UNIVERSIDAD DEL MAGDALENA

CIFRADO SIMETRICO CON ALGORITMOS MODERNOS APLICADO A DISPOSITIVOS DE ALMACENAMIENTO EXTRAIBLES PARA LA PROTECION DE DATOS PERSONALES EN WINDOWS

Autor: Camilo Monsalve, Lilia Maldonado

Profesor: Luis del Cristo Garrido barrios

Santa Marta - 2025

ÍNDICE

PROBLEMA

Pregunta problema:

¿Cómo garantizar la protección de datos personales privados almacenados en dispositivos de almacenamiento extraíble mediante la creación de un software con un esquema de cifrada basada en algoritmos modernos en sistemas Windows?

Descripción del problema:

Los dispositivos de almacenamiento extraíbles son los responsables de uno de los puntos más críticos cuando hablamos de seguridad informática a nivel mundial, debido a sus fugas de información. A nivel mundial se registran 190.000 incidentes de malware cada segundo [1], mientras que el 51% del código malicioso en el 2024 fue diseñado para infiltrarse en unidades de almacenamiento portátiles [2], el costo promedio de estas fallas en cuanto a seguridad esta evaluado en $4.88 millones de dólares en 2024 [3], todo esto mientras Windows que es el sistema más atacado tiene una cuota de mercado de 45.7% [3]. En Colombia la situación también es muy grave, con 36.000 millones de ataques cibernéticos registrados en todo el 2024 [4], posicionando al país como el cuarto más vulnerable de América latina. [4] [5]

La ausencia de mecanismos robustos de cifrado es la causante principal de estas vulnerabilidades, si a eso le sumamos el factor humano que intensifica la problemática un 74% por motivos de manipulación o ingeniería social, la cual se usa para engañar a los usuarios [6], también se incluyen la conexión de los dispositivos infectados a puertos USB lo que compromete su integridad [7], La fiscalía general de la nación advierte sobre el uso de técnicas como el “baiting” que busca ejecutar código malicioso en segundos y comprometer equipos mediante la conexión de estos dispositivos modificados [7], también se encontró que entre el 10% y el 15% de los ataques empresariales son mediante el uso de estos mismos dispositivos usados como puente de infiltración. [6] [4]

Las consecuencias de esta falta de protección genera inpactos económicos muy fuertes, esto debido a que las empresas grandes tienen costos promedios de $1.23 millones de dólares por incidentes de fuga de datos [8], mientras que en Colombia el 46% de las organizaciones han sufrido filtraciones de datos confidenciales en los últimos 3 años [8]. Las perdidas por activos intangibles alcanzaron un 19% mas de costo ante los activos tangibles [9] todo esto en Colombia que tiene el 17% de todos los incidentes ocurridos en la región [10] esto significa que las organizaciones colombianas registran pérdidas que oscilan entre 1 millón y 4,000 millones de pesos por fallas de seguridad informática [11] evidenciando la necesidad crítica de implementar mecanismos de protección especializados para dispositivos extraíbles.

JUSTIFICACION:

Con lo anterior dicho se demuestran la necesidad urgente de implementar soluciones de protección especializadas. Con Colombia registrando el 85% de las empresas incrementando sus presupuestos de ciberseguridad en 2024 [12] y proyecciones de crecimiento del 19% en inversión para 2025 [13] [5],existe un interés en herramientas que provean una protección efectiva. El MinTIC invirtió 15 mil millones de pesos en seguridad [14], mientras que las pérdidas por provocada por estos mismos alcanzan hasta 4,000 millones de pesos [11]. Estos hechos demuestran que las empresas entienden lo grave del problema y están dispuestas a invertir en herramientas que garanticen la protección de su información.

Nuestro proyecto de cifrado con algoritmos modernos se diferencia de las soluciones existentes como BitLocker o similares porque al estar específicamente diseñado para el contexto colombiano: Mientras que las herramientas actuales requieren configuraciones complejas o licencias empresariales costosas, nuestra aplicación proporcionará cifrado automático a nivel de kernel con una interfaz simplificada adaptada a usuarios colombianos. En este contexto, donde la Ley 1581 de 2012 regula la protección de datos personales [15]. El ser específico para Windows y el añadido de ser utilizado masivamente en Colombia permite optimizaciones de rendimiento y ventajas de usabilidad que las soluciones comunes no ofrecen.

Una vez dicho todo lo anterior, los aportes científicos y técnicos de este proyecto proporcionarán beneficios directos que transformarán los dispositivos extraíbles de puntos de riesgo en herramientas seguras de transporte informacional. La implementación del cifrado simétrico moderno garantizará protección robusta contra el robo de información [16] [17], eliminando la posibilidad de acceso no autorizado para dispositivos que han sido robados o extraviados. El proyecto contribuirá al conocimiento en seguridad informática mediante el uso de metodologías replicables de cifrado para dispositivos portátiles extraíbles, estableciendo precedentes para futuras investigaciones en protección de datos que aborde específicamente las vulnerabilidades documentadas en el contexto colombiano.

OBJETIVOS

OBJETIVO GENERAL:

Desarrollar un software de cifrado simétrico basado en algoritmos AES para dispositivos de almacenamiento extraíbles en sistemas Windows.

OBJETIVOS ESPECÍFICOS:

1. Analizar el contexto de vulnerabilidades en dispositivos de almacenamiento extraíbles para sistemas Windows asi como las leyes modernas de cifrado
2. Diseñar la plataforma de software de cifrado simétrico, definiendo la arquitectura y los componentes que integran el algoritmo AES con las APIs criptográficas.
3. Construir un prototipo funcional de la plataforma de cifrado para dispositivos de almacenamiento extraíbles, a partir de la arquitectura y los requisitos definidos.
4. Evaluar la plataforma desarrollada mediante pruebas de rendimiento, seguridad y usabilidad, identificando su comportamiento bajo diferentes escenarios de uso.
5. Comparar los resultados obtenidos por la plataforma con herramientas existentes como BitLocker y VeraCrypt, con el propósito de determinar sus ventajas, limitaciones y nivel de efectividad.

MARCO TEÓRICO

Fundamentos de criptografía

La criptografía tiene sus raíces en la palabra griega "kryptos", que significa "oculto". Se refiere a una forma de comunicación en la que los mensajes se esconden para que solo las personas autorizadas puedan entenderlos. Esto incluye diferentes maneras de transmitir información digital, como texto, imágenes, videos y sonidos. La criptografía hace que los mensajes sean ilegibles al convertirlos en un formato que no se puede leer fácilmente. La criptología es un campo más amplio que incluye tanto la criptografía como el criptoanálisis. Tiene fuertes conexiones con la informática y las matemáticas avanzadas. [18]

Los fundamentos de la criptografía moderna se diferencian de los enfoques antiguos en su énfasis en definiciones claras, suposiciones específicas y demostraciones sólidas de seguridad [19] [20].

Cifrado simétrico y algoritmos aes

Los sistemas de cifrado simétrico son una categoría básica que usan una clave secreta para cifrar y descifrar datos [19]. Tradicionalmente, se dividen en cifrados de flujo, que procesan datos bit por bit, y cifrados de bloque, que trabajan con bloques de tamaño fijo [19].

El Advanced Encryption Standard (AES), también llamado FIPS 197, es el estándar más usado en todo el mundo [21]. AES se basa en el algoritmo Rijndael, que trabaja con bloques de 128 bits y admite claves de 128, 192 o 256 bits [22].Su matemática se apoya en operaciones en el campo Galois GF(2^8), y organiza los datos en una matriz de 4×4 bytes [22].

Cada ronda de AES realiza cuatro operaciones básicas: SubBytes (intercambio de bytes de forma no lineal), ShiftRows (desplazamiento de filas), MixColumns (mezcla lineal) y AddRoundKey (XOR con la subclave) [22]. Los modos de uso incluyen ECB, CBC, CTR y GCM, cada uno con funciones distintas para diferentes usos [23] .

Seguridad en dispositivos USB y en sistemas Windows

Los dispositivos de almacenamiento portátiles tienen vulnerabilidades específicas debido a su movilidad y facilidad de conexión [24]. Investigaciones sobre dispositivos IronKey muestran que, incluso con certificación FIPS 140-2 Level 3, pueden tener vulnerabilidades explotables mediante manipulación de hardware [24]. Los ataques de "baiting" son una amenaza donde dispositivos aparentemente legales contienen hardware malicioso [25].

Microsoft Windows ofrece APIs criptográficas con Cryptography Next Generation (CNG) y Data Protección API (DPAPI) [26].CNG permite crear proveedores criptográficos basados en software o hardware, incluyendo integración con módulos HSM y TPM [26]. DPAPI ofrece funciones para proteger datos usando claves derivadas de las credenciales del usuario y secretos del sistema [26].

Los problemas de sanitización en dispositivos flash USB son un riesgo importante, ya que los métodos estándar de eliminación no siempre borran toda la información sensible [27]. Esto es aún más evidente por las diferencias entre fabricantes [27] [28].

Estándares criptográficos y marco normativo

El National Institute of Standards and Technology (NIST) establece las reglas básicas a través de publicaciones FIPS y Special Publications [29] . NIST SP 800-175B da guías sobre mecanismos criptográficos, recomendando longitudes de clave y algoritmos aprobados. [29] La validación se realiza mediante el Cryptographic Algorithm Validation Program (CAVP) [21]

En Colombia, la Ley 1581 de 2012 establece las reglas para proteger los datos personales, y pide medidas técnicas apropiadas, como el cifrado en dispositivos que almacenan datos sensibles. La Superintendencia de Industria y Comercio (SIC) actúa como autoridad de control. Además, el proyecto de modernización añadirá derechos como el olvido y la portabilidad de los datos. [5]

Las buenas prácticas incluyen usar algoritmos aprobados por NIST, tener longitudes de clave adecuadas, usar modos de operación seguros y gestionar bien las claves. La unión de las reglas colombianas y los estándares internacionales crea un marco que facilita soluciones que ofrecen seguridad fuerte y son fáciles de usar. [9]

MARCO CONCEPTUAL

1. Advanced Encryption Standard (AES): Es un algoritmo de cifrado de clave simétrica que se utiliza en la ciberseguridad para proteger la confidencialidad de la información. Utiliza una clave de 128, 192 o 256 bits para codificar y descodificar los datos. [31]
2. Cifrado Simétrico: El cifrado simétrico es un método criptográfico en el cual se usa una única clave compartida para cifrar y descifrar mensajes entre el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. [30]
3. CNG (Cryptography Next Generation): Es la nueva generación de APIs criptográficas de Microsoft proporcionando una interfaz más flexible y segura para operaciones criptográficas, permitiendo la implementación de más proveedores. [26]
4. DPAPI (Data Protection API): Es una sencilla interfaz de programación de aplicaciones criptográficas que permite a los desarrolladores cifrar claves utilizando claves simétricas derivada de los secretos de inicio de sesión del usuario. [32]
5. TPM (Trusted Platform Module): Es un chip especial integrado en portátiles y ordenadores que ofrece importantes funciones de seguridad para comprobar la integridad y la seguridad de los sistemas y el software en un entorno protegido. [33]
6. Kernel: El kernel es el componente central de un sistema operativo y sirve como interfaz principal entre el hardware físico de la computadora y los procesos que se ejecutan en ella a través del software. [34]
7. Texto Cifrado: El texto cifrado es el resultado de aplicar un algoritmo de cifrado sobre un texto plano utilizando una clave criptográfica. Este texto es ilegible para cualquier persona que no posea la clave de descifrado correspondiente. [27]

ESTADO DEL ARTE

Año	Autor(es)	Aporte al proyecto
2021	Juremi, J., Naidu Mahendran, C., Var Naseri, M., & Sulaiman, S.	Desarrollaron FlashSafe, un software similar que permite proteger datos personales usando cifrado. Nos ayuda a comprender la implementación práctica de cifrado AES en dispositivos USB. [16]
2021	Matsumoto, M. O. M., & Oguchi, M.	Propusieron un sistema para acelerar el cifrado en dispositivos IoT usando cifrado homomórfico, reduciendo significativamente la carga computacional. aportandonos optimización de rendimiento en dispositivos con recursos limitados. [18]
2023	Karageorgopoulou, A., Tsoukas, V., Spathoulas, G., & Kakarountas, A.	Implementaron el algoritmo Paillier para cifrado homomórfico en dispositivos portátiles logrando una reducción del 20% en el tiempo de ejecución. Demostrando que es posible usar uso de estos para obtener mejores tiempos. [17]
2024	Feng, S., Qin, Y., Zeng, Z., et al.	Propusieron un modelo ligero de protección de privacidad basado en cifrado homomórfico Paillier para redes de detección de multitudes móviles, logrando 98.84% protección, Contribuye apoyando el uso de estos algoritmos. [25]
2025	Rasheed, A. M., et al.	Desarrollaron algoritmos criptográficos ligeros para mejorar la seguridad en dispositivos IoT, demostrando valores NPCR de 99.6151 y UACI de 38.8925. Sirve para proporcionarnos métricas de evaluación de seguridad. [35]
2022	Dumitru, R., Wabnitz, A., Genkin, D., & Yarom, Y.	Presentaron el primer ataque de inyección fuera de ruta a la integridad de las comunicaciones USB, demostrando vulnerabilidades en hubs USB 2.0. Permite comprender los vectores de ataque específicos contra dispositivos USB. [36]

METODOLOGIA

La metodología Secure Scrum fue la escogida, que es una modificación del marco ágil Scrum diseñada específicamente para proyectos de desarrollo de software con necesidades críticas de seguridad, se utilizará para el desarrollo de nuestro software cifrado simétrico. Esta técnica incluye S-Tags (etiquetas de seguridad), que posibilitan la identificación y el rastreo de requerimientos de seguridad, tales como disponibilidad, confidencialidad e integridad, durante todo el ciclo de desarrollo.

Justificación de la metodología:

1. Desarrollo incremental y por iteraciones: Permite la validación constante de varios modos de operación y configuraciones de algoritmos AES a través de breves ciclos de desarrollo.
2. Perspectiva integrada en seguridad: Los S-Tags aseguran que los requerimientos de seguridad sean tomados en cuenta desde el comienzo y se mantengan a lo largo de todas las etapas del proyecto.
3. Capacidad de adaptación: Permite modificar las prioridades de acuerdo a los resultados de las pruebas de seguridad y rendimiento en cada iteración.
4. Validación académica: La estructura de sprints permite mostrar los avances al asesor académico con regularidad para una retroalimentación constante.
5. Documentación balanceada: Conserva la cantidad de documentación necesaria para un proyecto académico sin comprometer la rapidez del desarrollo.

Fases del Proceso Pensadas hasta el momento

1. Planificación del Proyecto

   En esta etapa, revisamos los estándares NIST FIPS 197 y la Ley 1581 de 2012. Analizamos vulnerabilidades en dispositivos de almacenamiento extraíbles usando información técnica. Recopilamos requisitos funcionales y no funcionales para el software. Creamos casos de uso para escenarios normales, de error y de seguridad. Elaboramos el Product Backlog con historias de usuario. Priorizamos y etiquetamos estas historias con S-Tags de seguridad: confidencialidad, integridad, disponibilidad, autenticación y auditoría. Definimos los roles del equipo de desarrollo. Asignamos responsabilidades a cada miembro. Establecemos requisitos técnicos y recursos necesarios. Planificamos sprints y entregables.

2. Diseño Inicial

   Basándonos en los requisitos, diseñamos una arquitectura modular. Esta tiene capas de presentación, lógica de negocio, acceso a hardware y seguridad. Seleccionamos variantes de AES y modos de operación (CBC, CTR, GCM) tras comparar rendimiento y seguridad.

Diseñamos la integración con APIs CNG para operaciones de cifrado y DPAPI para proteger claves. Consideramos la interacción con TPM. Creamos diagramas UML de componentes, secuencia y clases para documentar los flujos de cifrado y descifrado. Diseñamos la interfaz de usuario enfocándonos en la usabilidad. Validamos los wireframes.

3. Desarrollo Iterativo

Realizamos sprints de dos semanas para implementar funcionalidades del Product Backlog. En cada sprint, codificamos siguiendo estándares de código seguro. Validamos entradas, manejamos memoria de forma segura y aplicamos el principio de mínimo privilegio. Desarrollamos módulos de cifrado AES con CNG, gestión de claves con DPAPI, autenticación de usuarios e interfaz gráfica. Hacemos entregas periódicas para recibir evaluación y retroalimentación del asesor académico en las sprint reviews. Ejecutamos pruebas unitarias con cobertura mínima del 80% y pruebas de integración. Aplicamos pruebas de seguridad como intentos de bypass, resistencia a fuerza bruta y sanitización de memoria. Mejoramos el software según lo identificado en las retrospectivas.

4. Pruebas Continuas

Durante todo el desarrollo, realizamos pruebas funcionales y no funcionales para identificar y solucionar problemas rápidamente. Ejecutamos pruebas de rendimiento con herramientas como CrystalDiskMark y Performance Monitor. Medimos la velocidad de cifrado y descifrado en archivos de 1MB, 100MB y 1GB, y en USB 2.0, 3.0 y 3.1. Aplicamos cuestionarios System Usability Scale (SUS) a usuarios beta para evaluar la facilidad de uso e interfaz. Realizamos pruebas avanzadas de seguridad, incluyendo penetration testing. Comparamos el software con BitLocker y VeraCrypt usando una matriz que evalúa seguridad, rendimiento, usabilidad y cumplimiento normativo. Validamos el cumplimiento del estándar NIST FIPS 197 verificando las especificaciones del algoritmo y las longitudes de clave.

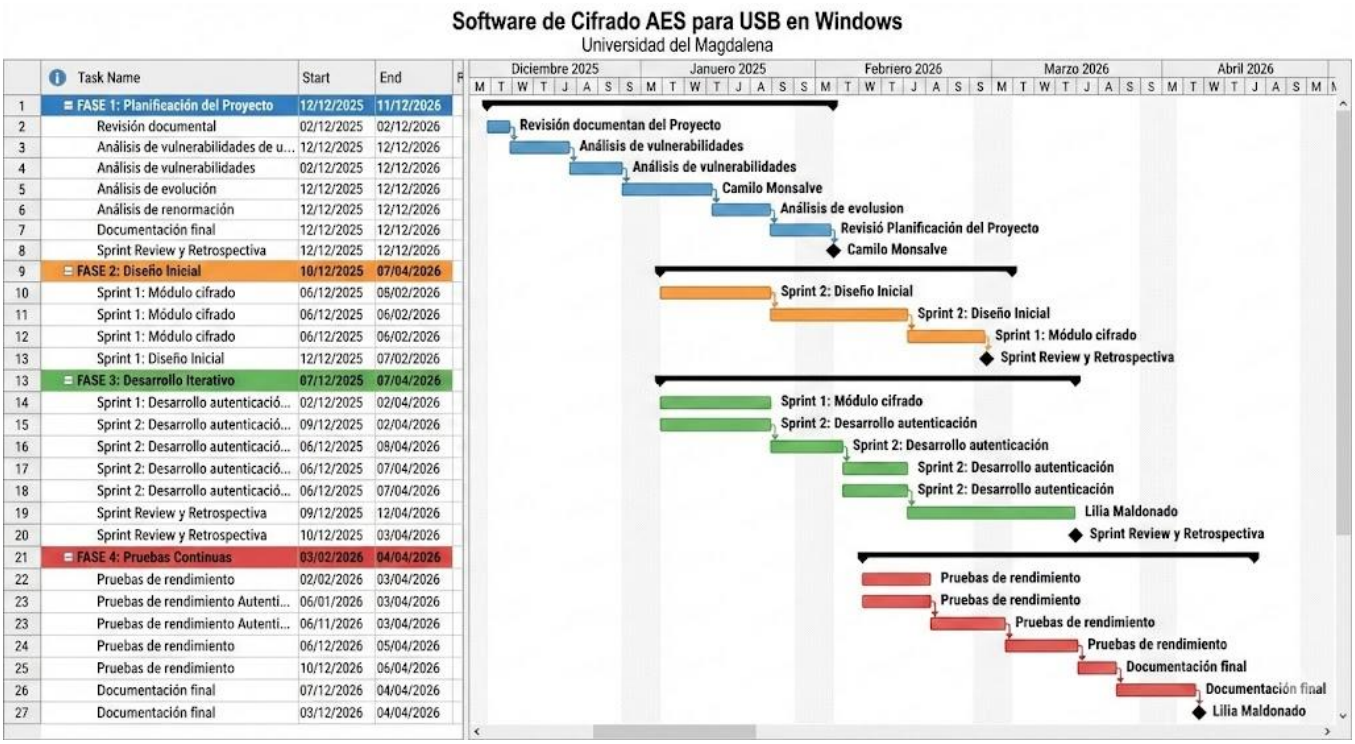
CRONOGRAMA

ID	Nombre de la Tarea	Duración	Inicio	Fin	Responsable	Entregable
1	FASE 1: Planificación del Proyecto	21 días	2/12/2025	23/12/2025	--	--

2	Revisión documental de estándares	5 días	2/12/2025	6/12/2025	Camilo & Lilia	Resumen NIST FIPS 197 y Ley 1581
3	Análisis de vulnerabilidades en USB	4 días	7/12/2025	10/12/2025	Camilo	Doc. análisis de vulnerabilidades
4	Recopilación de requisitos	3 días	11/12/2025	13/12/2025	Lilia	Matriz de requisitos
5	Desarrollo de casos de uso	4 días	14/12/2025	17/12/2025	Camilo & Lilia	Documento de casos de uso
6	Creación Product Backlog (S-Tags)	3 días	18/12/2025	20/12/2025	Camilo	Product Backlog priorizado
7	Definición de equipo y roles	2 días	21/12/2025	22/12/2025	Camilo & Lilia	Documento de asignación de roles
8	Planificación de sprints	1 día	23/12/2025	23/12/2025	Camilo & Lilia	Calendario de sprints
9	FASE 2: Diseño Inicial	21 días	6/1/2026	27/1/2026	--	--
10	Diseño arquitectura modular	5 días	6/1/2026	10/1/2026	Camilo	Diagrama de arquitectura
11	Selección algoritmos AES y modos	3 días	11/1/2026	13/1/2026	Camilo	Matriz comparativa CBC/CTR/GCM
12	Diseño integración CNG y DPAPI	5 días	14/1/2026	18/1/2026	Lilia	Especificación técnica de APIs
13	Elaboración diagramas UML	4 días	19/1/2026	22/1/2026	Lilia	Diagramas componentes/secuencia
14	Diseño de interfaz de usuario	3 días	23/1/2026	25/1/2026	Lilia	Wireframes y mockups
15	Validación de diseños	2 días	26/1/2026	27/1/2026	Camilo & Lilia	Prototipos validados
16	FASE 3: Desarrollo Iterativo	63 días	28/1/2026	1/4/2026	--	--
17	Sprint 1: Módulo cifrado AES (CNG)	14 días	28/1/2026	10/2/2026	Camilo	Módulo AES funcional
18	Sprint 1: Integración DPAPI	14 días	28/1/2026	10/2/2026	Lilia	Módulo DPAPI integrado
19	Sprint Review y Retrospectiva 1	1 día	11/2/2026	11/2/2026	Camilo & Lilia	Retroalimentación del asesor
20	Sprint 2: Desarrollo autenticación	14 días	12/2/2026	25/2/2026	Lilia	Sistema autenticación funcional
21	Sprint 2: Interfaz gráfica básica	14 días	12/2/2026	25/2/2026	Lilia	UI básica implementada
22	Sprint 2: Pruebas de integración	3 días	26/2/2026	28/2/2026	Camilo	Informe pruebas de integración
23	Sprint Review y Retrospectiva 2	1 día	1/3/2026	1/3/2026	Camilo & Lilia	Mejoras identificadas

24	Sprint 3: Optimización rendimiento	14 días	2/3/2026	15/3/2026	Camilo	Software optimizado
25	Sprint 3: Pruebas de seguridad	5 días	16/3/2026	20/3/2026	Camilo	Informe pruebas de seguridad
26	Sprint 3: Interfaz mejorada	10 días	16/3/2026	25/3/2026	Lilia	UI mejorada (feedback usuarios)
27	Sprint Review y Retrospectiva 3	1 día	26/3/2026	26/3/2026	Camilo & Lilia	Software versión beta
28	FASE 4: Pruebas Continuas	28 días	27/3/2026	23/4/2026	--	--
29	Pruebas rendimiento (benchmarking)	7 días	27/3/2026	2/4/2026	Camilo	Informe rendimiento y gráficas
30	Cuestionarios SUS (Usuarios Beta)	7 días	3/4/2026	9/4/2026	Lilia	Reporte SUS y matriz usabilidad
31	Pruebas avanzadas (Pentesting)	5 días	10/4/2026	14/4/2026	Camilo	Informe seguridad avanzada
32	Comparación BitLocker/VeraCrypt	5 días	15/4/2026	19/4/2026	Camilo	Matriz comparativa
33	Validación cumplimiento NIST FIPS 197	3 días	20/4/2026	22/4/2026	Lilia	Certificado de cumplimiento
34	Documentación final y Presentación	2 días	23/4/2026	24/4/2026	Camilo & Lilia	Documentación completa y slides

Grafica Gantt



PRESUPUESTO

PRESUPUESTO GENERAL	
RUBRO	**VALOR**
Personal	$4.000.000 COP
Equipos e insumos	$6.500.000 COP
Servicios técnicos	$1.850.000 COP
Software y herramientas	$950.000 COP
TOTAL PROYECTO	$13.300.000 COP (13,3 millones)

Presupuesto personal			
Investigador	**Rol**	**Dedicación**	**Valor**
Camilo Monsalve	Desarrollador Backend - Arquitectura de software, módulo de cifrado AES con CNG, integración con TPM, pruebas de rendimiento y seguridad	20 horas/semana (4.5 meses)	$2.000.000 COP
Lilia Maldonado	Desarrolladora Frontend - Diseño de interfaz de usuario, integración DPAPI, módulo de autenticación, pruebas de usabilidad y documentación	20 horas/semana (4.5 meses)	$2.000.000 COP
Subtotal Personal			$4.000.000 COP

Presupuesto equipo e insumos				
Descripción	**Cantidad**	**Justificación**	**Valor Unitario**	**Valor Total**
Laptop HP/Lenovo Intel i7, 16GB RAM, 512GB SSD, Windows 11 Pro	2	Equipos de desarrollo con capacidad para ejecutar entornos de compilación, pruebas y herramientas de seguridad	$2.500.000 COP	$5.000.000 COP
Kit de dispositivos USB 2.0/3.0/3.1 (8 unidades variadas)	1	Dispositivos de almacenamiento extraíbles de diferentes capacidades (8GB-128GB) para pruebas de compatibilidad y rendimiento	$800.000 COP	$800.000 COP
Disco duro externo 2TB	1	Respaldo de código fuente, documentación técnica, resultados de pruebas y datos del proyecto	$400.000 COP	$400.000 COP

Módulo TPM 2.0 externo	1	Para pruebas de integración con Trusted Platform Module en equipos sin chip integrado	$300.000 COP	$300.000 COP
Subtotal Equipos				$6.500.000 COP

Presupuesto servicios		
Servicio	**Descripción**	**Valor**
Licencias Windows 10/11 Pro	Licencias originales para 2 equipos con acceso completo a APIs empresariales CNG, DPAPI y gestión de TPM	$800.000 COP
Asesoría en ciberseguridad	Consultoría con experto certificado en seguridad informática para validación de arquitectura de cifrado y revisión de implementación de algoritmos AES	$600.000 COP
Servicio de penetration testing	Pruebas de seguridad avanzadas externas (ethical hacking) para identificar vulnerabilidades en el software desarrollado	$450.000 COP
Subtotal Servicios		$1.850.000 COP (1,85 millones)

Presupuesto software			
Herramienta	**Propósito**	**Licencia**	**Valor**
Visual Studio Professional 2022	Entorno de desarrollo integrado (IDE) para C#/.NET con depurador avanzado y soporte para Windows SDK	Anual (2 licencias)	$450.000 COP
GitHub Team	Control de versiones, repositorio privado compartido, gestión de código colaborativo	Anual	$120.000 COP
Jira Software	Gestión ágil del proyecto: sprints Scrum, Product Backlog, seguimiento de S-Tags de seguridad, reportes	Anual (2 usuarios)	$150.000 COP
Burp Suite Professional	Herramienta profesional de penetration testing y análisis de vulnerabilidades en aplicaciones	Anual	$180.000 COP
Lucidchart	Diseño de diagramas UML, arquitectura de software, wireframes y documentación visual	Anual (2 usuarios)	$50.000 COP
Subtotal Software			$950.000 COP

BIBLIOGRAFÍA

[1] J. Estenssoro Valasek, «AVG,» MALWARE, 5 Noviembre 2024. [En línea]. Available: https://www.avg.com/en/signal/malware-statistics. [Último acceso: 20 Septiembre 2025].

[2] S. Pateriya, «scalefusion,» sr, 19 Agosto 2025. [En línea]. Available: https://blog.scalefusion.com/es/usb-security-management/.

[3] E. Bonnie y A. Fitzgerald, «secureframe,» 24 Septiembre 2025. [En línea]. Available: https://secureframe-com.translate.goog/blog/data-breach-statistics?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc&_x_tr_hist=true. [Último acceso: 19 Septiembre 2025].

[4] K. Pinto Duitama, «larepublica.co,» LR, 12 07 2025. [En línea]. Available: https://www.larepublica.co/internet-economy/colombia-tuvo-36-000-millones-de-ciberataques-4178202.

[5] econexia, «econexia,» economia2025, 17 04 2025. [En línea]. Available: https://econexia.com/es/contenidos-articulo/industria-construccion-y-medio-ambiente/1537/Inversion-ciberseguridad-en-Colombia-2025.

[6] S. Gomez Pena, «domesicatueconomia,» es, 04 Septiembre 2025. [En línea]. Available: https://www.domesticatueconomia.es/pendrive-medidas-proteccion-uso-memorias-usb/.

[7] ambitojuridico, «ambitojuridico,» ambitojuridico, 03 09 2025. [En línea]. Available: https://www.ambitojuridico.com/noticias/penal/cuidado-con-conectar-usb-desconocida-ciberdelincuentes-podrian-robarle.

[8] D. Dorado, «latinpyme,» 4 febrero 2025. [En línea]. Available: https://latinpyme.com/fugas-de-datos-afectan-al-46-de-las-empresas-en-colombia/.

[9] cibercorp, «cibercorp,» cibercorp, 13 01 2025. [En línea]. Available: https://www.cibercorp.com.mx/post/ciberataques-en-colombia.

[10] newnetsa, «newnetsa,» seguridad, 25 04 2025. [En línea]. Available: https://www.newnetsa.com/ciberataques-en-colombia/.

[11] Coordinacion TIC, «incp.org.co,» tecgov, 25 07 2019. [En línea]. Available: https://incp.org.co/publicaciones/infoincp-publicaciones/informacion-para-empresas/entorno/innovation/2019/07/aumenta-monto-perdidas-economicas-ciberataques-colombia/.

[12] acis, «acis,» gov.co, 18 09 2025. [En línea]. Available: https://www.acis.org.co/blog/noticias-2/el-mercado-de-la-ciberseguridad-en-colombia-una-frontera-estrategica-para-la-resiliencia-digital-2761.

[13] acis, «acis.org.co,» colombia, [En línea]. Available: https://www.acis.org.co/blog/noticias-2/colombia-el-cuarto-pais-con-mas-ciberataques-en-america-latina-36-000-millones-de-intentos-en-2024-1266.

[14] CLARO, «CLARO,» 17 09 2025. [En línea]. Available: https://www.claro.com.co/empresas/noticias-interes/ciberseguridad-colombia/.

[15] datalawsas, «datalawsas,» 04 07 2025. [En línea]. Available: https://datalawsas.com/proteccion-datos-ley-colombia.

[16] J. Juremi, C. Naidu Mahendran, M. Var Naseri y S. Sulaiman, «FlashSafe: USB Flash Drives Encryption Tool with AES Algorithm,» IEEE EXPLORER, Kuala Lumpur, 2021.

[17] A. Karageorgopoulou, V. Tsoukas, G. Spathoulas y A. Kakarountas, «). Porting the Paillier Algorithm for Homomorphic Encryption on Portable Devices.,» IEEE EXPLORER, Lamia, Grecia, 2023.

[18] M. O. M. Matsumoto, «Speeding Up Encryption on IoT Devices Using Homomorphic Encryption,» IEEE EXPLORER, Tokyo, Japon, 2021.

[19] J. Katz y Y. Lindell, Introduction to Modern Cryptography, vol. 3rd Edition, New york: Chapman and Hall/CRC, 2020.

[20] J. Daemen y V. Rijmen, The Design of Rijndael, vol. I, berlin: Springer Berlin, Heidelberg, 2002.

[21] U. D. o. Commerce, Advanced Encryption Standard (AES), Gaithersburg: National Institute of Standards and Technology, 2023.

[22] k. Avinash , AES: The Advanced Encryption Standard, West Lafayette, 2025.

[23] D. Chakraborty y F. Rodriguez-Henriquez, Block Cipher Modes of Operation from a Hardware, Ciudad de mexico, 2008.

[24] S. Skorobogatov , Teardown and feasibility study of IronKey - the most secure USB Flash drive, Cambridge: Cryptography and Security (cs.CR), 2021.

[25] W. Chun-Yi y H. Fu-hau, USBIPS Framework: Protecting Hosts from Malicious USB Peripherals, Taoyuan, 2024.

[26] microsoft, «microsoft.com,» microsoft, 06 06 2023. [En línea]. Available: https://learn.microsoft.com/en-us/windows/win32/seccng/cng-dpapi.

[27] J. Schneider y I. Lautner, In Search of Lost Data: A Study of Flash Sanitization Practices, Leiden: Digital Forensics Research Conference Europe, 2025.

[28] J. Conacher y K. Renaud, Caveat Venditor, Used USB Drive Owner, Dundee, 2020.

[29] E. Barker , Guideline for Using Cryptographic Standards in the Federal Government:Cryptographic Mechanisms, new york: NIST, 2020.

[30] Wikipedia, «Wikipedia,» 25 04 2024. [En línea]. Available: https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica.

[31] msmk, «msmk university,» 12 09 2024. [En línea]. Available: https://msmk.university/advanced-encryption-standard-aes/.

[32] Wikipedia users, «Wikipedia,» 22 11 2020. [En línea]. Available: https://es.wikipedia.org/wiki/API_de_protecci%C3%B3n_de_datos.

[33] I. editorial, «Ionos,» 10 06 2023. [En línea]. Available: https://www.ionos.com/es-us/digitalguide/servidores/configuracion/trusted-platform-module/.

[34] J. Horcajuelo Muñoz, «salesystems,» 6 1 2024. [En línea]. Available: https://salesystems.es/que-es-un-kernel/.

[35] A. M. Rasheed, Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT, US: Frontiers, 2025.

[36] R. W. A. G. D. &. Y. Y. Dumitru, The Impostor Among US(B): Off-Path Injection Attacks on USB Communications, Moscu: USENIX Security Symposium, 2022.