UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

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

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE DATOS DEL SISTEMA INFORMÁTICO DEL CUERPO DE BOMBEROS DE LA CIUDAD DE GUARANDA, AÑO 2023.

AUTORA:
MICAELA JASMIN GUAMÁN MANOBANDA

DIRECTOR:
ING. DARWIN CARRIÓN BUENAÑO

GUARANDA – ECUADOR
2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE DATOS DEL SISTEMA INFORMÁTICO DEL CUERPO DE BOMBEROS DE LA CIUDAD DE GUARANDA, AÑO 2023.

AGRADECIMIENTO

Esta presente investigación agradezco a Dios, por darme salud, vida, fuerza y valentía, para seguir adelante día a día.

A mis padres Iván y Norma, quienes me han formado como una verdadera guerrera ante las peores batallas y adversidades que me encontrado en la vida, a mis hermanos, que siempre confiaron en que lo lograría, a mi niño que es mi mayor debilidad, Noe por darme esa fuerza de no de caer y ser mi luz para brillar.

A mi mascota "Buggy" que me dió los ánimos porque sé, que en el lugar en donde estes me cuida a lo largo del camino.

A mis docentes que me guiaron desde muy abajo e impartieron sus conocimientos para hoy ser una profesional más y así poder finalizar esta etapa y comenzar una nueva.

Mi Tutor Ing. Darwin Carrión, por ser mi guía en todo este proceso de titulación, por darme las pautas a seguir y la seguridad de que si se puede y a mis pares académicos Dr. Carlos Taco e Ing. Manuel Galarza, por ser quienes en el transcurso de este camino me supieron dar sus sugerencias que fueron claves para culminar este proyecto.

Micaela J. Guamán

DEDICATORIA

Mi proyecto de investigación la dedico a mis padres, expresando mi gratitud hacia ellos que me han apoyado desde un comienzo. Sin su generosidad y compromiso, este trabajo no habría sido posible.

Además, agradecer a mis hermanos y a mi hijo por sus palabras de apoyo, que han sido una fuente constante de motivación para mí.

Gracias a todos los que han formado parte de este importante logro en mi vida académica y profesional.

Micaela J. Guamán

CERTIFICADO DE VALIDACIÓN

Ing. Darwin Carrión, Dr. Carlos Taco y Lic. Juan Manuel Galarza, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE DATOS DEL SISTEMA INFORMÁTICO DEL CUERPO DE BOMBEROS DE LA CIUDAD DE GUARANDA, AÑO 2023" desarrollado por la señorita Guamán Manobanda Micaela Jasmin.

CERTIFICAN

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

Guaranda, 09 de junio del 2023

Firmado electrónicamente por:
DARWIN PAUL CARRION BUENANO

Ing. Darwin Carrión
Director

Firmado electrónicamente por:
CARLOS ENRIQUE TACO PADILLA

Dr. Carlos Taco
Par Académico

Firmado electrónicamente por:
JUAN MANUEL GALARZA SCHOENFELD

Lic. Juan Manuel Galarza
Par Académico

DERECHOS DE AUTOR

Yo, **Micaela Jasmin Guamán Manobanda** portadora de la cédula de identidad **N° 0250053733** respectivamente**,** en calidad de autora y titular de los derechos morales y patrimoniales del Trabajo de Titulación: **ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE DATOS DEL SISTEMA INFORMÁTICO DEL CUERPO DE BOMBEROS DE LA CIUDAD DE GUARANDA, AÑO 2023,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedo a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

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

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

Firmado electrónicamente por:
MICAELA JASMIN
GUAMAN MANOBANDA

Micaela Jasmin Guamán Manobanda
CI. 0250053733

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. (Marrero Travieso, 2019)

Los algoritmos criptográficos se utilizan en una amplia gama de aplicaciones, desde transacciones financieras y comunicaciones gubernamentales hasta servicios de correo electrónico y mensajería instantánea. Los algoritmos criptográficos también son importantes para proteger la privacidad de los datos personales almacenados en bases de datos y sistemas de información, encargado de desarrollar algoritmos para cifrar mensajes y salvaguardar su contenido. (Ghosh, 2022)

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encriptación se hacen más fáciles de quebrar debido al avance de la velocidad y potencia de los equipos de computación. (Marrero Travieso, 2019)

Es importante entender cómo funcionan los algoritmos criptográficos para poder implementar y utilizar sistemas de seguridad informática efectivos. Los algoritmos criptográficos pueden ser vulnerables a diferentes tipos de ataques, y es necesario evaluar constantemente y actualizar los sistemas de seguridad para garantizar su eficacia y proteger la información crítica.

Por otro lado, el análisis de seguridad se enfoca en evaluar la resistencia de un algoritmo criptográfico ante diferentes tipos de ataques, permitiendo probar la efectividad del algoritmo y su capacidad para resistir diferentes tipos de amenazas.

Existen muchos tipos diferentes de algoritmos criptográficos, desde simples códigos de sustitución hasta complejos sistemas de clave pública. Todos ellos comparten el objetivo de proteger la información de accesos no autorizados y garantizar la integridad de los datos transmitidos. (Rajeev Kumar, 2022)

Otro uso importante de las funciones criptográficas, es asegurar la integridad de los mensajes.

Esta investigación tiene como objetivo presentar un algoritmo criptográfico que proporcione una alta seguridad en la protección de la información, así como un alto rendimiento en el procesamiento de los datos. Para ello, se llevó a cabo un análisis detallado de los algoritmos criptográficos existentes, con el fin de identificar las fortalezas y debilidades de cada uno de ellos.

Una vez evaluados los algoritmos existentes, se propuso el que mejor se adapte al sistema del Cuerpo de Bomberos de Guaranda, un nuevo algoritmo criptográfico que supere las limitaciones de los algoritmos actuales, obteniendo mayor seguridad y eficiencia en la protección de la información.

Se abordará temas como la teoría de la criptografía, los principales algoritmos criptográficos utilizados actualmente, el análisis de algoritmos criptográficos. Así mismo, se realizará un sistema ejemplo para evaluar la efectividad del algoritmo propuesto.

RESUMEN

En la actualidad, la protección de datos es esencial para garantizar la seguridad de la información en los sistemas informáticos. Por esta razón, es importante conocer los principales algoritmos criptográficos que se utilizan para proteger los datos y entender sus debilidades y fortalezas en los diferentes tipos de ataques informáticos.

Entre los algoritmos criptográficos más utilizados se encuentran AES 256, DES, SHA 256, ECC, RSA, Blowfish y DSA.

Se ha destacado que cada algoritmo posee características distintas en términos de sus funciones, seguridad, velocidad y tamaño de clave, dado que los hace más o menos adecuados para diferentes aplicaciones y contextos.

Por lo tanto, en el análisis general, se ha evidenciado que AES 256 es uno de los algoritmos más seguros, siendo ampliamente utilizado en la protección de la privacidad y la seguridad de los datos, mientras que DES es menos seguro pero su velocidad es moderada. ECC y RSA son algoritmos de criptografía de clave pública, Blowfish y DSA son de clave simétrica; SHA 256 que es un estándar de un alto nivel de seguridad.

De acuerdo al análisis planteado se recomendaría la utilización del algoritmo en el sistema del Cuerpo de Bomberos de Guaranda. Determinando que en el desarrollo de la investigación el algoritmo más adecuado es AES 256, definiendo que es más seguro y eficiente en comparación a los demás algoritmos, en el cifrado y descifrado de claves. Al definir algoritmos de criptografía mejora la seguridad de un sistema, evitando que sus datos sean vulnerados.

Palabras claves: Criptografía | seguridad informática | algoritmos criptográficos | AES 256

ABSTRACT

Nowadays, data protection is essential to ensure the security of information in computer systems. For this reason, it is important to know the main cryptographic algorithms used to protect data and to understand their weaknesses and strengths in different types of computer attacks.

Among the most commonly used cryptographic algorithms are AES 256, DES, SHA 256, ECC, RSA, Blowfish and DSA.

It has been pointed out that each algorithm has different characteristics in terms of its functions, security, speed and key size, making them more or less suitable for different applications and contexts.

Therefore, in the overall analysis, it has been evidenced that AES 256 is one of the most secure algorithms, being widely used in privacy protection and data security, while DES is less secure but its speed is moderate. ECC and RSA are public key cryptography algorithms, Blowfish and DSA are symmetric key algorithms; SHA 256 is a standard with a high level of security.

According to the analysis, the use of the algorithm in the Guaranda Fire Department system would be recommended. Determining that in the development of the research the most appropriate algorithm is AES 256, defining that it is more secure and efficient compared to other algorithms, in the encryption and decryption of keys. By defining cryptographic algorithms, it improves the security of a system, preventing its data from being breached.

Keywords: Cryptography | computer security | cryptographic algorithms | AES 256.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1 Descripción del Problema

Los problemas de seguridad de la información aparecen con más énfasis con los nuevos desarrollos tecnológicos, la era de la tecnología de información, las comunicaciones digitales aumentan, por lo tanto, surgen nuevas amenazas que tratan de vulnerar a estos medios de comunicación y datos almacenados en medios informáticos y en ordenadores. (Acero, 2019)

Siempre hay fallas en el diseño, la estructura o el código de los sistemas informáticos y las aplicaciones que generan vulnerabilidades. No importa cuán pequeño sea un error, siempre representa una amenaza para los sistemas y la información; actúa como puerta de entrada a ataques externos o internos. (Nelson, 2016)

El sistema implementado en la institución del Cuerpo de Bomberos tiene por objetivo gestionar cuatro departamentos, Operación, talento humano, gestión de transporte y financiero, procura mantener un sistema centralizado dentro de la institución, facilitando a la administración del personal, uno de los problemas más comunes en los sistemas muestra la falta de seguridad donde; tienden a ser débiles, surge la pérdida de información y causa grandes problemas internos. Otro problema es la falta de seguridad, causa que el sistema no este actualizado, existiendo diferentes ataques, que dañan la información.
La ciberseguridad tiende **automatizar procesos críticos** para minimizar o eliminar el factor de riesgo; en **malas prácticas o la falta conocimiento.**

Así como, grandes instituciones ya sean públicas o privadas, están expuestas a las amenazas como malware, phishing, entre otros, que vulneran los medios de comunicación y datos almacenados en servidores o repositorios; recurriendo al uso de sistemas criptográficos, los cuales cuentan con algoritmos complejos a fin de proporcionar seguridad a la información. (Zanabria, 2018).

1.2 Formulación del Problema

Realizar un análisis de algoritmos criptográficos para la protección de datos del sistema informático del Cuerpo de Bomberos de la ciudad de Guaranda, año 2023.

1.3 Preguntas de Investigación

- ¿Cómo se clasifican los principales algoritmos criptográficos para la protección de datos?
- ¿Cuáles son las debilidades y fortalezas de los algoritmos frente a los diferentes tipos de ataques informáticos?
- ¿Qué elementos caracterizan a la aplicación de los algoritmos en el sistema informático del Cuerpo de Bomberos de Guaranda (CBG)?
- ¿Cómo aplicar los algoritmos criptográficos en un sistema informático con el método de prevención para la transmisión de datos?

1.4 Justificación

La criptografía surge de la necesidad de hacer privada la transmisión de datos, este método utilizado para cifrar y descifrar los mensajes; de esta forma, sólo el texto plano es visible para el emisor y receptor de dicho mensaje. Es completamente ilegible para cualquiera que lo intercepte en tránsito, lo que a su vez es lo suficientemente seguro frente a posibles ataques que comprometan la información que se transmite.

El estudio criptográfico permite al usuario conocer que herramientas usar como medidas o protocolos de seguridad de sus datos, existen varias amenazas hacia la seguridad de la información. Una de las propuestas más comunes en la actualidad es para personas u organizaciones, que están optando por el uso de algoritmos criptográficos propios o personalizados, para garantizar la seguridad y protección en sus computadores, servidores o bases de datos. (Acero, 2019)

Es difícil determinar la calidad de un algoritmo de cifrado. Los algoritmos que parecen prometedores a veces resultan ser fáciles de romper, dado el ataque adecuado. Al seleccionar un algoritmo de cifrado, es una buena idea elegir una que

esté en uso durante varios años y que ha resistido correctamente a varios ataques. (Alvin Ashcraft, 2022)

Hacer un repaso de los diferentes tipos de problemas, que, según los expertos, potencialmente será combatir desde el punto de vista por la seguridad informática, con la finalidad de considerar aspectos físicos, lógicos de forma que se mitiguen riesgos existentes. (Alfaro Gómez, 2020)

Que hacen referencia a la privacidad, confidencialidad, integración y autenticación, analizando que algoritmos criptográficos, ayudan a la protección de datos, como claves secretas y claves públicas.

La necesidad de conocimiento e interés de las entidades públicas y privadas, se inclinan por adaptarse a la nueva era tecnológica, con el fin de, evitar violaciones de seguridad en su sistema, alteración de datos y accesos no autorizados, etc.
El propósito es, analizar que algoritmo criptográfico es el más seguro y confiable en términos de la seguridad de la información. Con el algoritmo criptográfico seleccionado, se busca cifrar y descifrar contraseñas, garantizando la protección y la integridad de los datos.
El presente proyecto está bajo la línea de investigación "Ingeniería de Software, Redes y Telecomunicaciones", dentro de la sub-linea de "Seguridades de Aplicaciones".

1.5 Objetivos

Objetivos General:

Analizar algoritmos criptográficos para la protección de datos del sistema informático del Cuerpo de Bomberos de la ciudad de Guaranda, año 2023.

Objetivos Específicos:

- Identificar los principales algoritmos criptográficos para la protección de datos.
- Analizar las debilidades y las fortalezas de los algoritmos frente a los diferentes tipos de ataques informáticos.
- Evaluar las características que diferencian la aplicación de los algoritmos en el sistema informático del Cuerpo de Bomberos de la ciudad de Guaranda (CBG).

- Definir algoritmos de criptografía para el sistema informático como método de prevención para la transmisión de datos.

1.6 Idea a Defender

El uso de algoritmos criptográficos brinda una mejor protección de datos para el sistema informático del Cuerpo de Bomberos de la ciudad de Guaranda, año 2023.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes

Para el desarrollo de la presente propuesta investigativa se ha considerado los siguientes argumentos de investigación que se utilizarán como sustento del proyecto.

Tema: Algoritmo para transmisión de información segura en dispositivos NFC.
Autores: Héctor Caballero Hernández, Vianney Muñoz Jiménez y Marco A. Ramos Corchado.
Hernández, Muñoz y Ramos (2018) afirman que:

"Existen varios estándares para mejorar la transmisión de datos ya sea a corta o larga distancia. Indicando que este artículo científico es de gran importancia, por optar mecanismos de seguridad, teniendo mayor protección y resguardo de la información, manifestando que se ha implementado un nuevo algoritmo seguro para la transmisión de información como es el NFC, permitiendo la comunicación de dispositivos electrónicos, mejorando las actividades humanas en diferentes ámbitos".

Tema: Determinación de los factores que afectan el diseño de algoritmos criptográficos por medio de un meta-modelo cibernético, validado con análisis-Q

Autores: Ali Norouzzadeh GilMolk, Reza Ramazani Khorshiddoust y Mohammad Aref

GilMolk, Ramazani y Aref (2020) manifiestan que:

"Otro punto a destacar es el cifrado informático, considerando que es un medio de protección de datos los cuales pueden ser alterados e incluso hacerlo indescifrable, tomando en cuenta que existen algoritmos criptográficos donde se delimita que tan confiables y vulnerables son, considerando que los mensajes pueden ser cifrados gracias al uso de algoritmos como el AES, DES, los más utilizados para este tipo de seguridad criptográfica, así determinando el desarrollo del resultado, basándose

en una metodología del enfoque cibernético en modelos de algoritmos criptográficos donde reconoce y controla las funcionalidades simétricas y asimétricas del sistema".

Tema: Comparación del rendimiento y nivel de seguridad en los algoritmos criptográficos ligeros Present, Clefia, Keccak y Hight: una revisión sistemática.

Autores: César Alvarito Coronel González y Lohana Mariella Lema Moreta

Coronel y Lema (2018) mencionan:

"Actualmente, vivimos en una era en donde toda información generada por todo el mundo en su gran parte es digitalizada, como a la red colectiva de dispositivos como lo es el internet de las cosas ha estado en un constante desarrollo y con un gran crecimiento hoy en día, con el propósito de medir el nivel de seguridad y su rendimiento en los algoritmos criptográficos, dando a conocer cuáles serán sus riesgos y ataques frente a estos mecanismos, preservando la confidencialidad de la información utilizando técnicas y algoritmos de encriptación, debido a que se ha generado la necesidad de cifrado de resiliencia debido a los ataques existentes, teniendo en cuenta los parámetros de confidencialidad, autenticidad, integridad y disponibilidad".

2.2 Científico

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

La norma ISO 27000 ayuda a las organizaciones a establecer y mantener prácticas efectivas de seguridad de la información para proteger sus activos críticos y reducir los riesgos de seguridad. (Blandonnet, 2018)

ISO/IEC 27001: Es una norma muy conocida a nivel mundial para los sistemas de gestión de seguridad de la información (SGSI) y sus requisitos. Además, existen otras normas dentro de la familia ISO/IEC 27000 que proporcionan buenas prácticas en protección de datos y resiliencia cibernética. (Mahmoud, 2022)
En conjunto, estas normas permiten a organizaciones de todos los sectores y tamaños manejar la seguridad de sus activos, como información financiera, propiedad intelectual, datos de empleados e información confiada por terceros.

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

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

Estándar PKCS

Estos son estándares de criptografía de clave pública proporcionados por RSA1 Laboratories y tienen como objetivo promover el uso de tecnología de clave pública. Además, tienden a tener propósitos para agilizar el manejo de la criptografía de cifrar la clave pública. PKCS también puntualiza sintaxis de algoritmos separados para firmas digitales, sobres digitales y certificados extendidos. (Aida Ormaza, 2017)

Niveles Características (PKCS)

PKCS 1.- Concreta como un mecanismo para el cifrado y la firma de datos utilizando el criptosistema de clave pública RSA.
PKCS 3.- Puntualiza un registro de acuerdo de claves Diffie-Hellman.
PKCS 5.- Describe cómo cifrar una cadena con una clave privada derivada de una contraseña.
PKCS 6.- Se restringe en la versión 3 de X.509.

PKCS 7.- Determina de alguna manera general para los mensajes que contienen extensiones criptográficas, como firmas digitales y cifrado.

PKCS 8.- Describe el formato de la información de la clave privada y el algoritmo de clave pública, manejando como un par de atributos.

PKCS 9.- Especifica los tipos de atributos seleccionados para su uso con otros estándares PKCS.

PKCS 10.- Determina una actividad en la sintaxis de una solicitud de certificado

PKCS 11.- Define una interfaz gráfica de programación en la tecnología conocida como Cryptoki, que suele estar en ciertos instrumentos criptográficos como tarjetas PCMCIA.

PKCS 12.- Especifica un estándar digital que puede almacenar claves privadas de usuario, certificados, etc.

PKCS 13.- Tiende a definir los mecanismos tanto para el cifrado de datos y firma criptografía de curva elíptica.

PKCS 14.- Su desarrollo actualmente genera los números pseudoaleatorios.

PKCS 15.- Tiene un poco de relación con el estándar 11, por lo que se utiliza en el formato de generar credenciales que son almacenadas como tokens. (Aida Ormaza, 2017)

2.3 Conceptual

Algoritmo

Los algoritmos se utilizan en muchos campos de la informática, como la programación, la inteligencia artificial, la criptografía, la teoría de la computación, la optimización de procesos, entre otros. Son fundamentales para la creación de programas y aplicaciones de software, que permiten a los desarrolladores diseñar soluciones eficientes y escalables para problemas complejos**.**

Según Vivar (2018), un algoritmo bien diseñado es aquel que es fácil de entender, implementar y mantener. Además, debe ser eficiente en términos de tiempo y espacio, lo que significa que debe ser capaz de manejar grandes volúmenes de datos y producir resultados precisos en un tiempo razonable.

AES (Advanced Encryption Standard)

Es un estándar de cifrado de acceso público basado en sustituciones, permutaciones y transformaciones lineales, cada una realizada en bloques de 16 bytes; estas acciones se repiten muchas veces, se llaman rondas. En cada ronda, se calcula una clave de ronda única a partir de la clave de cifrado y se incluye en el cálculo. (Domingues, 2017)

AES 256

La clave de cifrado de 256 bits que utiliza AES 256 es muy difícil de descifrar, incluso para los atacantes más sofisticados. Por esta razón, el algoritmo se utiliza ampliamente en todo el mundo para proteger datos confidenciales, como información gubernamental, datos de la industria militar, información financiera y datos personales. (Berhanu Aebissa, 2023)

Aplicaciones más comunes de AES 256:

Seguridad de la información. AES 256 se utiliza para cifrar datos sensibles en muchas aplicaciones, incluyendo el cifrado de archivos, el cifrado de bases de datos y el cifrado de transacciones en línea.

Comunicaciones seguras. AES 256 se utiliza para cifrar comunicaciones sensibles, como el correo electrónico, la mensajería instantánea y las comunicaciones de voz y video.

Protección de la privacidad. AES 256 se utiliza para proteger la privacidad de los datos personales en muchas aplicaciones, incluyendo el cifrado de información de identificación personal (PII), como nombres, direcciones y números de seguridad social.

Seguridad del comercio electrónico. AES 256 se utiliza para cifrar transacciones en línea y proteger la información financiera del usuario, como números de tarjeta de crédito y detalles de transacciones.

Seguridad en la nube. AES 256 se utiliza para cifrar datos en la nube y protegerlos contra ataques cibernéticos.

Seguridad en dispositivos móviles. AES 256 se utiliza para cifrar datos en dispositivos móviles, como teléfonos inteligentes y tabletas, para proteger la privacidad de los usuarios y los datos personales almacenados en estos dispositivos. (Sánchez, 2022)

Amenazas a la seguridad de la información.

Una amenaza a la seguridad de las TIC puede definirse como "cualquier circunstancia o evento capaz de explotar, intencionalmente o no, una vulnerabilidad específica en un sistema de TIC, lo que resulta en una pérdida de confidencialidad, integridad y disponibilidad de la información manipulada. (Domingues, 2017)

- *Amenazas lógicas.* Hay todo tipo de programas que pueden dañar nuestro sistema de una forma u otra y se crean intencionalmente como malware; llamado malware o simplemente errores, que pueden ser errores o agujeros.
- *Software malicioso.* las amenazas al sistema más comunes son causadas por errores inadvertidos por parte de los desarrolladores del sistema o de la aplicación.
- *Herramientas de seguridad.* Todas las herramientas de seguridad son un arma de doble filo: así como un administrador las usa para identificar y reparar sus sistemas o una subred completa, un futuro intruso puede usarlas para descubrir y explotar las mismas fallas. equipos ofensivos.

- *Puertas traseras.* durante el desarrollo de grandes aplicaciones o sistemas operativos, es común que los desarrolladores agreguen "atajos".
- *Virus.* Es una secuencia de código que se agrega a un archivo ejecutable para que cuando se ejecute el archivo, el virus haga lo mismo y se inserte en otros programas.
- *Gusanos.* Este es un programa que puede iniciarse y propagarse a través de las redes, a veces transportando virus o explotando errores en los sistemas conectados para dañarlos.
- *Caballos de Troya.* Son instrucciones ocultas en un programa que parecen realizar tareas que el usuario espera que realice. pero en realidad realiza funciones ocultas sin el conocimiento del usuario.
- *Usuarios.* En su mayoría, las miradas indiscretas y los crackers realizan ataques pasivos que se pueden cambiar a activos; mientras que terroristas y exempleados llevan a cabo ataques puramente activos. (Chávez, 2016)

Aspectos de seguridad que compromete un ataque

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

- *Confidencialidad:* La información llegue solamente a las personas autorizadas, por lo cual al no ser confidencial puede haber filtraciones de cierta información, como también de accesos no autorizados.
- *Integridad:* La información al ser manipulada está violando la seguridad, afectando a las empresas u organizaciones. Lo que se debe garantizar que los datos e información deben estar seguros para no sufrir pérdidas o alteraciones.
- *Disponibilidad:* Garantiza el paso a quienes cuenten con las credenciales requeridas para tener acceso a los servicios para ser usados cuando sea necesario. La falta de disponibilidad afecta a los servicios, interrumpiendo en la productividad de las empresas. (Lisboa Díaz, 2020)

Ataque informático

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

Para minimizar el impacto negativo de un ataque, existen procedimientos y mejores prácticas que pueden facilitar la lucha contra la actividad delictiva y reducir significativamente el alcance de un ataque.

Comprender las diferentes etapas que componen un ataque cibernético le brinda la ventaja de aprender a pensar como un atacante y nunca subestimar su propio estado de ánimo. (Chávez, 2016)

- *Reconocimiento.* Esta etapa recopila información sobre las posibles víctimas, que pueden ser personas u organizaciones. Por lo general, en esta etapa, los datos objetivo se recopilan a través de varias fuentes de Internet como Google, etc.
- *Investigación.* En la segunda fase, la información obtenida en la primera fase se utiliza para sondear el objetivo e intentar obtener información sobre el sistema de la víctima, como dirección IP, nombre de host, datos de autenticación, etc.
- *Obtener acceso.* Algunos de los métodos que un atacante puede usar son ataques de desbordamiento de búfer, denegación de servicio (DoS), denegación de servicio distribuida (DDos), filtrado de contraseñas y secuestro de sesión.
- *Generar acceso.* El ataque comienza explotando las vulnerabilidades y los errores del sistema descubiertos durante la fase de reconocimiento e investigación. Algunos de los métodos que un atacante puede usar son ataques de desbordamiento de búfer, denegación de servicio (DoS), denegación de servicio distribuida (DDos), filtrado de contraseñas y secuestro de sesión.

- *Mantener el acceso.* Una vez que los atacantes obtienen acceso al sistema, intentarán implementar herramientas que les permitan acceder nuevamente en el futuro, independientemente de dónde puedan acceder a Internet.
- *Eliminar los registros.* Una vez que un atacante logra obtener y mantener el acceso a un sistema, intentará eliminar todo rastro de la intrusión para evitar que lo detecten los profesionales de seguridad o los administradores de red. (Félix, 2018)

Autenticación de usuario

El usuario se identifica mediante su ID, que es conocido tanto por el administrador del sistema como por el resto de usuarios, y con la que puede crear su propia contraseña secreta.

- El usuario solicita acceso al recurso.
- El sistema solicita al usuario su método de autenticación.
- El usuario proporciona su información de autenticación.
- El sistema verifica las credenciales del usuario.
- El sistema bloquea o permite el acceso del usuario al recurso.

Autenticación en lo que el usuario posee.

Estos métodos se basan en que el usuario tenga un token, que podemos dividir en tokens de memoria y tokens inteligentes.

Las tarjetas inteligentes amplían su funcionalidad al conectar uno o más circuitos integrados. Una de sus ventajas es que requieren una contraseña para habilitarlo y, por lo tanto, una identificación falsa para autenticarse.

Supone una cierta desventaja en cuanto a su coste o implementación para los usuarios que en cierto modo optan por sistemas más sencillos y menos complejos cuando pueden utilizarlo. (Félix, 2018)

Autenticación en lo que el usuario sabe

Los sistemas de autenticación más utilizados son los sistemas de identificación basados en información que utilizan, por ejemplo, un nombre de usuario y una

contraseña; la ventaja de estos sistemas es que también conocen rápidamente a los usuarios; son muy fáciles y económicos de implementar, y en un entorno adecuadamente administrado y controlado, pueden proporcionar un alto nivel de seguridad.

Criptografía

El uso de la criptografía en la vida cotidiana presta un servicio seguro y se encarga de proteger al usuario frente a los ataques existentes, ya sea en la utilización de servicios online o navegación en la web.

La criptografía nos asegura y garantiza la confidencialidad y la integridad de los datos, teniendo en cuenta los conceptos que derivan los sistemas modernos en criptografía, en poder entender su funcionamiento de distintos sistemas de cifrado. Es el campo de la seguridad de la información que hoy en día está experimentando una mayor explosión, debido a que permite la transmisión eficiente y eficaz de la información, basado en tres principios como son; confiabilidad, autenticación e integridad de datos. (Hans Delfs, 2019)

Tipos de criptografía

- Cifrado simétrico: Clave secreta, clave única para cifrar y para descifrar utilizada para privacidad y confidencialidad.

- Cifrado asimétricos: Clave pública claves distintas para el cifrado y el descifrado usado para autenticación e intercambio de claves.
- Función Hash: utiliza una transformación matemática, como cifrado de información irreversible; genera una huella digital, utilizada para la integridad de los mensajes. (Regina Paiva Melo MARIN, 2021)

Ciberseguridad informática

La ciberseguridad es un término ampliamente utilizado que se refiere a la seguridad de los sistemas de información y datos. Se define como la protección de los activos de información contra amenazas que amenazan la información procesada, desarrollada y transmitida por los sistemas de información interconectados.

Debilidades de seguridad comúnmente explotadas

Códigos maliciosos

Los atacantes suelen utilizar troyanos junto con otros tipos de código malicioso, para que de forma remota la mayor parte del tiempo puedan intervenir y filtrar la información evitando que los administradores de red se den cuenta de sus acciones.

Contraseñas

La protección de la información se determina en tener claves seguras, utilizando métodos y sistemas de autenticación, aumentando los niveles de seguridad para que los atacantes o intrusos se limiten a cifrar sus contraseñas

Una contraseña de más de diez caracteres que la gente recuerde es mucho más efectiva que una contraseña de cuatro dígitos, pero los atacantes a menudo aprovechan otros problemas. (Rea, 2020)

Usar la misma contraseña para varias cuentas y otros servicios causan:

- El acceso a información donde se requiere de autenticidad en lugares públicos, los intrusos colocan con anterioridad software o dispositivos para verificar los datos sin mucho esfuerzo.
- Uso de protocolos de comunicación inseguros que transmiten información en texto claro, como correo electrónico, navegación web, chat, etc.
- Tecnologías como la vigilancia para evitar los controles de seguridad.

Configuraciones predeterminadas

En los sistemas operativos, aplicaciones y dispositivos implementados en el entorno informático, son otra debilidad a la que se suele prestar poca atención, porque se cree erróneamente que son factores triviales que no están en la lista del atacante.

Factor Insiders

Desde esta perspectiva, se deben utilizar estrategias de defensa internas y específicas para gestionar posibles ataques contra el personal de la organización. Estas estrategias de defensa actúan como contramedidas en defensa de los ataques que se presenten. (Rea, 2020)

Inteligencia de código abierto

Uno de los primeros aspectos de un ataque informático es recopilar información utilizando diversas técnicas como reconocimiento, descubrimiento, rastreo o pirateo de Google; y más específicamente inteligencia de código abierto. (Rea, 2020)

Los ejemplos específicos del tipo y la sensibilidad de la información que un atacante puede obtener:

- Sistemas operativos utilizados por la organización, principales programas utilizados, lenguajes de programación, plataformas especiales, fabricantes de equipos de red, estructura de archivos, nombres de archivos, plataforma del servidor web y más.
- Debilidades físicas, estación base, señales activas, terminal, imágenes satelitales.
- Documentos confidenciales enviados accidental o intencionalmente a cuentas personales de personas que actualmente no tienen conexión con la organización más que pasar por ella.
- Vulnerabilidades de productos usados, problemas personales, comunicados internos, anuncios, políticas institucionales. (Rea, 2020)

PBKDF2

Es una función iterativa que utiliza una sal aleatoria y un número configurable de iteraciones para aumentar la complejidad del hash.

La sal es un valor aleatorio único que se agrega a la entrada de la contraseña antes de aplicar la función hash, lo que hace que la salida sea única incluso si la entrada es la misma.

Las iteraciones se utilizan para ralentizar la función hash y hacerla más resistente a los ataques de fuerza bruta.

Se utiliza comúnmente en aplicaciones criptográficas para generar claves de cifrado a partir de contraseñas de usuario. Debido a que las contraseñas suelen ser

relativamente débiles y fáciles de adivinar, la derivación de claves basada en contraseña es una técnica importante para garantizar que los datos estén seguros.

Salt

En criptografía, una "salt" es un valor aleatorio único que se utiliza junto con una clave o contraseña como entrada para una función de hashing o derivación de clave. La sal se agrega a la entrada de la clave antes de aplicar la función de hashing, lo que hace que la salida del hash sea única incluso si la entrada es la misma. Esto aumenta la seguridad del hash y hace que sea más difícil de crackear mediante ataques de diccionario o fuerza bruta.

Secret Key

La clave es "secreta" porque solo las partes autorizadas conocen la clave, y es "simétrica" porque la misma clave se utiliza para cifrar y descifrar los datos.

Análisis de los algoritmos criptográficos simétricos y asimétricos

Algoritmos criptográficos

Está diseñado para cifrar y descifrar información de forma segura y protegerla de posibles ataques malintencionados, que se utilizan para garantizar la privacidad, la integridad y la autenticidad de la información en diferentes aplicaciones. (Tamara Luiza Dall Agnol Pinto, 2020)

Existen varios tipos de algoritmos criptográficos, los cuales se pueden clasificar en dos categorías principales:

Algoritmos de cifrado simétrico

También conocidos como algoritmos de clave secreta, donde se utiliza la misma clave para cifrar y descifrar, ambas partes deben conocer la clave para poder realizar la comunicación segura. Algunos ejemplos de algoritmos de cifrado simétrico son *AES, DES y Blowfish.*

Algoritmos de cifrado asimétrico

Es un método de cifrado, que utilizan un par de claves diferentes (clave pública y clave privada) para cifrar y descifrar los datos. La clave pública se comparte, mientras que la clave privada se mantiene en secreto.

Además, existen otros tipos de algoritmos criptográficos que se utilizan en diferentes aplicaciones y escenarios, tales como:

Funciones hash: Son algoritmos que transforman cualquier cantidad de datos en una cadena de caracteres fija de longitud fija, conocida como el valor hash. Ejemplos de funciones hash son *SHA-256 y MD5*.

Firmas digitales: Son utilizadas para garantizar la autenticidad e integridad de los datos. Utilizan un par de claves, para crear una firma digital que puede ser verificada por cualquier persona con la clave pública correspondiente. Ejemplos de algoritmos de firma digital son *RSA y DSA*.

Cada tipo de algoritmo criptográfico tiene sus propias ventajas y desventajas, y su elección depende de la aplicación específica y de los requisitos de seguridad. (David Gerault, Computing AES related-key differential characteristics with constraint programming, 2020)

Algoritmo de cifrado AES-256 (Advanced Encryption Standard)

Es un estándar de cifrado simétrico utilizado para proteger la privacidad y la seguridad de los datos en diversas aplicaciones. Es un algoritmo de bloque que cifra bloques de datos de 128 bits y utiliza una clave de 256 bits para el cifrado y descifrado de datos. (Liandeng Li, 2020)

AES-256 toma una clave de cifrado de 256 bits y la utiliza para cifrar bloques de datos de 128 bits a través de una serie de transformaciones matemáticas. El resultado es un bloque de datos cifrado que es prácticamente imposible de descifrar sin la clave de cifrado adecuada.

Las principales características del algoritmo de cifrado AES-256 son las siguientes:

Seguridad: AES-256 es un algoritmo de cifrado simétrico altamente seguro que proporciona una protección sólida contra posibles ataques de fuerza bruta y otros ataques criptográficos.

Eficiencia: Es un algoritmo rápido y eficiente que puede cifrar grandes cantidades de datos en poco tiempo, lo que lo hace adecuado para aplicaciones en tiempo real.

Versatilidad: AES-256 es adecuado para una amplia gama de aplicaciones de seguridad de datos, incluyendo el cifrado de datos confidenciales, la protección de la privacidad y la seguridad de las comunicaciones.

Amplia adopción: Es ampliamente utilizado en todo el mundo y es uno de los estándares de cifrado más aceptados en la actualidad.
Flexibilidad: Admite una variedad de modos de operación, lo que lo hace adecuado para diferentes requisitos de seguridad y aplicaciones. (Carlos Gomez, 2021)

Ventajas:

- *Seguridad*. Ofrece una protección sólida contra posibles ataques de fuerza bruta y otros ataques criptográficos.
- *Eficiencia. E*s un algoritmo rápido y eficiente que puede cifrar grandes cantidades de datos en poco tiempo, lo que lo hace adecuado para aplicaciones en tiempo real.
- *Amplia adopción.* Es ampliamente utilizado y es uno de los estándares de cifrado más aceptados en todo el mundo.

Desventajas:

- *Complejidad. E*s un algoritmo complejo que requiere una implementación adecuada y cuidadosa para garantizar su seguridad. Si no se implementa correctamente, pueden surgir vulnerabilidades.
- *Recursos.* La encriptación y descifrado con AES-256 requiere recursos computacionales significativos, especialmente para grandes cantidades de datos. Por lo tanto, puede ser menos adecuado para dispositivos con recursos limitados.
- *Limitaciones.* A pesar de su alta seguridad, no puede proteger contra todas las posibles formas de ataques, como los ataques de ingeniería social o los ataques que explotan vulnerabilidades en el software o en los sistemas operativos. (Carlos Gomez, 2021)

Algoritmo DES (Data Encryption Standard)

Es un algoritmo de cifrado simétrico que se utiliza para proteger la privacidad y la seguridad de los datos. DES fue desarrollado en los años 70 por IBM en colaboración con la Agencia de Seguridad Nacional de los Estados Unidos (NSA), y es uno de los primeros estándares de cifrado ampliamente adoptados en todo el mundo.

El algoritmo DES utiliza una clave de cifrado de 56 bits para cifrar bloques de datos de 64 bits. Funciona mediante la realización de una serie de transformaciones matemáticas en los datos de entrada utilizando la clave de cifrado, y la generación de un bloque de datos cifrado de 64 bits como resultado. (Rocha, 2020)

Aunque DES ha sido uno de los estándares de cifrado más utilizados en el pasado, ha sido reemplazado en gran medida por algoritmos de cifrado más seguros, como AES (Advanced Encryption Standard). Sin embargo, DES sigue siendo un algoritmo importante en la historia de la criptografía y en la comprensión de los principios básicos de la criptografía simétrica.

La función principal del algoritmo DES

Es proteger la privacidad y la seguridad de los datos mediante el cifrado de información sensible. Específicamente, DES toma una clave de cifrado de 56 bits y la utiliza para cifrar bloques de datos de 64 bits a través de una serie de transformaciones matemáticas.

Características importantes del algoritmo DES (Data Encryption Standard):

- Es un algoritmo de cifrado simétrico, lo que significa que utiliza la misma clave para cifrar y descifrar los datos.
- Utiliza una clave de cifrado de 56 bits, lo que significa que hay 2^56 posibles claves.
- El algoritmo cifra los datos en bloques de 64 bits, lo que significa que cualquier bloque de datos mayor de 64 bits debe dividirse en bloques más pequeños y cifrarse por separado.
- El algoritmo DES es eficiente en términos de recursos, lo que lo hace adecuado para su uso en sistemas con recursos limitados.
- DES fue utilizado en una amplia variedad de aplicaciones, desde la protección de comunicaciones militares hasta la seguridad de transacciones financieras.

Ventajas:

- Es un algoritmo bien conocido y utilizado en una variedad de aplicaciones de cifrado, por lo que hay muchas herramientas, bibliotecas y recursos disponibles para implementarlo y usarlo.

- Es rápido y eficiente en términos de recursos, lo que lo hace adecuado para su uso en sistemas con recursos limitados.
- Tiene una buena seguridad en su tiempo, DES fue considerado un algoritmo de cifrado seguro en su época.

Desventajas:

- La longitud de la clave de 56 bits es relativamente corta en comparación con los estándares actuales, lo que hace que el algoritmo sea más vulnerable a ataques y criptoanálisis.
- El tamaño del bloque de datos de 64 bits limita su uso en aplicaciones que requieren cifrado de bloques de datos más grandes.
- Dado que DES es un algoritmo antiguo y se han encontrado varias vulnerabilidades y debilidades en su diseño a lo largo del tiempo, lo que lo hace menos seguro en comparación con los algoritmos de cifrado más avanzados y modernos.

Algoritmo de criptografía de curva elíptica (ECC)

Es un método de cifrado que utiliza la teoría de curvas elípticas para proteger la información. Se basa en la complejidad computacional de encontrar puntos en una curva elíptica, lo que la convierte en una alternativa más eficiente y segura que otros métodos de cifrado.

Esta propiedad se utiliza para generar claves de cifrado que son difíciles de descifrar sin la clave de descifrado correspondiente.

Se utiliza en una amplia variedad de aplicaciones, como la seguridad de la comunicación inalámbrica, la protección de datos de tarjetas inteligentes y la autenticación de dispositivos móviles. (Maldonado, 2020)

La función principal del algoritmo de criptografía de curva elíptica

Es proteger la información mediante el cifrado de los datos. Esto se logra mediante la generación de claves de cifrado que son difíciles de descifrar sin la clave correspondiente.

Algunas características del algoritmo de criptografía de curva elíptica (ECC) son:

- *Eficiencia.* Es más eficiente que otros algoritmos criptográficos, ya que utiliza claves más pequeñas y requiere menos tiempo y recursos de computación para cifrar y descifrar los datos.
- *Menor consumo de energía.* Utiliza menos energía y recursos de procesamiento, lo que lo hace ideal para dispositivos móviles y otros sistemas con limitaciones de energía.
- *Flexibilidad.* Es altamente flexible y puede ser adaptado a diferentes plataformas y entornos de aplicación.

Menor tamaño de claves. Las claves de cifrado son más pequeñas que en otros algoritmos criptográficos, lo que significa que son más fáciles de transmitir y almacenar. (Maldonado, 2020)

Ventajas del algoritmo de criptografía de curva elíptica (ECC) son:

Alta seguridad. Proporciona una mayor seguridad que otros algoritmos criptográficos.

Tamaño de clave más pequeño. Utiliza claves más pequeñas, lo que las hace más fáciles de almacenar y transmitir.

Resistencia a ataques cuánticos. Tener una buena opción para aplicaciones que requieren una seguridad a largo plazo.

D***esventajas del algoritmo ECC son:***

- *Complejidad.* La implementación de ECC puede ser compleja y requiere conocimientos especializados.
- *Patentes.* Algunos aspectos están protegidos por patentes, lo que puede limitar su adopción en algunas aplicaciones.
- *Interoperabilidad.* La interoperabilidad entre diferentes implementaciones de ECC, limita su uso en algunos entornos.

Algoritmo RSA

Es un algoritmo de criptografía de clave pública que se utiliza para cifrar y firmar digitalmente datos en aplicaciones de seguridad de la información.

La función principal de RSA

Es proporcionar un método seguro para la comunicación de datos mediante el cifrado y la firma digital. Utiliza claves públicas y privadas para el cifrado y descifrado de datos y para la firma y verificación de firmas digitales.

Algunas características importantes del algoritmo RSA:

- Es un algoritmo asimétrico, lo que significa que las claves utilizadas para cifrar y descifrar los datos son diferentes.
- Es un algoritmo seguro y utilizado en aplicaciones de seguridad de la información, como la autenticación y el cifrado de datos.

RSA se utiliza para cifrar datos y garantizar la confidencialidad de los mismos, así como para firmar digitalmente datos y garantizar su integridad y autenticidad.

Ventajas:

RSA es un algoritmo seguro y confiable utilizado ampliamente en aplicaciones de seguridad de la información.

Es un algoritmo de clave pública, lo que significa que no es necesario intercambiar claves secretas entre las partes que desean comunicarse.

Es compatible con una amplia variedad de plataformas y sistemas operativos.

Desventajas:

Puede ser lento en comparación con algunos algoritmos de cifrado más nuevos.

El cifrado RSA requiere claves grandes para proporcionar una seguridad adecuada, lo que puede hacer que el proceso de cifrado sea más lento.

RSA puede ser vulnerable a ciertos ataques, como el ataque de factorización de números primos, si las claves utilizadas no son lo suficientemente grandes.

Algoritmo Blowfish

Es un algoritmo de bloque que cifra y descifra datos en bloques de 64 bits y utiliza claves de cifrado de entre 32 y 448 bits. Blowfish es conocido por ser rápido, seguro y fácil de implementar en software y hardware.

Es utilizado en aplicaciones de seguridad de redes, como encriptación de archivos, correo electrónico y contraseñas. Es uno de los pocos algoritmos de cifrado simétrico que es de dominio público, lo que significa que se puede utilizar libremente sin restricciones legales o de patentes.

Su función principal es cifrar y descifrar datos rápidamente, lo que lo hace adecuado para su uso en aplicaciones que requieren un alto rendimiento y seguridad.

Algunas características del algoritmo Blowfish:

- *Clave variable.* Utiliza claves de cifrado de longitud variable, que van desde 32 hasta 448 bits.
- *Modo de operación.* Blowfish emplea el modo de operación ECB (Electronic Codebook), que cifra cada bloque de datos de forma independiente.
- *Estructura de Feistel.* Una estructura de Feistel, que divide los datos en dos partes y aplica varias rondas de cifrado y descifrado a cada parte.
- *Velocidad.* Es un algoritmo de cifrado rápido, lo que lo hace adecuado para su uso en aplicaciones que requieren un alto rendimiento. (Santos, 2022)

Las ventajas del algoritmo Blowfish son:

- *Seguridad. U*tiliza un cifrado fuerte que ha resistido los ataques criptográficos más comunes.
- *Velocidad. E*s capaz de cifrar y descifrar grandes cantidades de datos rápidamente, lo que lo hace adecuado para su uso en aplicaciones que requieren un alto rendimiento.
- *Eficiencia. E*s fácil de implementar en software y hardware, lo que lo hace adecuado para una amplia gama de dispositivos y sistemas.
- *Flexibilidad. P*ermite el uso de claves de cifrado de diferentes longitudes, lo que permite un mayor nivel de seguridad.
- *Dominio público.* Es de dominio público, lo que significa que se puede utilizar libremente sin restricciones legales o de patentes.

Las desventajas del algoritmo Blowfish son:

- *Tamaño del bloque.* Utiliza un tamaño de bloque de 64 bits, lo que significa que no es adecuado para cifrar datos más grandes sin dividirlos en bloques más pequeños.
- *Vulnerabilidades potenciales. E*s considerado un algoritmo seguro, puede haber vulnerabilidades desconocidas que podrían ser descubiertas en el futuro.
- *Limitaciones de la clave. P*ermite el uso de claves de diferentes longitudes, es posible que las claves más cortas no proporcionen un nivel suficiente de seguridad.
- *Limitaciones en el cifrado asimétrico.* Es un algoritmo de cifrado simétrico, lo que significa que no puede ser utilizado para cifrado asimétrico y no proporciona una solución completa para todas las necesidades de seguridad. (Gómez, 2019)

Algoritmo DSA (Digital Signature Algorithm)

Es un algoritmo de criptografía de clave pública utilizado para la firma digital y el intercambio de claves. Fue desarrollado por el gobierno de los Estados Unidos como un estándar federal en 1991.

La principal función del algoritmo DSA

Es la generación de firmas digitales que se pueden utilizar para verificar la autenticidad y la integridad de un mensaje. También se puede utilizar para el intercambio de claves para el cifrado y descifrado de mensajes.

Las características del algoritmo DSA

- Su seguridad se basa en la complejidad del problema matemático de la factorización y la dificultad de calcular logaritmos discretos en cuerpos finitos.
- El tamaño de clave recomendado es de al menos 1024 bits y el tamaño de hash utilizado en el algoritmo es de 160 bits.

Ventajas del algoritmo DSA:

- *Eficiencia:* Es más eficiente en términos de rendimiento y velocidad en comparación con otros algoritmos de criptografía.
- *Compatibilidad con otros algoritmos:* El algoritmo DSA se puede utilizar en combinación con otros algoritmos de criptografía para proporcionar una seguridad adicional a los sistemas.
- *No requiere licencia:* El algoritmo DSA es de dominio público, lo que significa que se puede utilizar sin restricciones de licencia.
- *No hay peligro de exposición de claves privadas.* A diferencia de los algoritmos de cifrado simétricos, el algoritmo DSA no implica la exposición de claves privadas, lo que lo hace más seguro.

El algoritmo DSA tiene algunas desventajas:

- *Complejidad.* Aunque el DSA es un algoritmo bien diseñado, su complejidad hace que sea difícil de entender y programar.
- *No es adecuado para cifrado.* A diferencia de otros algoritmos criptográficos, el DSA no se utiliza para cifrar datos, sino que se utiliza para firmarlos. Esto significa que no es adecuado para ciertas aplicaciones que requieren cifrado.
- *No es ampliamente utilizado.* Esto puede deberse en parte a las limitaciones del tamaño de la clave y la complejidad del algoritmo.

(Ali Norouzzadeh-GilMolk, 2020)

Algoritmo SHA-256

Es un algoritmo de función hash criptográfica que se utiliza para convertir datos de cualquier tamaño en un valor hash fijo de 256 bits.

Su función principal, es proporcionar integridad de datos y seguridad de mensajes mediante la verificación de que los datos no han sido manipulados o alterados de ninguna manera durante la transmisión o el almacenamiento.

Características:

- SHA-256 es un algoritmo de función hash criptográfica que genera un valor hash de 256 bits.

- Es resistente a la colisión, lo que significa que es difícil generar dos valores hash idénticos a partir de entradas diferentes.
- SHA-256 es ampliamente utilizado en aplicaciones de seguridad de la información, como la autenticación de mensajes y la validación de archivos. (Julio C. Mendoza-Tello, 2020)

Ventajas:

- Proporciona una alta seguridad de datos y confidencialidad.
- Es fácil de implementar y utilizar en una amplia variedad de aplicaciones de seguridad.
- Los valores hash generados son únicos y fiables, lo que permite verificar la integridad de los datos transmitidos o almacenados.

Desventajas:

- SHA-256 no es una solución completa para la seguridad de la información y debe utilizarse junto con otros protocolos y medidas de seguridad.
- Aunque es resistente a la colisión, aún existe la posibilidad de que se generen valores hash idénticos a partir de entradas diferentes.
- SHA-256 es un algoritmo de función hash unidireccional, lo que significa que no se puede recuperar la entrada original a partir del valor hash generado. (Julio C. Mendoza-Tello, 2020)

Estudio comparativo de los algoritmos criptográficos.

Tabla 1

Estudio de los algoritmos criptográficos.

Algoritmo	Función principal	Tamaño de clave	Tamaño de hash	Seguridad	Velocidad	Tipo
AES 256	Cifrado simétrico	256 bits	N/A	Alta	Alta	Bloques
DES	Cifrado simétrico	56 bits	N/A	Baja	Media	Bloques
ECC	Cifrado asimétrico	160-521 bits	N/A	Alta	Alta	Curvas elípticas
RSA	Cifrado asimétrico	1024-4096 bits	N/A	Alta	Baja	Números enteros
Blowfish	Cifrado simétrico	32-448 bits	N/A	Alta	Media	Bloques
DSA	Firma digital	1024-3072 bits	N/A	Alta	Baja	Números enteros
SHA 256	Función hash	N/A	256 bits	Alta	Media	Criptográfica

Fuente: (Alfaro Gómez, 2020).
Elaborado por: Micaela Guamán.

Análisis: En el siguiente cuadro comparativo proporciona una visión general de los algoritmos criptográficos más comunes. En cuanto a la función principal, todos estos algoritmos se utilizan para cifrar y proteger los datos, aunque algunos son más adecuados para ciertos tipos de datos o aplicaciones que otros.

Tabla 2

Análisis general: AES 256, DES y SHA 256

Algoritmo	Función principal	Características	Ventajas	Desventajas	Seguridad	Velocidad
AES 256	Cifrado de bloques de datos (simétrico)	Tamaño de clave: 256 bits Tamaño de bloque: 128 bits	Mayor seguridad que DES Ampliamente utilizado en aplicaciones de seguridad de datos.	Configuración compleja No es compatible con versiones anteriores de AES.	Alta	Alta
DES	Cifrado de bloques de datos (simétrico)	Tamaño de clave: 56 bits Tamaño de bloque: 64 bits	Rápido y fácil de implementar Es ampliamente compatible	Tamaño de clave pequeño que lo hace menos seguro No es adecuado para aplicaciones de alta seguridad	Baja	Media
SHA 256	Función hash criptográfica	Tamaño de hash: 256 bits	Tiene un alto rendimiento	Configuración compleja	Alta	Media

	No permite la recuperación de datos originales a partir del hash.	Requiere mayor potencia de procesamiento y memoria No es compatible con versiones anteriores de SHA.

Fuente: (Gómez, 2019)
Elaborado por: Micaela Guamán

Análisis:

Después de analizar el cuadro comparativo de AES 256, DES y SHA 256 en función, características, ventajas y desventajas, podemos determinar lo siguiente:

AES 256 es el algoritmo más seguro y eficiente de los tres. La seguridad de cualquier algoritmo de cifrado depende de factores como la longitud y la complejidad de la clave de cifrado.

Puntuación de cada categoría de los tres algoritmos seleccionados en una escala del 1 al 5:

Bajo: *1-2*

Medio:*3-4*

Alto:*5*

Tabla 3

Puntuación de la comparación de los tres algoritmos criptográficos

Algoritmo	Función	Características	Ventajas y desventajas	Seguridad	Velocidad	Puntuación
AES 256	5	5	4	5	5	**24**
DES	2	2	2	2	4	**12**
SHA 256	4	4	4	5	4	**21**

Fuente: (Gómez, 2019)
Elaborado por: Micaela Guamán

Análisis de las ponderaciones de los algoritmos criptográficos:

AES 256: El algoritmo criptográfico obtiene una puntuación alta en todas las categorías, por su alta seguridad y resistencia a ataques lo hacen el mejor algoritmo en términos generales, obteniendo una puntuación total de 24.

DES: Obtiene la puntuación más baja en todas las categorías. Debido a su baja seguridad y a la disponibilidad de algoritmos más modernos y seguros, no es una buena opción para su uso en la actualidad, obteniendo una puntuación total de 12.

SHA 256: Obtiene puntuaciones relativamente buenas en todas las categorías, especialmente en seguridad, lo que lo hace una buena opción para la generación de hash. Obtiene una puntuación total de 21.

Análisis General:

Algoritmo criptográfico AES 256

En base al cuadro comparativo, se puede concluir que el algoritmo AES 256, obtuvo la mayor puntuación en la mayoría de las categorías evaluadas, incluyendo la función principal, características, ventajas, desventajas, seguridad y velocidad. Considerando que es uno de los algoritmos criptográficos más fuertes y seguros disponibles en la actualidad.

Además, AES 256 tiene un tamaño de clave más grande que DES, lo que lo hace más resistente a los ataques de fuerza bruta. También tiene una velocidad de cifrado y descifrado relativamente rápida en comparación con otros algoritmos criptográficos, lo que lo hace adecuado para aplicaciones que requieren un alto rendimiento.

En cuanto a la seguridad, AES 256 tiene una longitud de clave suficientemente grande para resistir ataques criptográficos modernos, y es uno de los algoritmos criptográficos recomendados por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) para proteger información clasificada.

2.4 Legal

Ley Orgánica de Protección de Datos

De acuerdo al artículo 66 numeral 19 de la Ley Orgánica de Protección de Datos, reconoce y garantiza a las personas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley". (Valencia, 2014)

Según la Constitución del Ecuador en el artículo 92, manifiesta que: "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico

Así mismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos".

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. (Constitución del Ecuador, 2008)

Ley de comercio electrónico, firmas y mensajes de datos

Ley de Comercio Electrónico, Firmas y Mensajes de Datos en Ecuador el 17 de abril del 2002, también conocida como la Ley de Comercio Electrónico, publicada en el año 2002.

Objetivo. - Establecer un marco jurídico para las transacciones comerciales realizadas por medios electrónicos en Ecuador.

La Ley de Comercio Electrónico reconoce la validez jurídica de las transacciones comerciales realizadas por medios electrónicos, siempre y cuando se cumplan ciertos requisitos. Estos requisitos incluyen la utilización de firmas electrónicas, mensajes de datos y registros electrónicos, entre otros.

Establece las obligaciones y responsabilidades de los proveedores de servicios de comercio electrónico, así como las obligaciones de los consumidores y usuarios. Además, plantea medidas para proteger la privacidad y seguridad de los datos personales y financieros de los usuarios. (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2002)

CAPITULO III

METODOLOGÍA

3.1 Tipo de Investigación

Esta investigación es de tipo explicativa, según (Arias, 2020) expone que,

"Se encarga de buscar el porqué de los hechos mediante el establecimiento de relaciones causa-efecto, que por sus resultados y conclusiones contemplan un profundo análisis", analizando los algoritmos criptográficos del sistema, que protegen la información y da seguridad a la comunicación de la entidad pública del Cuerpo de Bomberos de la ciudad de Guaranda."

3.2 Enfoque de la investigación

El enfoque que toma la investigación es cualitativo, donde se recopilará la información necesaria, basada en teorías, conceptos, opiniones; analizando que algoritmos criptográficos brindan mayor protección de los datos, considerando tener varias respuestas, a través de entrevistas a realizar, al personal encargado de cada departamento del Cuerpo de Bomberos de Guaranda.

3.3 Métodos de Investigación

En la investigación se distingue el método analítico, como menciona (Zoila Mendoza, 2018):

"Se fundamenta en la premisa de que a partir del todo absoluto se puede conocer y explicar las características de cada una de sus partes y de las relaciones entre ellas", estudiando todos los algoritmos criptográficos que me permitirán una protección de los mismos, en el sistema informático del Cuerpo de Bomberos de la ciudad de Guaranda.

Según (Andrés Rodríguez, 2019), afirma que:

"Para la construcción de conocimientos, demostrando ser de gran utilidad para la búsqueda y procesamiento de la información teórica y metodológica", que se utilizó para analizar la investigación referente a los algoritmos criptográficos, que permite

la extracción de los elementos más importantes que se relacionan con el objeto de estudio.

3.4 Técnicas e Instrumentos de Recopilación de Datos

Para la recolección de datos se determina el uso de las técnicas e instrumentos, como es la entrevista y encuesta, donde se reunirá la información de manera organizada.

Entrevista

La entrevista aplicada, se usa para el intercambio de ideas u opiniones, entre el investigador y el entrevistado, manteniendo un diálogo, expresando sus puntos de vista, siendo necesarios para aclarar ciertas dudas sobre los algoritmos criptográficos, llegando a un acuerdo en el tema investigativo, realizada al desarrollador del sistema informático de la institución.

Encuesta

La encuesta se basó en un cuestionario, con la finalidad de recopilar la información necesaria y conocer las opiniones de los directores de cada departamento del Cuerpo de Bomberos de Guaranda, tales como; Talento Humano, Operación, Gestión de Transporte y Financiero.

3.5 Universo, Población y Muestra

Universo

Para la presente investigación se ha considerado como universo, a los miembros que conforman el Cuerpo de Bomberos de Guaranda, personas quienes son encargadas de cada departamento dentro de la institución.

por cuanto la población y la muestra es menor a 100.

La técnica que se utiliza para extraer la muestra en la presente investigación es el muestreo no probabilístico, que se basa en la selección especifica de la población, donde se utilizó criterios determinados y las razones representativas de la población; dentro del muestreo mencionado existe el tipo de muestreo por convivencia, donde se indaga características personales del investigador, que influyen en la investigación.

3.6 Procesamiento de la Información

Para el análisis de datos cualitativos, (Rodríguez Sabiote, Lorenzo Quiles, & Herrera Torres, 2018) manifiesta; “al manipular información por los investigadores establece relaciones, interpreta, extrae significados y conclusiones”; basándose en preguntas abiertas, cabe recalcar que la información obtenida permite tener detalles de quienes se encuestaron ya sea por las dos técnicas utilizadas. Utilizando la herramienta Excel para obtener los datos según los criterios de los encuestados.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1 Análisis, Interpretación y Discusión de Resultados

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS INFORMÁTICAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

Objetivo: Conocer los riesgos y dificultades del sistema del Cuerpo de Bomberos de Guaranda, en el campo de la seguridad criptográfica y sus tecnologías informáticas.

Dirigido a: Ing. Alex Campana; desarrollador del sistema.

Entrevistador: Micaela Guamán

ENTREVISTA
SISTEMA DE CUERPO DE BOMBEROS

1. **¿Cuál es su opinión acerca de la criptografía?**

Es necesario fundamentar el desarrollo de las plataformas en cuanto es al logueo, cuando se tiene los servicios publicados y cuando se maneja la parte del loguin, de manera general con ese concepto englobo a la criptografía. Y en temas financieros también se involucra más el tema tratado.

Análisis:

Considera que es importante el desarrollo en las plataformas digitales y financieros, en la protección de datos e información.

2. **¿Realizó un estudio previo para poder realizar el sistema de Cuerpo de Bomberos?**

Buscar una debilidad vacía en la parte del Cuerpo de Bomberos para poder proponer una solución tecnológica y automatizar.

Análisis:

Se puede deducir que para el estudio previo el desarrollador busco las debilidades existentes que tuvo dentro de la institución, por ende, surgió la necesidad de buscar una solución.

3. ¿Cuál es el enfoque principal para realizar el sistema propuesto?

Solventar esa debilidad lo cual no se tenía, las solicitudes en línea, pagos en línea, permisos de funcionamiento en línea y no tener digitalizado los partes de emergencia.

Análisis:

El enfoque general que tuvo el desarrollador frente al desarrollo del sistema, es verificar las falencias, de las cuales se presentaron como la no digitalización de documentos y permisos, lo que conllevo tener todo esto en línea para evitar tediosos trámites a mano.

4. ¿Para realizar el sistema que se maneja en la institución, que aspectos se tomaron en cuenta para su desarrollo?

Netamente se basó, en los requisitos del Cuerpo de Bomberos, se hizo la entrevista de la necesidad en base a cómo trabajan actualmente y en base a eso se levantaron los requisitos.

Análisis:

En base a la opinión del entrevistado, se analiza que primero se obtuvo los requerimientos que surgen a través de la necesidad que actualmente trabajan en la institución, para poder iniciar el desarrollo.

5. ¿En la implementación del sistema con que lenguaje de programación se trabajó para el desarrollo de la aplicación?

Se tiene conocimiento de frameworks, básicamente esta implementado en el lenguaje de programación Java y está en el servidor Linux CentOS, utilizando apache, php, Java striped, bootstrap, html, obteniendo una capa de presentación y una capa de acceso como el frontend y backend.

Análisis:

Para el desarrollo de la aplicación el desarrollador del sistema utilizó el lenguaje de programación Java, teniendo en cuenta las necesidades del cliente y el uso de las herramientas adecuadas en el desarrollo del proyecto.

6. **¿Utilizó algoritmos criptográficos para el desarrollo del sistema informático?**

En este caso, no existe el uso de ningún algoritmo de criptografía, lo único que realiza el sistema es que este encriptado con Loguin, cuanto el usuario se loguea existen caracteres conformados con la contraseña, fecha y un par de algoritmos extra 255 caracteres que se genera un token y se empieza hacer peticiones y si algún momento se caduca el token o alguien lo elimina por cookies y todo, se deja de mantener la sesión y ya no tienes respuesta.

Análisis:

Se pudo analizar que el sistema como tal no tienen en sí, un algoritmo de seguridad, tan solo cuenta con un token de seguridad que permite generar el acceso a una clave y a una aplicación, considerando peticiones y los tokens en tiempos de respuesta.

7. **¿El sistema que fue implementado en la institución del Cuerpo de Bomberos de Guaranda cuenta con un certificado de comunicación segura?**

Si cuenta con uno de ellos y en el sistema tiene instalado el certificado de SSL.

Análisis:

El protocolo de seguridad utilizado en el sistema, Capa de sockets seguros (SSL), permite que los datos compartidos puedan ser navegados de manera más confiable y segura, gracias a que el certificado cuenta con un mecanismo de encriptación.

8. **¿En las actualizaciones de parches de seguridad informática, su sistema cuenta con uno de ellos para evitar ciertas amenazas que dañen al software?**

En cuestiones de servidor si, se realiza un Update, para que los parches de seguridad sean actualizados y evitar ciertos ataques que puedan afectar al sistema.

Análisis:

Los parches de seguridad son necesarios en mejorar las actualizaciones como en la seguridad de Windows Update, permitiendo este software solucionar y reparar errores que se presenten en la funcionalidad del sistema.

9. **¿Utiliza actualmente mecanismos de seguridad en la autenticación del manejo del sistema de Cuerpo de Bomberos?**

Para el sistema nos basamos en un mecanismo de un token de software, que funciona como medida de seguridad, ejemplo si se llega perder información se eliminará los datos almacenados.

Análisis:

Se estima que las medidas de seguridad que manejan en el sistema es el token de autenticación, que permite al usuario acceder al sistema de forma segura y confiable, considerando que los datos están siendo protegidos.

10. **¿En las pruebas de desarrollo que se realiza en cada fase, el sistema presentó errores o fallos en su funcionalidad?**

No, al momento de realizar las pruebas no hubo no ha sufrido ninguna inconsistencia en la funcionalidad del sistema.

Análisis:

Cabe destacar que, al realizar las pruebas, el sistema no presento fallos a lo largo de su desarrollo.

Análisis general:

Se puede concluir que para el desarrollo del sistema tuvo por consecuencia un estudio previo, donde surgió la necesidad de recabar información necesaria, identificando que debilidades existen dentro de la institución, con el fin de dar buscar una solución.

El sistema propuesto tiene como objetivo solventar los pagos y solicitudes manuales, en pagos digitales, contando con métodos y protocolos de comunicación segura, aplicando varias tecnologías según la necesidad del cliente. Considerando que no cuenta como tal, un algoritmo criptográfico que permita que los datos protegidos ante las vulnerabilidades y que el sistema sea más seguro y confiable.

ENCUESTA

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS INFORMÁTICAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

Objetivo: Recabar información sobre el análisis de los algoritmos criptográficos y la seguridad del sistema de Cuerpo de Bomberos de Guaranda

Dirigido a: Directores

La presente encuesta forma parte del proyecto de titulación: "Análisis de los algoritmos criptográficos"

La información proporcionada es de carácter confidencial y reservado; de manera que los resultados obtenidos serán manejados solo para la investigación.

Pregunta N°1: ¿Tiene conocimiento previo sobre la seguridad informática?

Tabla 4

Respuesta pregunta 1

Alternativas	Respuestas	Porcentaje
Si	4	100%
No	0	0%
Total	4	100%

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

Al hablar de seguridad informática, todas las personas encuestadas tienen conocimiento sobre este tema, que hoy en día es importante contando con una totalidad del 100%.

Pregunta N°2: ¿Tiene conocimiento usted que el Cuerpo de Bomberos de Guaranda cuenta con un sistema de seguridad?

Tabla 5

Respuestas pregunta 2

Alternativas	Respuestas	Porcentaje
Si	3	75%
No	1	25%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

En 75% de los encuestados afirman que el sistema que actualmente utilizan cuenta con un sistema de seguridad, lo que genera confianza al momento de realizar cualquier actividad, mientras que un 25% manifiesta que no tiene conocimiento previo a la seguridad del sistema.

Pregunta N°3: ¿Usted cree que es confiable el sistema que actualmente utiliza la institución?

Tabla 6

Respuestas pregunta 3

Alternativas	Respuestas	Porcentaje
Si	4	100%
No	0	0
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

El sistema del Cuerpo de Bomberos de Guaranda según la encuesta realizada a los directores responsables de cada departamento afirma que es confiable en un 100%.

Pregunta N°4: ¿Cuál es su nivel de confianza en la seguridad del sistema de Cuerpo de Bomberos de Guaranda?

Tabla 7

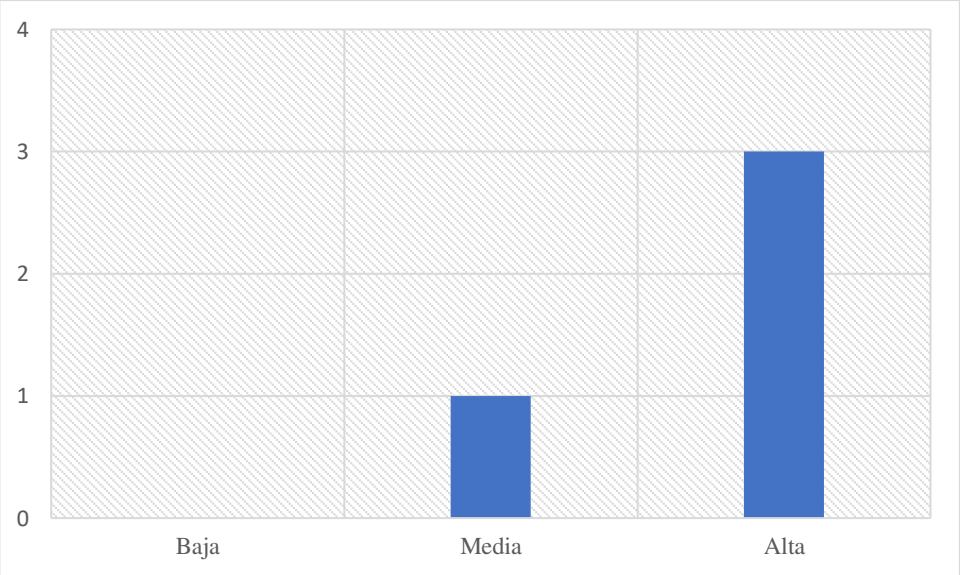
Respuestas pregunta 4

Alternativas	Respuestas	Porcentaje
Baja	0	0%
Media	1	25%
Alta	3	75%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Ilustración *1*

Respuestas pregunta 4



Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

La confianza que brinda el sistema a quienes le dan uso es del 75%, obteniendo un nivel alto de confiabilidad por parte del usuario, mientras que un 25% considera un nivel medio en la seguridad del sistema.

Pregunta N°5: ¿En qué tiempo considera usted que sea necesario actualizar el sistema de seguridad del Cuerpo de Bomberos de Guaranda?

Tabla 8

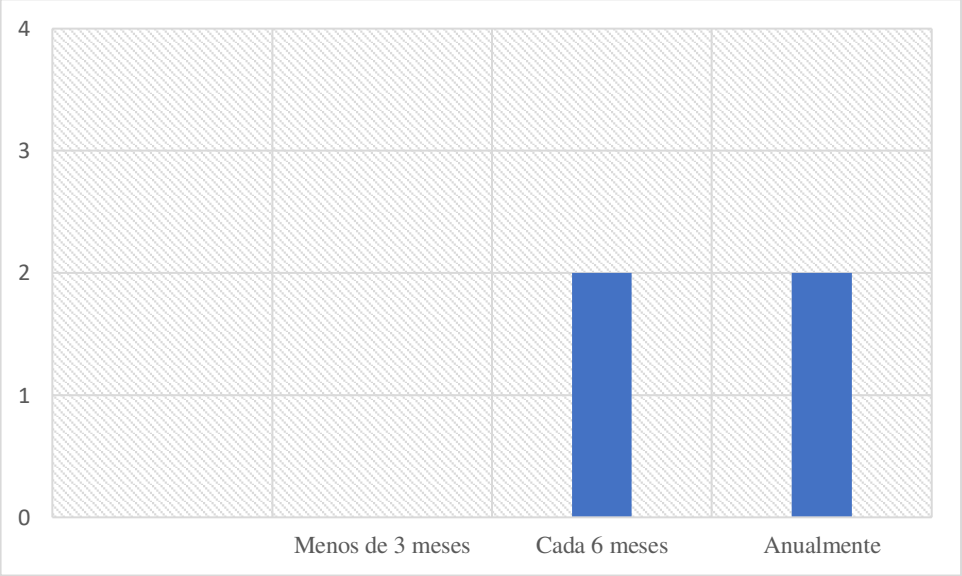
Respuestas pregunta 5

Alternativas	Respuestas	Porcentaje
Menos de 3 meses	0	0%
Cada 6 meses	2	50%
Anualmente	2	50%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Ilustración 2

Respuestas pregunta 5



Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

El 50% de los encuestados consideran que debe ser actualizado cada seis meses, el sistema para mayor seguridad, sin embargo, el otro 50% manifiesta que es necesario actualizarlo anualmente.

Pregunta N°6: ¿Conoce usted algunas aplicaciones de criptografía?

Tabla 9

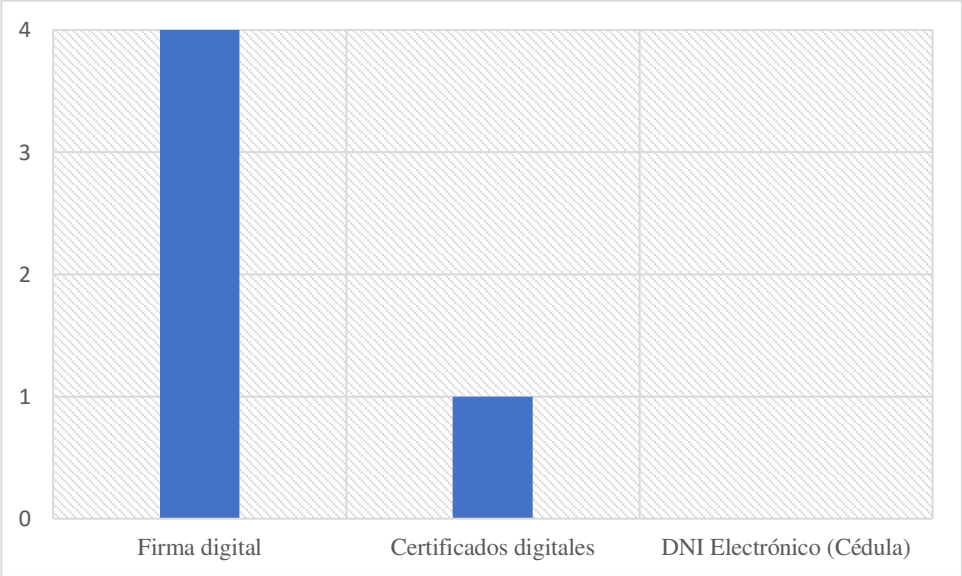
Respuestas pregunta 6

Alternativas	Respuestas	Porcentaje
Firma digital	4	100%
Certificados digitales	1	25%
DNI Electrónico (Cédula)	0	0%

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Ilustración *3*

Respuestas pregunta 6



Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

Los encuestados manifiestan que conocen la firma digital en su totalidad del 100%, mientras un 25% conoce el certificado digital y la otra parte desconoce la existencia de otras aplicaciones como el DNI electrónico.

Pregunta N°7: ¿Ha utilizado alguna vez una aplicación de seguridad criptográfica para proteger sus datos?

Tabla 10

Respuesta pregunta 7

Alternativas	Respuestas	Porcentaje
Si	2	50%
No	2	50%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

Con los datos obtenidos se deduce que el 50% de los encuestados han utilizado una aplicación que brinde seguridad para la protección de sus datos, tomando en cuenta el 50% faltante no ha usado una aplicación de seguridad informática.

Pregunta N°8: ¿Cree que la criptografía es importante para la seguridad de la información en línea?

Tabla 11

Respuestas pregunta 8

Alternativas	Respuestas	Porcentaje
Si	4	100%
No	0	0
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

Los datos recolectados en las encuestas realizadas muestran que existe un total del 100% de afirmación, en la importancia de la criptografía dentro de la seguridad informática online.

Pregunta N°9: ¿Está de acuerdo en compartir sus datos personales con terceros, considerando que cuenta con un nivel de seguridad alto (criptográfico)?

Tabla 12

Respuestas pregunta 9

Alternativas	Respuestas	Porcentaje
Si	0	0%
No	4	100%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

En su totalidad nadie está de acuerdo en compartir sus datos con terceros, porque genera desconfianza por parte de los usuarios y la falta de información hace que no exista un grado de confiabilidad en la seguridad de sus datos.

Pregunta N°10: ¿Qué medidas adicionales cree que se deberían tomar para garantizar la seguridad de la información?

Tabla 13

Respuestas pregunta 10

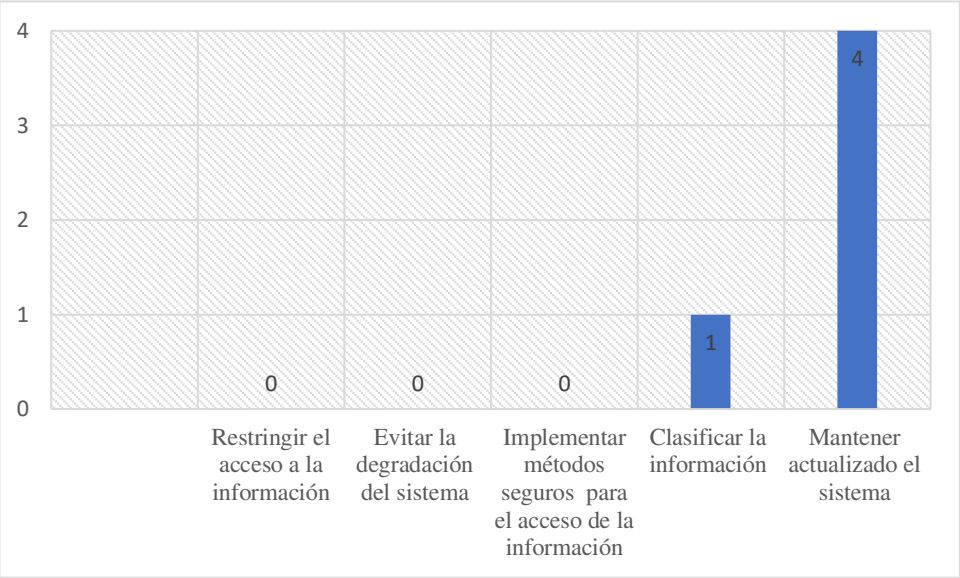
Alternativas	Respuestas	Porcentaje
Restringir el acceso a la información	0	0%
Evitar la degradación del sistema	0	0%
Implementar métodos seguros para el acceso de la información	0	0%
Clasificar la información	1	25%

Mantener actualizado el sistema	4	100%

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Ilustración *4*

Respuestas pregunta 10



Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

La medida que garantiza la seguridad informática más acertada en la encuesta realizada fue mantener actualizado el sistema, teniendo el 100% de aceptación, mientras que la otra parte del 25% considera que es necesario clasificar la información en medida de seguridad.

Pregunta N°11: ¿Qué amenaza cree usted que merece más atención en el campo de la ciberseguridad?

Tabla 14

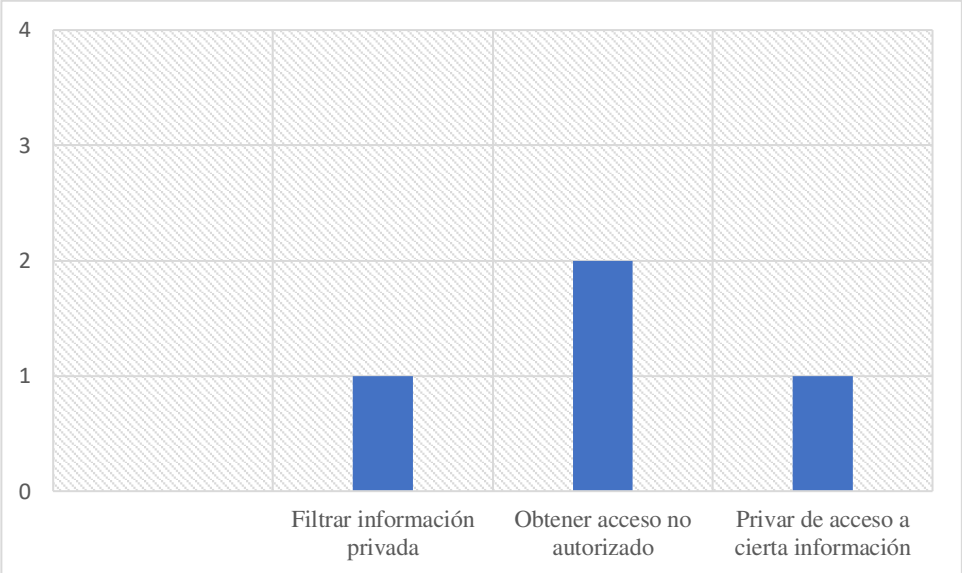
Respuestas pregunta 11

Alternativas	Respuestas	Porcentaje
Filtrar información privada	1	25%
Obtener acceso no autorizado	2	50%
Privar de acceso a cierta información	1	25%
Total	**4**	**100%**

Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Ilustración *5*

Respuestas pregunta 11



Fuente: Cuerpo de Bomberos de Guaranda
Elaborado por: Micaela Guamán

Análisis Interpretativo:

La amenaza que debe tener más importancia es la obtención de acceso no autorizado al sistema, teniendo un 50% de alcance por parte de los encuestados, sin embargo, el filtrar información y privar el acceso cuenta con un 25% considerando a tener atención como alerta de amenaza y ser tomadas en cuenta dentro del campo de seguridad.

CAPITULO V

PROPUESTA

Garantizar la integridad y resguardo de información, con el algoritmo criptográfico AES-256 en un sistema ejemplo.

1. Resumen

En la propuesta investigativa, se plantean dos campos que se relacionan con la criptografía y la seguridad informática. El algoritmo criptográfico principal AES-256, que cifra y descifra datos, que al desarrollar cuyo algoritmo en base a un ejemplo permite conocer la clave generada en código y la clave inicial.

El algoritmo AES-256 es un algoritmo de cifrado simétrico que es utilizado para proteger datos sensibles en aplicaciones y sistemas informáticos.

Es considerado uno de los algoritmos más seguros disponibles actualmente, utilizando una clave de cifrado de 256 bits que es difícil de descifrar sin conocer la clave correcta.

En general, AES 256 es una excelente opción para proteger datos confidenciales y mantener la privacidad en la era digital actual, donde la seguridad es una preocupación cada vez mayor.

Al final de la investigación, con el ejemplo planteado se estima obtener un resultado que muestre el cifrado y descifrado de una clave con el algoritmo criptográfico AES 256, donde cuyo algoritmo determinará que es eficiente y seguro en el manejo de los datos.

2. Introducción

La criptografía es una disciplina que se encarga de proteger la información a través de técnicas de codificación y decodificación de datos. En este contexto, los algoritmos criptográficos son herramientas fundamentales para garantizar la seguridad de la información en la era digital. (Mouna Bedoui, 2021)

La seguridad informática se dedica a proteger los sistemas informáticos de amenazas externas e internas. Siendo las amenazas externas como ataques

informáticos, virus, robos de información. Las amenazas internas son las que provienen del sistema como los errores humanos, fallos o desactualizaciones de software y hardware. (Kérly Winques, 2022)

El principal propósito del algoritmo AES-256 es proporcionar una alta seguridad para los datos sensibles que se almacenan, procesan o transmiten en sistemas informáticos. Es resistente a los ataques, que implican probar todas las combinaciones de teclas posibles para descifrar los datos. La implementación del algoritmo también puede mejorar la confianza de los usuarios en la seguridad de los sistemas y aplicaciones que utilizan.

Sin embargo, es importante tener en cuenta que la seguridad del algoritmo también depende de la fortaleza de la clave utilizada, así como de la implementación del propio algoritmo.

3. Objetivo

Garantizar la integridad y resguardo de información, con el algoritmo criptográfico AES-256 en un sistema ejemplo.

4. Desarrollo

Determinando generar códigos únicos en base a un estándar con el que se pudieran asegurar documentos o datos informáticos frente a cualquier agente externo que desee modificarlos. Este algoritmo fue y es un gran avance en el camino a garantizar la privacidad del contenido en el procesamiento de información. (Joonsang Baek, 2021)

Algunos de los propósitos del algoritmo AES-256

Seguridad: AES-256 es considerado uno de los algoritmos de cifrado más seguros y robustos disponibles, y es utilizado por gobiernos, empresas y organizaciones de todo el mundo para proteger datos sensibles.

Privacidad: Se utiliza para proteger la privacidad de los datos, lo que significa que sólo las personas autorizadas pueden acceder a ellos, protege la información personal, financiera y empresarial de acceso no autorizado.

Cumplimiento normativo: Es un estándar de cifrado reconocido internacionalmente y es requerido por muchas leyes y regulaciones de seguridad de datos en todo el mundo. La implementación del algoritmo AES-256 en aplicaciones y sistemas ayuda a las organizaciones a cumplir con las normas y regulaciones de seguridad de datos.

Confianza: Puede mejorar la confianza de los clientes y usuarios en la seguridad de los sistemas y aplicaciones que utilizan. Los usuarios se sienten más seguros al saber que los datos sensibles están protegidos mediante un algoritmo de cifrado robusto y seguro. (Nathaly Nieto Ramirez, 2019)

Las funciones de AES 256 incluyen:

Confidencialidad: AES 256 cifra los datos de manera que solo las personas con la clave correcta pueden descifrarlos. Esto proporciona confidencialidad a los datos protegidos por AES 256.

Integridad: AES 256 también se utiliza para garantizar la integridad de los datos. Esto significa que los datos cifrados con AES 256 no pueden ser modificados sin que se detecte. Si alguien intenta modificar los datos cifrados, la función de integridad de AES 256 detectará el cambio.

Autenticación: AES 256 también se puede utilizar para autenticar la identidad de una persona o entidad. Esto se logra mediante el cifrado de un mensaje con la clave privada de la entidad y la verificación del mensaje cifrado utilizando la clave pública de la entidad.

Seguridad: AES 256 es un algoritmo de cifrado altamente seguro que se utiliza en muchas aplicaciones de seguridad, incluyendo el cifrado de archivos, el cifrado de correo electrónico, y el cifrado de datos en transacciones en línea. (Joonsang Baek, 2021)

Algoritmo de cifrado y descifrado mediante AES-256

```
package aes256;

import javax.crypto.Cipher;

import javax.crypto.SecretKey;

import javax.crypto.SecretKeyFactory;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.spec.PBEKeySpec;

import javax.crypto.spec.SecretKeySpec;

import java.nio.charset.StandardCharsets;

import java.security.InvalidAlgorithmParameterException;

import java.security.InvalidKeyException;

import java.security.NoSuchAlgorithmException;

import java.security.spec.InvalidKeySpecException;

import java.security.spec.KeySpec;

import java.util.Base64;

import javax.crypto.BadPaddingException;

import javax.crypto.IllegalBlockSizeException;

import javax.crypto.NoSuchPaddingException;


public class AES256 {

  private static final String SECRET_KEY = "abcsd";

  private static final String SALT = "abcdsk";


  public static String encrypt(String strToEncrypt) {
```

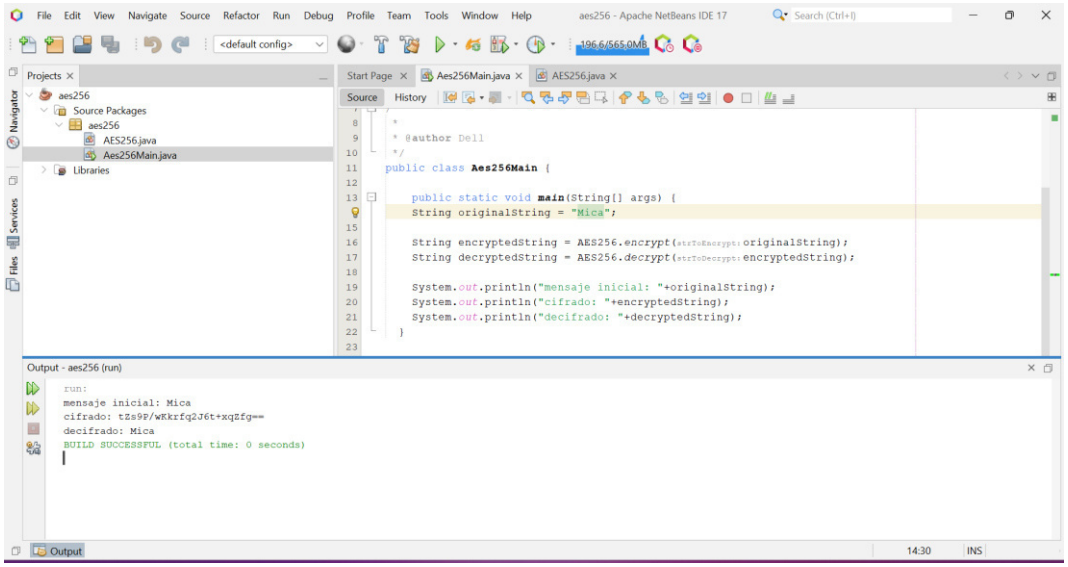
```
    try {
      byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
      IvParameterSpec ivspec = new IvParameterSpec(iv);

      SecretKeyFactory factory =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
      KeySpec spec = new PBEKeySpec(SECRET_KEY.toCharArray(),
SALT.getBytes(), 65536, 256);
      SecretKey tmp = factory.generateSecret(spec);
      SecretKeySpec secretKey = new SecretKeySpec(tmp.getEncoded(), "AES");

      Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
      cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);
      return Base64.getEncoder()

.encodeToString(cipher.doFinal(strToEncrypt.getBytes(StandardCharsets.UTF_8)
));
    } catch (InvalidAlgorithmParameterException | InvalidKeyException |
NoSuchAlgorithmException | InvalidKeySpecException | BadPaddingException |
IllegalBlockSizeException | NoSuchPaddingException e) {
      System.out.println("Error while encrypting: " + e.toString());
    }
    return null;
  }
```

```
  public static String decrypt(String strToDecrypt) {


    try {

      byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};

      IvParameterSpec ivspec = new IvParameterSpec(iv);


      SecretKeyFactory factory =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");

      KeySpec spec = new PBEKeySpec(SECRET_KEY.toCharArray(),
SALT.getBytes(), 65536, 256);

      SecretKey tmp = factory.generateSecret(spec);

      SecretKeySpec secretKey = new SecretKeySpec(tmp.getEncoded(), "AES");


      Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");

      cipher.init(Cipher.DECRYPT_MODE, secretKey, ivspec);

      return new
String(cipher.doFinal(Base64.getDecoder().decode(strToDecrypt)));

    } catch (InvalidAlgorithmParameterException | InvalidKeyException |
NoSuchAlgorithmException | InvalidKeySpecException | BadPaddingException |
IllegalBlockSizeException | NoSuchPaddingException e) {

      System.out.println("Error while decrypting: " + e.toString());

    }

    return null;

  }

}
```

Demostración del código AES-256 en el lenguaje de programación Java

Ilustración *6*

Resultado del código AES 256



Fuente: (Hans Delfs, 2019)
Elaborado por: Micaela Guamán

Análisis:

En la ilustración 6, se evidencia que al cifrar el mensaje inicial con la palabra "Mica" nos retorna **tZs9P/wKkrfq2J6t+xqZfg==**, cuyo mensaje es encriptado es el que se deberá almacenar en la base de datos, de la misma manera este mensaje pasa a la función desencriptar, dando como resultado el mensaje original "Mica".

CONCLUSIONES

- Se concluye que los algoritmos criptográficos como AES 256, DES, SHA 256, ECC, RSA, Blowfish y DSA, tienen diferentes características que los hacen adecuados para diferentes usos y medidas de seguridad.
- Es importante considerar que cada algoritmo criptográfico tiene sus fortalezas y debilidades, optando por métodos que nos permiten dar una mejor seguridad al sistema e integridad de su información.
- Del estudio realizado se evidenció que, el algoritmo AES 256 es el más adecuado de tal manera que cumple con los requisitos necesarios para la seguridad y manejo de información, en un sistema informático.
- Los algoritmos criptográficos son una herramienta crucial para proteger la información sensible que garantiza la privacidad y la seguridad en el mundo digital de hoy en día.

RECOMENDACIONES

- Para la protección de datos, es recomendable utilizar algoritmos criptográficos ampliamente reconocidos y probados, como AES 256 que brinda mayor seguridad en la protección de datos.
- Para garantizar la máxima seguridad, es importante mantener los sistemas actualizados incluyendo los parches de seguridad disponibles.
- Se recomienda elegir de manera minuciosa el algoritmo criptográfico más adecuado para el sistema informático, el cual se va a complementar su uso con medidas adicionales de seguridad.
- Se debe definir una política clara de uso de algoritmos criptográficos en el sistema informático del Cuerpo de Bomberos de Guaranda, con el fin de capacitar al personal en su uso adecuado para garantizar la seguridad en la transmisión de datos.

BIBLIOGRAFÍA

Abreu, J. L. (2014). El Método de la Investigación. *Daena: International Journal of Good Conscience*, 10.

Acero, S. W. (2019). *Optimización del Algoritmo Estándar de Encriptación Avanzada (AES) para la protección de la información [Tesis de ingeniería, Universidad Peruana los Andes].* Repositorio UPLA, Lima, Perú. Obtenido de https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1364/T037_43278620_T.pdf?sequence=1

Aida Ormaza, J. C. (2017). Estándares criptográficos aplicados a la estructura e clave pbulica de america del sur. En J. C. Aida Ormaza, *3c Tecnologías* (págs. 14-32). 23.

Alfaro Gómez, V. M. (2020). Estrategia de negocio para el servicio de CiberSeguridad Entel S.A. *REPOSITORIO ACADÉMICO de la Univesidad de Chile*, 51. Obtenido de https://repositorio.uchile.cl/handle/2250/176772

Ali Norouzzadeh-GilMolk, R. R.-K. (2020). Determinación de los factores que abandonan el diseño de algoritmos criptográficos por medio de un meta-modelo cibernético, validado con análisis-Q. *Revista INGENIERÍA UC, 27*(1), 29-40. Obtenido de https://www.redalyc.org/journal/707/70763088005/70763088005.pdf

Alvin Ashcraft, m. w. (23 de 09 de 2022). *microsoft.* Obtenido de microsoft: https://learn.microsoft.com/es-es/windows/win32/seccrypto/data-encryption-and-decryption

Andrés Rodríguez, A. P. (2016). Métodos científicos de indagación y de construcción del conocimiento. *Scielo*, 22.

Arias, F. (2020). *tesisplus.com.* Obtenido de tesisplus.com: https://tesisplus.com/investigacion-explicativa/investigacion-explicativa-segun-autores/

Berhanu Aebissa, G. D. (2023). El efecto directo e indirecto de la justicia organizacional en la intención de los empleados de cumplir con la política de seguridad de la información: el caso de los bancos etíopes. (Elsevier, Ed.) *Informática y Seguridad*. Obtenido de https://www.sciencedirect.com/science/article/pii/S016740482300158X?via%3Dihub

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

Carlos Gomez, J. V. (02 de 12 de 2021). Compression and Encryption of Vital Signals Using an SoC-FPGA. *DYNA, 88*(219), 9. Obtenido de https://doi.org/10.15446/dyna.v88n219.92532

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

Constitución del Ecuador. (20 de 0ctubre de 2008). *asambleanacional.gob.ec*. Obtenido de www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

David Gerault, P. L. (2020). Computing AES related-key differential characteristics with constraint programming. En El SEVIER, & D. S. Thiebaux (Ed.), *Artificial Intelligence* (Vol. 278). Australia. doi:https://doi.org/10.1016/j.artint.2019.103183

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

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

Ghosh, S. K. (2022). Building more performant large scale. *Universidad de Cincinnati. OhioLINK*, 215. Obtenido de

https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=ucin1669722110080274&disposition=inline

Gómez, C. E. (Marzo-Junio de 2019). Estudos críticos sobre algoritmos: um ponto de encontro entre engenharia e ciências sociais? *Revista Iberoamericana de Ciencia, Tecnología y Sociedad-CTS, 14*(41), 215-232. Obtenido de https://www.redalyc.org/articulo.oa?id=92460273013

Hans Delfs, H. K. (2019). Introduction to Cryptography, Principles and Applications. Segunda edición. En H. Mirjalili, *Introduction to Cryptography* (págs. 1-2). Switzerland: Springer & Business Media.

Joonsang Baek, S. R. (26 de 12 de 2021). Information Security and Privacy. En S. Nature, & S. Ruj (Ed.). Suiza.

Julio C. Mendoza-Tello, A. A.-B.-C. (2020). *Blockchain y el mecanismo de consenso a través de la función hash SHA-256 [CICIC, Univesidad Central del Ecuador].* Conference Paper, Quito, Ecuador.

Kérly Winques, R. R. (2022). Dos Meios às Mediações (Algorítmicas): Mediação, Recepção e Consumo em Plataformas Digitais. *Matrizes, 16*(2), 151-172. Obtenido de https://doi.org/10.11606/issn.1982-8160.v16i2p151-172

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (17 de abril de 2002). *Art. 36*.

Liandeng Li, J. F. (2020). Efficient AES implementation on Sunway TaihuLight supercomputer: A systematic approach. En *Computing, Journal of Parallel and Distributed* (págs. 178-189). Tsinghua. Obtenido de doi.org/10.1016/j.jpdc.2019.12.013

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

Mahmoud, M. S. (2022). ISO/IEC 27001 Information security management systems. *ISO*, 19. Obtenido de https://www.iso.org/

Maldonado, J. (2020). Criptografía de Curva Elíptica (ECC), el corazón de la seguridad en el mundo cripto y de Internet. *COINTELEGRAPH*, 5.

Marrero Travieso, Y. (2019). La criptografia como elemento de la seguridad informática. *ACIMED*, 11. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

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

Mouna Bedoui, H. M. (2021). An improvement of both security and reliability for AES implementations. En K. Saud, *Journal of King Saud University – Computer and Information Sciences* (Vol. 13, págs. 9844-9851). Saudi Arabia. Obtenido de doi.org/10.1016/j.jksuci.2021.12.012

Nathaly Nieto Ramirez, R. N. (2019). Implementación hardware de la función Hash SHA3-256 usando una. *Revista Chilena*, 43-51.

Nelson, J. (2016). The Development of a Human Operator Informatic Model (HOIM) incorporating the Effects of Non-Invasive Brain Stimulation on Information Processing while performing Multi-Attribute Task Battery (MATB). *Wright State University*, 172. Obtenido de http://rave.ohiolink.edu/etdc/view?acc_num=wright1461066834

Rajeev Kumar, R. C. (2022). Advancements in multimedia security in the context of Artificial Intelligence and Cloud Computing. *Journal of Information Security and Applications*. Obtenido de https://www.sciencedirect.com/journal/journal-of-information-security-and-applications/about/call-for-papers#advancements-in-multimedia-security-in-the-context-of-artificial-intelligence-and-cloud-computing

Rea, Á. M. (2020). Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad. *Archivo Digital UPM*, 466. Obtenido de https://doi.org/10.20868/UPM.thesis.65871.

Regina Paiva Melo MARIN, J. G. (05 de 2021). ENSINANDO CONCEITOS BÁSICOS DE CRIPTOGRAFIA NO ENSINO MÉDIO PROFISSIONAL.

Revista on line de Política e Gestão Educacional, 25(2), 1282-1296. Obtenido de https://doi.org/10.22633/rpge.v25i2.14469

Rocha, L. L. (2020). Como ser cidadão: política, globalização. *Matrizes, 14*(2), 327-332. Obtenido de https://www.redalyc.org/journal/1430/143066518004/143066518004.pdf

Rodríguez Sabiote, C., Lorenzo Quiles, O., & Herrera Torres, L. (2018). Teoría y práctica del análisis de datos cualitativos. *Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM*, 23.

Sánchez, A. N. (2022). Evaluación de sobrecarga por cifrado en redes multisalto para la internet de las cosas médicas. *CICESE*, 170. Obtenido de https://cicese.repositorioinstitucional.mx/jspui/bitstream/1007/3695/1/tesis_Adrian_Neftali_Sanchez_28%20mar%202022.pdf

Santos, R. O. (2022). Algoritmos, engajamento, redes sociais e educação. (U. E. Maringá, Ed.) *Acta Scientiarum. Education, 44*. Obtenido de https://doi.org/10.4025/actascieduc.v44i1.52736

Tamara Luiza Dall Agnol Pinto, A. d. (2020). As criptomoedas e a liberdade contratual no direito privado internacional e no sistema jurídico brasileiro. *MISES: Interdisciplinary Journal of Philosophy Law and, 8*. Obtenido de doi.org/10.30800/mises.2020.v8.1325

Valencia, C. A. (2014). *Es necesario reformar el código penal, incorporando en su normatividad disposiciones que impidan la violación de la intimidad personal por los medios informáticos relacionada con los datos personales [Tesis de tercer nivel, Universidad Nacional de Loja].* Repositorio Digital . Obtenido de https://dspace.unl.edu.ec/jspui/handle/123456789/5228

Vivar, J. M. (04 de 2018). Algoritmos, aplicaciones y Big data, nuevos paradigmas en el proceso de comunicación y de enseñanza-aprendizaje del periodismo de datos. *Redalyc*, 25. doi:https://doi.org/10.26441/RC17.2-2018-A12

Zanabria, A. L. (2018). *Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información [Tesis de maestría, Universidad Ricardo Palma].* Repositorio URP, Lima. Obtenido de https://repositorio.urp.edu.pe/bitstream/handle/20.500.14138/1509/ALSAMANIEGOZ.pdf?sequence=1&isAllowed=y

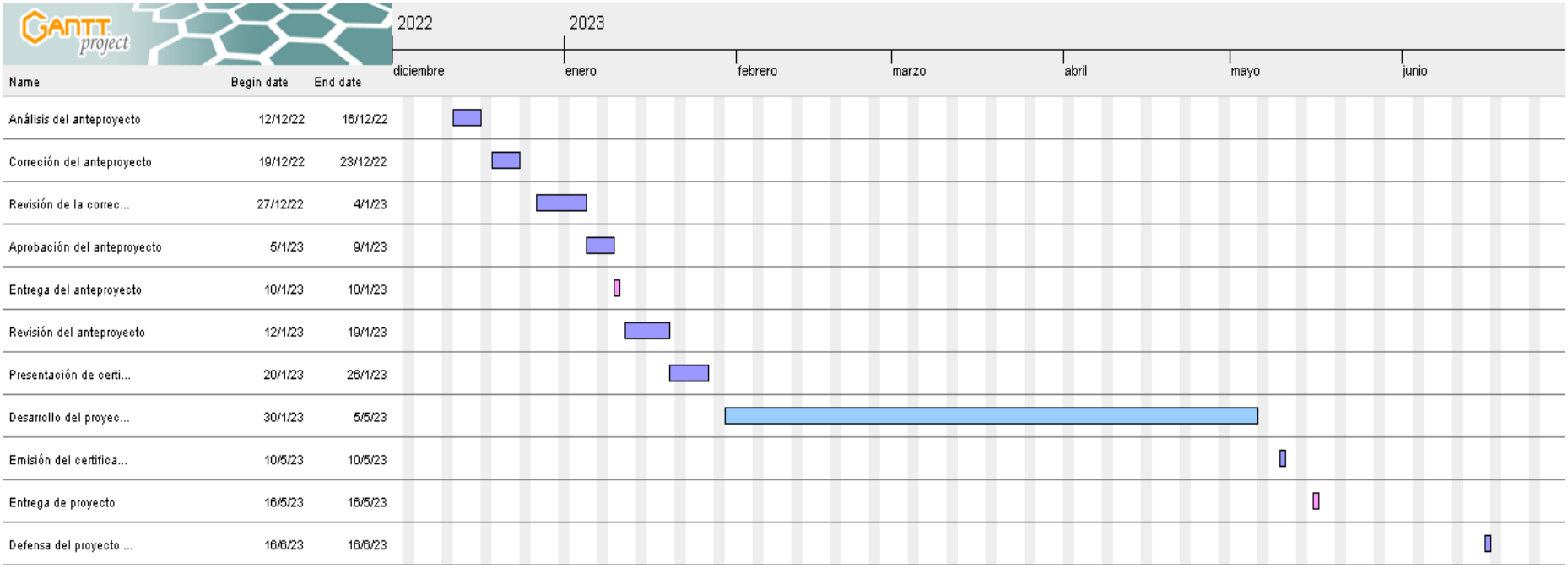
ANEXOS

ANEXO 1

Cronograma (Gantt)

Ilustración 7

Cronograma de actividades Gantt



Elaborado por: Micaela Guamán

ANEXO 2

Presupuesto Ejecutado

Presupuesto ejecutado

El desarrollo del presente proyecto se expuso el tema de investigación a quienes son asignados como pares académicos y tutor, quienes aportaran con ideas y opiniones sobre el cumplimiento de los objetivos propuestos.

Recursos:

- Laptop
- Internet
- Servicios Básicos
- Alimentación
- Transporte
- Impresiones
- Copias

Tabla 15

Presupuesto

Cantidad	Recurso	Valor	Total
1	Laptop	750	750
1	Internet	250	250
1	Servicios Básicos	100	100
1	Alimentación	200	200
1	Transporte	100	100
1	Impresiones	50	50
1	Copias	30	30
Total, del presupuesto		1480	1480

Elaborado por: Micaela Guamán

ANEXO 3

Carta de aceptación

CUERPO DE BOMBEROS GUARANDA

Oficio N.º 006 C.B.G. TH
Guaranda, diciembre 9, 2022

Ingeniera
Galuth García.
COORDINADORA UIC SOFTWARE
UNIVERSIDAD ESTATAL DE BOLIVAR

Presente.

De mi consideración:

En atención a oficio 036-2022-UIC-SOF de fecha 7 de diciembre de 2022, debo manifestar que se acepta a la señorita estudiante de la carrera de Software Guamán Manobanda Micaela Jasmin C.I, 0250053733, con el objetivo que realice el Proyecto de investigación denominado "Análisis de Algoritmos Criptográficos para la protección de datos del sistema Informático del Cuerpo de Bomberos de la ciudad de Guaranda.

Particular que comunico para los fines pertinentes.

Atentamente,

ABNEGACIÓN Y DISCIPLINA

CUERPO DE BOMBEROS GUARANDA
TALENTO HUMANO

Ing. Iván Velasco
JEFE DE TALENTO HUMANO CUERPO DE BOMBEROS GUARANDA.

ANEXO 4

Instrumentos de recopilación de datos

FACULTAD DE CIENCIAS INFORMÁTICAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

Objetivo: Conocer los riesgos y dificultades del sistema del Cuerpo de Bomberos de Guaranda, en el campo de la seguridad criptográfica y sus tecnologías informáticas.

Dirigido a: Ing. Alex Campana; desarrollador del sistema.

Entrevistador: Micaela Guamán

ENTREVISTA

SISTEMA DE CUERPO DE BOMBEROS

1. ¿Cuál es su opinión acerca de la criptografía?
2. ¿Realizó un estudio previo para poder realizar el sistema de Cuerpo de Bomberos?
3. ¿Cuál es el enfoque principal para realizar el sistema propuesto?
4. ¿Para realizar el sistema que se maneja en la institución, que aspectos se tomaron en cuenta para su desarrollo?
5. ¿En la implementación del sistema con que lenguaje de programación se trabajó para el desarrollo de la aplicación?
6. ¿Utilizó algoritmos criptográficos para el desarrollo del sistema informático?
7. ¿El sistema que fue implementado en la institución del Cuerpo de Bomberos de Guaranda cuenta con un certificado de comunicación segura?
8. ¿En las actualizaciones de parches de seguridad informática, su sistema cuenta con uno de ellos para evitar ciertas amenazas que dañen al software?
9. ¿Utiliza actualmente mecanismos de seguridad en la autenticación del manejo del sistema de Cuerpo de Bomberos?
10. ¿En las pruebas de desarrollo que se realiza en cada fase, el sistema presentó errores o fallos en su funcionalidad?

La encuesta se aplicó a los directores de cada departamento del Cuerpo de Bomberos de Guaranda, con el objetivo de recabar información acerca de la seguridad del sistema que administran.

ENCUESTA

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS INFORMÁTICAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

Objetivo: Recabar información sobre el análisis de los algoritmos criptográficos y la seguridad del sistema de Cuerpo de Bomberos de Guaranda.

Dirigido: Directores

La presente encuesta forma parte del proyecto de titulación: "Análisis de los algoritmos criptográficos"

La información proporcionada es de carácter confidencial y reservado; de manera que los resultados obtenidos serán manejados solo para la investigación.

1. **¿Tiene conocimiento previo sobre la seguridad informática?**

   Si ( )

   No ( )

2. **¿Tiene conocimiento usted que el Cuerpo de Bomberos de Guaranda cuenta con un sistema de seguridad?**

   Si ( )

   No ( )

3. **¿Usted cree que es confiable el sistema que actualmente utiliza la institución?**

   Si ( )

   No ( )

4. **¿Cuál es su nivel de confianza en la seguridad del sistema de Cuerpo de Bomberos de Guaranda?**

   Bajo ( )

   Medio ( )

   Alto ( )

5. **¿En qué tiempo considera usted que sea necesario actualizar el sistema de seguridad del Cuerpo de Bomberos de Guaranda?**

   Menos de 3 meses ( )

   Cada 6 meses ( )

   Anualmente ( )

6. **¿Conoce usted algunas aplicaciones de criptografía?**

   Firma digital ( )

   Certificados digitales ( )

   DNI Electrónico (Cédula) ( )

7. **¿Ha utilizado alguna vez una aplicación de seguridad criptográfica para proteger sus datos?**

   Si ( )

   No ( )

8. **¿Cree que la criptografía es importante para la seguridad de la información en línea?**

   Si ( )

   No ( )

9. **¿Está de acuerdo en compartir sus datos personales con terceros, considerando que cuenta con un nivel de seguridad alto (criptográfico)?**

   Si ( )

No ( )

10. ¿Qué medidas adicionales cree que se deberían tomar para garantizar la seguridad de la información?

Restringir el acceso a la información ( )

Evitar la degradación del sistema ( )

Implementar métodos seguros para el acceso a la información ( )

Clasificar la información ( )

Mantener actualizado el sistema ( )

11. ¿Qué amenaza cree usted que merece más atención en el campo de la ciberseguridad?

Filtrar información privada ( )

Obtener acceso no autorizado a un sistema ( )

Privar de acceso a cierta información ( )

ANEXO 5

Prueba del sistema ejemplo AES 256

Ilustración 8

Código de encriptación AES 256

```
public static String encrypt(String strToEncrypt) {
  try {
    byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
    IvParameterSpec ivspec = new IvParameterSpec(iv);

    SecretKeyFactory factory = SecretKeyFactory.getInstance(algorithm: "PBKDF2WithHmacSHA256");
    KeySpec spec = new PBEKeySpec(password: SECRET_KEY.toCharArray(), salt: SALT.getBytes(), iterationCou
    SecretKey tmp = factory.generateSecret(keySpec:spec);
    SecretKeySpec secretKey = new SecretKeySpec(key:tmp.getEncoded(), algorithm: "AES");

    Cipher cipher = Cipher.getInstance(transformation: "AES/CBC/PKCS5Padding");
    cipher.init(opmode: Cipher.ENCRYPT_MODE, key:secretKey, params: ivspec);
    return Base64.getEncoder()
        .encodeToString(src:cipher.doFinal(input: strToEncrypt.getBytes(charset:StandardCharsets.UTF_8
  } catch (InvalidAlgorithmParameterException | InvalidKeyException | NoSuchAlgorithmException |
    System.out.println("Error while encrypting: " + e.toString());
  }
  return null;
}
```

Elaborado por: Micaela Guamán

Ilustración 9

Código de desencriptación AES 256

```
public static String decrypt(String strToDecrypt) {
  //strToDecrypt= "tZs9P/wKkrfq2J6t+xqZfg==";

  try {
    byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
    IvParameterSpec ivspec = new IvParameterSpec(iv);

    SecretKeyFactory factory = SecretKeyFactory.getInstance(algorithm: "PBKDF2WithHmacSHA256");
    KeySpec spec = new PBEKeySpec(password: SECRET_KEY.toCharArray(), salt: SALT.getBytes(), iterationCou
    SecretKey tmp = factory.generateSecret(keySpec:spec);
    SecretKeySpec secretKey = new SecretKeySpec(key:tmp.getEncoded(), algorithm: "AES");

    Cipher cipher = Cipher.getInstance(transformation: "AES/CBC/PKCS5PADDING");
    cipher.init(opmode: Cipher.DECRYPT_MODE, key:secretKey, params: ivspec);
    return new String(bytes: cipher.doFinal(input: Base64.getDecoder().decode(src:strToDecrypt)));
  } catch (InvalidAlgorithmParameterException | InvalidKeyException | NoSuchAlgorithmException |
    System.out.println("Error while decrypting: " + e.toString());
  }
  return null;
}
}
```

Elaborado por: Micaela Guamán

ANEXO 6

Fotografías

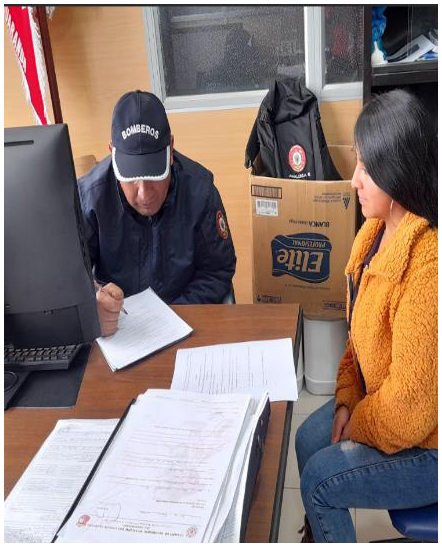
Ilustración 10

Encuestas realizadas en la institución

Fuente: Cuerpo de Bomberos de Guaranda

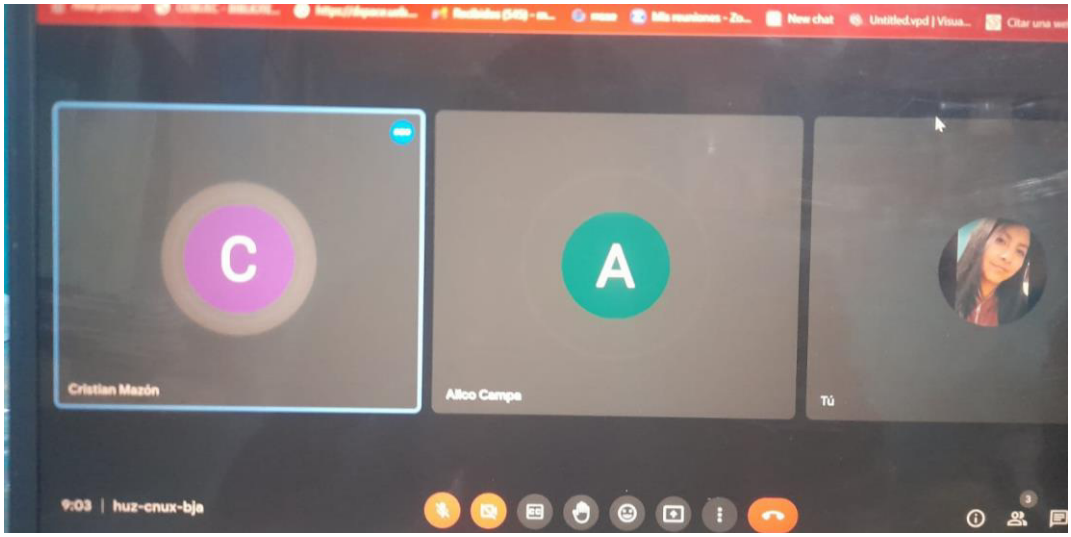
Ilustración 11

Encuestas realizadas en la institución



Fuente: Cuerpo de Bomberos de Guaranda

Ilustración 12
Entrevista



Fuente: Entrevista con el desarrollador del sistema del Cuerpo de Bomberos de Guaranda

ANEXO 7

Certificado de análisis de plagio

ING. DARWIN PAUL CARRION BUENAÑO EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

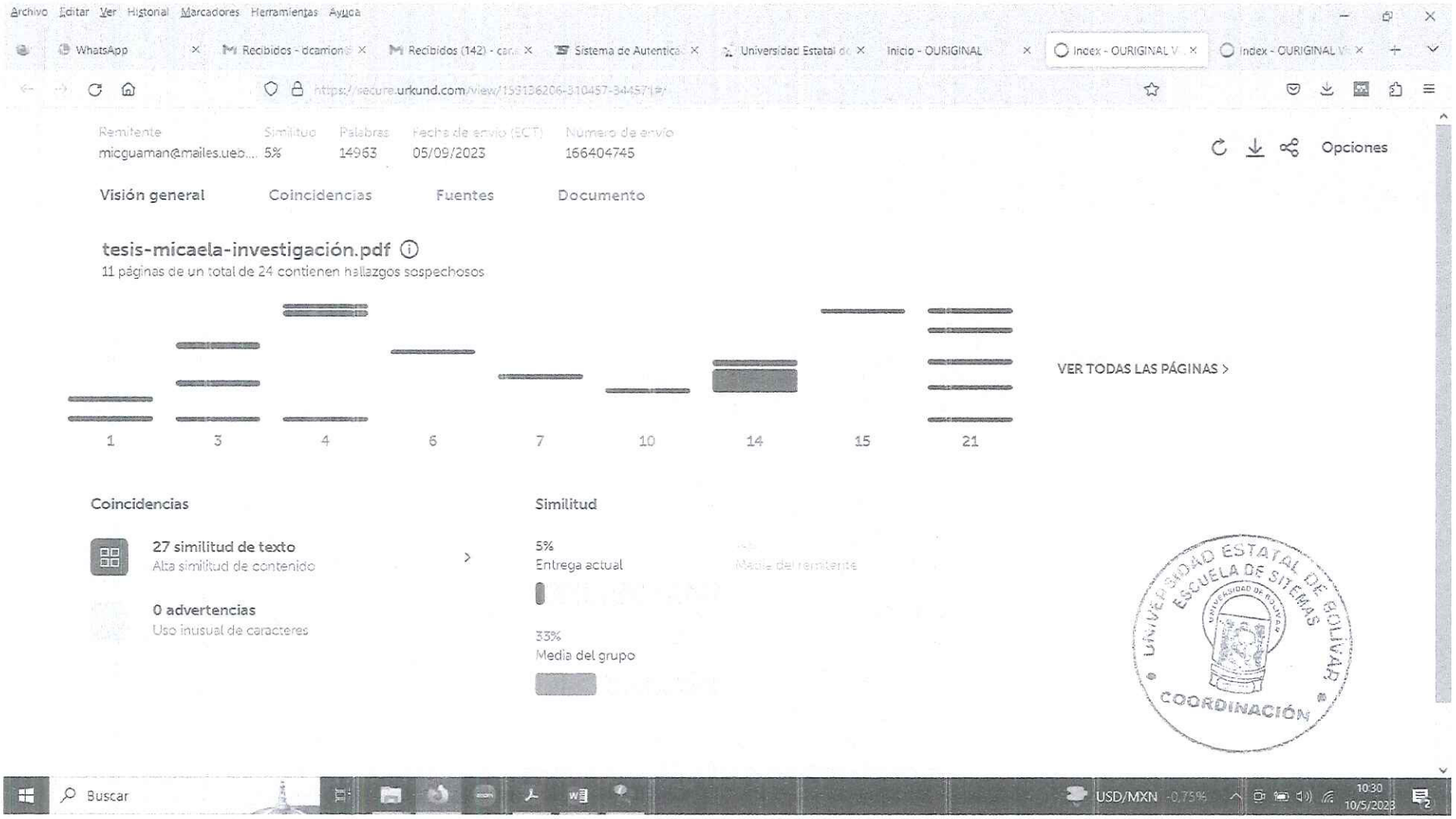
Que el trabajo de integración curricular denominado "**ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE DATOS DEL SISTEMA INFORMÁTICO DEL CUERPO DE BOMBEROS DE LA CIUDAD DE GUARANDA, AÑO 2023"**, presentado por MICAELA JASMIN GUAMÁN MANOBANDA estudiante de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta URKUND, reflejando un **porcentaje de similitud del 5%** como se puede evidenciar en el documento adjunto.

Guaranda, 10 de mayo del 2023

Atentamente,

Ing. Darwin Carrión Buenaño
Director

UNIVERSIDAD ESTATAL DE BOLÍVAR
ESCUELA DE SISTEMAS
COORDINACIÓN


Archivo Editar Ver Historial Marcadores Herramientas Ayuda
WhatsApp
Recibidos - dcamion
Recibidos (142) - car
Sistema de Autentica
Universidad Estatal d
Inicio - OURIGINAL
Index - OURIGINAL
Index - OURIGINAL
https://secure.urkund.com/view/153136206-310457-344571#/
Remitente
micguaman@mailes.ueb....
Similitud
5%
Palabras
14963
Fecha de envío (ECT)
05/09/2023
Número de envío
166404745
Opciones
Visión general
Coincidencias
Fuentes
Documento
tesis-micaela-investigación.pdf
11 páginas de un total de 24 contienen hallazgos sospechosos
1
3
4
6
7
10
14
15
21
VER TODAS LAS PÁGINAS >
Coincidencias
27 similitud de texto
Alta similitud de contenido
0 advertencias
Uso inusual de caracteres
Similitud
5%
Entrega actual
Media del remitente
33%
Media del grupo
UNIVERSIDAD ESTATAL DE BOLÍVAR
ESCUELA DE SISTEMAS
COORDINACIÓN
Buscar
USD/MXN -0,75%
10:30
10/5/2023