00478938 del Registro de Personas Jurídicas de Lima de AFP Horizonte S.A la escisión fusión celebrada con Profuturo AFP y AFP Integra.

Capital mínimo

La Superintendencia de Banca, Seguros y AFP mediante la CIRCULAR N° AFP-182-2023 ha dispuesto la actualización anual del capital mínimo de las Administradoras Privadas de Fondos de Pensiones (AFP) para el año 2023, el cual es de S/ 3,484,483; (S/. 3,212,714 para el 2022).


Profuturo
AFP del grupo Scotiabank
Reglamento del Comité
de Buen Gobierno Corporativo
y de Nombramientos y Remuneraciones

Profuturo AFP S.A.

Estados Financieros

31 de diciembre de 2023 y de 2022

(Con el Dictamen de los Auditores Independientes)

Firmado Digitalmente por:
JOSWILB VEGA UGARTE
Fecha: 22/03/2024 06:36:20 p.m.


Profuturo
AFP del grupo Scotiabank
Políticas de
Gobierno Corporativo


Scotiabank®
Código de Conducta
Scotiabank
Efectivo a partir de Noviembre 1, 2020


Profuturo
AFP del grupo Scotiabank
Reglamento
de Directorio

TRIBUNAL CONSTITUCIONAL

EXP. N.° 06482-2006-PA/TC
LIMA
JESÚS GARCÍA GONZA

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

En Lima, a los 11 días del mes de mayo de 2007, la Sala Segunda del Tribunal Constitucional integrada por los señores magistrados Gonzales Ojeda, Vergara Gotelli y Mesía Ramírez, con el fundamento de voto del magistrado Vergara Gotelli, pronuncia la siguiente sentencia

ASUNTO

Recurso de agravio constitucional interpuesto contra la resolución de la Segunda Sala Civil de la Corte Superior de Justicia de Lima, de fojas 59, su fecha 30 de marzo de 2006, que declara improcedente la demanda de autos.

ANTECEDENTES

Con fecha 24 de junio de 2005, la recurrente interpone demanda de amparo contra la Administradora de Fondo de Pensiones – AFP Profuturo. Al respecto, de autos fluye que, en puridad, el objeto de la demanda es que se permita la libre desafiliación de la demandante del Sistema Privado de Pensiones.

El Sexagésimo Segundo Juzgado Especializado en lo Civil de la Corte Superior de Justicia de Lima declara improcedente, *in limine*, la demanda.

La recurrida confirma la apelada.

FUNDAMENTOS

1. En la sentencia recaída en el Expediente N.º 1776-2004-AA/TC, este Colegiado estableció jurisprudencia sobre la posibilidad de retorno parcial de los pensionistas del Sistema Privado de Pensiones al Sistema Nacional de Pensiones. Por otro lado, el Congreso de la República ha expedido la Ley N.º 28991 –Ley de libre desafiliación informada, pensiones mínima y complementarias, y régimen especial de jubilación anticipada– publicada en el diario oficial *El Peruano* el 27 de marzo de 2007.

1. Sobre el mismo asunto, en la sentencia recaída en el Expediente N.º 07281-2006-PA/TC, el Tribunal Constitucional, en sesión de Pleno Jurisdiccional, ha emitido pronunciamiento respecto a las causales de solicitud de desafiliación, incluida, desde luego, la referida a la falta, insuficiente o errónea información, y ha establecido dos precedentes vinculantes, a saber: el primero sobre la insuficiencia de información (*Cfr.*

TRIBUNAL CONSTITUCIONAL

EXP. N.° 3618-2006-PA/TC
LIMA
TEODOMIRA YAURI LEÓN

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

En Lima, a los 11 días del mes de mayo de 2007, la Sala Segunda del Tribunal Constitucional integrada por los señores magistrados Landa Arroyo, Alva Orlandini y Vergara Gotelli, con el fundamento de voto del magistrado Vergara Gotelli, pronuncia la siguiente sentencia

ASUNTO

Recurso de agravio constitucional interpuesto contra la resolución de la Sexta Sala Civil de la Corte Superior de Justicia de Lima, de fojas 30, su fecha 21 de noviembre de 2005, que declara improcedente la demanda de autos.

ANTECEDENTES

Con fecha 31 de enero de 2005, el recurrente interpone demanda de amparo contra la Administradora de Fondo de Pensiones – AFP Profuturo y la Superintendencia de Banca y Seguros y Fondos de Pensiones. Al respecto, de autos fluye que, en puridad, el objeto de la demanda es que se permita la libre desafiliación del demandante del Sistema Privado de Pensiones.

El Décimo Octavo Juzgado Especializado en lo Civil de la Corte Superior de Justicia de Lima declara improcedente la demanda.

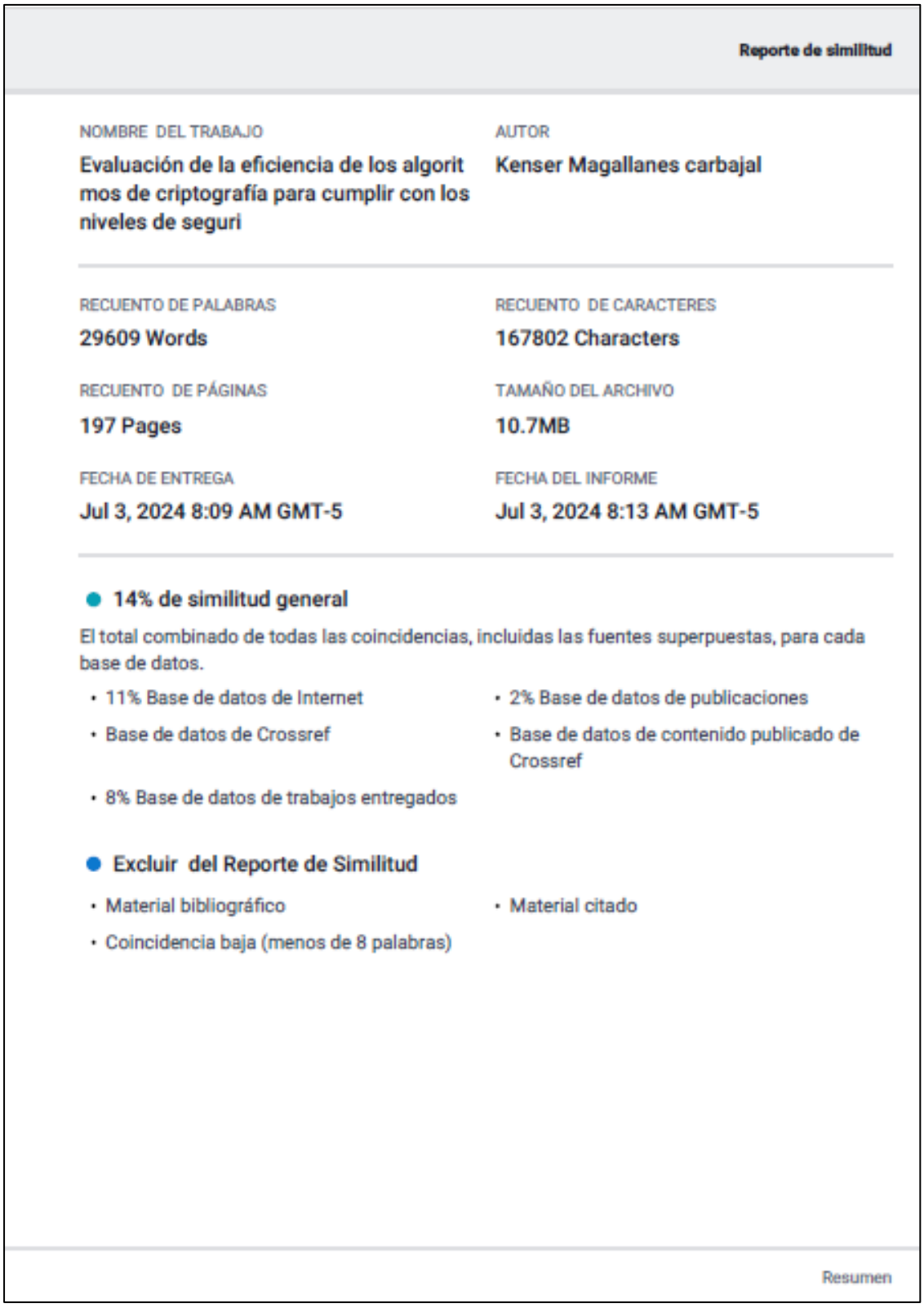
La recurrida confirma la apelada.

FUNDAMENTOS

1. En la sentencia recaída en el Expediente N.º 1776-2004-AA/TC, este Colegiado estableció jurisprudencia sobre la posibilidad de retorno parcial de los pensionistas del Sistema Privado de Pensiones al Sistema Nacional de Pensiones. Por otro lado, el Congreso de la República ha expedido la Ley N.° 28991 –Ley de libre desafiliación informada, pensiones mínima y complementarias, y régimen especial de jubilación anticipada– publicada en el diario oficial *El Peruano* el 27 de marzo de 2007.

2. Sobre el mismo asunto, en la sentencia recaída en el Expediente N.° 07281-2006-PA/TC, el Tribunal Constitucional, en sesión de Pleno Jurisdiccional, ha emitido pronunciamiento respecto a las causales de solicitud de desafiliación, incluida, desde luego, la referida a la falta, insuficiente o errónea información, y ha establecido dos precedentes vinculantes, a saber: el primero sobre la información (*Cfr.* fundamento N.° 27) y el segundo, sobre las pautas a seguir respecto al procedimiento de desafiliación

Anexo 9. Reporte Turnitin



Reporte de similitud

NOMBRE DEL TRABAJO
Evaluación de la eficiencia de los algorit mos de criptografía para cumplir con los niveles de seguri

AUTOR
Kenser Magallanes carbajal

RECUENTO DE PALABRAS
29609 Words

RECUENTO DE CARACTERES
167802 Characters

RECUENTO DE PÁGINAS
197 Pages

TAMAÑO DEL ARCHIVO
10.7MB

FECHA DE ENTREGA
Jul 3, 2024 8:09 AM GMT-5

FECHA DEL INFORME
Jul 3, 2024 8:13 AM GMT-5

● 14% de similitud general

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

- 11% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 8% Base de datos de trabajos entregados

● Excluir del Reporte de Similitud

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

Resumen