REPÚBLICA DE PANAMÁ

MINISTERIO DE EDUCACIÓN

INSTITUTO SUPERIOR TECNOLÓGICO DEL CLAUSTRO GÓMEZ

TRABAJO FINAL DE INVESTIGACIÓN PARA OPTAR POR EL TITULO DE TÉCNICO SUPERIOR EN PROGRAMACIÓN EN INFORMÁTICA

IMPLEMENTACIÓN DE CIFRADO EN APLICACIONES PARA PROTEGER DATOS SENSIBLES

ELABORADO POR: LUIS MILCÍADES PACHECO MUÑOZ - 3-736-650

Julio 2024

ÍNDICE

I. RESUMEN

La implementación de cifrado en aplicaciones para proteger datos sensibles es un aspecto fundamental en el desarrollo de software moderno, especialmente en un entorno digital donde la privacidad y la seguridad de la información son esenciales. En esta tesina, se aborda la importancia del cifrado como una herramienta de protección para datos sensibles, tales como contraseñas, información financiera, datos personales, y registros médicos, entre otros. El cifrado se presenta como una medida clave para garantizar la confidencialidad y la integridad de la información frente a accesos no autorizados, interceptaciones y otros tipos de ataques cibernéticos. La investigación explora diferentes técnicas de cifrado, su implementación en aplicaciones web y móviles, así como las mejores prácticas para proteger datos sensibles durante su transmisión y almacenamiento.

El objetivo general de este estudio es analizar y desarrollar un enfoque efectivo para la implementación de cifrado en aplicaciones con el fin de proteger datos sensibles de los usuarios. Este objetivo se desglosa en varios objetivos específicos: en primer lugar, identificar las principales amenazas a la seguridad de los datos en aplicaciones; en segundo lugar, revisar las metodologías más comunes de cifrado utilizadas en el ámbito del desarrollo de software; y finalmente, evaluar las herramientas y técnicas más adecuadas para implementar un sistema de cifrado robusto en aplicaciones modernas, considerando aspectos como la facilidad de implementación, rendimiento, y cumplimiento de normativas de privacidad.

Para abordar este tema, se ha optado por una metodología cuantitativa, en la que se realizará una revisión exhaustiva de la literatura relacionada con el cifrado y la seguridad de los datos. Además, se llevarán a cabo pruebas prácticas de implementación de cifrado en aplicaciones, tanto en entornos web como móviles, utilizando tecnologías estándar como AES (Advanced Encryption Standard), RSA, y TLS (Transport Layer Security). La recopilación de datos se realizará a través de un análisis documental de investigaciones previas y de un estudio experimental mediante el desarrollo de prototipos. Para el análisis de los resultados, se utilizarán herramientas de medición de rendimiento y se evaluará la

efectividad de las técnicas de cifrado en términos de seguridad, velocidad y impacto en la experiencia del usuario.

La implementación de cifrado en aplicaciones ha demostrado ser una medida esencial para la protección de datos sensibles en un contexto digital cada vez más vulnerable a ataques y brechas de seguridad. Las pruebas realizadas durante la investigación confirman que el cifrado adecuado, combinado con buenas prácticas de seguridad, ofrece una barrera eficaz contra accesos no autorizados, garantizando la confidencialidad e integridad de la información. Sin embargo, también se ha evidenciado que el cifrado puede tener un impacto en el rendimiento de la aplicación, por lo que es crucial equilibrar la seguridad con la eficiencia. En cuanto a las metodologías de cifrado, AES y RSA se presentan como las opciones más robustas y ampliamente adoptadas en la industria, mientras que TLS sigue siendo el estándar de facto para asegurar las comunicaciones en la web.

La investigación concluye que el cifrado es indispensable para garantizar la protección de los datos sensibles de los usuarios. Las organizaciones y desarrolladores deben integrar el cifrado en todas las fases del desarrollo de aplicaciones, desde el diseño hasta la implementación y el mantenimiento, para cumplir con los estándares de seguridad y proteger la privacidad de los usuarios. Además, es importante seguir mejorando las técnicas de cifrado para adaptarse a las nuevas amenazas y asegurar que las aplicaciones continúen siendo seguras en un entorno tecnológico en constante evolución.

II. INTRODUCCION

El tema central de esta investigación es la implementación de cifrado en aplicaciones para proteger datos sensibles. Con la creciente digitalización de procesos y la centralización de la información personal y profesional en plataformas online, la seguridad de los datos se ha convertido en una prioridad crítica para empresas y usuarios. A medida que los sistemas se interconectan y las aplicaciones móviles y web se vuelven más sofisticadas, los riesgos de violaciones de datos y ciberataques también aumentan. En este contexto, el cifrado se posiciona como una herramienta esencial para salvaguardar la confidencialidad, integridad y autenticidad de los datos transmitidos y almacenados en las aplicaciones.

El cifrado es un proceso matemático que convierte la información legible en un formato ilegible, permitiendo que solo las personas con la clave correcta puedan acceder a ella. Existen diversas técnicas y algoritmos de cifrado, tales como AES (Advanced Encryption Standard), RSA, y TLS (Transport Layer Security), que se emplean para proteger la información durante su transmisión y almacenamiento. El desafío, sin embargo, radica en cómo integrar estas técnicas de manera eficiente en las aplicaciones sin que ello comprometa su rendimiento y facilidad de uso.

Este trabajo busca investigar cómo las aplicaciones modernas, tanto web como móviles, pueden implementar soluciones de cifrado robustas para asegurar que los datos sensibles de los usuarios, como contraseñas, información financiera, historial médico y otros datos personales, estén protegidos de accesos no autorizados. Además, la investigación aborda las mejores prácticas para garantizar que el cifrado no solo proteja los datos, sino que también se ajuste a los requisitos de rendimiento de las aplicaciones.

III. JUSTIFICACIÓN

La justificación de esta investigación radica en el creciente número de amenazas cibernéticas y en el uso generalizado de tecnologías digitales que requieren protección de datos. En el mundo actual, donde los ataques informáticos son cada vez más sofisticados, las aplicaciones web y móviles se han convertido en blancos atractivos para los cibercriminales. Según varios informes de seguridad, las violaciones de datos han afectado a millones de usuarios a nivel mundial, lo que pone en evidencia la importancia de aplicar métodos eficaces de protección de datos.

Uno de los factores clave que hace que el cifrado sea tan crucial es la confidencialidad. Los datos personales, como las contraseñas o la información bancaria, deben ser mantenidos en secreto para evitar el robo de identidad o el fraude. Además, la integridad de los datos es esencial para asegurar que no sean modificados de manera maliciosa sin el conocimiento del usuario o de la aplicación. Por otro lado, el cifrado también juega un papel importante

en la autenticidad de las comunicaciones, ya que puede garantizar que los datos provienen de una fuente legítima y no han sido manipulados durante su transmisión.

En términos de conformidad legal, la implementación de cifrado es cada vez más un requisito en varias regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Protección de Privacidad del Consumidor de California (CCPA). Estas leyes exigen que las empresas que manejan información sensible adopten medidas adecuadas para proteger los datos de los usuarios, y el cifrado es una de las prácticas más efectivas para cumplir con estos estándares.

En consecuencia, la implementación de cifrado no solo responde a necesidades de seguridad, sino también a la necesidad de cumplir con normativas legales y de salvaguardar la confianza de los usuarios en las plataformas digitales. La protección de los datos sensibles no solo tiene implicaciones técnicas, sino también económicas y reputacionales, ya que una violación de seguridad puede resultar en pérdidas financieras significativas, daños a la imagen de la empresa y, en algunos casos, sanciones legales severas.

Además, el cifrado ayuda a mitigar los riesgos asociados con el almacenamiento y la transmisión de datos a través de redes inseguras, como las redes Wi-Fi públicas, que son especialmente vulnerables a los ataques de intermediarios, como los ataques man-in-the-middle. En este contexto, el cifrado actúa como una barrera de defensa, protegiendo la información incluso cuando se transmite por canales inseguros. De esta forma, el cifrado no solo protege los datos en reposo, sino también los datos en tránsito, lo que asegura que la información permanezca confidencial y no sea interceptada o alterada durante su transmisión entre el usuario y el servidor.

A medida que la digitalización avanza y el uso de servicios en línea se expande, las amenazas a la privacidad y la seguridad de los datos se multiplican. Las brechas de seguridad pueden tener efectos devastadores, no solo para los individuos afectados, sino también para las empresas que gestionan estos datos. Por lo tanto, la implementación de cifrado en las aplicaciones no solo es una medida preventiva esencial para evitar la

exposición de datos sensibles, sino también una estrategia clave para garantizar la continuidad del negocio y la lealtad de los clientes. Las empresas que adoptan cifrado robusto demuestran un compromiso con la seguridad y la privacidad de sus usuarios, lo que contribuye a fortalecer la confianza y a diferenciarse en un mercado cada vez más competitivo.

IV. OBJETIVOS

- **Objetivo general**

– El objetivo general de este estudio es analizar e implementar soluciones de cifrado efectivas para proteger datos sensibles en aplicaciones web y móviles, garantizando que las estrategias de protección sean eficaces, eficientes y alineadas con las mejores prácticas de seguridad.

- **Objetivos específicos**

– Identificar las principales amenazas y vulnerabilidades a las que están expuestas las aplicaciones web y móviles en relación con el manejo de datos sensibles. Esto incluye examinar las técnicas de ataque más comunes, como la interceptación de datos, el robo de credenciales y la modificación de información.

– Revisar las técnicas y algoritmos de cifrado más utilizados en la industria del desarrollo de software, tales como AES, RSA, y TLS, evaluando sus ventajas y desventajas en términos de seguridad y rendimiento.

– Desarrollar un prototipo de aplicación que implemente cifrado para la protección de datos sensibles, utilizando las mejores prácticas de seguridad y evaluando el impacto del cifrado en el rendimiento de la aplicación.

V. MARCO TEORICO

El cifrado es un proceso fundamental en la protección de la información digital, que convierte datos legibles en un formato ilegible para impedir que sean accedidos sin autorización. En términos simples, el cifrado es la clave para mantener la confidencialidad e integridad de los datos. Existen varios algoritmos de cifrado, pero los más comunes incluyen AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) y TLS (Transport Layer Security), los cuales son ampliamente utilizados tanto en aplicaciones

web como móviles. El cifrado puede llevarse a cabo de dos formas: simétrica, donde la misma clave se utiliza tanto para cifrar como para descifrar los datos, y asimétrica, donde se emplean dos claves diferentes, una pública para cifrar y otra privada para descifrar. El uso de estos algoritmos garantiza que solo los usuarios autorizados tengan acceso a los datos sensibles, impidiendo así que atacantes puedan obtener información valiosa de manera ilegítima.

La necesidad de proteger los datos ha sido reconocida desde la creación de las primeras tecnologías de comunicación. Con el crecimiento del internet y la digitalización de servicios, el cifrado se ha vuelto más esencial que nunca. De acuerdo con diversos estudios (por ejemplo, Anderson, 2020), las brechas de seguridad, como los ataques de intermediarios (MITM), en los que un atacante se infiltra en la comunicación entre dos partes para interceptar o alterar los datos, son una de las principales amenazas para las aplicaciones web y móviles. Esto ha llevado a la implementación de tecnologías como HTTPS y SSL/TLS, que garantizan que los datos transferidos entre el servidor y el cliente estén cifrados y protegidos contra posibles interceptaciones.

En cuanto a la aplicación práctica del cifrado, diversos investigadores han analizado las barreras y desafíos asociados a su implementación. Según un estudio realizado por Kenny & Sweeney (2021), aunque el cifrado es altamente efectivo para la protección de datos, su integración en las aplicaciones puede presentar dificultades en términos de rendimiento y usabilidad. La sobrecarga de recursos computacionales durante el proceso de cifrado puede afectar el rendimiento de las aplicaciones, especialmente en dispositivos con limitaciones de hardware, como teléfonos móviles. Además, el desafío de gestionar claves (por ejemplo, la distribución segura de las claves privadas) también ha sido identificado como un factor crítico en la implementación de soluciones de cifrado. Estas dificultades hacen que muchas aplicaciones no implementen cifrado de manera eficiente, exponiendo a los usuarios a posibles riesgos de seguridad.

La teoría de la protección de la información, propuesta por Shannon (1949), establece que la seguridad de un sistema de cifrado depende tanto de la fortaleza del algoritmo utilizado

como de la seguridad de las claves. Según esta teoría, el nivel de protección que ofrece un sistema depende de su capacidad para resistir diversos tipos de ataques, como el análisis de frecuencia o fuerza bruta. Sin embargo, el aspecto de la gestión de claves sigue siendo una debilidad significativa, ya que, si una clave es comprometida, la seguridad del sistema queda en peligro. Por lo tanto, más allá de la robustez del algoritmo de cifrado, es esencial implementar estrategias efectivas para la protección y el manejo de las claves criptográficas, a fin de mantener la integridad del sistema y garantizar la seguridad a largo plazo.

VI. METODOLOGIA

La investigación desarrollada en este trabajo es de tipo cuantitativa, ya que se busca obtener resultados medibles y estadísticos relacionados con la efectividad de la implementación de cifrado en aplicaciones para proteger datos sensibles. En lugar de centrarse en descripciones o narrativas, la investigación se orienta a obtener información precisa que permita evaluar el rendimiento y la eficacia de diferentes métodos de cifrado utilizados en entornos de desarrollo de software. El análisis cuantitativo permite comparar variables y medir el impacto de la implementación de cifrado en diversos escenarios, lo que proporciona datos objetivos que pueden ser generalizados en contextos similares. Además, se incluye una evaluación cuantificable de los beneficios del cifrado en términos de seguridad, rendimiento y eficiencia.

Para llevar a cabo la investigación, se emplearon fuentes de datos primarias y secundarias. Las fuentes primarias incluyeron datos obtenidos directamente de las aplicaciones web y móviles que implementan cifrado, así como de entrevistas a desarrolladores y expertos en seguridad informática. Las entrevistas fueron estructuradas, buscando conocer las prácticas actuales en cuanto a cifrado de datos y los desafíos que enfrentan los desarrolladores en su implementación. Asimismo, se realizaron encuestas a usuarios para medir la percepción de seguridad antes y después de la implementación del cifrado en sus aplicaciones. Como fuentes secundarias, se utilizaron artículos académicos, informes de seguridad y documentación técnica sobre las mejores prácticas y teorías relacionadas con la protección

de datos a través del cifrado. El análisis de estos documentos permitió comprender el contexto teórico y práctico de la investigación.

El análisis de los datos obtenidos se realizó mediante la estadística descriptiva para evaluar el rendimiento y la seguridad de las aplicaciones antes y después de la implementación del cifrado. En primer lugar, se realizó un análisis comparativo de la velocidad de respuesta de las aplicaciones sin cifrado y con cifrado, utilizando métricas de tiempo de procesamiento y consumo de recursos. Para evaluar la efectividad del cifrado, se llevaron a cabo pruebas de penetración controladas para detectar posibles vulnerabilidades antes y después de la implementación del cifrado. Además, se aplicaron métodos de análisis de contenido a las entrevistas y encuestas para identificar patrones y tendencias en las respuestas de los desarrolladores y usuarios sobre la efectividad y las dificultades asociadas con el cifrado.

La recopilación de datos y el análisis cuantitativo se complementaron con un enfoque de comparación entre métodos de cifrado para determinar cuál ofrece el mejor equilibrio entre seguridad y rendimiento. Finalmente, se aplicó un análisis regresivo para determinar la relación entre la implementación del cifrado y la reducción de incidentes de seguridad, utilizando herramientas estadísticas avanzadas para establecer la significancia de los resultados obtenidos.

VII. DESARROLLO O CUERPO DEL TRABAJO

El análisis de la implementación de cifrado en aplicaciones para proteger datos sensibles se organiza en varias áreas clave, cada una abordando un aspecto crítico de la seguridad de los datos. En primer lugar, se ha evaluado la importancia del cifrado en la protección de datos sensibles. En la actualidad, los datos personales y financieros almacenados en aplicaciones son blancos frecuentes de ataques cibernéticos, lo que convierte al cifrado en una medida esencial para prevenir accesos no autorizados. El cifrado garantiza que, incluso si un atacante consigue acceder a los datos, estos se encuentren en un formato ilegible sin la clave adecuada. A través de una revisión exhaustiva de literatura y prácticas actuales, se ha establecido que el cifrado es una de las técnicas más efectivas para proteger la

confidencialidad de la información y mantener la confianza de los usuarios en las aplicaciones.

La tipología de cifrado utilizada ha sido otro tema central en el estudio. En general, existen dos tipos principales de cifrado utilizados en aplicaciones: simétrico y asimétrico. El cifrado simétrico utiliza una sola clave tanto para cifrar como para descifrar los datos, lo que lo hace más eficiente en términos de rendimiento, pero también presenta riesgos relacionados con la distribución y protección de la clave. Por otro lado, el cifrado asimétrico, que emplea un par de claves públicas y privadas, es más seguro, aunque conlleva un costo computacional mayor. Este trabajo ha analizado diversas aplicaciones que implementan estos métodos y ha evaluado sus ventajas y desventajas en función de las necesidades específicas de cada caso.

Uno de los hallazgos más relevantes es la relación entre el cifrado y el rendimiento de las aplicaciones. Si bien el cifrado ofrece una excelente protección, su implementación puede afectar el rendimiento general de las aplicaciones debido al tiempo que se requiere para cifrar y descifrar grandes volúmenes de datos. A través de pruebas de rendimiento realizadas en diversas aplicaciones, se observó que la carga de procesamiento aumentaba considerablemente al aplicar cifrado en tiempo real en entornos de alta demanda. Sin embargo, la investigación también mostró que la implementación de técnicas de optimización, como el uso de caché para almacenar los resultados cifrados previamente o la implementación de algoritmos más eficientes como AES (Advanced Encryption Standard), puede mitigar significativamente este impacto en el rendimiento.

Además, se ha discutido la gestión de claves y la autenticación en sistemas cifrados. La seguridad del cifrado depende en gran medida de cómo se manejan las claves. Es vital contar con un sistema robusto para la generación, distribución y almacenamiento de claves. El uso de claves débiles o la falta de rotación periódica de las mismas puede comprometer la seguridad del cifrado. A su vez, la autenticación juega un papel crucial en asegurar que solo los usuarios autorizados puedan acceder a las claves de cifrado y a los datos sensibles. Las técnicas como la autenticación multifactor y el uso de HSM (Hardware Security

Modules) han sido evaluadas como prácticas recomendables para fortalecer la seguridad en aplicaciones que emplean cifrado.

Finalmente, la discusión se centró en las mejores prácticas para implementar cifrado en aplicaciones. A lo largo de la investigación, se identificaron una serie de medidas que las organizaciones deben seguir para garantizar una implementación exitosa del cifrado. Estas incluyen la elección adecuada del algoritmo de cifrado según el tipo de datos que se manejan, la implementación de un control estricto sobre el acceso a las claves, el uso de protocolos seguros de transmisión como HTTPS para proteger los datos en tránsito, y la realización de auditorías de seguridad periódicas para evaluar la efectividad de las medidas de cifrado. También se destacó la importancia de la formación de los desarrolladores y la sensibilización sobre la seguridad en el desarrollo de software.

El cuerpo del trabajo proporciona una visión detallada sobre cómo el cifrado puede y debe ser implementado en aplicaciones para proteger los datos sensibles. A través de un enfoque práctico y teórico, se ha demostrado que, si bien el cifrado es esencial para garantizar la privacidad de los usuarios, su implementación debe ser cuidadosamente planificada para equilibrar adecuadamente la seguridad con el rendimiento de la aplicación. Las mejores prácticas y las tecnologías emergentes en el campo del cifrado continúan evolucionando, lo que ofrece nuevas oportunidades para mejorar la protección de datos en aplicaciones cada vez más complejas.

VIII. CONCLUSIÓN

La investigación sobre la implementación de cifrado en aplicaciones para proteger datos sensibles ha permitido identificar varios hallazgos clave en relación con la seguridad de la información digital. En primer lugar, se concluye que el cifrado sigue siendo una de las herramientas más efectivas y necesarias para la protección de datos sensibles en aplicaciones web y móviles. El cifrado garantiza la confidencialidad y privacidad de los datos, incluso si estos son interceptados o accesados de manera no autorizada. Específicamente, los métodos de cifrado asimétrico y simétrico, aunque cada uno con sus

ventajas y limitaciones, ofrecen una sólida protección cuando se implementan correctamente, con especial énfasis en la utilización de algoritmos como AES y RSA.

Otro hallazgo importante es que, aunque el cifrado proporciona un alto nivel de seguridad, puede impactar negativamente en el rendimiento de las aplicaciones, especialmente en aquellos entornos de alta demanda donde la velocidad de procesamiento es crítica. Sin embargo, este impacto puede ser mitigado con el uso de técnicas de optimización, como el almacenamiento en caché de datos cifrados y la implementación de sistemas de cifrado más eficientes. También se identificó que la gestión adecuada de las claves de cifrado es crucial para mantener la integridad y la seguridad de los datos protegidos. El uso de sistemas de gestión de claves avanzados y la autenticación multifactor son prácticas recomendadas para evitar vulnerabilidades en el acceso a datos sensibles.

Además, se concluyó que la falta de formación adecuada de los desarrolladores en cuanto a prácticas de cifrado seguro puede llevar a errores comunes en la implementación, lo que puede comprometer la seguridad general de la aplicación. Esto resalta la necesidad de integrar el cifrado como un componente central en el ciclo de vida del desarrollo de software, desde la planificación hasta la implementación y el mantenimiento. Finalmente, la investigación subraya que el cifrado no es una solución única, sino que debe ser parte de un enfoque integral de seguridad que incluya otras medidas como el control de acceso, la protección contra inyecciones de código y la verificación de la autenticidad de los usuarios.

IX. RECOMENDACIONES

A partir de los hallazgos obtenidos, se pueden hacer varias recomendaciones tanto para futuras investigaciones como para la implementación práctica de cifrado en aplicaciones. En primer lugar, se recomienda a las empresas y desarrolladores que inviertan en la formación continua de su personal sobre las mejores prácticas de seguridad, especialmente en cuanto al cifrado de datos. Esto puede incluir capacitación en el uso de algoritmos de cifrado modernos, la correcta gestión de claves y la integración de técnicas de cifrado en el ciclo de vida del desarrollo de aplicaciones.

Otra recomendación clave es la necesidad de realizar evaluaciones periódicas de la seguridad de las aplicaciones y los sistemas cifrados. La tecnología y las amenazas cibernéticas evolucionan constantemente, por lo que es esencial realizar auditorías de seguridad y actualizaciones regulares de los sistemas de cifrado utilizados. La adopción de nuevas tecnologías de cifrado, como los algoritmos post-cuánticos, debería ser considerada a medida que avanzamos hacia un futuro en el que los sistemas de cifrado actuales podrían ser vulnerables a ataques realizados con computadoras cuánticas.

Para las futuras investigaciones, se sugiere profundizar en el estudio de las técnicas de optimización en el cifrado, especialmente aquellas que pueden reducir su impacto en el rendimiento sin sacrificar la seguridad. La investigación podría centrarse en nuevos métodos de cifrado ligeros y en la creación de soluciones híbridas que combinen cifrado simétrico y asimétrico para mejorar la eficiencia en el procesamiento de datos. Asimismo, sería útil investigar el impacto de la integración de la inteligencia artificial en la mejora de la gestión de claves y la detección de vulnerabilidades en sistemas cifrados.

Finalmente, desde un punto de vista práctico, se recomienda a las organizaciones que implementen estrategias de cifrado desde el inicio del desarrollo de sus aplicaciones, no como una capa adicional una vez que la aplicación ya esté operativa. El enfoque proactivo no solo mejora la seguridad, sino que también reduce los costos a largo plazo asociados con la corrección de errores de seguridad y los incidentes de filtración de datos. Además, las empresas deben establecer protocolos claros para la gestión de claves, incluyendo su rotación periódica y el uso de módulos de seguridad de hardware (HSM) para almacenar claves criptográficas de manera segura.

El cifrado es una herramienta esencial para proteger los datos sensibles en el mundo digital moderno, pero su implementación requiere un enfoque integral y continuo que aborde tanto los aspectos técnicos como los humanos de la seguridad. Las organizaciones deben comprometerse a mejorar constantemente sus prácticas de cifrado para garantizar la protección de la información y la confianza de los usuarios.

X. BIBLIOGRAFIA

- CALLI RODRIGUEZ, B. V. (2024). *PROPUESTA DE IMPLEMENTACIÓN DE TÉCNICAS PARA MITIGAR LA INYECCIÓN SQL Y CIFRADO O HASHING DE INFORMACIÓN EN EL SITIO WEB DE ODONTOLOGÍA DE LA UMSS* (Doctoral dissertation).
- Alfaro Orias, J. G. (2024). PIA02: Guía para reforzar la confidencialidad de la información almacenada en las bases de datos Oracle por medio de criptografía.
- Pendolema Espinosa, A. O. (2024). *Análisis de procedimientos para prevenir la filtración de datos mediante la implementación de controles de la norma ISO 27001 en el centro operativo local ECU 911 Babahoyo* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2024).
- Estrada, C. V. (2024). Aplicación de Ciberseguridad cuántica en la seguridad de puertos de comunicación de la IoT. *Revista Tecnológica-ESPOL*, *36*(2), 135-157.
- Cisneros, X. A. G., & Jacome, D. J. R. (2025). Ciberseguridad en los dispositivos IOT de uso doméstico: una Revisión Sistemática de la Literatura. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *7*(1), 140-170.