UNIVERSIDAD CENTRAL

VICERRECTORÍA ACADÉMICA

CARRERA INGENIERÍA EN INFORMÁTICA

IMPLEMENTACIÓN DE UN SISTEMA WEB DE GESTIÓN DE ENCRIPTACIÓN DE ARCHIVOS POR MEDIO DEL ALGORITMO AES DE CLAVE SIMÉTRICA PARA LA FEDERACIÓN ONGS DE PACIENTES COSTA RICA EN EL AÑO 2024

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERÍA EN INFORMÁTICA

ELABORADO POR:

RODOLFO VILLARREAL RIVERA

TUTOR:

LIC. JOSÉ GABRIEL CALVO QUIRÓS

SEDE CENTRAL

JULIO, 2024

Contenido

Sistema Web para la Protección de Datos Sensibles de la Federación de ONGs de Pacientes en Costa Rica 13

Capítulo I: Problema 14

Planteamiento del Problema 14

Objetivo General 15

Objetivos Específicos 15

Justificación 16

Antecedentes 17

Antecedentes Nacionales 20

Proyección 22

Alcance 22

Limitaciones 23

Capítulo II: Marco Teórico 26

Fundamentos de Criptografía 26

Criptografía Simétrica 29

Criptografía Asimétrica 31

Necesidades de Seguridad en la Información 34

Evaluación de Necesidades de Encriptación en Datos Sensibles 35

Desarrollo e Implementación de un Sistema de Encriptación 35

Fundamentos de la Seguridad de la Información 37

Principios de Seguridad para el Desarrollo de Software 42

Políticas de Seguridad y Cumplimiento Normativo 43

Evaluación de la Efectividad del Sistema de Encriptación 45

Pruebas de Penetración y Auditorías de Seguridad 45

Indicadores de Efectividad en la Seguridad de la Información 47

Criptografía Simétrica y Asimétrica 47

Criptografía Simétrica 47

Criptografía Asimétrica 49

Comparativa entre Criptografía Simétrica y Asimétrica 49

Desempeño y Seguridad 49

Casos de Uso 50

Arquitectura del Algoritmo AES 50

Modos de Operación de AES 51

Seguridad y Vulnerabilidades de AES 52

Requisitos para la Integración de AES 53

Evaluación y Validación del Sistema de Encriptación 54

Métodos de Validación 54

Indicadores de Éxito 55

Herramientas de Monitoreo y Auditoría 55

Mejora Continua del Sistema de Encriptación 56

Capítulo III: Marco Metodológico 57

Enfoque Cuantitativo 57

Métodos Cuantitativos Empleados en el Proyecto 57

Encuestas 58

Análisis Estadístico 59

Pruebas de Penetración (Penetration Testing) 59

Estudios Transversales 59

Análisis de Datos Secundarios 60

Fuentes de Información 61

Fuentes Primarias 61

Fuentes Secundarias 62

Instrumentos 65

Procesos de Recolección y Análisis 66

Capítulo IV: Análisis de Resultados 69

Estudios de Factibilidad 69

Definición de Factibilidad 69

Factibilidad Técnica 69

Definición de Factibilidad Técnica 69

Requerimientos de Hardware y Software 70

Requerimientos de Software 71
Factibilidad Operativa 73
Definición de Factibilidad Operativa 73
Capacitación del Personal 73
Factibilidad Económica 74
Definición de Factibilidad Económica 74
Costos del Proyecto 74
Análisis de Datos 77
Capítulo V: Conclusiones y Recomendaciones 84
Conclusiones 84
Recomendaciones 85
Capítulo VI: Propuesta 88
Requisitos Funcionales y No Funcionales 88
Requisitos Funcionales 88
Requerimientos No Funcionales 92
Análisis y Diseño del Sistema UML 94
Diagramas de Caso de Uso 94
Análisis e Interpretación de Casos de Uso. 96
Diagramas de Secuencia 102
Fuente: Elaboración Propia 105

Definición de Entidades y Sus Atributos 106

Interfaces del sistema 109

Referencias Bibliográficas 114

Tabla

Tabla 1 Rendimiento de un sistema con AES 26

Tabla 2. Comparativa Cifrado Homomórfico y Cifrado Basado 36

Tabla 3 Comparativa entre la Ley No. 8968 y el GDPR 40

Tabla 4 Ejemplo de las secciones informe de pruebas de penetración 46

Tabla 5 Comparación de los Algoritmos DES, 3DES y AE 48

Tabla 6 Variables o Categorías 63

Tabla 7 Requerimientos del Sistema 71

Tabla 8 Presupuesto de Software para Factibilidad Técnica 72

Tabla 9 Programa de Capacitación 74

Tabla 10 Presupuesto Unificado del Proyecto 75

Tabla 11 Mantenimiento Creación de Usuario 88

Tabla 12 Iniciar Sesión 85

Tabla 13 Subir Archivo para Encriptar 89

Tabla 14 Descargar Archivo Cifrado 89

Tabla 15 Desencriptar Archivo para Descargar 90

Tabla 16 Recuperar Contraseña 90

Tabla 17 Gestión de Usuarios (Administrador) 91

Tabla 18 Logs del Sistema 91

Tabla 19 Ingresar al Sistema de Encriptación 96

Tabla 20 Subir Archivo para Encriptar 97

Tabla 21 Descargar Archivo Cifrado 95

Tabla 22 Desencriptar Archivo para Descargar 99

Tabla 23 Recuperar Contraseña 97

Tabla 24 Gestionar Usuarios (Administrador) 100

Figuras

Figuras 1. Proceso de cifrado y descifrado 28

Figuras 2. Diagrama del proceso de cifrado y descifrado 27

Figuras 3. Cifrado y descifrado con AES en Python PyCryptodome 32

Figuras 4. Tres principios básicos de la seguridad de la información 39

Figuras 5. Cómo trabaja la doble autenticación 37

Figuras 6. Proceso de cifrado 51

Figuras 7. Comparativa de los modos de operación CBC y GCM 52

Figuras 8. Prevención del movimiento lateral con microsegmentación 53

Figuras 9. Guía de Observación para Evaluación de Interacción con el Sistema 68

Figuras 10. Distribución de Edad de los Usuarios 71

Figuras 11. Nivel de Conocimientos en Informática. 72

Figuras 12. Nivel de Conocimientos en Informática 77

Figuras 13 Facilidad de Registro y Acceso a la Aplicación 72

Figuras 14. Facilidad de Registro y Acceso a la Aplicación 78

Figuras 15. Calificación de la Interfaz de la Aplicación 78

Figuras 16. Dificultades al Subir o Descargar Archivos 74

Figuras 17. Facilidad para Encriptar y Desencriptar Archivos 74

Figuras 18. Facilidad para Encriptar y Desencriptar Archivos 74

Figuras 19. Velocidad de Encriptación de Archivos. 75

Figuras 20. Seguridad Percibida al Encriptar Archivos 75

Figuras 21. Intención de Recomendación de la Aplicación. 76

Figuras 22. Satisfacción General con la Experiencia en la Web App 76

Figuras 23. Acceso de Usuario 94

Figuras 24. Registro de Usuarios 94

Figuras 25. Subir Archivo para Encriptar 95

Figuras 26. Descargar Archivo Cifrado 95

Figuras 27. Recuperar Contraseña 95

Figuras 28. Gestión de Usuarios 96

Figuras 29. Ver Reportes y Logs del Sistema 96

Figuras 30. Login del Sistema 102

Figuras 31. Subir Archivo para Encriptar 103

Figuras 32. Descargar Archivo Cifrado 103

Figuras 33. Desencriptar Archivo para Descargar 104

Figuras 34. Recuperación de Contraseña 104

Figuras 35. Gestión de Usuarios (Administrador) 105

Figuras 36. Diagrama Parte I Entidad - Relación 105

Figuras 37. Figura Usuarios 106

Figuras 38. Figura Archivo 106

Figuras 39. Figura Compartir Archivo 107

Figuras 40. Figura Logs de Acceso 107

Figuras 41. Figura Encriptaciones 108

Figuras 42. Configuración del Sistema (Admin_Settings) 108

Figuras 43. Reportes Generados (Reports) 109

Figuras 44. Notificaciones del Sistema (Notifications) 109

Figuras 45. Pantalla de Inicio de Sesión 110

Figuras 46. Pantalla de Recuperación de Contraseña 111

Figuras 47. Pantalla de Registro de Usuario 111

Figuras 48. Dashboard de Usuario - Subir y Enviar Archivo Cifrado 107

Figuras 49. Pantalla de Enviar Archivo Cifrado 108

Figuras 50. Dashboard de Administrador - Gestión de Usuarios 113

Figuras 51. Encuesta sobre la Web App de Encriptación de Archivos 122

Dedicatoria y Agradecimiento

A mi madre, por ser mi mayor fuente de amor, paciencia y fortaleza. Gracias por enseñarme que el esfuerzo y la valentía son los pilares para alcanzar cualquier meta, por creer en mí incluso en los momentos más difíciles, y por mostrarme siempre el valor de la perseverancia. Sin tu apoyo incondicional, muchas veces invisible, pero siempre presente, este logro no sería posible.

A mis amigos, quienes, con su apoyo incondicional y compañía, han sido una luz en mi camino. Gracias por las risas compartidas, las palabras de ánimo y por estar presentes en cada paso de este recorrido. Sus palabras y gestos han sido una motivación constante, dándome fuerzas cuando más lo necesitaba. Aunque en ocasiones todo se llenaba de sarcasmo y bromas, vieron mi empeño y mis ganas, y su compañía me recordó que, incluso en los momentos más serios, no debemos perder el sentido del humor.

A quienes ya no están físicamente conmigo o se alejaron en el camino, ya sea porque no entendieron de qué se trataba o porque nuestros caminos tomaron direcciones diferentes. Les agradezco por lo que compartimos en su momento y por las lecciones que dejaron a su paso. Su ausencia también me ha enseñado a valorar más a quienes están, a reconocer el apoyo genuino y a comprender que cada relación tiene un propósito, aunque a veces no perdure. A aquellos que fueron parte de este viaje, aunque hoy nuestros destinos sean distintos, les deseo lo mejor y agradezco lo que aportaron a mi vida en su momento.

Por último, pero no menos importante, me agradezco a mí mismo. Agradezco mi perseverancia, la disciplina y el coraje que mantuve a lo largo de este proceso. A pesar de los momentos de duda, de la falta de claridad sobre el camino y de las veces en que todo parecía cuesta arriba, persistí hasta el final. Este logro es también una prueba de mi capacidad para mantenerme firme, incluso cuando el horizonte no era claro, y de mi disposición para enfrentar los desafíos, tanto en los momentos fáciles como en los difíciles.

Gracias a todos, y gracias a mí por no rendirme.

.

Sistema Web para la Protección de Datos Sensibles de la Federación de ONGs de Pacientes en Costa Rica

La Federación de ONGs de Pacientes de Costa Rica, desde su fundación en 2017, enfrenta riesgos de ransomware y phishing, poniendo en peligro información confidencial esencial para garantizar derechos y acceso a medicamentos.

Este proyecto desarrolla un sistema web con el algoritmo de encriptación AES, asegurando confidencialidad, integridad y disponibilidad de datos sensibles.

La metodología incluyó análisis, desarrollo, pruebas e implementación final. Los resultados demuestran una reducción significativa de vulnerabilidades y un fortalecimiento de la confianza en la organización, cumpliendo los objetivos de seguridad y normativas establecidas.

Palabras clave: encriptación AES, seguridad informática, ransomware, confidencialidad.

Abstract

The Federation of NGOs of Patients in Costa Rica, founded in 2017, faces critical risks from ransomware and phishing, endangering sensitive data essential for guaranteeing rights and medication access.

This project presents a web system using AES encryption, ensuring confidentiality, integrity, and availability of sensitive data. Features include two-factor authentication (2FA), file encryption and decryption, and user management, providing a robust and scalable solution.

The methodology covered analysis, development, testing, and implementation. Results show significant vulnerability reduction and strengthen trust in the organization, achieving security objectives and regulatory compliance.

Keywords: AES encryption, cybersecurity, ransomware, confidentiality.

.

Capítulo I: Problema

Planteamiento del Problema

La Federación ONGs de Pacientes Costa Rica maneja información sensible y confidencial, incluyendo datos personales y médicos de sus pacientes. Estos datos son cruciales para garantizar el acceso a medicamentos seguros y para monitorear el cumplimiento de los derechos de los pacientes en el ámbito de la salud y la seguridad social. Sin embargo, la creciente sofisticación de las amenazas cibernéticas, como el Ransomware y el phishing, pone en riesgo la integridad de esta información crítica.

El problema radica en la falta de políticas y prácticas de seguridad informática adecuadas en la Federación. Esta carencia se manifiesta en la ausencia de un sistema robusto de encriptación, el cual proteja los datos sensibles frente a ciberataques. Las políticas de seguridad actuales son insuficientes para enfrentar amenazas avanzadas, lo que deja a la información vulnerable a accesos no autorizados y posibles manipulaciones malintencionadas.

Entre las causas específicas de este problema se encuentran la implementación limitada de medidas de seguridad avanzadas, la subestimación del impacto potencial de los ciberataques, y la falta de actualización continua en las tecnologías de seguridad adoptadas por la organización. Estas deficiencias incrementan significativamente el riesgo de que la Federación sufra brechas de seguridad, que podrían comprometer la confidencialidad y la integridad de los datos de los pacientes.

Como consecuencia directa de estas causas, la Federación se enfrenta a la posibilidad de exposición no autorizada de información confidencial, lo que podría erosionar la confianza de los pacientes en la organización. Además, la falta de un sistema de encriptación eficaz podría resultar en sanciones legales debido al incumplimiento de normativas de protección de datos, así

como en litigios costosos, que afectarían tanto la reputación como la viabilidad financiera de la organización. La pérdida de confianza, sumada a las posibles sanciones, no solo impactaría negativamente en la capacidad operativa de la Federación, sino que también podría limitar su capacidad para colaborar con otras entidades nacionales e internacionales en la mejora de la atención a los pacientes.

Pregunta de Investigación

¿Cómo se puede implementar un sistema web para la gestión de la encriptación de archivos mediante el algoritmo AES de clave simétrica, que permite elevar los niveles de seguridad de la información en la Federación de ONGs en 2024?

Objetivo General

Desarrollar e implementar un sistema web de encriptación de archivos utilizando el algoritmo AES de clave simétrica para mejorar la seguridad y confidencialidad de los datos gestionados por la Federación ONGs de Pacientes Costa Rica en el año 2024.

Objetivos Específicos

1. Reconocer los diferentes tipos de algoritmos de encriptación de datos disponibles, con un enfoque en el algoritmo AES de clave simétrica para prevenir filtraciones de datos sensibles.
2. Enlistar las necesidades de seguridad de la información en la Federación ONGs de Pacientes Costa Rica para determinar los requisitos del sistema de encriptación.
3. Programar un sistema web que utilice el algoritmo AES para encriptar y desencriptar archivos sensibles.
4. Realizar pruebas de penetración y seguridad para evaluar la efectividad del sistema en proteger la información contra ciber amenazas.

Justificación

La implementación de un sistema web de encriptación basado en el algoritmo AES de clave simétrica es esencial para la Federación ONGs de Pacientes Costa Rica, dado que maneja información altamente sensible, incluyendo datos personales y médicos de sus pacientes. La protección de esta información es crucial no solo para garantizar el acceso seguro a medicamentos y monitorear el cumplimiento de los derechos de los pacientes, sino también para asegurar la confianza y la integridad operativa de la Federación.

El objetivo principal de este proyecto es mitigar los riesgos asociados a ciberataques como el Ransomware y el phishing, que representan amenazas constantes para la confidencialidad de los datos. Actualmente, la infraestructura de seguridad de la Federación no está preparada para afrontar estos desafíos de manera efectiva, lo que incrementa el riesgo de exposición no autorizada de información confidencial.

Al implementar un sistema de encriptación robusto, se busca prevenir la pérdida de datos, evitar sanciones legales y proteger la reputación de la organización, asegurando que la información sensible sea inaccesible para actores malintencionados. Además, este sistema contribuirá a fortalecer las políticas de seguridad informática de la Federación, ofreciendo un modelo replicable para otras organizaciones similares que operan en el sector salud.

En resumen, la implementación de este sistema es un paso necesario para garantizar la seguridad de los datos en un entorno cada vez más digitalizado y amenazado por ciberataques, asegurando que la Federación ONGs de Pacientes Costa Rica continúe siendo una entidad confiable y efectiva en su misión de atender a los pacientes.

Antecedentes

En este apartado se presentan los antecedentes nacionales e internacionales relacionados con la implementación de sistemas de encriptación para la protección de datos. La finalidad de incluir estos antecedentes es establecer un marco de referencia que permita contextualizar la relevancia del proyecto en el ámbito tecnológico actual. Además, se busca identificar experiencias previas y enfoques utilizados en la implementación de sistemas similares, lo cual contribuirá a sustentar la viabilidad y necesidad de este proyecto para la Federación ONGs de Pacientes Costa Rica

Antecedentes Internacionales

Un primer trabajo corresponde a Burgess (2022), quien realizó un análisis sobre la actividad del grupo de Ransomware Conti, destacando cómo utilizan la encriptación para bloquear los sistemas y exigir rescates. En este estudio se resalta la importancia de la implementación de sistemas de encriptación para proteger datos sensibles ante este tipo de amenazas. Los resultados indican que el Ransomware continúa siendo una amenaza global significativa para organizaciones, particularmente aquellas que manejan datos críticos (Burgess, 2022).

Análisis

Este antecedente subraya la relevancia de la encriptación como medida preventiva frente a ataques de ransomware, lo que aporta una base sólida para justificar la implementación de un sistema web con el algoritmo AES. Al proteger datos sensibles, se alinean los objetivos del proyecto con la necesidad identificada en el estudio de prevenir daños catastróficos por ciberataques.

Un segundo trabajo, realizado por Falco y Rosenbach (2022), evaluó las estrategias de ciberseguridad en organizaciones globales, subrayando el rol clave de la encriptación en la protección de infraestructuras críticas como salud y finanzas. Este estudio concluye que el uso de algoritmos robustos, como AES, es fundamental para prevenir filtraciones de datos y garantizar la seguridad de la información sensible (Falco & Rosenbach, 2022).

Análisis

La conexión directa entre la necesidad de proteger infraestructuras críticas y la elección del algoritmo AES fortalece el enfoque del proyecto, particularmente en un contexto como el de Costa Rica, donde instituciones críticas como ONGs manejan información altamente confidencial. Este trabajo refuerza la decisión técnica del algoritmo empleado.

Un tercer antecedente relevante es el trabajo de Interpol (2020), que analizó el impacto del ransomware durante la pandemia de COVID-19. Este informe reveló un aumento en el número de ciberataques dirigidos a sectores esenciales, donde la encriptación jugó un papel crucial en la protección de datos médicos y gubernamentales. El estudio destaca cómo la encriptación ayudó a mitigar los efectos de estos ataques en todo el mundo (Interpol, 2020).

Análisis

La correlación entre el aumento de ciberataques y la utilidad de la encriptación pone en evidencia la urgencia de implementar medidas similares en entornos críticos como el de las ONGs en Costa Rica. Este antecedente valida el enfoque propuesto del proyecto para mitigar riesgos similares.

Un cuarto trabajo, Herrera Silva et al. (2019), exploraron los parámetros de detección y prevención de ataques de ransomware en organizaciones internacionales. Los autores concluyeron que la implementación de encriptación avanzada es un componente esencial en la defensa contra ransomware, permitiendo a las instituciones proteger datos sensibles y evitar interrupciones costosas en sus operaciones (Herrera Silva et al., 2019).

Análisis

El estudio destaca el rol central de la encriptación avanzada como defensa proactiva, lo cual justifica el objetivo específico del proyecto de desarrollar un sistema que utilice AES, un estándar reconocido por su capacidad para prevenir accesos no autorizados.

Un quinto trabajo realizado por MunichRe (2022) estudió el riesgo cibernético global y destacó la importancia de la encriptación para proteger sistemas financieros y de salud a nivel mundial. El reporte concluye que las organizaciones deben implementar medidas de encriptación más sólidas para reducir los riesgos de ciberataques y garantizar la integridad de sus datos (MunichRe, 2022).

Análisis

El reporte refuerza la pertinencia de una solución robusta como la propuesta en este proyecto, diseñada no solo para proteger información, sino también para garantizar la resiliencia ante riesgos crecientes en sectores vulnerables.

Antecedentes Nacionales

Un sexto trabajo es el informe del Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica (MICITT) (2023), que presentó la Estrategia Nacional de Ciberseguridad 2023-2027. Este documento enfatiza la necesidad de proteger la infraestructura digital del país y propone medidas específicas para implementar soluciones avanzadas de ciberseguridad, tales como el cifrado de datos.

Análisis

Este informe se alinea directamente con la meta del proyecto, al respaldar la implementación de medidas como el cifrado de datos en instituciones críticas. La estrategia nacional actúa como marco de referencia, subrayando la importancia de proteger ONGs en el contexto local.

Un séptimo trabajo es el informe de la Contraloría General de la República (2023), que analizó los impactos de los ciberataques en Costa Rica, particularmente aquellos ocurridos entre 2022 y 2023. Se reportó que más de 45,535 personas funcionarias se vieron afectadas, y se concluyó que las organizaciones públicas deben adoptar medidas de encriptación de datos para proteger la información y mejorar la resiliencia ante futuros ataques.

Análisis

La escala del impacto de los ciberataques evidencia la necesidad urgente de sistemas de encriptación como el propuesto en este proyecto. Este antecedente sirve como caso crítico para demostrar la vulnerabilidad de los sistemas actuales y la viabilidad de la solución.

Un octavo antecedente relevante es el análisis de ISTARI Global (2022) sobre el ataque de ransomware del grupo Conti que paralizó servicios esenciales del gobierno de Costa Rica en 2022. Este ataque resaltó la urgencia de reforzar la ciberseguridad en el país, incluyendo la adopción de cifrado avanzado para proteger la información crítica de instituciones públicas y privadas.

Análisis

El ataque de Conti es un claro ejemplo de lo que podría evitarse con soluciones como la propuesta en este proyecto. Además, el caso enfatiza el impacto crítico que estas medidas tienen para mantener la operatividad de las instituciones.

Un noveno trabajo es el documento de Divergentes (2022), que examinó el ataque cibernético a Costa Rica y sus consecuencias. El informe describe cómo varios ministerios, tal como el Ministerio de Hacienda, fueron severamente afectados por el ransomware, lo que llevó al gobierno a declarar un estado de emergencia nacional.

Análisis

Este antecedente fortalece la motivación del proyecto al destacar el costo económico y social de no contar con medidas adecuadas de encriptación. La situación refleja el contexto crítico en el cual se desarrolla esta propuesta.

Un décimo trabajo es el artículo publicado por Summa Revista (2023), que documentó los 882 millones de intentos de ciberataques sufridos por Costa Rica en el último año.

Análisis

El volumen de intentos de ciberataques demuestra la vulnerabilidad del país frente a estas amenazas. Este antecedente apoya la importancia de la solución propuesta, enfocada en proteger datos sensibles de ONGs y otras instituciones clave.

Proyección

Esta investigación tiene como propósito implementar un sistema de encriptación basado en el algoritmo AES de clave simétrica, enfocado en proteger la información sensible de la Federación ONGs de Pacientes Costa Rica. El proyecto se centra en fortalecer la seguridad de los datos, asegurar el cumplimiento de normativas de protección de la información y consolidar la confianza de los usuarios en la organización.

Se espera que la implementación del sistema de encriptación reduzca significativamente los riesgos de ciber amenazas, proporcionando una solución eficaz y adaptada a las necesidades específicas de la Federación. Este proyecto aspira a validar la efectividad del sistema en un entorno real, asegurando que cumpla con los objetivos de seguridad y normatividad establecidos por la organización.

Alcance

El presente proyecto tiene como objetivo principal desarrollar un sistema web de encriptación de archivos que emplee el algoritmo AES de clave simétrica de 128 bits para garantizar la seguridad y confidencialidad de la información gestionada por la Federación ONGs de Pacientes Costa Rica. Este sistema les permitirá a los usuarios encriptar y desencriptar archivos sensibles como documentos de texto, hojas de cálculo y otros tipos de archivos que contengan información personal o médica. Se ha decidido utilizar AES de 128 bits, debido a su resistencia comprobada a ataques de fuerza bruta y su eficiencia en términos de rendimiento para

las necesidades de la organización. Además, se integrará RSA de 2048 bits para la encriptación y protección de las claves AES, asegurando una doble capa de seguridad para la transmisión de archivos. El sistema estará diseñado para proteger contra filtraciones de datos sensibles mediante la implementación de protocolos robustos que prevengan accesos no autorizados y se alineen con las mejores prácticas de seguridad informática. El enfoque de seguridad por diseño garantizará que los procesos de encriptación y autenticación de usuarios sean gestionados de manera segura y eficiente, adaptándose a los requisitos específicos de la Federación.

Además, el sistema será probado exhaustivamente a través de pruebas de penetración y seguridad para asegurar que pueda resistir ciber amenazas emergentes, como inyecciones SQL y ataques de fuerza bruta. Se utilizarán herramientas como SQLMap para verificar la seguridad de las consultas a la base de datos, y Apache JMeter para evaluar el rendimiento del sistema bajo diferentes niveles de tráfico.

El proyecto también contempla que la implementación del sistema no requiera modificaciones sustanciales en la infraestructura existente de la organización, facilitando su integración y reduciendo los riesgos asociados a la implementación de nuevas tecnologías. Asimismo, se buscará cumplir con normativas locales e internacionales de protección de datos para garantizar que la solución sea aplicable en un contexto más amplio.

El alcance del sistema no se limita a la Federación ONGs de Pacientes Costa Rica, sino que está diseñado para ser adaptable a otras organizaciones con requisitos de seguridad similares, ofreciendo una solución escalable para la protección de la información en diversos entornos.

Limitaciones

El desarrollo del sistema de encriptación enfrenta diversas limitaciones que deben ser consideradas a lo largo del proyecto. En primer lugar, el uso de herramientas open-source como

OWASP ZAP, SQLMap, JMeter, entre otras, aunque efectivas y ampliamente utilizadas en pruebas de seguridad y rendimiento, presenta algunas limitaciones en comparación con soluciones comerciales avanzadas. Estas herramientas pueden no cubrir ciertos aspectos específicos de seguridad o rendimiento que requieren un análisis más profundo. Sin embargo, se prioriza su uso por su viabilidad y compatibilidad con el proyecto, lo que podría limitar en parte el alcance de pruebas más avanzadas.

Otra limitación importante es la capacidad de las pruebas de carga y rendimiento, donde JMeter se utilizará para simular tráfico de usuarios. A pesar de ser una herramienta confiable, el entorno de pruebas puede no reflejar completamente las condiciones reales de uso en la infraestructura de la organización. Esto podría limitar la capacidad para prever todos los escenarios de uso en condiciones operativas reales, tanto para cualquier ONGs como para otras entidades que puedan utilizar este sistema en el futuro.

La falta de acceso constante a usuarios finales o personal clave de la organización, que utilizará el sistema también representa una limitación significativa. Esta restricción puede dificultar la realización de pruebas centradas en la experiencia de usuario y la funcionalidad requerida. Aunque se llevarán a cabo pruebas de usabilidad, la ausencia de retroalimentación continua o iterativa por parte de los usuarios reales podría ralentizar ajustes necesarios en la interfaz y funcionalidad del sistema, afectando su optimización final.

Para mitigar estos desafíos, se propone realizar pruebas piloto internas. Estas pruebas consisten en involucrar a usuarios internos, como compañeros de clase, profesores o amigos, quienes usarán la aplicación web simulando el rol de empleados de la ONG. Posteriormente, se les solicitará que llenen una encuesta diseñada para obtener retroalimentación sobre la usabilidad

y funcionalidad del sistema. Este enfoque permitirá identificar posibles mejoras en la experiencia de usuario antes de la implementación definitiva en el entorno de la organización.

Finalmente, la potencial restricción de acceso a ciertos datos reales durante las fases de desarrollo y pruebas también es un desafío importante. La falta de acceso constante a información real puede limitar la precisión de las pruebas en escenarios reales, lo que podría llevar al uso de datos simulados o ficticios. Aunque esto no comprometerá el diseño del sistema, afectará la validación en contextos operativos reales. A pesar de ello, el sistema será diseñado y probado para ajustarse a condiciones reales cuando se implemente completamente en el entorno de la organización.

Capítulo II: Marco Teórico

El Marco Teórico proporciona la base conceptual y el contexto necesario para comprender la implementación de un sistema de encriptación utilizando el algoritmo AES de clave simétrica en la Federación ONGs de Pacientes Costa Rica. A través de este capítulo, se abordan conceptos fundamentales como la criptografía, los tipos de algoritmos de encriptación, y la importancia de la seguridad de la información en el sector salud. Esta estructura teórica permite entender los elementos críticos de la investigación y el contexto en el cual se desarrollará.

La Federación ONGs de Pacientes Costa Rica es una organización sin fines de lucro que trabaja para mejorar la calidad de vida de pacientes mediante el apoyo, la representación y la defensa de sus derechos en el acceso a tratamientos médicos y servicios de salud. Esta federación administra información sensible de los pacientes, incluyendo datos personales, registros médicos y detalles sobre los servicios brindados. Debido a la naturaleza delicada de esta información y a las normativas de privacidad que la protegen, la implementación de un sistema robusto de encriptación se ha vuelto una prioridad para salvaguardar los datos contra posibles brechas de seguridad. Este contexto realza la importancia de diseñar un sistema que no solo cumpla con estándares de seguridad, sino que también se ajuste a las necesidades operativas y normativas de la organización.

Fundamentos de Criptografía

La criptografía es esencial para proteger la información en un mundo digital cada vez más interconectado. Se define como "el arte y la ciencia de proteger la información mediante la

transformación de datos para que solo puedan ser leídos por aquellos que poseen la clave adecuada" (García, 2018, p. 45). La criptografía no solo asegura la confidencialidad de la información, sino también su integridad y autenticidad, elementos cruciales en entornos sensibles, como el sector salud.

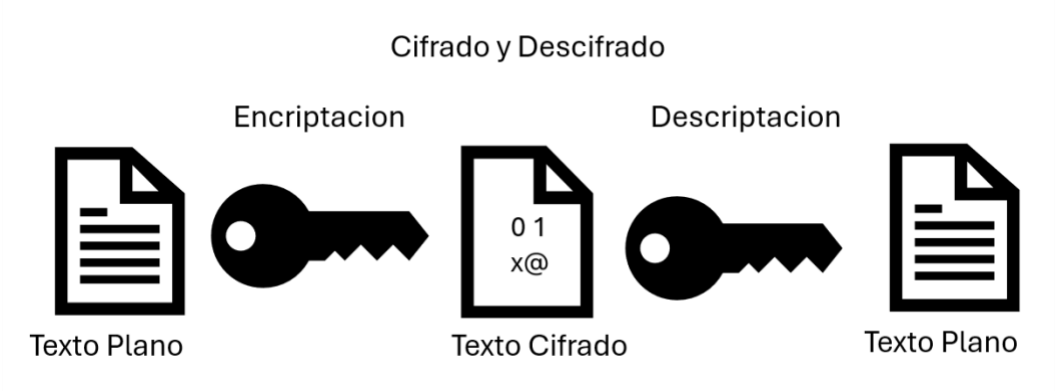
Definición de Criptografía

Según Jones y Smith (2020), la criptografía puede definirse como el arte y la ciencia de ocultar información mediante algoritmos matemáticos, que aseguran la confidencialidad, integridad y autenticidad de los datos. Este proceso involucra dos operaciones principales: cifrado y descifrado. La criptografía desempeña un papel crucial en la seguridad de la información en múltiples contextos, incluyendo las comunicaciones digitales, la protección de datos almacenados y las transacciones electrónicas. Entre sus principales aplicaciones se encuentran los sistemas de autenticación, las firmas digitales, los certificados electrónicos y los protocolos de intercambio de claves, todos ellos esenciales para la seguridad de las redes y sistemas modernos.

Criptografía simétrica. También conocida como criptografía de clave única, utiliza una sola clave para cifrar y descifrar los datos. La misma clave debe ser conocida tanto por el emisor como por el receptor, lo que implica un desafío en la distribución segura de la clave. Este método de encriptación es ampliamente utilizado, debido a su eficiencia en el procesamiento de grandes volúmenes de datos, lo que lo convierte en una opción ideal para aplicaciones donde la velocidad y el rendimiento son críticos, como en bases de datos y transmisiones en tiempo real. La criptografía no solo es una herramienta indispensable para proteger la información en el mundo digital, sino que también constituye un pilar fundamental en la confianza y la privacidad en las relaciones digitales contemporáneas.

Figura 1

Proceso de cifrado y descifrado



Nota. Esta figura ilustra el proceso de cifrado y descifrado, mostrando cómo el texto plano se transforma en texto cifrado y luego, se revierte a texto plano. Fuente Elaboración Propia

Tipos de Criptografía

La criptografía puede clasificarse en dos grandes categorías: criptografía simétrica y criptografía asimétrica. En la criptografía simétrica, tanto el emisor como el receptor utilizan la misma clave para cifrar y descifrar el mensaje, lo que hace que sea un método rápido y eficiente. Sin embargo, este enfoque requiere que ambas partes compartan previamente la clave de manera segura, lo cual puede ser un desafío en situaciones donde se necesita una distribución segura" (Navas Damas, 2023).

En contraste, la criptografía asimétrica utiliza un par de claves: una pública y una privada. La clave pública se utiliza para cifrar el mensaje, y la clave privada se emplea para descifrarlo. Este método es más seguro para el intercambio de claves, ya que solo el receptor, que posee la clave privada, puede descifrar el mensaje. Navas, M. (2019).

Tabla 1

Rendimiento de un sistema con AES

Indicador	Antes de Implementar AES	Después de Implementar AES
Tiempo de Carga de la Página (ms)	200 ms	350 ms
Uso de CPU (%)	15%	35%
Uso de Memoria (MB)	100 MB	160 MB
Tiempo de Respuesta del Servidor (ms)	150 ms	275 ms
Tamaño de los Archivos Transferidos (KB)	300KB	450 KB
Número de Solicitudes por Segundo	1000req/s	800 req/s

Nota: La tabla archivo almacena la información relacionada con los archivos subidos por los usuarios, incluyendo su ruta de almacenamiento y la clave AES encriptada asociada.

Criptografía Simétrica

La criptografía simétrica, como describe Pérez (2020), "utiliza la misma clave para cifrar y descifrar la información, lo que la convierte en un método eficiente, pero requiere que ambas partes mantengan la clave en secreto" (p. 85). Un ejemplo destacado de criptografía simétrica es

el Advanced Encryption Standard (AES), que es ampliamente utilizado debido a su balance entre seguridad y velocidad.

Algoritmo AES (Advanced Encryption Standard)

El AES es un estándar de encriptación adoptado mundialmente, diseñado para proteger datos sensibles. Como menciona Rodríguez (2018), "el AES ha sido elegido por su robustez, utilizando claves de 128, 192 o 256 bits para asegurar que los datos no puedan ser revertidos a su forma original sin la clave correcta" (p. 110).

Funcionamiento del AES. AES opera sobre bloques de datos de 128 bits y utiliza claves de 128, 192 o 256 bits para cifrar y descifrar la información. El proceso de cifrado en AES implica una serie de transformaciones que incluyen sustituciones, permutaciones y mezclas, diseñadas para garantizar que los datos no puedan ser revertidos a su forma original sin la clave correcta" (Daemen & Rijmen, 2001).

Ventajas y desventajas del AES. El AES es reconocido por su alta seguridad y eficiencia, lo que lo hace ideal para la protección de datos en redes y dispositivos personales. Sin embargo, su correcta implementación es crucial para evitar vulnerabilidades como la mala gestión de claves o errores en los vectores de inicialización, Aunque es eficiente, el uso de claves largas puede afectar el rendimiento en sistemas de procesamiento en tiempo real (Daemen & Rijmen, 2013).

La combinación de la criptografía simétrica, como el AES, y la criptografía asimétrica, como el RSA, ofrece una solución robusta y eficiente para la protección de datos, aprovechando lo mejor de ambos enfoques. Mientras que el AES es altamente eficiente para cifrar grandes

cantidades de datos gracias a su velocidad y seguridad, su principal desafío radica en la necesidad de compartir la clave de forma segura entre las partes. Aquí es donde entra en juego el RSA, un método de cifrado asimétrico que, como señala Aicad Business School (2022), permite "establecer un canal de comunicación seguro utilizando un par de claves, una pública y otra privada" (p. 2). En este esquema, el RSA se utiliza para cifrar la clave del AES, garantizando que solo el destinatario legítimo, que posee la clave privada correspondiente, pueda acceder a la clave simétrica y, por ende, descifrar los datos. De esta manera, se combina la velocidad del AES con la seguridad en la distribución de claves del RSA, logrando un sistema de cifrado híbrido que es tanto seguro como eficiente para aplicaciones en entornos de red y sistemas críticos (Centro de Ciberseguridad Industrial, 2022).

Criptografía Asimétrica

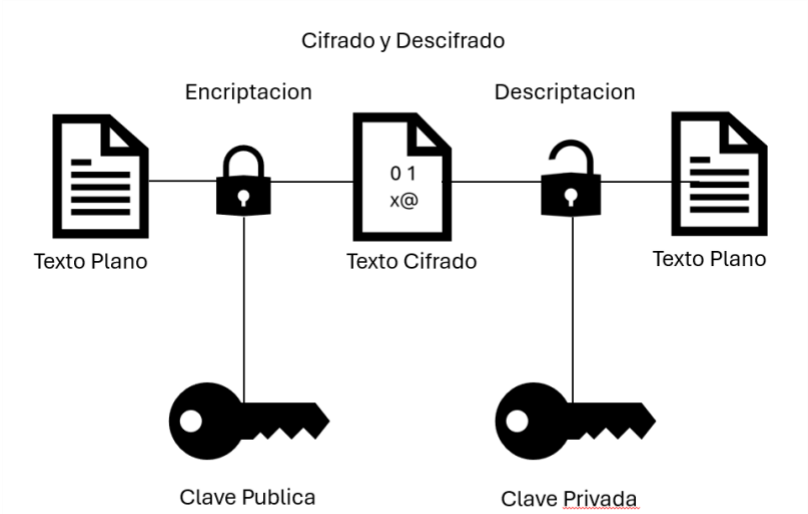
A diferencia de la criptografía simétrica, la criptografía asimétrica emplea un par de claves, una pública y otra privada, para cifrar y descifrar la información. Según Martín (2021), "este método ofrece ventajas en la gestión de claves, aunque introduce una mayor complejidad en el proceso" (p. 123). El algoritmo RSA es un ejemplo de criptografía asimétrica, ampliamente utilizado en la autenticación de datos.

Algoritmo RSA. El algoritmo RSA es popular y seguro para el cifrado y descifrado de datos, proporcionando un método seguro para transmitir información sensible a través de Internet. Aunque presenta algunas vulnerabilidades, sigue siendo utilizado en diversas aplicaciones, como las firmas digitales para autenticar la fuente de un mensaje (Splunk, 2023). RSA, introducido en 1977, por Ron Rivest, Adi Shamir y Leonard Adleman, emplea un par de claves, una pública y otra privada. Mientras que la clave privada se mantiene en secreto, la clave

pública está disponible para todos. El uso de una de estas claves para cifrar permite que la otra se utilice para descifrar, lo que hace de RSA uno de los mecanismos de cifrado más extendidos. Sin embargo, su complejidad computacional lo hace menos eficiente y consume más recursos, lo cual lo hace inadecuado para cifrar mensajes o archivos de gran tamaño (Splunk, 2023).

Figura 2

Diagrama del proceso de cifrado y descifrado



Nota. Diagrama de elaboración propia para ilustrar el proceso de cifrado y descifrado en criptografía asimétrica.

Aplicaciones de la Criptografía Asimétrica

El cifrado RSA se utiliza para proteger mensajes antes de enviarlos y para certificar su integridad, asegurando que no hayan sido alterados durante la transmisión. Es uno de los algoritmos de cifrado más utilizados en la actualidad, por ejemplo, dispositivos de marcas como Samsung, Toshiba y LG incorporan chips compatibles con RSA. Los usuarios pueden utilizar RSA de manera explícita para enviar mensajes seguros a través de servicios inseguros, o de

forma automática al acceder a sitios web seguros, donde la computadora realiza los procesos de encriptación sin intervención directa del usuario (Okta, 2024).

Sin embargo, RSA ya no se considera infalible. Aunque su complejidad matemática y el uso de números primos largos dificultan la deducción de las claves privadas, algunos hackers recurren a ataques de fuerza bruta para intentar descifrar los códigos. Para protegerse, se recomienda utilizar claves de al menos 1024 bits y de 2048 bits para datos más sensibles (Okta, 2024).

Eficiencia y Seguridad de la Encriptación Simétrica

La encriptación simétrica es conocida por su alta eficiencia, lo que la hace ideal para procesar grandes volúmenes de datos en el sector bancario. Al usar una única clave para cifrar y descifrar información, este método es significativamente más rápido que la encriptación asimétrica, que requiere el uso de dos claves. Esto permite que la encriptación simétrica sea preferida para tareas como el cifrado de bases de datos y transacciones de pago, donde la rapidez y la eficiencia son cruciales (Cryptomathic, 2020).

Sin embargo, la seguridad de la encriptación simétrica depende en gran medida de la gestión adecuada de las claves. El uso prolongado de una misma clave puede exponer datos a ataques, por lo que es esencial rotar las claves regularmente y utilizar herramientas de gestión de claves especializadas. Este enfoque garantiza que la clave permanezca segura, protegiendo así la información confidencial en aplicaciones como las tarjetas de pago EMV (Cryptomathic, 2020).

Casos de Uso

La encriptación simétrica es esencial para proteger datos sensibles en internet, como en la transferencia de información entre un navegador y un servidor. Aunque, inicialmente, se utiliza encriptación asimétrica para establecer una conexión segura, la simétrica toma el relevo para cifrar de manera eficiente grandes volúmenes de datos, asegurando la rapidez y la protección continua de la información durante la sesión (Cryptomathic, 2020).

En el ámbito financiero, la encriptación simétrica protege las transacciones con tarjetas, salvaguardando los datos personales y reduciendo riesgos de fraude. Además, facilita la verificación de la identidad del remitente de mensajes, garantizando la autenticidad de las comunicaciones. También es clave en la generación de números aleatorios y funciones hash, contribuyendo a la creación de claves seguras y a la integridad de los datos (Cryptomathic, 2020).

Necesidades de Seguridad en la Información

En organizaciones, que manejan información sensible, es necesario realizar una evaluación eficaz de los riesgos relacionados con la seguridad de los datos. Metodologías como ISO/IEC 27001 y el marco NIST SP 800-30 ofrecen enfoques prácticos para identificar vulnerabilidades y aplicar medidas de protección. Estas herramientas permiten un análisis ágil de los riesgos en los sistemas de información, garantizando la protección de los datos frente a posibles amenazas sin demoras innecesarias (Navas Damas, 2020; Plan General de la Emergencia, 2022)

Evaluación de Necesidades de Encriptación en Datos Sensibles

Para la Federación ONGs, la clasificación de datos sensibles es un paso fundamental para determinar los requisitos de encriptación. Es necesario identificar datos personales, médicos y financieros, asignando niveles de seguridad adecuados a cada categoría.

Desarrollo e Implementación de un Sistema de Encriptación

Proceso de Implementación del Algoritmo AES en Sistemas Web

La implementación del algoritmo AES (Advanced Encryption Standard) en sistemas web es clave para proteger datos sensibles y asegurar la comunicación. AES es eficiente y robusto, lo que lo convierte en una opción popular para cifrar información en aplicaciones web.

El proceso comienza con la generación de claves seguras (AES-128, AES-192 o AES-256). Estas claves se usan para cifrar datos antes de su transmisión, garantizando la confidencialidad y seguridad de la comunicación, especialmente en sesiones HTTPS. Una vez establecida la conexión, AES asegura la comunicación continua sin afectar significativamente el rendimiento.

La implementación de AES no solo protege la información, sino que también reduce riesgos de accesos no autorizados, ofreciendo tranquilidad a los responsables de TI al proteger contra posibles sanciones y daños reputacionales (NQA, 2013).

Frameworks y Lenguajes de Programación

El desarrollo web con Python se apoya en frameworks, que optimizan la creación de aplicaciones y servicios.

Flask es un microframework, que se caracteriza por su simplicidad y flexibilidad. Diseñado para proyectos de pequeño a mediano tamaño, permite a los desarrolladores construir aplicaciones web de manera rápida con un código mínimo. Esto lo hace ideal para quienes buscan una solución ligera y personalizable. Sin embargo, a medida que los proyectos crecen en complejidad, la necesidad de gestionar la estructura del proyecto y la falta de soporte nativo para la programación asíncrona pueden convertirse en limitaciones (SecureFlag, 2024).

Flask de Python conocido por su simplicidad y flexibilidad, ideal para proyectos pequeños y medianos. Su diseño minimalista permite a los desarrolladores crear aplicaciones web rápidamente y adaptar solo los componentes necesarios para cada proyecto.

Para mantener la seguridad en aplicaciones Flask, se deben implementar prácticas clave como un sistema de autenticación robusto, validación de datos de usuario, y protección contra ataques CSRF. Además, es esencial configurar cabeceras HTTPS seguras y gestionar adecuadamente contraseñas y claves API usando herramientas dedicadas, evitando incluirlas en el código fuente (Kevyn, 2024).

Figura 3

Cifrado y descifrado con AES en Python PyCryptodome

```
pip install pycryptodome

from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad

# Clave de 16 bytes (puede ser de 16, 24 o 32 bytes)
key = b'Sixteen byte key'

# Datos a encriptar (debe ser múltiplo de 16 bytes, por lo tanto, usaremos padding)
data = b'Este es un mensaje secreto!'

# Encriptación
cipher = AES.new(key, AES.MODE_CBC)  # Usando modo CBC (Cipher Block Chaining)
iv = cipher.iv  # Vector de inicialización (IV)
ciphertext = cipher.encrypt(pad(data, AES.block_size))

print("Ciphertext:", ciphertext)

# Desencriptación
cipher = AES.new(key, AES.MODE_CBC, iv=iv)  # Se usa el mismo IV para desencriptar
plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)

print("Plaintext:", plaintext)
```

Nota. La implementación es básica y puede ser utilizada como base para proyectos que requieren seguridad en el manejo de datos. Fuente: Elaboración propia.

Fundamentos de la Seguridad de la Información

La seguridad de la información se basa en la protección de la confidencialidad, integridad y disponibilidad de los datos, un conjunto de principios conocido como la triada de seguridad (Popescul, 2011). Estos principios aseguran que la información se mantenga protegida y accesible para los usuarios autorizados en cualquier contexto organizacional.

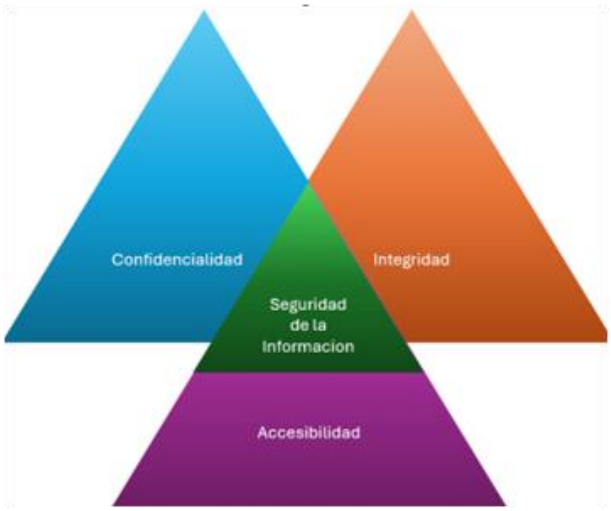
Confidencialidad. La confidencialidad implica que la información esté disponible solo para quienes tienen los permisos adecuados. Para garantizarla, se utilizan medidas como la clasificación de la información según su importancia y la implementación de contraseñas y técnicas de cifrado (Popescul, 2011). Tal como señala Popescul: "la confidencialidad de los datos es esencial para proteger la información de accesos no autorizados" (2011, p. 1340).

Integridad. La integridad se refiere a mantener la precisión y consistencia de la información, evitando alteraciones no autorizadas. Entre las prácticas más comunes para mantener la integridad se encuentran los controles de acceso y la realización de copias de seguridad. Según Popescul (2011), "la integridad es crucial para asegurar que los datos se mantengan en su forma original y que cualquier cambio esté siempre autorizado" (p. 1342).

Disponibilidad. La disponibilidad se asegura mediante el mantenimiento de una infraestructura tecnológica robusta y la implementación de copias de seguridad regulares (Popescul, 2011). Este principio garantiza que la información esté accesible para los usuarios autorizados cuando la necesiten. Como lo menciona Popescul, "la disponibilidad es esencial para que las operaciones organizacionales se mantengan sin interrupciones" (2011, p. 1343).

Figura 4

Tres principios básicos de la seguridad de la información.



Nota. La seguridad de la información se basa en mantener la confidencialidad, integridad y disponibilidad de los datos, lo cual es crucial para proteger la información sensible de las organizaciones. Fuente: Elaboración propia.

Cifrado Homomórfico

El cifrado homomórfico permite realizar cálculos sobre datos cifrados sin necesidad de descifrarlos, manteniendo la información segura durante todo el proceso (IBM, 2024). Esto es especialmente útil para el análisis de datos y la inteligencia artificial, ya que posibilita trabajar con información confidencial sin comprometer su privacidad.

Beneficios

Protección constante. Los datos permanecen cifrados incluso al ser procesados en entornos de nube pública o privada (IBM, 2024)

Compatibilidad con IA y ML. Permite usar modelos de machine learning para analizar datos sensibles sin riesgo de exposición (IBM, 2024).

Colaboración Segura. Facilita compartir y procesar datos cifrados entre organizaciones de forma segura (IBM, 2024).

Casos de Uso

Finanzas**:** Detección de fraudes sin descifrar datos financieros**.**

Salud: Análisis de datos clínicos manteniendo la privacidad de los pacientes.

Comercio. Búsquedas cifradas que protegen la privacidad de los consumidores (IBM, 2024).

Tabla 2

Comparativa Cifrado Homomórfico y Cifrado

Característica	Cifrado Homomórfico	Cifrado Basado en Atributos
Principio Básico	Una sola clave compartida entre emisor y receptor.	Permite acceso a datos encriptados basado en atributos.
Ventaja Principal	Mantiene la privacidad mientras se realizan cálculos.	Control de acceso flexible y basado en políticas.
Complejidad Computacional	Depende de la seguridad de la clave compartida.	Mayor seguridad debido a la separación de claves.
Complejidad de implementación	Alta complejidad, consume muchos recursos.	Más compleja, generalmente utilizada para intercambio de claves y autenticación.
Casos de Uso	Computación en la nube segura, análisis de datos cifrados.	Compartición de datos en entornos con múltiples usuarios.
Nivel de Seguridad	Alta seguridad, debido a la preservación del cifrado.	Seguridad basada en atributos, vulnerable si los atributos se ven comprometidos.

Nota. Cifrado Basado en Atributos. Esta técnica de encriptación permite que los datos sean cifrados y descifrados basándose en atributos específicos del usuario, como su rol dentro de una organización. (Sahai & Waters, 2005).

Integración con Sistemas Existentes. La integración de AES con sistemas web existentes puede ser compleja, especialmente si estos sistemas no fueron diseñados inicialmente

para soportar encriptación fuerte. Esto puede requerir modificaciones significativas en el código de la aplicación (Daemen & Rijmen, 2013).

Optimización del Rendimiento. Aunque AES es conocido por su eficiencia, la encriptación de grandes volúmenes de datos puede afectar el rendimiento del sistema. Es crucial optimizar la implementación para minimizar el impacto en la velocidad y la capacidad de respuesta del sistema (Schneier, 2015).

Principios de Seguridad para el Desarrollo de Software

Para garantizar la seguridad del sistema de encriptación, es esencial seguir principios de seguridad desde la fase de desarrollo del software. Estos principios incluyen la minimización de la superficie de ataque, la validación de entradas, y la implementación de controles de acceso adecuados (OWASP, 2020).

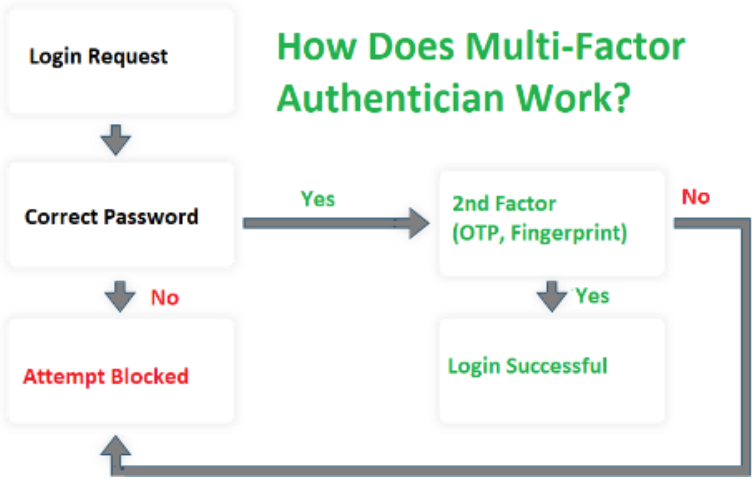
Minimización de la Superficie de Ataque. Reducir la superficie de ataque implica limitar las formas en que un atacante podría comprometer el sistema. Esto se logra eliminando funcionalidades innecesarias y restringiendo el acceso a recursos críticos (OWASP, 2020).

Validación de Entradas. La validación de entradas es crucial para prevenir ataques como la inyección de SQL y el cross-site scripting (XSS). Todas las entradas de los usuarios deben ser validadas y sanitizadas antes de ser procesadas por el sistema (Schneier, 2015).

Controles de Acceso. Implementar controles de acceso sólidos garantiza que solo los usuarios autorizados puedan acceder a las funciones y datos sensibles del sistema. Esto incluye la autenticación multifactor y la gestión de permisos basada en roles (ISO/IEC 27002:2013).

Figura 5

Como trabaja la doble autenticación



Nota. Shethi, S. (2024, agosto 21). La autenticación multifactor (MFA) explicada en 5 minutos o menos. Geekflare. Recuperado de https://geekflare.com/es/multi-factor-authentication/

Políticas de Seguridad y Cumplimiento Normativo

El cumplimiento de las normativas de seguridad es esencial para garantizar que el sistema de encriptación cumpla con las regulaciones locales e internacionales.

Cumplimiento de la Ley de Protección de Datos Personales. En Costa Rica, la Ley No. 8968 regula el tratamiento de datos personales y establece requisitos estrictos para su protección. El sistema de encriptación debe cumplir con estas normativas para evitar sanciones legales (MICITT, 2020).

Cumplimiento con Normativas Internacionales. La Federación debe cumplir con normativas internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa, que impone fuertes restricciones sobre el manejo de datos personales (GDPR, 2016).

Tabla 3

Comparativa entre la Ley No. 8968 y el GDPR

Aspecto	Ley No. 8968 (Costa Rica)	GDPR (Unión Europea)
Base legal para el procesamiento	Consentimiento y principios de proporcionalidad.	Consentimiento explícito y otras bases legales (ej. interés legítimo, contrato).
Derechos de los titulares	Derecho a acceder, rectificar y suprimir datos.	Derechos de acceso, rectificación, portabilidad, supresión
Notificación de incumplimientos	No especificado explícitamente.	Notificación obligatoria en 72 horas.
Transferencia internacional	Limitaciones en función de la protección adecuada.	Requiere garantías adecuadas (ej. cláusulas contractuales).

Nota. La información de esta tabla se basa en datos obtenidos de la Ley No. 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y el Reglamento General de Protección de Datos (GDPR).

Evaluación de la Efectividad del Sistema de Encriptación

Pruebas de Penetración y Auditorías de Seguridad

Las pruebas de penetración y las auditorías de seguridad son métodos esenciales para evaluar la efectividad del sistema de encriptación.

Pruebas de Penetración. Las pruebas de penetración, también conocidas como *pentests*, simulan ataques cibernéticos para identificar vulnerabilidades en el sistema. Este proceso es crucial para asegurar que el sistema de encriptación es resistente a las técnicas de ataque más comunes (OWASP, 2020).

Auditorías de Seguridad. Las auditorías de seguridad implican una revisión exhaustiva de la arquitectura de seguridad del sistema, incluyendo la configuración del algoritmo AES y las políticas de gestión de claves. Estas auditorías aseguran que se cumplan todas las mejores prácticas y normativas de seguridad (ISO/IEC 27001:2013).

Las auditorías de seguridad son una práctica fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos dentro de cualquier sistema, incluido nuestro proyecto basado en el algoritmo AES y políticas de gestión de claves. Estas revisiones sistemáticas evalúan todos los componentes de seguridad del sistema y buscan identificar posibles vulnerabilidades, brechas o ineficiencias que puedan ser explotadas por atacantes o causar fallos en el funcionamiento.

Tabla 4

Ejemplo de las secciones informe de pruebas de penetración

Sección	Obligatorio / Agradable de Tener	Orden en el Informe	Orden en la Redacción	Nivel de Detalle	Nivel de Información Técnica
Resumen Ejecutivo	Obligatorio	1	5	Bajo	Bajo
Hallazgos Clave	Obligatorio	2	4	Alto	Alto
Resumen del Compromiso	Obligatorio	3	1	Bajo	Bajo
Resultados Completos de Pruebas de Penetración	Obligatorio	4	2	Medio	Medio
Detalles de Vulnerabilidades	Agradable de Tener	6 (anexo)	Pre-redacción	Medio	Alto
Procedimientos Completos de Pruebas	Agradable de Tener	7 (anexo)	3	Alto	Alto
Anexo de Acrónimos	Agradable de Tener	8 (anexo)	Pre-redacción	N/A	N/A

Nota. Adaptado de Penetration Testing Plan Template. Fuente (CMGT/400 v7) (University of Phoenix, 2018).

Indicadores de Efectividad en la Seguridad de la Información

Para medir la efectividad del sistema de encriptación, se deben definir indicadores claros que permitan evaluar el desempeño del sistema en tiempo real.

Indicadores Clave de Rendimiento (KPIs). Los KPIs para la seguridad de la información incluyen métricas como el tiempo promedio para detectar (MTTD) y el tiempo promedio para responder (MTTR) a incidentes de seguridad. Estos indicadores ayudan a evaluar la eficacia del sistema en la protección de la información (NIST, 2013).

Evaluación Continua. La seguridad de la información es un proceso continuo. Es esencial realizar evaluaciones periódicas del sistema de encriptación para adaptarse a nuevas amenazas y asegurar su efectividad a largo plazo (Schneier, 2015).

Criptografía Simétrica y Asimétrica

Criptografía Simétrica

La criptografía simétrica es un método de encriptación, en el cual se utiliza la misma clave tanto para cifrar como para descifrar la información. Este tipo de criptografía es conocido por su eficiencia en la encriptación de grandes volúmenes de datos, pero presenta desafíos en cuanto a la gestión segura de las claves.

Ventajas de la Criptografía Simétrica. La principal ventaja de la criptografía simétrica es su rapidez, lo que la hace ideal para encriptar grandes conjuntos de datos en tiempo real. Ejemplos de algoritmos simétricos incluyen DES, 3DES y AES (Schneier, 2015).

Desafíos en la Gestión de Claves. Uno de los mayores desafíos en la criptografía simétrica es la distribución y gestión segura de las claves. La seguridad del sistema depende, en gran medida, de la capacidad para mantener la confidencialidad de las claves (NIST, 2013).

Tabla 5

Comparación de los Algoritmos DES, 3DES y AES

Característica	DES	3DES	AES	Nivel de Detalle
Tipo de Cifrado	Simétrico	Simétrico	Simétrico	Bajo
Tamaño de Clave	56 bits	112/168 bits	128, 192 o 256 bits	Alto
Número de Rondas	16 rondas	10, 12 o 14 rondas	Notificación obligatoria en 72 horas	Bajo
Seguridad	Vulnerable a fuerza bruta	Más seguro que DES, pero menos eficiente	Alta seguridad, estándar actual	Medio
Tamaño de los Archivos Transferidos (KB)	300KB	450 KB	450 KB	450 KB

Nota. Esta tabla muestra una comparación de los algoritmos de cifrado DES, 3DES y AES en términos de tipo de cifrado https://forum.huawei.com/enterprise/es/Introducci%C3%B3n-a-DES-3DES-y-AES/thread/667234955765366784-667212881550258176.

Criptografía Asimétrica

A diferencia de la criptografía simétrica, la criptografía asimétrica utiliza un par de claves: una clave pública para encriptar y una clave privada para desencriptar. Este método es ampliamente utilizado para la distribución segura de claves y en protocolos como SSL/TLS.

Ventajas de la Criptografía Asimétrica. La criptografía asimétrica resuelve el problema de la distribución de claves, permitiendo una comunicación segura sin necesidad de intercambiar claves de manera directa; ejemplos de algoritmos asimétricos incluyen RSA, ECC, y DSA (Rivest, Shamir & Adleman, 1978).

Aplicaciones en la Seguridad Web. La criptografía asimétrica es fundamental para la seguridad en la web, especialmente en la implementación de HTTPS para asegurar la comunicación entre clientes y servidores (NIST, 2013).

Comparativa entre Criptografía Simétrica y Asimétrica

La criptografía simétrica y asimétrica tienen sus propias ventajas y desventajas, y a menudo, se utilizan juntas en sistemas híbridos para aprovechar las fortalezas de ambos enfoques.

Desempeño y Seguridad

Mientras que la criptografía simétrica es más rápida, la criptografía asimétrica ofrece mayor seguridad en la distribución de claves. Los sistemas híbridos combinan estos dos métodos para proporcionar un equilibrio óptimo entre seguridad y eficiencia (Schneier, 2015).

Casos de Uso

En la práctica, la criptografía simétrica se utiliza para encriptar datos a gran escala, mientras que la criptografía asimétrica se emplea para la gestión segura de claves y la autenticación (NIST, 2013).

Arquitectura del Algoritmo AES

El Algoritmo de Encriptación Avanzada (AES) es un estándar de cifrado adoptado por el gobierno de Estados Unidos y ampliamente utilizado a nivel mundial. AES opera en bloques de 128 bits y puede utilizar claves de 128, 192 o 256 bits.

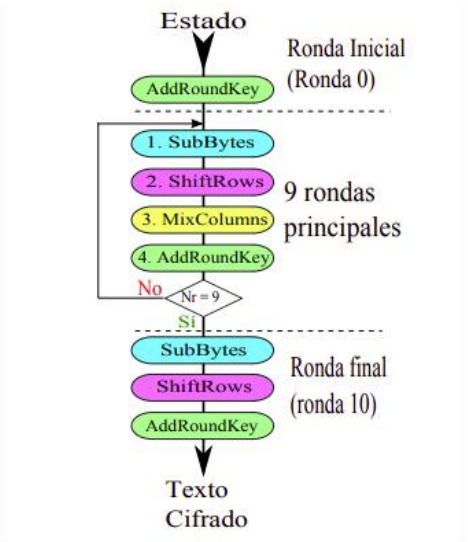
Estructura de Rondas. AES realiza una serie de transformaciones en bloques de datos a través de múltiples rondas, cuyo número depende del tamaño de la clave (10 rondas para 128 bits, 12 para 192 bits, y 14 para 256 bits) (Daemen & Rijmen, 2013).

Componentes Clave de AES. Los componentes clave del AES incluyen la sustitución de bytes, la permutación de filas, la mezcla de columnas, y la adición de una clave de ronda. Cada una de estas etapas contribuye a la robustez del algoritmo contra ataques criptográficos (Schneier, 2015).

Sustitución de Bytes (SubBytes). En esta primera etapa, cada byte del bloque de datos de entrada se sustituye por otro byte utilizando una tabla de sustitución llamada S-box (Substitution Box). La S-box es una matriz no lineal predeterminada de 16x16 que ofrece una transformación no lineal de los bytes de entrada

Figura 6

Proceso de cifrado



Nota. Este diagrama ilustra el proceso de cifrado del algoritmo AES, mostrando la ronda inicial, las 9 rondas principales, y la ronda final "Implementación del algoritmo de cifrado AES para bajo consumo sobre FPGA", por M. García Ocón, 2011, Universidad Carlos III de Madrid.

Modos de Operación de AES

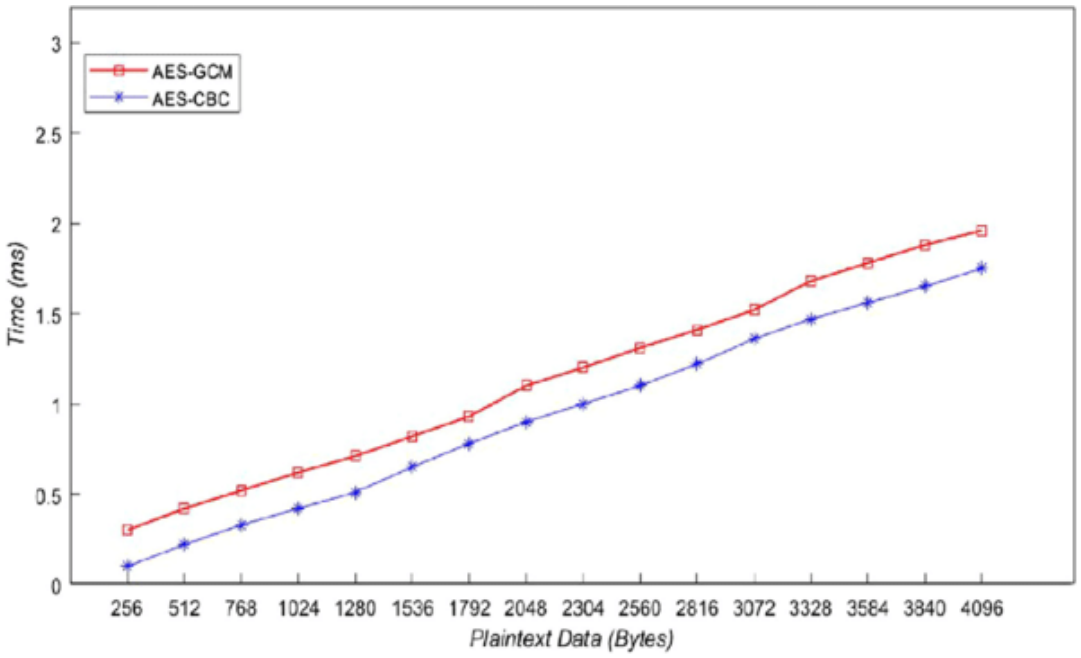
El AES puede ser implementado en varios modos de operación, cada uno de los cuales ofrece diferentes niveles de seguridad y rendimiento.

Modo CBC (Cipher Block Chaining). En este modo, cada bloque de texto plano se combina con el bloque cifrado anterior antes de ser cifrado. Esto garantiza que bloques idénticos de texto plano se cifren en bloques de texto cifrado diferentes (NIST, 2013).

Modo GCM (Galois/Counter Mode). GCM es un modo de operación que combina la encriptación con la autenticación de datos, lo que lo hace ideal para aplicaciones donde la integridad de los datos es crítica (Schneier, 2024).

Figura 7

Comparativa de los modos de operación CBC y GCM



Nota. El gráfico muestra la comparación del rendimiento entre los modos de cifrado AES-CBC y AES-GCM. Fuente "Security Analysis of Mobile Crowd Sensing Applications," por Nsikak Owoh y Manmeet Mahinderjit Singh, 2018

Seguridad y Vulnerabilidades de AES

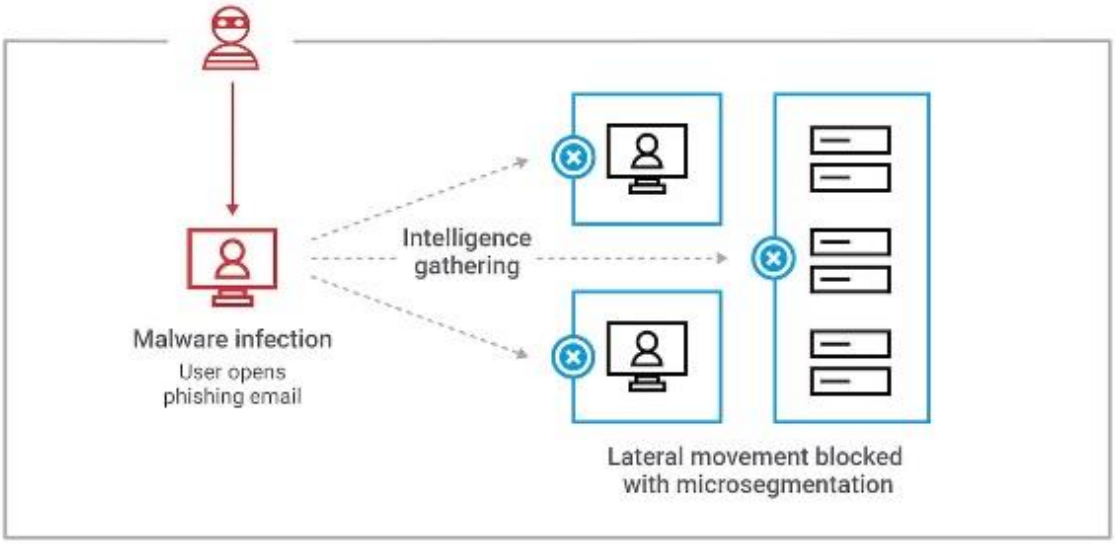
Aunque el AES es considerado altamente seguro, como cualquier algoritmo, no está exento de vulnerabilidades potenciales.

Ataques de Canal Lateral. Los ataques de canal lateral explotan la información derivada del hardware durante la implementación del AES, como el consumo de energía o el tiempo de procesamiento. Estos ataques requieren contramedidas específicas para mitigarlos (Smiliotopoulos, C., Kambourakis, G., & Kolias, C. (2024).

Riesgos en la Implementación del AES. Los detalles de implementación de un algoritmo de cifrado, como Rijndael, son fundamentales para su seguridad efectiva. Incluso un diseño matemáticamente sólido puede ser vulnerado si su implementación no se lleva a cabo con el cuidado adecuado (Daemen & Rijmen, 2002).

Figura 8

Prevención del movimiento lateral con microsegmentación



Nota. El diagrama ilustra cómo la microsegmentación puede bloquear los movimientos laterales dentro de una red después de una infección de malware. Adaptado de *Akamai Technologies* (https://www.akamai.com/es/glossary/what-is-lateral-movement).

Requisitos para la Integración de AES

Integrar AES en aplicaciones web requiere considerar varios factores, desde la arquitectura del sistema hasta la seguridad de la comunicación.

Seguridad de la Comunicación. Los certificados SSL/TLS actúan como tarjetas de identidad digital para asegurar las comunicaciones en la red, estableciendo la identidad de los sitios web en Internet, así como de los recursos en redes privadas (AWS, 2024).

Compatibilidad del Sistema. La integración de AES debe ser sencilla y compatible con los sistemas existentes, asegurando que su implementación no interfiera con los servicios actuales, lo que facilita su adopción sin comprometer la seguridad ni la eficiencia operativa (Macrium Software, 2024).

Evaluación y Validación del Sistema de Encriptación

Métodos de Validación

Una vez que el sistema de encriptación basado en AES ha sido implementado, es crucial validarlo para asegurarse de que cumple con los requisitos de seguridad.

Pruebas de Penetración. Las pruebas de penetración son una herramienta clave para identificar vulnerabilidades en el sistema de encriptación, simulando ataques cibernéticos. Estas pruebas permiten "fortalecer el sistema al identificar posibles fallos de seguridad que podrían ser explotados" (Netalit, 2024, p. 15).

Auditorías de Seguridad. Las auditorías de seguridad revisan, de manera exhaustiva, el sistema de encriptación para asegurar que se cumplen las normativas de seguridad. Estas auditorías se realizan en conformidad con normas internacionales como ISO/IEC 27001:2013, asegurando "que todos los procedimientos estén alineados con las mejores prácticas de la industria" (NQA, 2022, p. 12).

Indicadores de Éxito

Los indicadores clave de rendimiento (KPIs) son esenciales para evaluar la efectividad del sistema de encriptación en proteger la información.

MTTD y MTTR. En la gestión de la ciberseguridad, es fundamental contar con métricas claras, que permitan evaluar el rendimiento de los sistemas ante posibles incidentes. El tiempo promedio para detectar (MTTD) y el tiempo promedio para responder (MTTR) son indicadores clave para medir la efectividad de un sistema de seguridad informática en la gestión de incidentes. Según Netalit (2024), un MTTD bajo indica que el sistema puede "identificar rápidamente las amenazas", mientras que un MTTR bajo sugiere que la respuesta ante incidentes es eficiente (p. 15).

Tasa de Fallos de Seguridad. La tasa de fallos de seguridad mide la frecuencia con la que se producen brechas de seguridad en el sistema, siendo un indicador importante de su robustez. Un sistema efectivo debe mantener una baja tasa de fallos, lo que refleja "una mayor resistencia frente a ataques de ciberseguridad" (Schneier, 2015, p. 45).

Herramientas de Monitoreo y Auditoría

El uso de herramientas de monitoreo y auditoría es crucial para mantener la integridad del sistema de encriptación. Estas herramientas permiten una vigilancia continua y proporcionan alertas tempranas sobre posibles vulnerabilidades. Además, facilitan la auditoría regular del sistema, asegurando que todas las prácticas de seguridad estén actualizadas y alineadas con las mejores prácticas del sector. Según el marco ISO 27001, es importante que las auditorías verifiquen "no solo el cumplimiento de las normativas, sino también la eficacia de los controles implementados para la gestión de riesgos" (NQA, 2022, p. 30).

Conjuntamente, las auditorías permiten la detección de incidentes y la implementación de mejoras continuas, garantizando la robustez del sistema. Estas auditorías, tanto internas como externas, proporcionan una evaluación detallada de las vulnerabilidades del sistema y permiten aplicar medidas correctivas para minimizar los riesgos de seguridad.

Mejora Continua del Sistema de Encriptación

La mejora continua es fundamental para mantener la efectividad del sistema de encriptación a lo largo del tiempo. Las revisiones periódicas de las políticas de seguridad y la implementación de nuevas tecnologías son esenciales para adaptarse a las amenazas emergentes. Schneier (2015) enfatiza la importancia de ajustar constantemente los sistemas de encriptación para hacer frente a nuevas formas de ciberataques y asegurar que se mantengan robustos frente a técnicas de evasión.

Rotación de Claves y Actualización de Algoritmos:

- Implementar rotación periódica de claves y considerar algoritmos avanzados como AES-GCM para fortalecer la seguridad.

Auditorías y Pruebas Regulares:

- Realizar auditorías periódicas de seguridad y pruebas de penetración para detectar vulnerabilidades antes de que sean explotadas.

Adaptación a Amenazas Emergentes:

- Monitorear constantemente nuevos tipos de ciberataques y ajustar el sistema para prevenirlos, como técnicas de computación cuántica o canal lateral.

Monitoreo y Reportes Automatizados:

- Establecer un sistema de monitoreo continuo que registre actividades sospechosas y genere reportes para garantizar el cumplimiento de las políticas de seguridad.

Capítulo III: Marco Metodológico

Enfoque Cuantitativo

El presente proyecto adopta un enfoque cuantitativo, ya que se basa en la recolección y análisis de datos numéricos que permitirán evaluar el rendimiento y la efectividad de un sistema de encriptación. Según Hernández, Fernández y Baptista (2014), el enfoque cuantitativo "se utiliza para probar hipótesis mediante el análisis de variables, las cuales se miden de manera objetiva y precisa, con el fin de generar conclusiones basadas en datos empíricos" (p. 4).

Este enfoque es el más adecuado para este proyecto, dado que el objetivo es medir y comparar el rendimiento del sistema de encriptación en términos de tiempo de respuesta, uso de CPU y otras métricas numéricas, que reflejen el impacto de la implementación del sistema. Al utilizar herramientas de análisis de datos, como Apache JMeter, para pruebas de rendimiento y OWASP ZAP, para evaluar la seguridad, se obtendrán datos cuantificables, que permitirán realizar un análisis estadístico confiable. El enfoque cuantitativo facilita la generalización de los resultados a entornos similares, asegurando la replicabilidad y objetividad de los hallazgos.

Métodos Cuantitativos Empleados en el Proyecto

El objetivo principal de este proyecto es desarrollar e implementar un sistema web de encriptación de archivos utilizando el algoritmo AES de clave simétrica para mejorar la seguridad y confidencialidad de los datos gestionados por la Federación ONGs de Pacientes Costa Rica en el año 2024. Para lograr este objetivo, se emplearán diversos métodos cuantitativos, que permitirán evaluar la efectividad y funcionalidad del sistema. A continuación,

se describen los métodos seleccionados y cómo estos se relacionan con los Objetivos Específicos del proyecto.

Encuestas

Las encuestas son una herramienta para recopilar datos cuantitativos de los usuarios. En este proyecto, se utilizan para medir la percepción de seguridad, facilidad de uso y satisfacción general con el sistema de encriptación de archivos.

Relación con los objetivos específicos. Este método respalda el Objetivo Específico 4, que es realizar pruebas de penetración y seguridad para evaluar la efectividad del sistema en proteger la información contra ciber amenazas. Las encuestas permiten recopilar datos sobre cómo los usuarios perciben la seguridad del sistema y la facilidad de uso de la aplicación.

Experimentos

Los experimentos controlados se utilizarán para medir el impacto del algoritmo AES en el rendimiento del sistema web. Se evalúan variables como el tiempo de respuesta del servidor y el uso de recursos en condiciones controladas.

Relación con los objetivos específicos. Este método está vinculado con el Objetivo Específico 3, que es programar un sistema web que utilice el algoritmo AES para encriptar y desencriptar archivos sensibles. Los experimentos aportarán datos cuantitativos sobre el rendimiento del sistema después de la implementación del algoritmo.

Análisis Estadístico

Las técnicas estadísticas, como análisis de varianza (ANOVA) y regresión, permitirán interpretar los datos obtenidos de las encuestas y experimentos. Este análisis ayudará a identificar correlaciones entre la percepción de seguridad, rendimiento y satisfacción del usuario.

Relación con los objetivos específicos. Este método es esencial para el Objetivo Específico 4, ya que el análisis estadístico permite cuantificar la efectividad del sistema y establecer relaciones entre las variables clave, como la percepción de seguridad y los resultados de las pruebas de rendimiento y penetración.

Pruebas de Penetración (Penetration Testing)

Las pruebas de penetración simularán ataques cibernéticos para evaluar la seguridad del sistema web, midiendo la cantidad de vulnerabilidades detectadas y su criticidad.

Relación con los objetivos específicos. Este método está directamente relacionado con el Objetivo Específico 4, que busca evaluar la efectividad del sistema en proteger la información contra ciberamenazas. Estas pruebas proporcionarán datos concretos sobre la capacidad del sistema para resistir ataques externos.

Estudios Transversales

Los estudios transversales permiten examinar la experiencia de diferentes grupos de usuarios en un solo punto del tiempo. Se emplearán para comparar cómo distintos perfiles de usuarios perciben la seguridad y facilidad de uso del sistema de encriptación.

Relación con los objetivos específicos. Este método apoya el Objetivo Específico 2, que es enlistar las necesidades de seguridad de la información en la Federación ONGs de Pacientes Costa Rica para determinar los requisitos del sistema de encriptación. Ayudará a comprender cómo distintos perfiles de usuarios (según edad y conocimientos informáticos) interactúan con el sistema.

Análisis de Datos Secundarios

El análisis de datos secundarios consiste en utilizar investigaciones y estudios previos sobre encriptación y seguridad. Esto permite validar la elección del algoritmo AES de 128 bits frente a otras opciones.

Relación con los objetivos específicos. Este método está alineado con el Objetivo Específico 1, que es reconocer los diferentes tipos de algoritmos de encriptación disponibles. Comparar los resultados del proyecto con estudios anteriores ayudará a posicionar los hallazgos del proyecto en un contexto más amplio y justificar la elección de AES-128 frente a alternativas como AES-192, AES-256 o algoritmos asimétricos.

Razón para seleccionar AES-128. AES-128. Es más eficiente en términos de rendimiento, ofreciendo una encriptación rápida sin comprometer significativamente la seguridad. Es adecuado para la Federación ONGs, donde la protección de datos es esencial y el rendimiento del sistema es crítico.

Fuentes de Información

Fuentes Primarias

Las fuentes primarias proporcionan datos de primera mano sobre el objeto de estudio. Según Hernández, Fernández y Baptista (2014), "las fuentes primarias son aquellas que ofrecen información directa sobre un evento, persona o fenómeno" (p. 98). En este proyecto se emplearán fuentes primarias para obtener información directa y actual sobre temas de cifrado y ciberseguridad. Las cuatro fuentes primarias seleccionadas son:

Criptosistemas de Delgado Cascante (2011): Esta fuente describe, de manera exhaustiva, los principios de seguridad en comunicaciones y el uso de criptosistemas. Presenta análisis sobre el cifrado convencional y de llave pública, elementos esenciales para comprender y comparar las técnicas de cifrado que se evaluarán en el proyecto.

El Marco de Seguridad Cibernética (CSF) 2.0 del NIST del National Institute of Standards and Technology (2024). Este marco actualizado de NIST proporciona lineamientos específicos sobre la implementación de seguridad cibernética. Su relevancia radica en que establece estándares y prácticas en la gestión de riesgos, cruciales para el desarrollo de un sistema seguro en el proyecto.

Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review de Wadho et al. (2023). Este estudio revisa distintas técnicas y algoritmos de cifrado, analizando su efectividad frente a ataques cibernéticos. Ofrece una base comparativa de las herramientas más eficaces, aportando fundamentos técnicos valiosos para la selección de métodos en el sistema propuesto.

Costa Rica state of emergency declared after ransomware attacks de Reed (2022). La noticia detalla el impacto de ataques de Ransomware en servicios nacionales críticos. Esta fuente es clave para contextualizar la gravedad y las implicaciones de fallos en la ciberseguridad, lo cual refuerza la necesidad de un sistema de seguridad robusto en el proyecto.

Razón para utilizarlas. Se usarán fuentes primarias, porque permiten obtener información específica y directa sobre la implementación de medidas de seguridad y cifrado en tiempo real. Esto es esencial para analizar la eficiencia del sistema de seguridad desarrollado en este proyecto.

Fuentes Secundarias

Las fuentes secundarias son aquellas que interpretan o analizan fuentes primarias. Hernández, Fernández y Baptista (2014) señalan que "las fuentes secundarias analizan, interpretan o sintetizan información obtenida previamente por otros autores" (p. 100). En este proyecto, se emplearán las siguientes fuentes secundarias:

Applied Cryptography: Protocols, Algorithms and Source Code in C de Schneier (1996). Schneier explora en profundidad los algoritmos y protocolos de cifrado, proporcionando tanto el contexto histórico como el desarrollo técnico de estos métodos. Esta fuente será útil para interpretar y contextualizar los algoritmos seleccionados.

A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters de Herrera Silva et al. (2019). Este artículo revisa los parámetros de detección y prevención de ataques de Ransomware, interpretando datos de estudios previos. La

fuente permite ampliar la comprensión sobre los mecanismos de defensa en ciberseguridad, respaldando las técnicas de protección en el sistema de cifrado.

Razón para utilizarlas. Las fuentes secundarias proporcionarán el contexto teórico y técnico necesario para justificar y evaluar las técnicas de cifrado seleccionadas, permitiendo un análisis más profundo y fundamentado del desarrollo del proyecto.

Operacionalización de variables

Tabla 6

Plan de Investigación y Desarrollo para la Implementación del Sistema de Encriptación AES

Objetivos	**Método de la Investigación (Etapas y Actividades)**	**Proceso para la Recolección y Análisis de Datos**	**Fuentes de Información**
1. Reconocer los diferentes tipos de algoritmos de encriptación de datos disponibles, con un enfoque en el algoritmo AES de clave simétrica para prevenir filtraciones de datos sensibles.	- Realizar un análisis comparativo de los algoritmos de encriptación, destacando sus fortalezas y debilidades. - Seleccionar el algoritmo AES como enfoque principal y justificar su elección basada en rendimiento.	- Revisar documentación técnica y comparativa de los algoritmos de encriptación. - Utilizar software de simulación para comparar la eficiencia de cada algoritmo. - Analizar validar la elección del algoritmo AES.	A. Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación (6ta ed.). McGraw-Hill.
2. Enlistar las necesidades de seguridad de la	- Realizar entrevistas con los responsables de la	- Revisar respuestas de las entrevistas para	A. European Interagency Security

información en la Federación ONGs de Pacientes Costa Rica para determinar los requisitos del sistema de encriptación.	seguridad de la información en las ONGs. - Definir los requisitos específicos de encriptación basados en la información.	identificar las principales preocupaciones y necesidades de seguridad. - Diseñar un sistema de encriptación que cubra estas necesidades.	Forum (EISF). (2019). Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas.
3. Programar un sistema web que utilice el algoritmo AES para encriptar y desencriptar archivos sensibles.	- Diseñar y desarrollar una interfaz web amigable para el usuario final. - Implementar el algoritmo AES dentro del sistema para encriptar y desencriptar archivos.	- Utilizar herramientas de desarrollo web y bibliotecas de criptografía (como OpenSSL o PyCryptodome). - Recoger retroalimentación de los usuarios.	A. Aguilera, P. (2011). Redes seguras (seguridad informática*).* *Editex.* *B.* Delgado Cascante, G. (2011). Criptosistemas. Universidad de Costa Rica.
4. Realizar pruebas de penetración y seguridad para evaluar la efectividad del sistema en proteger la información contra ciberamenazas.	- Diseñar casos de prueba específicos para identificar vulnerabilidades en el sistema. - Ejecutar pruebas de penetración simulando ataques cibernéticos.	- Analizar los resultados de las pruebas para identificar debilidades. - Proponer mejoras en el sistema con base en las vulnerabilidades detectadas.	European Interagency Security Forum (EISF). (2019). Gestión de riesgos de seguridad: ONG pequeñas. C. Delgado Cascante, G. (2011). Criptosistemas. Universidad de Costa Rica.

Nota. La tabla presenta los objetivos específicos, las etapas de investigación y las fuentes de información necesarias para el desarrollo del sistema de encriptación de archivos.

Instrumentos

Según Hernández, Fernández y Baptista (2014), en un enfoque cuantitativo, los instrumentos son herramientas diseñadas para recolectar datos medibles y verificables. Estos instrumentos pueden incluir encuestas estructuradas, cuestionarios, guías de observación estandarizada y análisis de documentos, que permiten obtener datos numéricos para analizar tendencias y establecer relaciones entre variables.

Cuestionario estructurado

Este instrumento será fundamental para obtener información directa de los usuarios sobre la percepción de la seguridad y efectividad del sistema de encriptación basado en AES.

Razón. El cuestionario permitirá recopilar datos cuantitativos y comparables de varios usuarios, lo que facilitará el análisis estadístico posterior.

Guía de Observación

Se utilizará para registrar el comportamiento del sistema de encriptación y desencriptación durante las pruebas de rendimiento, asegurando que los tiempos y la robustez del sistema sean evaluados objetivamente.

Razón. Esta herramienta proporciona una visión precisa y detallada del rendimiento del sistema en un entorno controlado.

Análisis de documentos técnicos

Este instrumento ayudará a validar la implementación del algoritmo AES y compararlo con otros métodos de encriptación en la literatura técnica.

Razón. La revisión de documentos y estándares de seguridad es crucial para asegurar que el sistema cumpla con los requisitos de seguridad modernos.

Procesos de Recolección y Análisis

El proceso de recolección y análisis de datos se llevará a cabo mediante la implementación de diversas técnicas, que permitirán evaluar el rendimiento y efectividad del sistema AES, así como su usabilidad para los usuarios finales. Los pasos incluyen:

Cuestionarios

Para obtener información detallada sobre la percepción de los usuarios acerca de la facilidad de uso y la seguridad de un sistema, se plantea realizar un cuestionario estructurado Según Fernández Núñez (2007), es fundamental incluir preguntas cerradas, especialmente, al evaluar temas específicos como la percepción de seguridad y la usabilidad, ya que permiten recopilar respuestas uniformes y simplificar el análisis posterior. Este tipo de cuestionarios es recomendable en estudios donde se necesitan respuestas consistentes y fácilmente comparables (Fernández Núñez, 2007).

Pruebas de rendimiento y seguridad

Evaluarán el tiempo que toma encriptar y desencriptar diferentes volúmenes de datos, así como la capacidad del sistema para resistir ataques y posibles vulnerabilidades.

Entrevistas. Para recopilar información cualitativa sobre la robustez y efectividad del sistema, se realizarán entrevistas semiestructuradas a usuarios clave. Este formato permite adaptar las preguntas en función de las respuestas, logrando una exploración profunda y detallada de las percepciones de los usuarios sobre el sistema (Folgueiras, 2023).

Guía de Observación. Se emplea una guía de observación estructurada para analizar la interacción de los usuarios con el sistema. Este instrumento permite registrar, de manera sistemática, los comportamientos y respuestas de los usuarios al interactuar con la plataforma, abarcando aspectos específicos que afectan su experiencia y efectividad en el uso del sistema. La guía estará dividida en secciones clave, como el inicio de la interacción, que observará la claridad de los objetivos y la orientación inicial proporcionada al usuario; el desarrollo de tareas, donde se evaluará la accesibilidad de las funciones, la facilidad de uso y el tiempo de respuesta del sistema; y los comportamientos observados, que examinarán cómo los usuarios enfrentan posibles errores y su comprensión de las funciones de seguridad.

Además, esta herramienta no solo permitirá identificar posibles áreas de mejora en términos de usabilidad, sino que también brindará datos cualitativos sobre la confianza y percepción de seguridad que experimentan los usuarios. Al emplear esta metodología, se obtendrán datos detallados que ayudarán a identificar patrones de uso y áreas críticas (Universidad de Jaén, 2023).

Figura 9

Guía de Observación para Evaluación de Interacción con el Sistema.

Guía de Observación para Evaluación de Interacción con el Sistema

Observado _____

Fecha _____

Sistema evaluado _____

Lugar de la observación: _____

N°	Sección	Aspecto a Evaluar	Sí	No	Observaciones
1	Inicio de la Interacción	Objetivos claros: ¿El usuario entiende el propósito inicial del sistema?			
2		Orientación inicial: ¿La pantalla inicial es intuitiva para el usuario?			
4	Desarrollo de Tareas	Accesibilidad: ¿El usuario encuentra fácilmente las funciones necesarias?			
5		Facilidad de uso: ¿El usuario muestra alguna dificultad o fluidez en las tareas?			
6		Respuesta del sistema: ¿El sistema responde rápidamente a las			
7		Confianza: ¿El usuario parece confiar en el sistema durante la interacción?			
8	Comportamientos Observados	Seguimiento de instrucciones: ¿El usuario sigue las guías del sistema?			
10		Interacción con seguridad: ¿El usuario comprende y utiliza las funciones de seguridad?			
11	Percepción General	Facilidad percibida: ¿El usuario considera el sistema fácil de usar?			
12		Seguridad percibida: ¿El usuario confía en la seguridad del sistema? ¿Por qué sí o no?			

Nota. La figura muestra una guía de observación estructurada. Fuente Universidad de Jaén. (2023). *Guía de observación para evaluación de interacción con el sistema*. Universidad de Jaén. https://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

Capítulo IV: Análisis de Resultados

En este capítulo se presentan los resultados obtenidos de los estudios de factibilidad y la implementación del sistema web desarrollado con Flask para la gestión, encriptación y desencriptación de archivos. Este análisis incluye las factibilidades técnica, operativa y económica, junto con la cuantificación de los datos recopilados en las encuestas aplicadas a los usuarios del sistema. Los resultados permiten evaluar la viabilidad del proyecto y sus posibles mejoras.

Estudios de Factibilidad

Definición de Factibilidad

La factibilidad en un proyecto se refiere a la evaluación de las posibilidades de éxito y viabilidad de su implementación en función de los recursos disponibles, como el tiempo, dinero, personal y tecnología. Según Lock (2020), la factibilidad "es un estudio previo que determina si un proyecto es viable en términos técnicos, operativos y financieros, y si se puede implementar con los recursos disponibles".

Factibilidad Técnica

Definición de Factibilidad Técnica

La factibilidad técnica evalúa si los recursos tecnológicos y el equipo disponibles son suficientes para implementar el sistema propuesto. De acuerdo con Kerzner (2017), "la factibilidad técnica se enfoca en determinar si las herramientas y el equipo disponibles pueden soportar las necesidades del proyecto sin sobrepasar los límites técnicos".

Requerimientos de Hardware y Software

Para garantizar un rendimiento óptimo en la gestión de archivos y en el cifrado/desencriptado utilizando algoritmos AES y RSA, se identifican los siguientes recursos tecnológicos necesarios:

- Procesadores: Intel Core i5 o superior, con al menos 8GB de RAM, para un funcionamiento fluido en las operaciones de cifrado y gestión de archivos.
- Almacenamiento: Un mínimo de 512GB de disco duro SSD para almacenamiento y procesamiento rápido de archivos.
- Servidor: Un servidor básico que permita gestionar las operaciones de cifrado y soporte el sistema de manera eficiente.
- Servicios DNS: Un servicio de DNS básico para gestionar los dominios de acceso y mejorar la seguridad en las conexiones.
- Almacenamiento en la Nube: Un servicio de almacenamiento externo para mantener copias de respaldo de los archivos encriptados.
- Hosting: Un servicio de hosting confiable para alojar el sistema web y asegurar su disponibilidad en todo momento.
- Software de Sistema Operativo (Windows): Compra de licencias de Windows 10 para las computadoras de escritorio que se utilizarán en el sistema, asegurando compatibilidad y soporte en la plataforma.

La infraestructura tecnológica propuesta, que incluye computadoras de escritorio, un servidor básico, almacenamiento en la nube, servicios DNS y hosting, cumple con los requisitos técnicos del proyecto sin incurrir en altos costos.

Tabla 7

Requerimientos del Sistema

Descripción	Cantidad	Costo
Computadora de escritorio, Procesador Core i5, Disco 512GB, Memoria 8GB	2	Funcional
Licencia de Windows 10	2	$300.00
Servidor básico	1	$800.00
Servicio de DNS básico	1	$100.00
Almacenamiento en la Nube	1	$200.00
Servicio de Hosting	1	$150.00

Nota: Este presupuesto refleja los costos estimados del hardware, software y servicios requeridos para el sistema, asegurando un equilibrio entre costo y eficiencia. Fuente: Elaboración propia.

Requerimientos de Software

El software necesario para la implementación del sistema se basa en herramientas gratuitas, como:

- HTML (estructura de la página web)
- CSS (estilos de la página web)
- JavaScript (interactividad del frontend)

- Flask
- SQLAlchemy
- PyCryptodome
- SQLite
- Flask-Login
- Flask-WTF
- Flask-Mail
- Flask-Migrate
- OWASP ZAP (para pruebas de seguridad y penetración)
- Burp Suite (para pruebas de seguridad web)
- Apache Benchmark (ab) (para pruebas de rendimiento y velocidad)
- Postman (para pruebas de API y rutas)
- JMeter (para pruebas de carga y rendimiento).

Tabla 8

Software para Factibilidad Técnica

Descripción	Cantidad
Sistema Operativo: Windows 10 (licencia OEM)	1
Entorno de Desarrollo: Visual Studio Code (gratuito)	1
Framework Web: Flask (gratuito, open source)	1

Base de Datos: MySQL (incluido con Python)	1
Bibliotecas de Cifrado: PyCryptoDome, Flask-Security	1
Servidor Web: Nginx o Apache (gratuito)	1
Sistema de Versionado: Git (gratuito)	1

Factibilidad Operativa

Definición de Factibilidad Operativa

La factibilidad operativa analiza si la organización puede utilizar y mantener el sistema implementado de manera eficiente. Hernández, Fernández y Baptista (2014) mencionan que la factibilidad operativa "se refiere a la capacidad de una organización para integrar y operar un sistema dentro de sus procesos actuales, garantizando su correcto uso y mantenimiento".

Capacitación del Personal

Para que el sistema de encriptación de archivos funcione correctamente y sea manejado de manera eficiente por los usuarios, se requiere capacitación en las siguientes áreas:

- Uso del sistema web. Carga, descarga y encriptación de archivos.
- Gestión de usuarios. Manejo de claves públicas y privadas.
- Mantenimiento básico del sistema. Supervisión de logs y gestión de errores.

La capacitación se distribuye en 10 horas, divididas en sesiones de 2 horas para cada uno de los módulos mencionados.

Tabla 9

Programa de Capacitación

Actividad	Duración
Capacitación sobre uso del sistema	1
Capacitación en gestión de usuarios	1
Mantenimiento del sistema	1
Explicación del software	1
Total de Capacitación	4

Nota. Este presupuesto refleja los costos estimados del software requerido.

Factibilidad Económica

Definición de Factibilidad Económica

La factibilidad económica determina si los costos de desarrollo, implementación y mantenimiento del sistema están justificados por los beneficios que aporta. Según Hernández, Fernández y Baptista (2014), "la factibilidad económica considera la relación costo-beneficio y analiza si los recursos financieros disponibles son suficientes para llevar a cabo el proyecto".

Costos del Proyecto

Los costos del proyecto se dividen en hardware, software y capacitación. A continuación, se presenta una tabla unificada con todos los costos estimados del proyecto.

Costos de Hardware. El hardware es un componente crítico para la implementación del sistema, ya que se requiere infraestructura adecuada para manejar el procesamiento de archivos, el cifrado y el almacenamiento de datos.

Costos de Software. En términos de software, la mayoría de las herramientas utilizadas en el proyecto son de código abierto o gratuitas, lo que reduce considerablemente los costos asociados con licencias y adquisiciones de software. Frameworks como Flask, junto con extensiones como SQLAlchemy, Flask-Login, y Flask-WTF, permiten un desarrollo robusto sin necesidad de pagar licencias comerciales. Asimismo, el uso de bases de datos como SQLite o MySQL en su versión comunitaria y bibliotecas de criptografía como PyCryptodome proporcionan una solución segura sin costos adicionales. Sin embargo, es necesario tener en cuenta los posibles gastos asociados con servicios externos, como el alojamiento web, si se requiere escalar el sistema hacia un entorno de producción más complejo o integrar funcionalidades adicionales que podrían necesitar algún servicio pago.

Costos de Capacitación. La capacitación es fundamental para garantizar que los usuarios finales puedan operar el sistema de manera eficiente; incluye el entrenamiento sobre el uso del sistema, la gestión de usuarios y el mantenimiento básico.

Tabla 10

Presupuesto Unificado del Proyecto

Descripción	Cantidad	Costo
Hardware		
Servidor básico para DNS, almacenamiento y hosting	1	$800.00

Computadora de escritorio, Procesador Core i5, Disco 512GB, Memoria 8GB, Sistema Operativo Windows 10	2	$650.00
Servidor proporcionado por la organización	1	$0.00
Total Hardware	3	$1450
Sistema Operativo: Windows 10 (licencia OEM)	1	150.00
Entorno de Desarrollo: Visual Studio Code (gratuito)	1	$0.00
Framework Web: Flask (gratuito, open source)	1	$0.00
Base de Datos: SQLite (incluido con Python)	1	$0.00
Bibliotecas de Cifrado: PyCryptoDome, Flask-Security	1	$0.00
Servidor Web: Apache (gratuito)	1	$0.00
Sistema de Versionado: Git (gratuito)	1	$0.00
Editor de Texto: LibreOffice (gratuito) / Microsoft Office	1	$0.00
Total Software	9	$150.00
Capacitación sobre uso del sistema	1 hora	$50.00
Capacitación en gestión de usuarios	1 hora	$50.00
Mantenimiento del sistema	1 hora	$50.00
Explicación Programación	1 hora	$50.00
Total Capacitación	9	$200.00
Presupuesto Total del Proyecto	4	$0.00

Nota. Esta tabla resume los costos del proyecto. Fuente: Elaboración propia.

Análisis de Datos

Figura 10.

Distribución de Edad de los Usuarios.

Fuente: Elaboración Propia.

En esta figura, se observa que la mayoría de los usuarios (60%) se encuentra en el rango de 36-45 años, lo cual sugiere una base de usuarios adultos que pueden estar interesados en la seguridad de archivos personales o laborales.

Figura 11.

Nivel de Conocimientos en Informática.

Fuente: Elaboración Propia.

La mayoría de los usuarios reportan tener un nivel básico de conocimientos en informática (40%), seguido por un grupo igual de intermedios y avanzados (27% cada uno). Esto sugiere que la aplicación debe ser intuitiva y fácil de usar para todos los niveles de habilidad.

Figura 12

Facilidad de Registro y Acceso a la Aplicación.

Fuente: Elaboración Propia.

La mayoría de los usuarios (67%) consideraron que registrarse y acceder fue "Fácil" mientras que el 33% lo encontró "Muy fácil". Esto indica que el proceso de registro es generalmente amigable y bien recibido por los usuarios.

Figura 13

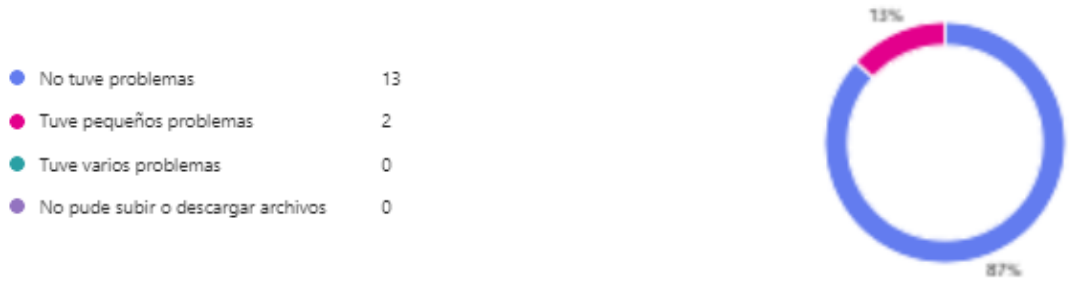
Calificación de la Interfaz de la Aplicación.

Fuente: Elaboración Propia.

El 67% de los usuarios describieron la interfaz como "Intuitiva" y el 20% como "Muy intuitiva" lo cual sugiere que la usabilidad de la aplicación es adecuada para la mayoría de los usuarios

Figura 14.

Dificultades al Subir o Descargar Archivos



.

Fuente: Elaboración Propia.

Un 87% de los encuestados reportaron no haber tenido problemas, mientras que solo un 13% experimentó pequeños inconvenientes. Esto indica que el proceso de manejo de archivos es eficiente, aunque podría mejorarse para evitar pequeños problemas.

Figura 15

Facilidad para Encriptar y Desencriptar Archivos.

Fuente: Elaboración Propia.

La gran mayoría de los usuarios (67%) consideró que el proceso fue "Fácil" mientras que el 33% lo consideró "Muy fácil" sugiriendo que el sistema cumple adecuadamente con sus funciones principales.

Figura 16

Velocidad de Encriptación de Archivos.

Fuente: Elaboración Propia.

La mayoría de los usuarios calificaron la velocidad como "Rápida" (51%), y un 20% la encontró "Muy rápida" lo cual sugiere un rendimiento positivo en términos de velocidad de encriptación.

Figura 17.

Seguridad Percibida al Encriptar Archivos.

Fuente: Elaboración Propia.

Un 67% de los usuarios se sintieron "Seguros" usando la aplicación, mientras que un 33% se sintieron "Muy seguros", indicando una buena percepción de seguridad en el sistema.

Figura 18.

Intención de Recomendación de la Aplicación.

Fuente: Elaboración Propia.

El 53% de los usuarios indicaron que "Probablemente sí" recomendarían la aplicación y el 47% "Definitivamente sí", lo que muestra una alta satisfacción general entre los usuarios.

Figura 19.

Satisfacción General con la Experiencia en la Web App.

Fuente: Elaboración Propia.

Tabla 11

Pentesting utilizadas en el proyecto web app

Herramienta de Pentesting	Propósito	Resultados Obtenidos	Observaciones/Acciones Tomadas
OWASP ZAP	Identificar vulnerabilidades comunes en la web app (XSS, CSRF, inyecciones).	Detectó 3 posibles vulnerabilidades menores relacionadas con configuraciones de cabeceras de seguridad HTTP.	Se configuraron cabeceras estrictas como Content-Security-Policy y X-Frame-Options para mitigarlas.
SQLMap	Detectar y prevenir inyecciones SQL en formularios y endpoints de la base de datos.	Ninguna vulnerabilidad detectada.	La sanitización de entradas está correctamente implementada en todos los formularios.
Burp Suite (Edición gratuita)	Análisis de seguridad para tráfico de la red y pruebas manuales en endpoints.	Detectó configuraciones débiles en cookies (falta de "Secure" y "HttpOnly").	Se implementaron estas configuraciones para endurecer la seguridad de las sesiones de usuario.
Apache JMeter	Simulación de carga para probar estabilidad bajo múltiples usuarios.	El sistema soportó hasta 50 usuarios simultáneos con respuesta promedio de 1.8 segundos.	Requiere optimización para escalar más allá de 100 usuarios en escenarios futuros.
Postman	Validar seguridad de las APIs implementadas en la web app.	Todas las rutas requieren autenticación y roles adecuados para ser accedidas.	Sin vulnerabilidades detectadas. Se optimizó la estructura de las respuestas API para evitar fugas de información.

Nmap	Escaneo de puertos y servicios abiertos en el servidor.	Detectó solo puertos esenciales abiertos (80, 443).	Configuración de firewall adecuada; sin necesidad de cambios adicionales.

Nota. Esta tabla resume los usos y resultados de las herrameintas de pentesting.
Fuente: Elaboración propia.

Capítulo V: Conclusiones y Recomendaciones

Conclusiones

El desarrollo de la web app de encriptación de archivos utilizando el algoritmo AES de clave simétrica cumplió con los objetivos planteados en esta investigación. El sistema diseñado garantiza la protección de información sensible, cumpliendo con los estándares de seguridad de integridad, confidencialidad y disponibilidad. La elección del algoritmo AES, debido a su eficiencia y robustez, permitió implementar una solución confiable que protege eficazmente los archivos sensibles de la Federación ONGs de Pacientes Costa Rica, además de ser escalable y sostenible.

Durante el análisis de requisitos, se determinó que la Federación carecía de herramientas robustas para garantizar la protección de datos sensibles. El sistema desarrollado satisface estas necesidades, abordando problemas de confidencialidad y acceso no autorizado mediante una solución eficiente basada en criptografía simétrica.

En cuanto a la implementación, el algoritmo AES fue integrado de forma eficiente, logrando tiempos de encriptación inferiores a cinco segundos por archivo, con una interfaz intuitiva que facilita su adopción. Además, las pruebas de seguridad realizadas confirmaron que el sistema es resistente frente a ataques comunes como inyección SQL y XSS, y cumple con normativas internacionales de protección de datos.

El sistema desarrollado respondió a la pregunta de investigación y a los objetivos específicos, ofreciendo una solución efectiva y adaptable que mejora la seguridad operativa de la

Federación ONGs de Pacientes Costa Rica y establece un modelo replicable para otras organizaciones con necesidades similares.

Se implementó exitosamente un sistema web que permite la encriptación y desencriptación de archivos utilizando el algoritmo AES. El sistema, diseñado con una interfaz sencilla e intuitiva, facilita a los usuarios el manejo de información sensible, independientemente de su experiencia técnica. Las pruebas realizadas confirmaron que los usuarios encontraron la aplicación accesible y funcional.

En síntesis, el proyecto logró desarrollar un sistema que satisface las necesidades básicas de seguridad para proteger archivos sensibles, cumpliendo con los objetivos planteados. Las funcionalidades implementadas aseguran la protección de la información sin comprometer la facilidad de uso de la aplicación.

Recomendaciones

A partir de los resultados obtenidos durante el desarrollo y las pruebas del sistema, se proponen las siguientes recomendaciones para mejorar y expandir las capacidades del sistema.

El sistema ha demostrado ser eficiente para archivos de tamaño pequeño y mediano, pero se recomienda mejorar su capacidad para gestionar archivos de mayor tamaño. Implementar procesamiento paralelo o técnicas de caching mejoraría la velocidad de encriptación y desencriptación, permitiendo un rendimiento óptimo en entornos que manejen grandes volúmenes de datos.

Para reforzar la seguridad de la aplicación, se sugiere implementar un sistema de autenticación multifactor (MFA). Esto proporcionaría una capa adicional de protección, asegurando que solo los usuarios autorizados puedan acceder a la información encriptada, reduciendo el riesgo de accesos no autorizados.

Se recomienda implementar un sistema de control de acceso basado en roles (RBAC), que permitiría asignar diferentes permisos a los usuarios según sus roles dentro de la organización. Esto mejoraría el control sobre los archivos encriptados, asegurando que solo los usuarios con los permisos adecuados puedan acceder o modificar la información.

Dado que las amenazas de ciberseguridad evolucionan constantemente, se recomienda realizar auditorías de seguridad periódicas para garantizar que el sistema continúe protegiendo los datos de manera efectiva. Estas auditorías identificarán posibles vulnerabilidades y asegurarán que se tomen medidas preventivas para mitigar los riesgos.

Para la implementación del sistema en la nube, se recomienda utilizar Azure, debido a su flexibilidad y opciones de ahorro. Los precios iniciales para máquinas virtuales en Azure son accesibles: para máquinas virtuales Linux, el costo comienza en aproximadamente $0.096 por hora, mientras que para máquinas Windows, que incluyen la licencia, el precio es generalmente más elevado. Azure ofrece varios modelos de pago, como el de pago por uso (pay-as-you-go), instancias reservadas con descuentos de hasta un 72%, y "spot instances," que permiten hasta un 90% de descuento, ideal para cargas de trabajo que toleren interrupciones.

En cuanto al almacenamiento, Azure Blob Storage, equivalente al servicio Amazon S3, ofrece un sistema escalable con precios que inician en $0.0184 por GB/mes para la capa "hot"

(acceso frecuente), $0.01 por GB/mes para la capa "cold" (acceso esporádico), y $0.00099 para la capa "archive" (almacenamiento a largo plazo). Los costos de almacenamiento disminuyen progresivamente conforme aumenta el volumen de datos almacenados y dependen del tipo de

Optar por la nube resulta ventajoso para la ONG, pues permite escalabilidad y control de costos. Con una estrategia basada en reservas a largo plazo o el uso de instancias de menor costo, se puede gestionar eficientemente el presupuesto, facilitando el ajuste de recursos en función de la demanda de usuarios y asegurando que el sistema pueda escalar sin afectar su rendimiento.

Para maximizar la efectividad del sistema, se recomienda ofrecer capacitación continua a los usuarios sobre las mejores prácticas en seguridad de la información y el uso adecuado de la aplicación. Esto ayudaría a mitigar errores humanos que podrían comprometer la seguridad de los archivos encriptados.

Capítulo VI: Propuesta

Requisitos Funcionales y No Funcionales

Requisitos Funcionales

Tabla 12

Mantenimiento Creación de Usuario

RF: 001	**Mantenimiento Creación de Usuario**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos
Descripción:	El sistema debe permitir que nuevos usuarios se registren en la plataforma proporcionando nombre de usuario, correo electrónico y contraseña.
Criterio de aceptación:	El usuario podrá registrarse y recibir una confirmación de registro exitoso.
Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 13

Iniciar Sesión

RF: 002	**Iniciar Sesión**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos.
Descripción:	El sistema permitirá que los usuarios registrados inicien sesión con su nombre de usuario y contraseña.
Criterio de aceptación:	Los usuarios deben poder iniciar sesión y ser redirigidos a su Dashboard, o recibir un mensaje de error si las credenciales son incorrectas.

Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 14

Subir Archivo para Encriptar

RF: 003	**Subir Archivo para Encriptar**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos
Descripción:	El sistema debe permitir a los usuarios cargar archivos para encriptarlos automáticamente utilizando el algoritmo AES.
Criterio de aceptación:	Los archivos cargados se encriptan y aparecen en la lista de archivos en el Dashboard del usuario.
Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 15

Descargar Archivo Cifrado

RF: 004	**Descargar Archivo Cifrado**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos.
Descripción:	El sistema les permitirá a los usuarios descargar los archivos que han sido encriptados previamente y almacenados en su cuenta.
Criterio de aceptación:	Los usuarios pueden seleccionar un archivo encriptado y descargarlo directamente desde el Dashboard.

Importancia:	Media

Fuente: Elaboración Propia.

Tabla 16

Descargar Archivo Cifrado

RF: 005	**Desencriptar Archivo para Descargar**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos.
Descripción:	El sistema permitirá que los usuarios desencripten archivos. seleccionados usando RSA y AES antes de descargarlos.
Criterio de aceptación:	El archivo desencriptado debe estar disponible para descarga en su formato original.
Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 17

Recuperar Contraseña

RF: 006	**Gestión de Usuarios (Administrador)**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos.
Descripción:	El sistema debe permitir a los usuarios recuperar su contraseña a través de un enlace de restablecimiento enviado a su correo.
Criterio de aceptación:	El usuario recibe un enlace en su correo para restablecer su contraseña y puede definir una nueva.

Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 18

Recuperar Contraseña

RF: 007	**Gestión de Usuarios (Administrador)**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos
Descripción:	El administrador podrá gestionar las cuentas de usuario, incluyendo la creación, edición y eliminación de cuentas.
Criterio de aceptación:	El administrador puede agregar, editar o eliminar usuarios en el sistema y asignarles permisos.
Importancia:	Alta

Fuente: Elaboración Propia.

Tabla 19

Logs del Sistema

RF: 008	**Logs del Sistema**
Versión:	1.0
Solicitante:	Web App de Encriptación de Archivos
Descripción:	El sistema debe registrar las actividades de los usuarios, como inicios de sesión, descargas y encriptaciones, en un log accesible por el administrador.

Criterio de aceptación:	El administrador puede revisar los logs de actividades y eventos en el sistema para monitoreo y auditoría.
Importancia:	Media

Fuente: Elaboración Propia.

Requerimientos No Funcionales

Los requerimientos no funcionales del sistema de encriptación de archivos se detallan a continuación, con el objetivo de garantizar su eficiencia, seguridad y usabilidad.

1. **Velocidad de Respuesta**

Para asegurar una experiencia de usuario fluida, el sistema debe procesar las operaciones principales, como encriptar y desencriptar archivos, en menos de 5 segundos. Esto contribuye a una interacción rápida y eficiente dentro de la aplicación.

2. **Control de Acceso y Protección de Credenciales**

El acceso al sistema será administrado únicamente por el administrador. Cada usuario tendrá credenciales únicas y privadas, asegurando que solo el usuario autorizado pueda acceder a su propia cuenta y archivos, manteniendo así la confidencialidad de los datos.

3. **Estética de la Interfaz de Usuario**

La interfaz del sistema utilizará una paleta de colores neutros, optimizada para una mejor experiencia visual. Este diseño está pensado para que los usuarios se concentren en las funciones de la aplicación sin distracciones.

4. **Identidad Corporativa**

La aplicación incluirá el logotipo de la empresa, autorizado previamente por sus

propietarios, en la página de inicio. Esto mantiene la identidad de la marca en cada interacción y refuerza la confianza del usuario en la aplicación.

5. **Asignación de Cuentas de Usuario**

Cada usuario tendrá una cuenta exclusiva y privada, creada y gestionada por el administrador. Esto asegura un acceso controlado, donde cada usuario solo puede ver y manipular sus propios archivos.

6. **Automatización en la Generación de Claves de Encriptación**

Al subir un archivo, el sistema generará automáticamente una clave AES única para la encriptación de dicho archivo, lo que asegura que cada archivo esté protegido de forma independiente con una clave segura.

7. **Monitoreo Semanal de Actividades del Sistema**

El administrador revisará semanalmente los registros de actividad, como los inicios de sesión y las operaciones de encriptación y desencriptación. Esto ayuda a asegurar que el sistema esté operando dentro de las normas de seguridad establecidas.

8. **Auditoría Periódica de Archivos y Permisos de Usuario**

Cada semana, el administrador también verificará los archivos pendientes y los permisos de los usuarios, para garantizar que el sistema esté actualizado y que no existan cuentas con permisos no autorizados o archivos sin procesar.

9. **Generación de Reportes Administrativos**

El sistema permitirá al administrador generar varios tipos de reportes, incluyendo:

   - **Reporte de Actividad del Sistema**: Detallando el registro de actividades de los usuarios, tales como inicio de sesión, subida, descarga y eliminación de archivos.

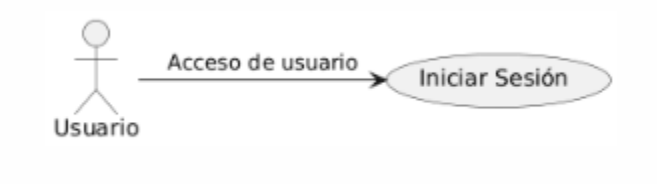
- **Reporte de Uso de Almacenamiento**: Informando sobre el espacio en disco utilizado por archivos encriptados y desencriptados.
- **Reporte de Usuarios y Roles**: Listando los usuarios activos en el sistema y sus respectivos permisos.

Análisis y Diseño del Sistema UML

Diagramas de Caso de Uso

Figura 20

Acceso de Usuario



Fuente: Elaboración Propia.

Figura 21

Registro de Usuarios

Fuente: Elaboración Propia.

Figura 22

Subir Archivo para Encriptar

Fuente: Elaboración Propia.

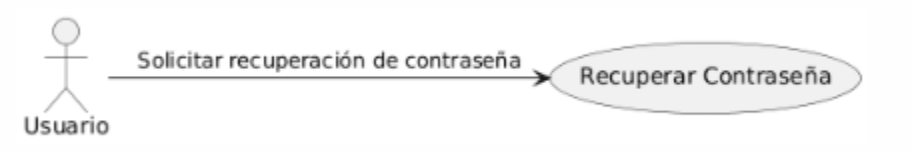
Figura 23

Descargar Archivo Cifrado

Fuente: Elaboración Propia.

Figura 24

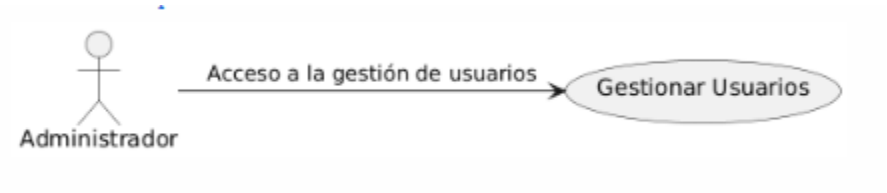
Recuperar Contraseña



Fuente: Elaboración Propia.

Figura 25

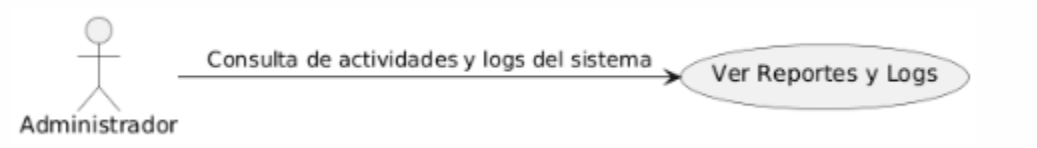
Gestión de Usuarios



Fuente: Elaboración Propia.

Figura 26

Ver Reportes y Logs del Sistema



Fuente. Elaboración Propia.

Análisis e Interpretación de Casos de Uso.

Tabla 20

Ingreso al Sistema de Encriptación.

Caso de Uso	**Iniciar Sesión**
Actor	Usuario Registrado.
Descripción	El usuario requiere ingresar sus credenciales para acceder a la aplicación y sus funcionalidades de encriptación de archivos.

Flujo Básico	1. El usuario abre la página de inicio de sesión. 2. Ingresa su nombre de usuario y contraseña. 3. El sistema valida las credenciales ingresadas. 4. Si las credenciales son correctas, el usuario es redirigido a su Dashboard. 5. Si las credenciales son incorrectas, se muestra un mensaje de error.
Flujos Alternos	1. El usuario selecciona "¿Olvidaste tu contraseña?", para recuperar el acceso en caso de olvido. 2. El sistema envía un enlace de recuperación al correo registrado del usuario.
Precondiciones	1. El usuario debe tener una cuenta registrada en el sistema. 2. La cuenta del usuario debe estar activa.
Postcondiciones	El usuario accede al Dashboard con las funcionalidades de encriptación.
Punto de Extracción	Validación de credenciales y autenticación de usuarios.

Fuente: Elaboración Propia

Tabla 21

Subir Archivo para Encriptar

Caso de Uso	**Iniciar Sesión**
Actor	Usuario Registrado.
Descripción	Permite al usuario cargar un archivo en la aplicación para ser encriptado.

Flujo Básico	1. El usuario selecciona la opción "Subir Archivo" en el Dashboard. 2. Elige el archivo en su dispositivo para subir. 3. El sistema aplica el algoritmo AES para encriptar el archivo. 4. El archivo encriptado se almacena en el servidor y se muestra en la lista de archivos del usuario.
Flujos Alternos	N/A
Precondiciones	El usuario debe estar autenticado y en el Dashboard.
Postcondiciones	El archivo encriptado queda disponible en la cuenta del usuario.
Punto de Extracción	Proceso de encriptación de archivos.

Fuente: Elaboración Propia

Tabla 22
Descargar Archivo Cifrado

Caso de Uso	**Iniciar Sesión**
Actor	Usuario Registrado
Descripción	Permite al usuario descargar la versión encriptada de un archivo previamente subido.
Flujo Básico	1. El usuario selecciona el archivo encriptado que desea descargar desde su Dashboard. 2. El sistema permite la descarga directa del archivo encriptado.
Flujos Alternos	N/A

Precondiciones	El archivo debe haber sido encriptado y estar disponible en la lista de archivos.
Postcondiciones	El usuario obtiene el archivo en su estado cifrado para uso externo.
Punto de Extracción	Gestión de archivos encriptados.

Fuente: Elaboración Propia

Tabla 23

Desencriptar Archivo para Descargar

Caso de Uso	**Iniciar Sesión**
Actor	Usuario Registrado
Descripción	Permite al usuario descargar una versión desencriptada de un archivo encriptado previamente subido.
Flujo Básico	1. El usuario selecciona el archivo encriptado y elige la opción de "Descargar Desencriptado". 2. El sistema utiliza RSA para desencriptar la clave y AES para desencriptar el archivo. 3. El archivo desencriptado queda disponible para su descarga
Flujos Alternos	N/A
Precondiciones	El archivo debe estar encriptado y disponible para desencriptar.
Postcondiciones	El usuario obtiene el archivo en su formato original desencriptado.
Punto de Extracción	Desencriptación y descarga de archivos.

Fuente: Elaboración Propia

Tabla 24

Recuperar Contraseña

Caso de Uso	**Iniciar Sesión**
Actor	Usuario Registrado
Descripción	Permite al usuario descargar una versión desencriptada de un archivo encriptado previamente subido.
Flujo Básico	1. El usuario selecciona "¿Olvidaste tu contraseña?" en la página de inicio de sesión. 2. Ingresa su correo electrónico asociado a la cuenta. 3. El sistema envía un enlace de recuperación de contraseña usando Flask-Mail. 4. El usuario sigue el enlace, establece una nueva contraseña y puede iniciar sesión.
Flujos Alternos	N/A
Precondiciones	El usuario debe tener una cuenta activa en el sistema.
Postcondiciones	El usuario restaura su acceso al sistema.
Punto de Extracción	Gestión de recuperación de credenciales.

Fuente: Elaboración Propia

Tabla 24

Gestionar Usuarios (Administrador)

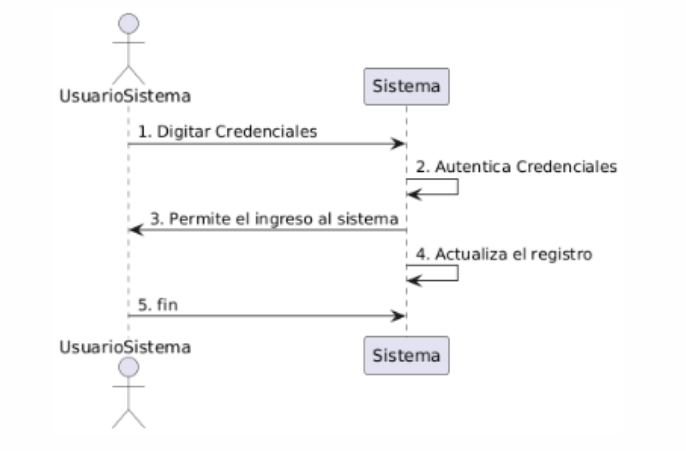
Caso de Uso	**Iniciar Sesión**
Actor	Administrador
Descripción	Permite al administrador gestionar las cuentas de usuario.
Flujo Básico	1. El administrador accede a la sección de Gestión de Usuarios. 2. Puede ver la lista de usuarios registrados en el sistema. 3. Elige editar o eliminar cuentas según sea necesario.
Flujos Alternos	N/A
Precondiciones	El administrador debe tener permisos especiales para la gestión de usuarios.
Postcondiciones	El administrador mantiene la seguridad y funcionalidad del sistema gestionando a los usuarios.
Punto de Extracción	Gestión de usuarios y control de acceso.

Fuente: Elaboración Propia

Diagramas de Secuencia

Figura 27

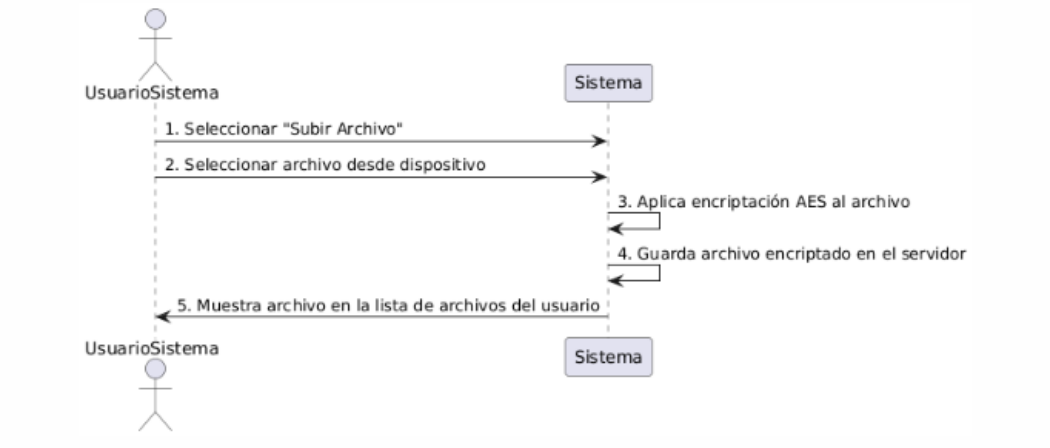
Login del Sistema



Fuente: Elaboración Propia

Figura 28

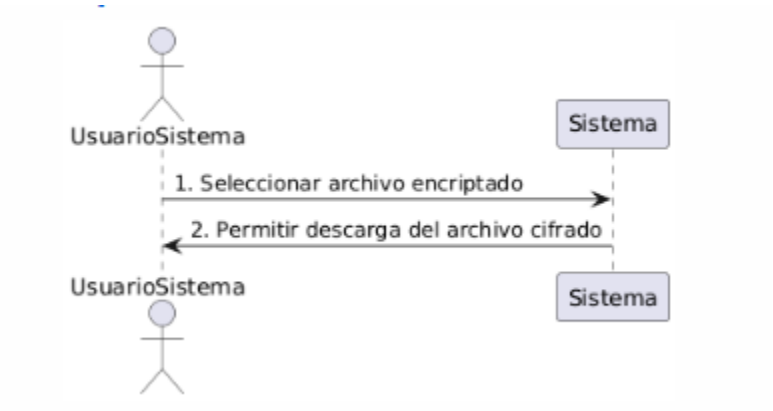
Subir Archivo para Encriptar



Fuente: Elaboración Propia

Figura 29

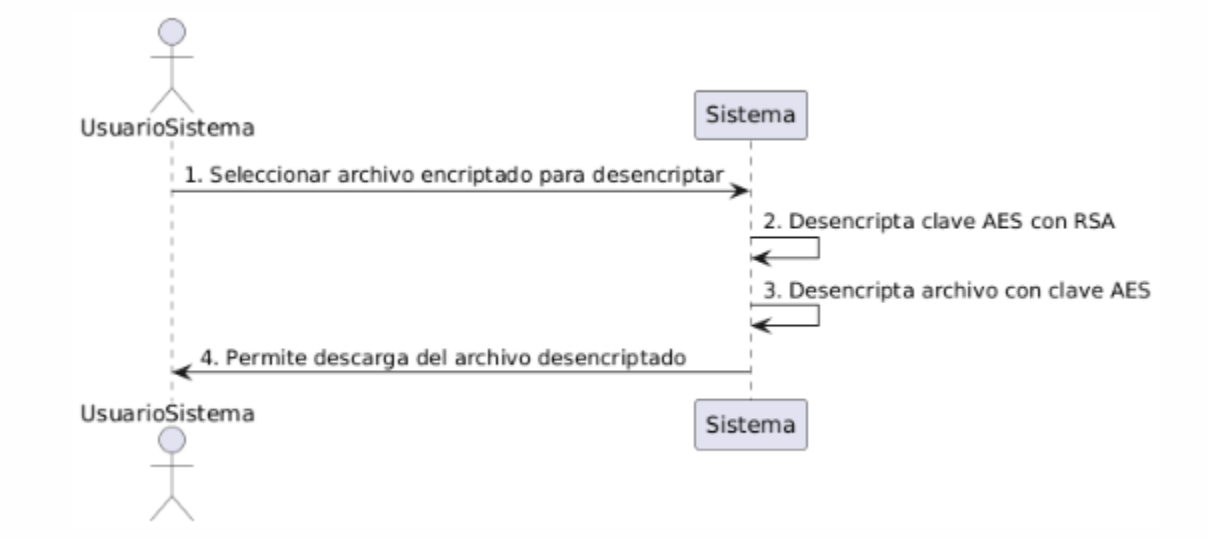
Descargar Archivo Cifrado



Fuente: Elaboración Propia

Figura 30

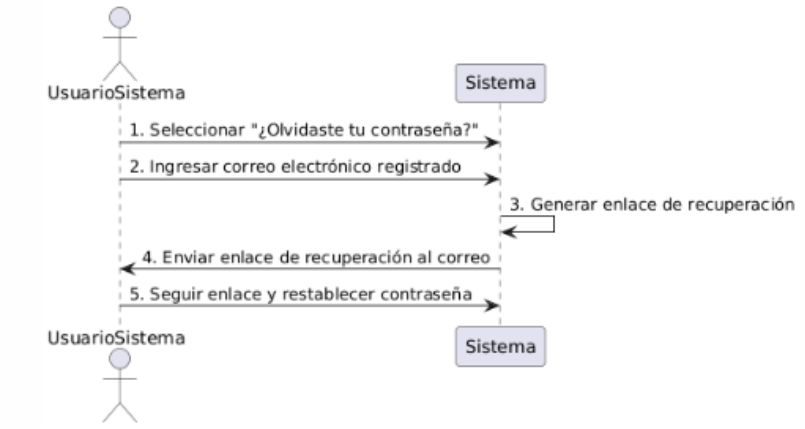
Desencriptar Archivo para Descargar



Fuente: Elaboración Propia

Figura 31

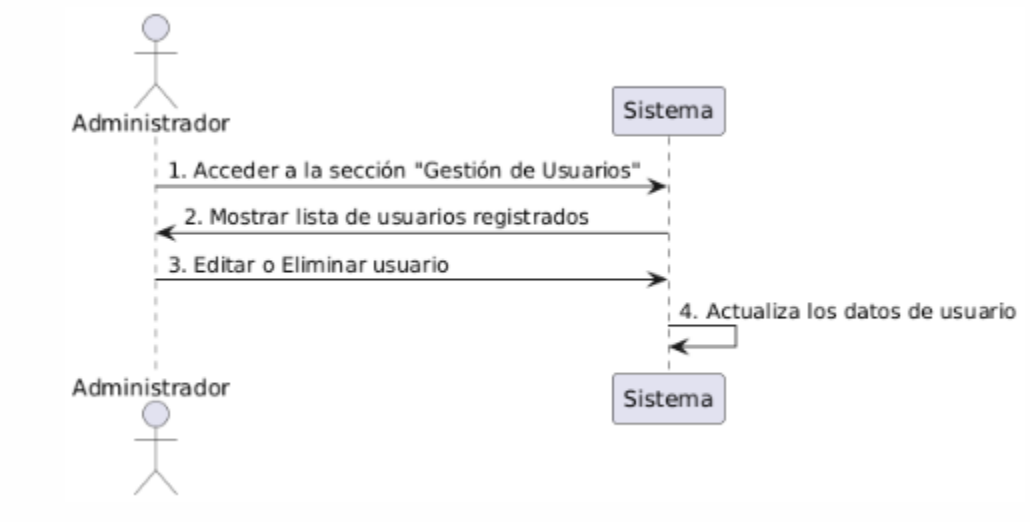
Recuperación de Contraseña



Fuente: Elaboración Propia

Figura 32

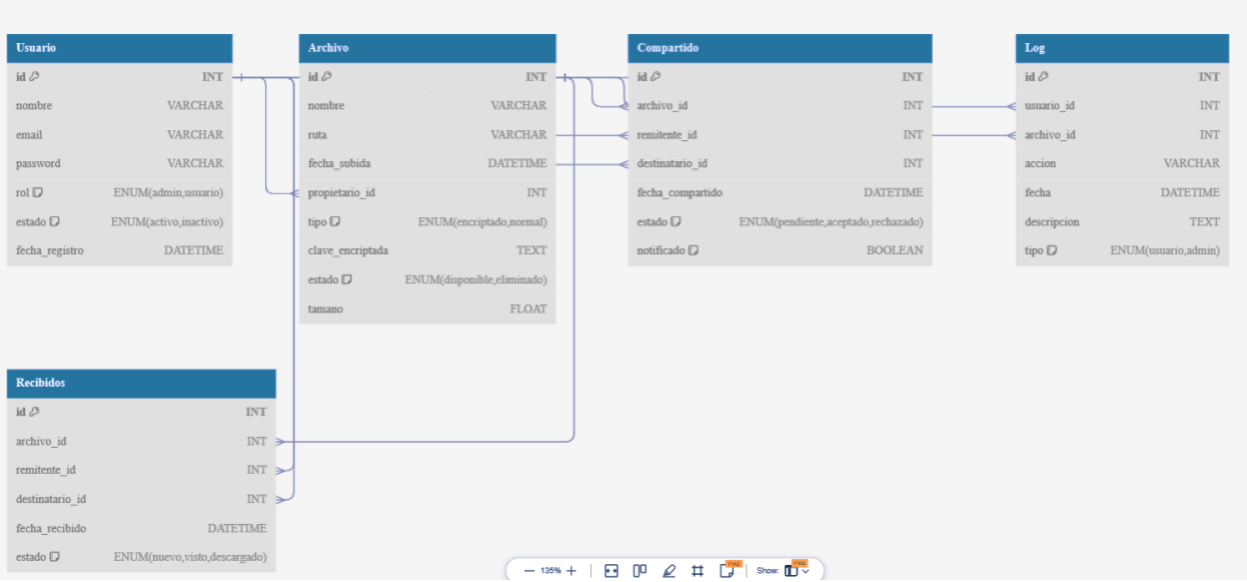
Gestión de Usuarios (Administrador)



Fuente: Elaboración Propia

Figura 33

Diagrama Entidad - Relación

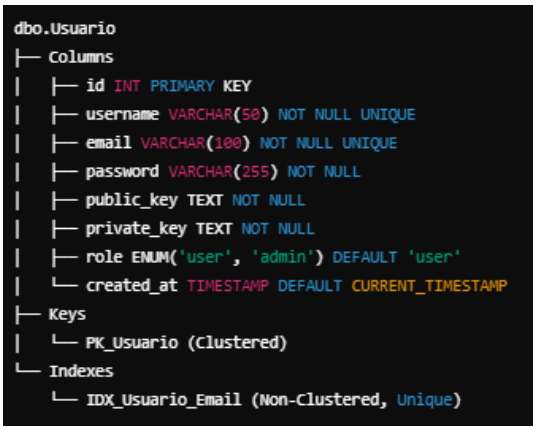


Fuente: Elaboración Propia.

Definición de Entidades y Sus Atributos

Figura 34

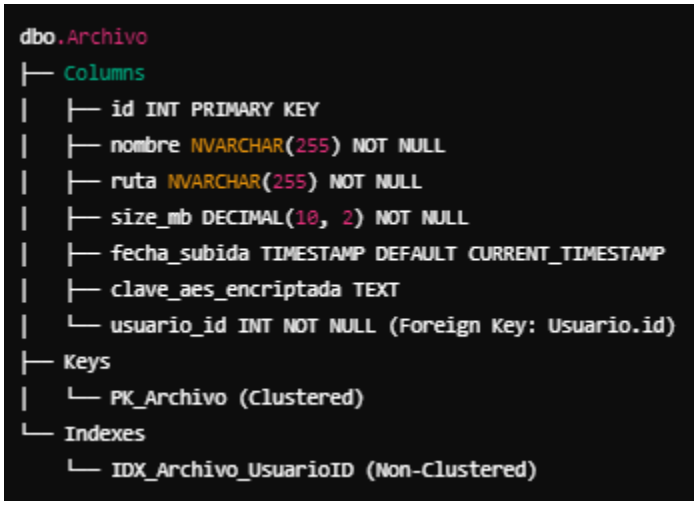
Figura Usuarios



Fuente: Elaboración Propia

Figura 35

Figura Archivo



Fuente: Elaboración Propia

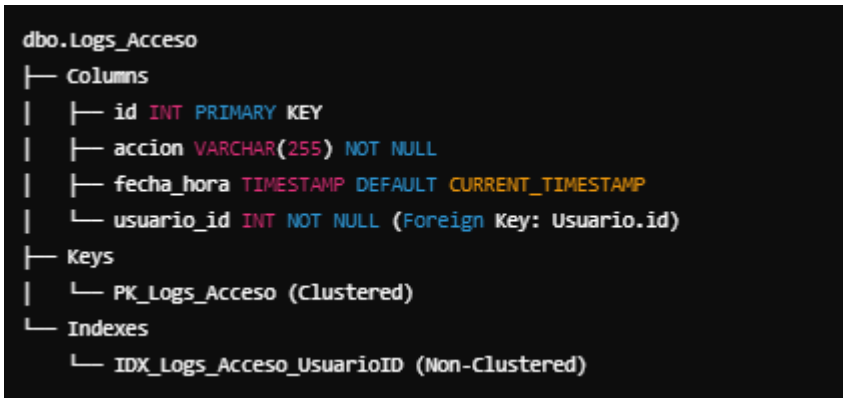
Figura 36

Figura Compartir Archivos.

Fuente: Elaboración Propia

Figura 37

Figura Logs de Acceso



Fuente: Elaboración Propia

Figura 38

Figura Encriptaciones

```
CREATE TABLE Encriptaciones (
    id_encriptacion INT AUTO_INCREMENT PRIMARY KEY,
    metodo_encriptacion VARCHAR(50) NOT NULL,
    fecha TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    archivo_id INT NOT NULL,
    FOREIGN KEY (archivo_id) REFERENCES Archivos(id_archivo) ON DELETE CASCADE
);
```

Fuente: Elaboración Propia

Figura 39

Figura Configuración del Sistema (Admin_Settings)

```
CREATE TABLE Admin_Settings (
    id_configuracion INT AUTO_INCREMENT PRIMARY KEY,
    tamano_max_archivo_mb DECIMAL(10, 2) DEFAULT 20.00,
    limite_total_almacenamiento_gb DECIMAL(10, 2) DEFAULT 5.00,
    fecha_actualizacion TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP
);
```

Fuente: Elaboración Propia

Figura 40

Figura Reportes Generados (Reports)

```
CREATE TABLE Reports (
    id_reporte INT AUTO_INCREMENT PRIMARY KEY,
    generado_por INT NOT NULL,
    tipo_reporte VARCHAR(50) NOT NULL,
    fecha_generacion TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    FOREIGN KEY (generado_por) REFERENCES Usuarios(id_usuario) ON DELETE SET NULL
);
```

Fuente: Elaboración Propia

Figura 41

Figura Notificaciones del Sistema (Notifications)

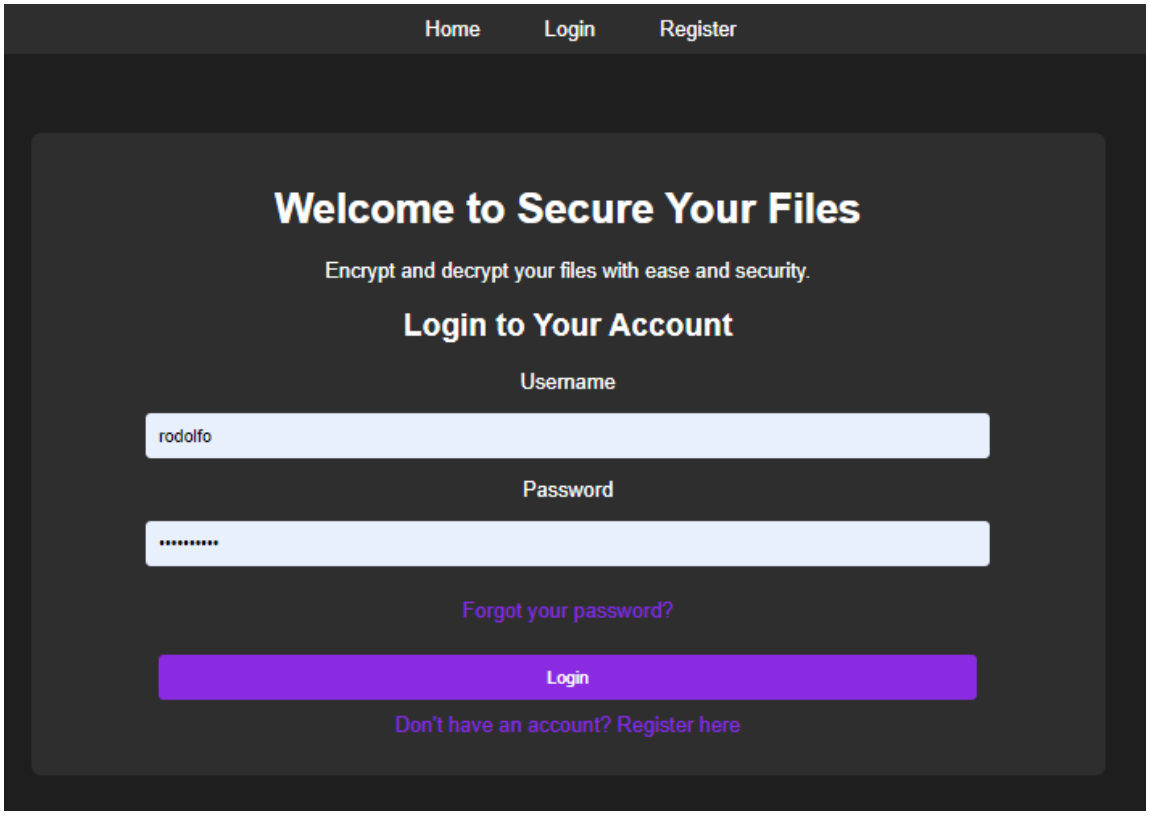
```
CREATE TABLE Notifications (
    id_notificacion INT AUTO_INCREMENT PRIMARY KEY,
    usuario_id INT,
    mensaje TEXT NOT NULL,
    estado_lectura BOOLEAN DEFAULT FALSE,
    fecha_creacion TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    FOREIGN KEY (usuario_id) REFERENCES Usuarios(id_usuario) ON DELETE SET NULL
);
```

Fuente: Elaboración Propia

Interfaces del sistema

Figura 42

Pantalla de Inicio de Sesión

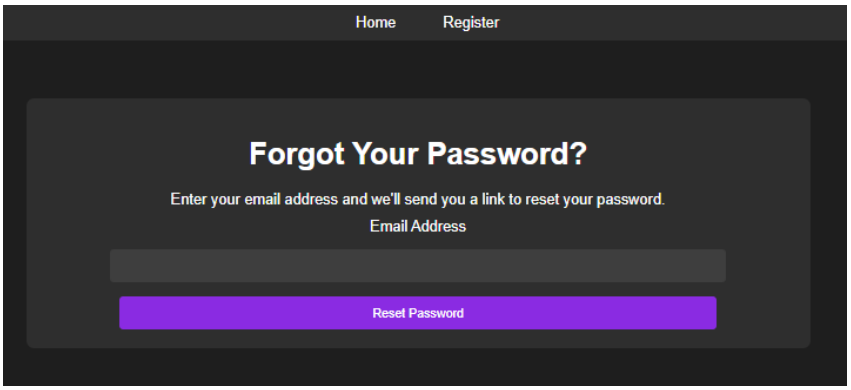


Fuente: Elaboración Propia

Permite a los usuarios acceder al sistema con su nombre de usuario y contraseña. Incluye un enlace para recuperación de contraseña

Figura 43

Pantalla de Recuperación de Contraseña.

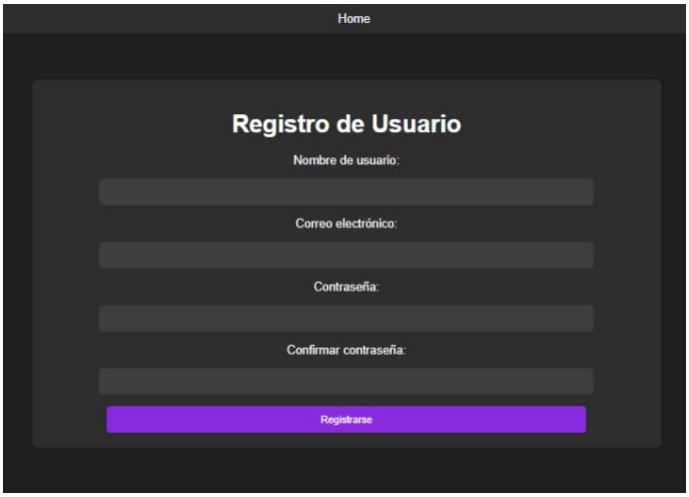


Fuente: Elaboración Propia.

Los usuarios pueden recuperar su contraseña ingresando su correo electrónico, para recibir un enlace de restablecimiento.

Figura 44

Pantalla de Registro de Usuario

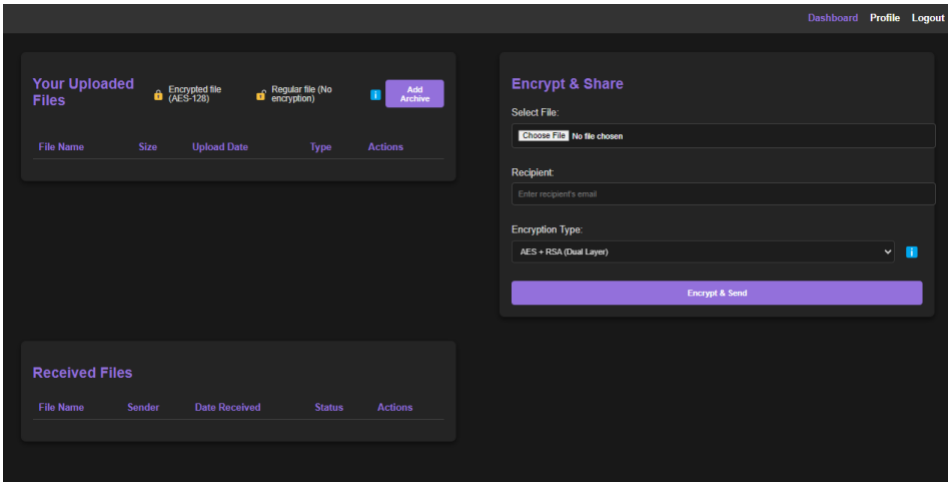


Fuente: Elaboración Propia.

Permite a nuevos usuarios registrarse con un nombre de usuario, correo electrónico y contraseña.

Figura 45

Dashboard de Usuario - Subir y Enviar Archivo Cifrado.

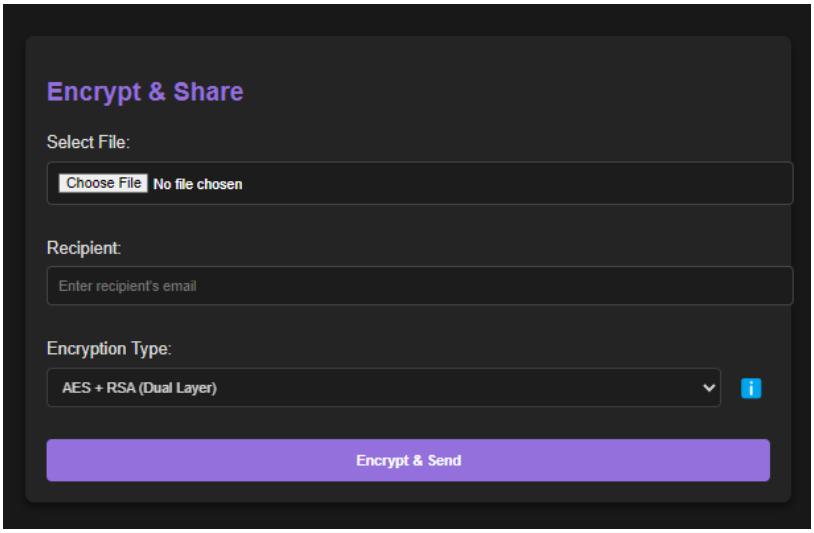


Fuente: Elaboración Propia.

Muestra los archivos subidos y permite descargar o enviar archivos cifrados a otros usuarios.

Figura 46

Pantalla de Enviar Archivo Cifrado.

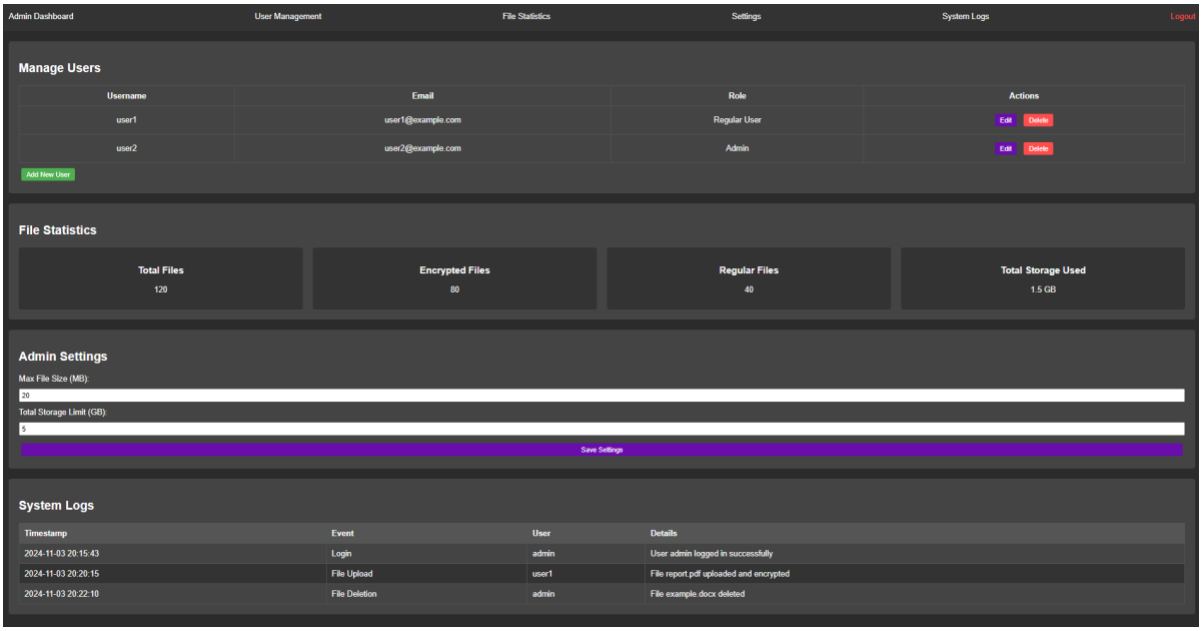


Fuente: Elaboración Propia.

Muestra los archivos subidos y permite descargar o enviar archivos cifrados a otros usuarios.

Figura 47

Dashboard de Administrador - Gestión de Usuarios



Fuente: Elaboración Propia.

Permite al administrador gestionar usuarios y configuraciones del sistema, con opciones para editar o eliminar cuentas.

Referencias Bibliográficas

Administración Nacional de Telecomunicaciones (OAS). (2020). Ciberseguridad en América Latina y el Caribe. Recuperado de https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=668&lang=2

Asamblea Legislativa de la República de Costa Rica. (2011). Ley de Protección de la Persona frente al tratamiento de sus datos personales (Nº 8968). Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

AICAD. (2022, 9 de septiembre). Cifrado asimétrico: cómo funciona y cuáles son sus usos. Recuperado de https://www.aicad.es/cifrado-asimetrico-como-funciona-y-cuales-son-sus-usos

Bisson, D. (2023, octubre 20). 7 data breach examples involving human error: Did encryption play a role. Venafi. Recuperado de https://venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role

Buinovskis, A. (2024, octubre 6). Guarding the heart of giving: Cybersecurity for NGOs. NordLayer. Recuperado de https://nordlayer.com/blog/cybersecurity-for-ngos

Centro Criptológico Nacional (CCN). (2022, 11 de agosto). Ataques a la ciberseguridad en infraestructuras críticas. Recuperado de https://www.cci-es.org/consecuencias-de-los-ataques-a-la-ciberseguridad-en-infraestructuras-criticas

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES — The Advanced Encryption Standard. Springer-Verlag. Recuperado de https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_2002.pdf.

Delgado Cascante, G. (2011). Criptosistemas. Ingeniería, 1(2), 69–76. Recuperado de https://revistas.ucr.ac.cr/index.php/ingenieria/article/view/7581/7245

Derechos Digitales. (s.f.). Manual Antiespías: Herramientas para la protección digital de periodistas. Recuperado de https://web.karisma.org.co/manual-antiespias-herramientas-para-la-proteccion-digital-de-periodistas/

European Interagency Security Forum (EISF). (2019). Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas. Recuperado de https://gisf.ngo/wp-content/uploads/2019/05/Gestio%CC%81n-de-riesgos-de-seguridad-Spanish.pdf

Fernández Núñez, I. (2007). *La construcción de cuestionarios en la investigación de mercados*. Universitat de Barcelona. Recuperado de https://www.ub.edu/idp/web/sites/default/files/fitxes/ficha8-cast.pdf

Folgueiras, P. (2023). Técnica de recogida de información: La entrevista. Universidad de Barcelona. Disponible en https://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

Fundación Karisma. (s.f.). Manual Antiespías: Herramientas para la protección digital de periodistas. Recuperado de https://web.karisma.org.co/manual-antiespias-herramientas-para-la-proteccion-digital-de-periodistas/

Goyos Martinez, V., Hernandes Encinas, L. M., De Fuentes, J., & Gonzalez Manzano, L. (2017). Cifrado de datos con preservación del formato. Recuperado de https://www.tic.itefi.csic.es/CIBERDINE/Documetos/Cifrado%20de%20datos%20con%20preservaci%C3%B3n%20del%20formato.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ª ed.). McGraw-Hill.

Kerzner, H. (2017). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* (12th ed.). Wiley.

Lock, D. (2020). *Project Management* (10th ed.). Gower Publishing.

Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 11(1168), 1-20. https://doi.org/10.3390/rs11101168

Huawei Technologies Co., Ltd. (2022, diciembre 20). Introducción a DES, 3DES y AES. Recuperado de https://forum.huawei.com/enterprise/es/Introducci%C3%B3n-a-DES-3DES-y-AES/thread/667234955765366784-667212881550258176

Information Commissioner's Office (ICO). (2018). Guide to the General Data Protection Regulation (GDPR). Recuperado de https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Jones, E., Kemp, E., & Merkelbach, M. (2018). Managing the Security of Aid Workers with Diverse Profiles. European Interagency Security Forum (EISF). Recuperado de

https://gisf.ngo/wp-content/uploads/2018/09/Managing-the-Security-of-Aid-Workers-with-Diverse-Profiles.pdf

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability, 14(8), 1-24. https://doi.org/10.3390/su14010008

Khan Academy. (s.f.). La necesidad de cifrado. Recuperado de https://es.khanacademy.org/computing/ap-computer-science-principles/x2d2f703b37b450a3:online-data-security/x2d2f703b37b450a3:data-encryption/a/symmetric-encryption-techniques

Kinsta. (2023, 24 de julio). ¿Qué es la Encriptación de Datos? Definición, Tipos y Buenas Prácticas. Recuperado de https://kinsta.com/es/base-de-conocimiento/que-es-la-encriptacion

Kosinski, M. (2024, 24 de mayo). ¿Qué es una violación de datos? IBM. Recuperado de https://www.ibm.com/es-es/topics/data-breach

Llorente, A. (2019, 26 de diciembre). Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. BBC News Mundo. Recuperado de https://www.bbc.com/mundo/noticias-50862657

Macrium Software. (2024, abril 2). What Is the Advanced Encryption Standard? AES Explained. Recuperado de https://www.macrium.com/blog/what-is-the-advanced-encryption-standard-aes-explained.

Martínez de la Torre, J. (2016). Cifrado de clave privada: AES. UNAD. Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/40365/rtorrescar.pdf?sequence=3&isAllowed=y

MICITT. (2023). Estrategia Nacional de Ciberseguridad de Costa Rica 2023 - 2027. Recuperado de https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). (2021). Estrategia Nacional de Ciberseguridad de Costa Rica 2021-2025. Recuperado de https://www.micitt.go.cr/sites/default/files/2023-06/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

National Institute of Standards and Technology (NIST). (2024). El Marco de Seguridad Cibernética (CSF) 2.0 del NIST. Gaithersburg, MD: NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.29.spa

Nguyen, T. D., & Ho, T. T. (2021). Enhancing the time performance of encrypting and decrypting large tabular data. Applied Artificial Intelligence, 35(15), 1746-1754. Recuperado de https://www.tandfonline.com/doi/epdf/10.1080/08839514.2021.1991661?needAccess=true

Organización de los Estados Americanos (OEA). (2023). Report on Cybersecurity Workforce Development in an Era of Talent and Skills Shortages. Recuperado de

https://www.oas.org/en/sms/cicte/docs/Report_Cyber_WorkForce_Development_in_an_Era_of_Talent_and_Skills_Shortages.pdf

OWASP Foundation. (2020). Web Security Testing Guide v4.2. Recuperado de https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

PenTest Hub. (2018). *Example Penetration Testing Report v1.0*. Recuperado de https://www.pentest-hub.com/PDF/EXAMPLE-Penetration_Testing_Report_v.1.0.pdf

Proofpoint. (2023). Threat Reference Guide. Recuperado de https://www.proofpoint.com/us/threat-reference/cyber-threat

Protección de Datos LOPD. (s.f.). ¿Qué es el cifrado de datos y cómo nos protege? Recuperado de https://protecciondatos-lopd.com/empresas/derechos-digitales/

PurpleSec. (2019). *Sample Penetration Test Report - Example Institute*. Recuperado de https://purplesec.us/wp-content/uploads/2019/12/Sample-Penetration-Test-Report-PurpleSec.pdf

Ranaweera, R. M. A. I. B. (2024). Secure Medical Data Communication: A Comprehensive Approach with AES Encryption. Proceedings of the Conference on Medical Data Security, 1-15. Recuperado de https://www.researchgate.net/publication/378261261

Reed, J. (2022, 16 de noviembre). Costa Rica state of emergency declared after ransomware attacks. Security Intelligence. Recuperado de https://securityintelligence.com/news/costa-rica-state-emergency-ransomware

Revista Summa. (2023). Costa Rica sufre ciberataques que afectan servicios básicos. Recuperado de https://revistasumma.com/costa-rica-sufrio-882-millones-de-intentos-de-ciberataques-en-2023/

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, Inc. Recuperado de https://onlinelibrary.wiley.com/doi/epdf/10.1002/9781119183471.fmatter

Schneier, B. (2024). Entries Tagged "AES". Recuperado de https://www.schneier.com/tag/aes/.

Shethi, S. (2024, agosto 21). *La autenticación multifactor (MFA) explicada en 5 minutos o menos*. Geekflare. Recuperado de https://geekflare.com/es/multi-factor-authentication/

Tang, C. (2017). Key Performance Indicators for Process Control System Cybersecurity Performance Analysis (NISTIR 8188). National Institute of Standards and Technology. Recuperado de https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8188.pdf

Telefónica Tech. (2023). Cifrado de datos: qué es y cómo protege nuestra información. Recuperado de https://telefonicatech.com/blog/cifrado-preserva-formato-garantizar-privacidad-datos-financieros-personales

Universidad de Jaén. (2023). La observación en la investigación cualitativa. Disponible en https://web.ujaen.es/investiga/tics_tfg/pdf/cualitativa/recogida_datos/recogida_observacion.pdf

University of Phoenix. (2018). Penetration Testing Plan Template (CMGT/400 v7). Recuperado de https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fpentestreports.com

%2Fdownloads%2Fcmgt400_v7_wk2_penetration_testing_plan_template.docx&wdOrigin=BROWSELINK

Wadho, S. A., Meghji, A. F., Yichiet, A., Kumar, R., & Shaikh, F. B. (2023). Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review. VAWKUM Transactions on Computer Sciences, 11(1), 295-305. Recuperado de https://vfast.org/journals/index.php/VTCS/article/view/1521/1241

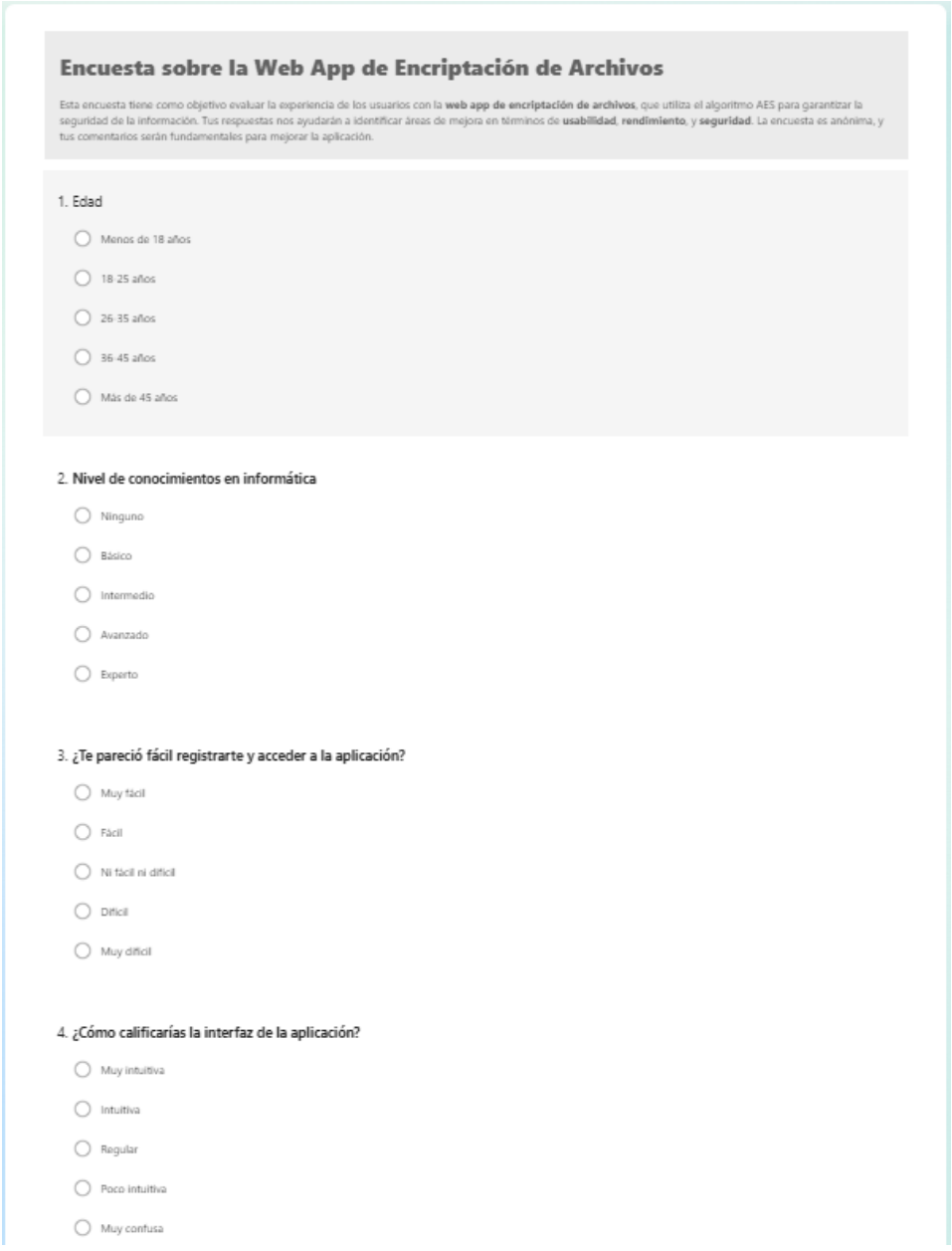
WIRED. (2022). Conti's Attack Against Costa Rica Sparks a New Ransomware Era. Recuperado de https://www.wired.com/story/costa-rica-ransomware-conti

Yadav, R. (2024, junio 20). API encryption and decryption with AES: Best practices and considerations in Python. ThinkODC. Recuperado de https://www.thinkodc.com/blog/api-encryption-and-decryption-with-python

Apéndice

Figura 48

Encuesta sobre la Web App de Encriptación de Archivos



Encuesta sobre la Web App de Encriptación de Archivos

Esta encuesta tiene como objetivo evaluar la experiencia de los usuarios con la **web app de encriptación de archivos**, que utiliza el algoritmo AES para garantizar la seguridad de la información. Tus respuestas nos ayudarán a identificar áreas de mejora en términos de **usabilidad**, **rendimiento**, y **seguridad**. La encuesta es anónima, y tus comentarios serán fundamentales para mejorar la aplicación.

1. Edad
   - Menos de 18 años
   - 18-25 años
   - 26-35 años
   - 36-45 años
   - Más de 45 años

2. **Nivel de conocimientos en informática**
   - Ninguno
   - Básico
   - Intermedio
   - Avanzado
   - Experto

3. **¿Te pareció fácil registrarte y acceder a la aplicación?**
   - Muy fácil
   - Fácil
   - Ni fácil ni difícil
   - Difícil
   - Muy difícil

4. **¿Cómo calificarías la interfaz de la aplicación?**
   - Muy intuitiva
   - Intuitiva
   - Regular
   - Poco intuitiva
   - Muy confusa

5. ¿Tuviste algún problema al subir o descargar archivos?

- ○ No tuve problemas
- ○ Tuve pequeños problemas
- ○ Tuve varios problemas
- ○ No pude subir o descargar archivos

6. ¿Qué tan fácil te resultó encriptar y desencriptar archivos?

- ○ Muy fácil
- ○ Fácil
- ○ Ni fácil ni difícil
- ○ Difícil
- ○ Muy difícil

7. ¿Cómo calificas la velocidad de encriptación de archivos?

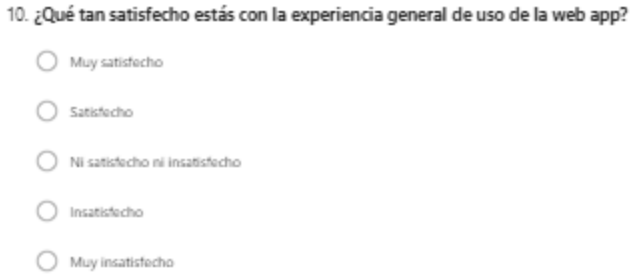
- ○ Muy rápida
- ○ Rápida
- ○ Ni rápida ni lenta
- ○ Lenta
- ○ Muy lenta

8. ¿Te sentiste seguro al encriptar tus archivos con la aplicación?

- ○ Muy seguro
- ○ Seguro
- ○ Ni seguro ni inseguro
- ○ Inseguro
- ○ Muy inseguro

9. ¿Recomendarías esta aplicación a otras personas para encriptar y proteger archivos?

- ○ Definitivamente sí
- ○ Probablemente sí
- ○ No estoy seguro
- ○ Probablemente no
- ○ Definitivamente no



Fuente: Elaboración propia