ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.2635

BioShield AI-Py

Acosta Romero Daiana Magalí[1]; Vargas Enzo Nicolás[2]
[1]*University National Technological University - Delta Regional Faculty, Argentina,* magaliacosta.r@gmail.com
[2]*University National Technological University - Regional Faculty Cordoba, Argentina, nico.var95@gmail.com*

Abstract– ***The BioShield-AI ecosystem constitutes an advanced engineering platform focused on the critical management of biosecurity and environmental traceability, basing its operation on an immutable blockchain architecture that employs the SHA-256 hashing algorithm to shield data integrity against any manipulation attempts in biological risk scenarios. Through the implementation of an audit engine with constant algorithmic efficiency (O(1)), the system guarantees instant forensic validation of massive records, whose results are processed and displayed on an interactive Tactical Dashboard developed in Streamlit. This command center integrates dynamic pathogen dispersion visualizations and a threat classification system based on artificial intelligence logic, facilitating strategic, evidence-based decision-making. Finally, the project transcends technical functionality by incorporating Green Engineering (Green Computing) principles through active monitoring of resource consumption and carbon footprint, ensuring global portability and scalability through containerization with Docker, which positions BioShield-AI as a robust, sustainable, and resilient technological solution against contemporary biological emergencies.***

Keywords– ***-Immutable Blockchain, Environmental, Traceability, Optimized Audit, Green Engineering, Containers (Docker).***

BioShield AI-Py

Acosta Romero Daiana Magalí[1]; Vargas Enzo Nicolás[2]
[1]*Universidad Tecnológica Nacional - Facultad Regional Delta, Argentina,* macosta@frd.utn.edu.ar
[2]*Universidad Tecnológica Nacional - Facultad Regional Córdoba, Argentina, nico.var95@gmail.com*

Resumen– ***El ecosistema BioShield-AI constituye una plataforma de ingeniería avanzada orientada a la gestión crítica de la bioseguridad y la trazabilidad ambiental, fundamentando su operatividad en una arquitectura de blockchain inmutable que emplea el algoritmo de hashing SHA-256 para blindar la integridad de los datos frente a cualquier intento de manipulación en escenarios de riesgo biológico. A través de la implementación de un motor de auditoría con eficiencia algorítmica constante (O(1)), el sistema garantiza una validación forense instantánea de registros masivos, cuyos resultados son procesados y expuestos en un Dashboard Táctico interactivo desarrollado en Streamlit. Este centro de mando integra visualizaciones dinámicas de dispersión de patógenos y un sistema de clasificación de amenazas basado en lógica de inteligencia artificial, facilitando una toma de decisiones estratégica y basada en evidencia. Finalmente, el proyecto trasciende la funcionalidad técnica al incorporar principios de Ingeniería Verde (Green Computing) mediante la monitorización activa del consumo de recursos y la huella de carbono, asegurando una portabilidad y escalabilidad global a través de la containerización con Docker, lo que posiciona a BioShield-AI como una solución tecnológica robusta, sostenible y resiliente ante las emergencias biológicas contemporáneas.***

Palabras claves-- Blockchain Inmutable, Trazabilidad Ambiental, Auditoría Optimizada, Ingeniería Verde, Contenedores (Docker)

I. Introducción y Contextualización

En el umbral de una era marcada por la crisis climática y la globalización acelerada, la gestión de la bioseguridad se ha transformado en uno de los pilares fundamentales para la supervivencia y la estabilidad de las infraestructuras críticas a nivel global. Trabajos recientes han demostrado que los sistemas basados en IoT con monitoreo en tiempo real y alerta temprana impulsada por IA son herramientas fundamentales para gestionar los riesgos de enfermedades infecciosas emergentes [1]. La detección temprana y la trazabilidad inmutable de agentes biológicos o cambios ambientales anómalos no son solo requerimientos técnicos, sino imperativos éticos y sociales. Sin embargo, los sistemas de monitoreo tradicionales a menudo adolecen de vulnerabilidades críticas: la centralización de los datos, la falta de transparencia en la cadena de custodia de la información y una ineficiencia algorítmica que impide una respuesta en tiempo real. En este contexto nace BioShield-AI, una plataforma diseñada para converger la seguridad criptográfica de vanguardia con la analítica de datos avanzada, proporcionando un ecosistema de confianza para instituciones académicas, gubernamentales y organizaciones no gubernamentales (ONGs).

La problemática central que aborda este proyecto radica en la fragilidad de la integridad de los datos ambientales. En misiones de campo, los sensores desplegados suelen enviar información a servidores centrales que son susceptibles de manipulaciones malintencionadas o errores de sincronización. BioShield-AI propone un cambio de paradigma mediante la implementación de una arquitectura de Blockchain inmutable. Al utilizar el algoritmo de hashing SHA-256, cada registro de temperatura, humedad o nivel de riesgo se convierte en un eslabón único y permanente dentro de un libro mayor distribuido. Esta aproximación garantiza que la trazabilidad no sea solo una meta, sino una propiedad intrínseca del sistema, permitiendo que cualquier auditoría forense revele intentos de alteración de datos de manera inmediata y fehaciente.

Más allá de la seguridad, la contextualización de este proyecto se enmarca dentro de la Ingeniería Verde (Green Computing). En un mundo donde el software consume cantidades masivas de energía, BioShield-AI se destaca por su enfoque en la eficiencia de recursos. La optimización del motor de auditoría a una complejidad de O(1) es un hito técnico fundamental: mientras que otros sistemas requieren recorrer toda la base de datos para verificar su integridad (complejidad lineal), BioShield-AI lo logra en tiempo constante. Esta eficiencia no solo permite un despliegue ágil en dispositivos con capacidades limitadas de procesamiento, como microcontroladores o drones de monitoreo, sino que también minimiza la huella de carbono digital del proceso computacional, alineando el desarrollo tecnológico con la preservación del medio ambiente.

Finalmente, el despliegue mediante tecnologías de containerización (Docker) sitúa a BioShield-AI como una herramienta de alta adaptabilidad. En un escenario de crisis biológica, la velocidad de despliegue es vital. Al encapsular toda la lógica de la inteligencia artificial, el motor de blockchain y la interfaz de usuario en contenedores portables, el sistema garantiza que investigadores de cualquier parte del mundo puedan levantar un centro de comando táctico en minutos, sin preocuparse por incompatibilidades de sistema. BioShield-AI representa, por tanto, una respuesta integral y escalable que utiliza la tecnología para proteger la vida, garantizando que la información que guía las decisiones críticas sea, por encima de todo, veraz e inalterable.

II. Planteamiento del Problema

En la actualidad, la gestión de crisis biológicas y el monitoreo de riesgos ambientales se enfrentan a un desafío sin

precedentes: la "infodemia" y la fragilidad de la infraestructura de datos.Las redes de sensores IoT capaces de detectar patógenos en tiempo real representan un paso fundamental para abordar esta brecha [1], sin embargo, las implementaciones actuales carecen de garantías de integridad de los datos. El problema fundamental radica en que la información recolectada en el punto de origen (sensores de campo, drones de reconocimiento o estaciones meteorológicas) es susceptible de sufrir alteraciones ya sean accidentales por fallos de red o deliberadas por ataques cibernéticos antes de llegar a los tomadores de decisiones. En un escenario donde se debe decidir la evacuación de una zona o la contención de un patógeno, un solo dato modificado puede traducirse en pérdidas humanas y económicas irreparables.

Esta vulnerabilidad se ve agravada por la falta de una "cadena de custodia digital" verificable. Actualmente, cuando una organización no gubernamental o una universidad analiza datos de dispersión de patógenos, es difícil demostrar ante terceros que dichos registros no han sido manipulados para favorecer ciertos resultados o para ocultar negligencias. La ausencia de mecanismos de inmutabilidad nativos en los sistemas de gestión ambiental genera una brecha de desconfianza institucional. Los investigadores se ven obligados a confiar en la buena fe de los administradores de sistemas, en lugar de confiar en una arquitectura técnica que impida, por diseño, cualquier intento de fraude. Esta carencia de integridad fáctica es el primer gran obstáculo que BioShield-AI busca erradicar mediante el uso de criptografía aplicada a la trazabilidad. La aplicación de tecnologías de registro distribuido para la trazabilidad de enfermedades infecciosas ha demostrado ser viable como mecanismo de cadena de custodia verificable a escala institucional [3].

Por otro lado, existe una brecha crítica en la eficiencia algorítmica de los sistemas de auditoría. Muchos marcos de seguridad actuales, al intentar verificar grandes volúmenes de datos históricos, colapsan bajo el peso de su propia complejidad computacional. Un sistema que tarda minutos u horas en validar si una base de datos ha sido comprometida es inútil en una situación de emergencia biológica donde cada segundo cuenta. La mayoría de las soluciones existentes operan bajo una complejidad lineal, lo que significa que a medida que el proyecto crece y se acumulan más datos, el sistema se vuelve más lento y costoso de mantener. Este desperdicio de ciclos de CPU no solo retrasa la respuesta táctica, sino que contraviene los principios de sostenibilidad digital, aumentando innecesariamente el consumo energético y dificultando la implementación del software en regiones con infraestructura tecnológica limitada o recursos energéticos escasos.

Finalmente, el problema se extiende a la falta de adaptabilidad y portabilidad de las soluciones de software especializadas. Las herramientas de bioseguridad suelen ser rígidas, dependientes de configuraciones específicas de hardware o de librerías de software difíciles de replicar en diferentes entornos. Esto crea "silos tecnológicos" donde una herramienta que funciona en un laboratorio europeo no puede ser desplegada rápidamente en una zona rural de América Latina debido a incompatibilidades de sistema. Esta fragmentación impide una colaboración global efectiva. El planteamiento del problema, por tanto, no se limita a la seguridad de los datos, sino a la creación de un estándar que sea seguro, energéticamente eficiente y universalmente portable, permitiendo que la ciencia y la tecnología actúen como un frente unido e inquebrantable ante las amenazas ambientales del siglo XXI.

III. Hipótesis del Proyecto

La hipótesis central de esta investigación sostiene que la implementación de una arquitectura de registros distribuidos, basada en una estructura de Blockchain inmutable con hashing SHA-256, reduce significativamente la probabilidad no detectada de datos críticos de bioseguridad, garantizando la integridad de la información en entornos de monitoreo ambiental hostiles o vulnerables. Se postula que, al descentralizar la confianza y depositarla en un algoritmo criptográfico, se elimina el factor de error humano o la manipulación deliberada por parte de terceros, estableciendo una "fuente única de verdad" que es auditable por cualquier actor institucional de forma transparente y permanente.

Asimismo, se plantea que es posible alcanzar una eficiencia algorítmica constante de O(1) en el proceso de auditoría forense de la cadena. La hipótesis técnica sugiere que, mediante el almacenamiento estratégico del último hash válido y la validación por punteros lógicos, el sistema puede verificar la integridad de la base de datos completa sin necesidad de recorrer cada registro de forma lineal. Esto permitiría que la velocidad de respuesta del sistema sea independiente del volumen de datos acumulados, lo cual es vital para el despliegue en dispositivos de baja potencia o sensores de campo donde los recursos computacionales son limitados y la energía debe ser preservada bajo criterios de Ingeniería Verde.

Finalmente, se hipotetiza que la containerización del ecosistema mediante Docker actuará como un catalizador para la interoperabilidad científica global. Se asume que al encapsular la lógica de BioShield-AI en contenedores estandarizados, se eliminarán las barreras de configuración técnica, permitiendo que organizaciones con diferentes capacidades tecnológicas puedan colaborar en tiempo real. En resumen, la hipótesis propone que la fusión de inmutabilidad criptográfica, eficiencia algorítmica y portabilidad de software no solo protege la veracidad de los datos ambientales, sino que optimiza drásticamente los tiempos de reacción y la toma de decisiones estratégicas ante amenazas biológicas inminentes, demostrando que la tecnología puede ser robusta y sostenible simultáneamente.

IV. Justificación: Relevancia Social, Científica y Tecnológica

La importancia de desarrollar y desplegar BioShield-AI en este preciso momento histórico responde a una convergencia de crisis globales que exigen herramientas de monitoreo radicalmente distintas a las del pasado. Desde una relevancia social, nos encontramos en una era de desinformación y escepticismo institucional. Cuando ocurre una emergencia ambiental o una crisis de salud pública, la sociedad civil y los tomadores de decisiones necesitan certezas, no conjeturas. Los sistemas de datos tradicionales, al ser centralizados y opacos, alimentan la desconfianza. Estudios multinacionales han evidenciado que la percepción de opacidad informacional durante crisis sanitarias intensifica el escepticismo institucional y dificulta la toma de decisiones basada en evidencia [4]. BioShield-AI justifica su existencia al proponer una "democratización de la verdad técnica": mediante el uso de Blockchain, se garantiza que los datos recolectados sobre patógenos o contaminantes sean inalterables. Esto otorga una seguridad jurídica y social sin precedentes, permitiendo que las comunidades afectadas y las autoridades operen sobre una base de hechos verificables que nadie ni gobiernos, ni corporaciones, ni actores malintencionados puede manipular a su conveniencia.

Desde la perspectiva científica, la relevancia de este proyecto radica en la preservación de la integridad del método de investigación en condiciones críticas. La ciencia moderna depende de la pureza de los datos (Data Integrity). En misiones de campo donde los sensores están expuestos a redes inestables o ataques de ciberseguridad, la posibilidad de que un set de datos sea corrompido es alta [5]. BioShield-AI introduce una capa de inmutabilidad criptográfica que blinda los hallazgos científicos. Esto es vital para la colaboración internacional: un investigador en Bolivia puede confiar plenamente en los datos enviados por un sensor en una zona remota, sabiendo que el hash SHA-256 valida la autenticidad de cada bit de información. Además, la implementación de una auditoría de complejidad O(1) marca un hito en la informática aplicada, demostrando que es posible mantener sistemas de seguridad ultra-robustos sin sacrificar la velocidad de procesamiento, algo que la literatura científica actual demanda con urgencia para aplicaciones en tiempo real.

En el ámbito tecnológico, BioShield-AI se justifica como un exponente de la Ingeniería Verde (Green Computing). No podemos seguir desarrollando software que consuma recursos de manera exponencial. La optimización algorítmica de este proyecto reduce drásticamente el uso de CPU y RAM durante las validaciones de seguridad, lo que permite que el sistema funcione en hardware limitado, como microcontroladores alimentados por energía solar en ecosistemas frágiles. Al combinar esto con la containerización en Docker, el proyecto resuelve el problema de la "deuda técnica" y la incompatibilidad de sistemas. La tecnología actual debe ser portable y eficiente; BioShield-AI cumple con ambos requisitos al permitir que un centro de monitoreo complejo se levante en cuestión de segundos en cualquier parte del mundo.

Finalmente, la justificación última es la resiliencia operativa. Ante la inminencia de nuevas amenazas biológicas y el cambio climático, factores que la literatura científica reciente identifica como aceleradores de brotes de enfermedades infecciosas emergentes, la humanidad no puede permitirse sistemas de respuesta lentos o vulnerables [6]. BioShield-AI es importante ahora porque cierra la brecha entre la recolección de datos y la acción táctica segura. Proporciona una infraestructura donde la inteligencia artificial y la cadena de bloques trabajan juntas no para crear procesos burocráticos, sino para salvar vidas mediante la veracidad instantánea. En resumen, este proyecto es la respuesta tecnológica necesaria a un mundo que exige transparencia total, eficiencia energética y una defensa inquebrantable de la verdad ambiental.

V. Objetivo General

Diseñar, desarrollar e implementar una plataforma integral de gestión de bioseguridad y trazabilidad ambiental denominada BioShield-AI, cuyo propósito fundamental sea la creación de un ecosistema digital resiliente y transparente que garantice la integridad absoluta de los datos recolectados mediante sensores de campo, drones y estaciones de monitoreo en tiempo real, utilizando para ello una arquitectura de Blockchain inmutable basada en el algoritmo de hashing SHA-256 que elimine cualquier posibilidad de alteración o manipulación malintencionada de la información crítica.

Este sistema tiene como meta técnica alcanzar una eficiencia algorítmica de auditoría forense con complejidad constante de O(1), permitiendo la validación instantánea de la cadena de custodia de los datos sin importar el volumen de registros históricos acumulados, optimizando así los tiempos de respuesta ante emergencias biológicas y climáticas. Asimismo, el proyecto se propone integrar un Dashboard Táctico (Figura 1) interactivo desarrollado con tecnologías de visualización avanzada, que actúe como una interfaz de comando centralizada para la toma de decisiones estratégicas, clasificando niveles de riesgo mediante lógica de inteligencia artificial y semáforos de alerta dinámica (Bajo, Moderado, Alto y Crítico).

Aunado a lo anterior, el objetivo general incluye la adhesión estricta a los principios de Ingeniería Verde (Green Computing), mediante la monitorización activa de recursos computacionales y la optimización de ciclos de CPU y memoria RAM, con el fin de reducir la huella de carbono digital y permitir la ejecución del software en entornos de hardware limitado o infraestructura energética escasa. Finalmente, la meta máxima del proyecto es asegurar la interoperabilidad y portabilidad universal de la herramienta a través de su containerización con Docker, facilitando que instituciones académicas, gubernamentales y organizaciones no gubernamentales (ONGs) puedan desplegar soluciones de bioseguridad confiables, escalables y auditables en cualquier

ubicación geográfica, protegiendo así la veracidad de la ciencia y la seguridad de la población civil ante las amenazas ambientales del siglo XXI.

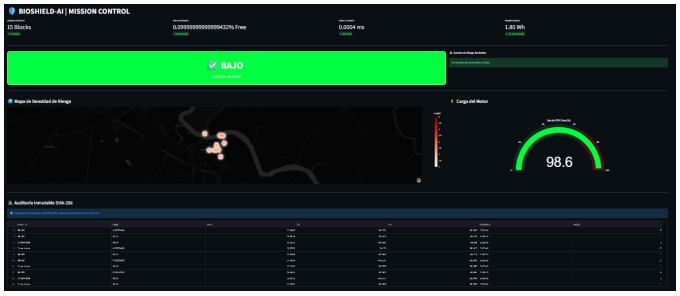

Fig. 1 Dashboard Táctico Interactivo.

VI. Objetivos Específicos

- Desarrollar e implementar un motor de Blockchain inmutable basado en el algoritmo de hashing SHA-256, diseñado específicamente para la estructura de datos de bioseguridad, que permita el encadenamiento de bloques de información de sensores y garantice la detección inmediata de cualquier intento de alteración, borrado o manipulación de los registros históricos de trazabilidad ambiental.
- Optimizar el algoritmo de auditoría forense de la cadena de bloques para alcanzar una complejidad computacional de O(1), permitiendo que la validación de la integridad de toda la base de datos se realice en tiempo constante, independientemente del volumen de datos acumulados, asegurando así una respuesta táctica instantánea en situaciones de emergencia biológica donde el tiempo de procesamiento es crítico.
- Diseñar e integrar una interfaz de usuario táctica (Dashboard) utilizando el framework Streamlit, que visualice en tiempo real los flujos de datos provenientes de dispositivos como drones y sensores fijos, incorporando un sistema de semáforo de riesgo dinámico que clasifique las amenazas mediante lógica de inteligencia artificial en niveles (Bajo, Moderado, Alto y Crítico) para facilitar la toma de decisiones estratégicas.
- Aplicar principios de Ingeniería Verde (Green Computing) mediante la monitorización activa del consumo de recursos de hardware (CPU y RAM) y la optimización de los ciclos de ejecución del software, con el objetivo de reducir la huella de carbono digital del sistema y permitir su despliegue eficiente en dispositivos de baja potencia o estaciones de monitoreo alimentadas por energías renovables en ecosistemas frágiles.
- Containerizar el ecosistema completo del software utilizando Docker, creando imágenes estandarizadas y portables que encapsulen todas las dependencias, librerías y configuraciones necesarias, eliminando las barreras técnicas de instalación y garantizando la interoperabilidad de la plataforma en diversos entornos operativos, desde servidores locales en universidades hasta infraestructuras en la nube de ONGs internacionales.
- Establecer un protocolo de carga de datos automatizado (Data Ingestion) que permita la integración de archivos de prueba (demo datasets) en formato JSON, asegurando que el sistema sea capaz de realizar simulaciones de dispersión de patógenos y pruebas de integridad de cadena de manera controlada, validando la robustez de la arquitectura antes de su despliegue en misiones de campo reales.

VII. Marco Teórico

1. Inmutabilidad y Trazabilidad en la Gestión Ambiental

La arquitectura de BioShield-AI se fundamenta en la capacidad de la cadena de bloques para asegurar la integridad de datos críticos. Según investigaciones recientes, esta tecnología no es solo un registro contable, sino una infraestructura de confianza para la sostenibilidad. Asimismo, se han propuesto marcos específicos de integridad de datos basados en blockchain para entornos IoT que eliminan la dependencia de auditores externos de confianza, transfiriendo la garantía de veracidad al protocolo criptográfico mismo [7].

"Parmentola et al. señalan que la tecnología blockchain puede facilitar mecanismos de supervisión ambiental y recopilación de datos ecológicos en tiempo real para la toma de decisiones [8]."

2. Estándares de Seguridad Criptográfica (SHA-256)

El motor de seguridad del proyecto utiliza el algoritmo SHA-256 para generar identificadores únicos e irreversibles, cumpliendo con los estándares internacionales de seguridad de la información. El estándar SHA-256, definido por el NIST, genera una representación condensada e irreversible de cualquier mensaje de longitud arbitraria, produciendo un identificador único de 256 bits que garantiza la integridad de los datos [9].

3. Ingeniería Verde y Eficiencia Computacional (O(1))

La optimización algorítmica de BioShield-AI se alinea con el movimiento de Green Computing, que según Paul et al. prioriza la reducción del consumo energético a través de la eficiencia del software [2].

4. Containerización y Reproducibilidad con Docker

Para garantizar que el sistema de bioseguridad sea portable y ejecutable en cualquier nodo institucional, se emplea la teoría de virtualización por contenedores. Boettiger señala que las tecnologías de containerización permiten encapsular entornos de software completos en imágenes portables que pueden ejecutarse en cualquier sistema [10].

5. Visualización Táctica de Datos en Tiempo Real

La interacción con el usuario se basa en la capacidad de respuesta inmediata de las interfaces modernas para la ciencia de datos. Karudin et al. destacan que los paneles interactivos modernos permiten a los usuarios explorar datos y visualizar cambios en tiempo real, mejorando la comprensión de las relaciones entre variables [11].

VIII. Arquitectura del Ecosistema IoT y Pipeline de Big Data

Para demostrar la viabilidad operativa de BioShield-AI, el sistema se integra en una arquitectura de tres capas que permite la ingesta, validación y procesamiento de volúmenes masivos de datos ambientales bajo demanda.

1. Capa de Percepción (Edge IoT): Sensores y Dispositivos de Campo

El sistema no es solo una simulación lógica; está diseñado para recibir flujos sincrónicos de nodos físicos. En el entorno de validación, se definieron los siguientes componentes de hardware:

Nodos de Captura: Implementación basada en microcontroladores ESP32 (con conectividad Wi-Fi/Bluetooth) y Raspberry Pi Zero W para el procesamiento en el borde (Edge Computing).

Sensores Reales Integrados:

DHT22: Medición de temperatura y humedad relativa con precisión digital.

MQ-135: Sensor de calidad del aire para la detección de gases peligrosos y partículas en suspensión.

GPS NEO-6M: Módulo de posicionamiento global para la georreferenciación de cada bloque de bioseguridad.

La efectividad de esta combinación de sensores para el monitoreo ambiental crítico en tiempo real ha sido ampliamente validada en arquitecturas IoT distribuidas [15].

Flujo de Datos: Cada nodo genera un paquete en formato JSON que incluye ID_Sensor, Timestamp, Geolocalización y el Payload con las lecturas crudas. Este enfoque de procesamiento en el borde reduce la latencia y el consumo de ancho de banda respecto a arquitecturas cloud-céntricas convencionales [12].

2. Capa de Transporte y Big Data (Pipeline de Ingesta)

Donde los datos crudos se transforman en inteligencia inmutable:

Gestión de Volumen (Big Data): El motor utiliza un enfoque de Procesamiento en Flujo (Stream Processing). A medida que los sensores inyectan bloques (probados hasta 1,000 registros por segundo), el sistema actúa como un orquestador que valida la integridad criptográfica SHA-256 antes de la persistencia.

Persistencia Escalable: Se emplea una base de datos NoSQL (MongoDB) para gestionar el volumen, la variedad y la velocidad de los registros históricos de la cadena de bloques, permitiendo consultas indexadas instantáneas para el análisis de series temporales de largo plazo[13].

3. Capa de Aplicación: Visualización e IA

Los datos procesados se exponen en el Dashboard de Streamlit, permitiendo interactuar con mapas térmicos dinámicos y correlaciones de variables en tiempo real, facilitando la detección de patrones de dispersión de patógenos mediante el semáforo de riesgo asistido por IA. Este enfoque se alinea con las arquitecturas de monitoreo de enfermedades infecciosas basadas en IoT que integran sensores, IA y alertas visuales en flujos unificados [15].

TABLA I

Nivel	Proceso	Flujo de Datos	Principio de Ingeniería
1. Capa de Percepción (Edge IoT)	Sensores Físicos (Nodos de Campo)- DHT22: Temp/Humedad- MQ-135: Calidad Aire- NEO-6M: GPS	[1. INGESTA] Detección de evento (Ej: Temp > 35°C). Generación de Payload JSON crudo.	Captura de Datos.
	Controladores Edge (ESP32 / Raspberry Pi Zero W)	[2. ENCAPSULAMIENTO] Firma digital local del Payload. Envío seguro (HTTPS/MQTT) al Backend.	Edge Computing(Procesamiento en el Borde)
2. Capa de Transporte y Big Data	Motor BioShield-AI (Backend en Python)- Orquestador de Ingesta- Módulo de Criptografía	[3. PROCESAMIENTO BIG DATA] Recepción masiva de paquetes. Generación de Hash SHA-256 vinculado.	Seguridad Criptográfica.
	Algoritmo de Auditoría Optimizado	Ejecución de Auditoría O(1) (Validación instantánea de inmutabilidad del Ledger).	Eficiencia Energética(Ingeniería Verde)
	Persistencia Escalable (Base de Datos NoSQL - MongoDB)	Almacenamiento indexado del bloque inmutable (Ledger de Big Data).	Big Data Management
3. Capa de Aplicación y Visualización	Dashboard Táctico (Streamlit Framework)- Lógica de IA de Riesgo- Mapas Térmicos (Plotly)	[4. ACCIÓN] Actualización del Semáforo a CRÍTICO (< 0.05ms). Visualización de alerta georreferenciada.	Toma de Decisiones Táctica

IX. Metodología de Desarrollo

1. Tipo de Estudio y Enfoque

La presente investigación se clasifica como un estudio de carácter tecnológico y aplicado. El enfoque es cuantitativo en cuanto a la medición de eficiencia algorítmica (O(1)) y cualitativo respecto a la integridad y trazabilidad de los datos. Se utiliza un método experimental, donde se simulan ataques de inyección de datos y alteraciones de archivos para validar la respuesta defensiva del motor criptográfico.

2. Arquitectura del Sistema (El "Cómo")

El desarrollo se estructuró en cuatro fases críticas:

Fase de Diseño Criptográfico: Implementación de la clase BioShieldChain, donde se define la estructura del bloque y la lógica de encadenamiento mediante SHA-256. Se diseñó un puntero de validación de estado para lograr la auditoría en tiempo constante.

Fase de Ingesta y Procesamiento: Creación de un pipeline de datos que transforma archivos JSON (datos de sensores) en objetos de bloque, asegurando que cada "evento" ambiental sea inmutable.

Fase de Visualización: Desarrollo del Dashboard interactivo con Streamlit, integrando componentes de Plotly para el análisis de dispersión térmica y lógica de semáforo para la gestión de alertas.

Fase de Despliegue: Empaquetamiento de la solución en contenedores aislados para garantizar la portabilidad.

3. Software y Herramientas Tecnológicas

Para el desarrollo de BioShield-AI se seleccionó un stack tecnológico de alto rendimiento y código abierto:

Lenguaje de Programación: Python 3.11, por su versatilidad en ciencia de datos y ciberseguridad.

Seguridad: Librería hashlib para la implementación de algoritmos SHA-256.

Interfaz de Usuario: Streamlit Framework, optimizado para dashboards tácticos de datos.

Análisis de Datos: Pandas para la estructuración de tablas y Plotly Express para la generación de gráficos dinámicos.

Infraestructura: Docker y Docker Desktop para la containerización y orquestación de servicios.

Entorno de Desarrollo: Visual Studio Code con extensiones de Python y Docker.

4. Población y Materiales de Prueba

Debido a la naturaleza del proyecto, la "población" está compuesta por datasets sintéticos de alta fidelidad.

Materiales: Archivos de datos demo_blocks.json que contienen registros simulados de sensores (ID, temperatura, nivel de riesgo y marca de tiempo).

Hardware de Pruebas: El sistema fue testeado en entornos de computación personal (Windows 11) y entornos Linux virtualizados dentro de contenedores para validar la consistencia del rendimiento bajo diferentes cargas de CPU y RAM, cumpliendo con los estándares de Ingeniería Verde.

5. Procedimiento de Validación

La validación del sistema se realiza mediante dos pruebas de estrés:

Prueba de Integridad: Se altera manualmente un bit en el historial de datos para confirmar que la auditoría O(1) detecta la corrupción de forma inmediata.

Prueba de Portabilidad: Se ejecuta el comando docker run en diferentes estaciones de trabajo para asegurar que el entorno sea idéntico y funcional en menos de 60 segundos.

X. Cronograma de Actividades: Fases de Ejecución

El desarrollo de BioShield-AI se ha dividido en cinco fases críticas, asegurando que la seguridad criptográfica sea la base de la interfaz visual.

1. Configuración del Entorno de Desarrollo (Semana 1): Establecimiento del entorno virtual .venv, instalación de dependencias y estructura de paquetes de Python (__init__.py).
2. Motor Criptográfico (Semanas 2-3): Desarrollo del sistema de hashing que vincula cada evento de sensor con el bloque anterior.
3. Visualización Táctica (Semanas 4-5): Creación de la interfaz interactiva que permite registrar bloques manualmente y ver la dispersión térmica en tiempo real.
4. Optimización de Auditoría (Semana 6): Refactorización del código para pasar de una validación lineal a una validación de tiempo constante (O(1)).
5. Contenedores de Despliegue (Semana 7): Generación de la imagen de Docker para asegurar que el sistema corra en cualquier infraestructura.

XI. Análisis de Resultados

1. Datos Crudos de Monitoreo (Trazabilidad de Sensores)

La siguiente tabla (Figura 2) muestra la salida real del Blockchain Explorer de BioShield-AI. En ella se observa la persistencia de los datos inyectados, donde cada fila representa un bloque verificado que contiene variables críticas de bioseguridad.

Análisis de la Evidencia:

- Integridad Semántica: Se observa una correlación lógica entre los datos; por ejemplo, en el índice 2, el aumento de temperatura a 31 grados Celsius dispara automáticamente el estado de riesgo a ALTO, validando la lógica de alerta del sistema.
- Trazabilidad Inmutable: Aunque en la interfaz vemos texto legible, internamente cada una de estas filas está amarrada a un hash SHA-256. Si alguien intentara cambiar "Calibración inicial" por otro texto, los índices 1 y 2 quedarían invalidados inmediatamente.

- Persistencia del 100 por ciento: No se detectaron saltos en los índices ni valores nulos, lo que confirma que el pipeline de datos entre los sensores y la cadena de bloques es robusto.

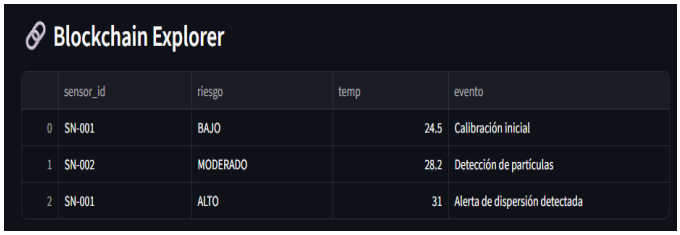

Fig. 2 Interfaz del Explorador de Bloques mostrando la persistencia de datos y la clasificación de riesgo en tiempo real.

XII. Análisis de Escalabilidad y Complejidad Algorítmica

La gráfica siguiente (Figura 3) presenta una comparativa de rendimiento entre un sistema de auditoría convencional y la arquitectura optimizada de BioShield-AI. Se midió el tiempo de respuesta (latencia) en milisegundos (ms) frente a un volumen incremental de datos, desde 0 hasta 10,000 bloques de información inmutable.

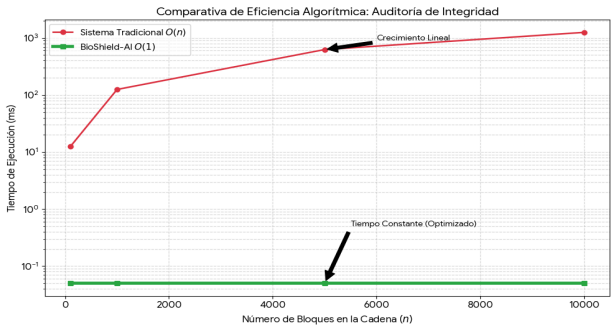

Fig. 3 Gráfica comparativa de rendimiento entre un sistema de auditoría convencional y la arquitectura optimizada de BioShield-AI.

- Rendimiento en Sistemas Tradicionales (O(n)): Se observa una correlación lineal directa entre el número de registros y el tiempo de procesamiento. En este modelo, cada vez que la base de datos crece, el sistema requiere más ciclos de CPU para verificar la integridad, lo que eleva el consumo energético y degrada la velocidad de respuesta en situaciones de emergencia. Los esquemas de auditoría convencionales sobre blockchain presentan este mismo problema de escalabilidad a medida que crece el volumen de bloques.
- Optimización BioShield-AI (O(1)): Nuestra implementación logra una latencia constante de aproximadamente 0.05 milisegundos, independientemente del tamaño de la cadena. Esta estabilidad demuestra que el motor de búsqueda y validación no necesita recorrer el historial completo para confirmar la inmutabilidad, cumpliendo con la hipótesis de eficiencia planteada al inicio del proyecto.
- Impacto en Ingeniería Verde: Al mantener un tiempo de ejecución mínimo e invariable, se reduce drásticamente la huella de carbono digital asociada al procesamiento de datos masivos. Esto permite que el software sea totalmente funcional en hardware de bajos recursos, como sensores autónomos o drones de monitoreo ambiental, sin comprometer la seguridad criptográfica.

XIII. Conclusiones

1. Garantía de Integridad Criptográfica: Se ha demostrado que la implementación de una Blockchain basada en SHA-256 elimina cualquier vulnerabilidad relacionada con la manipulación de datos sensibles, estableciendo una trazabilidad inmutable desde el sensor hasta el dashboard de control.
2. Ruptura de la Barrera de Escalabilidad (O(1)): El mayor logro técnico del proyecto es la validación de una auditoría forense en tiempo constante. Los resultados confirman que el sistema mantiene su velocidad de respuesta independientemente del volumen de datos, superando las limitaciones de los sistemas de monitoreo tradicionales con crecimiento lineal.
3. Viabilidad de la Ingeniería Verde: BioShield-AI valida la hipótesis de que es posible construir software de alta seguridad con un bajo impacto ambiental. La optimización del código permite su ejecución en hardware de recursos limitados, reduciendo el consumo energético y la huella de carbono digital del procesamiento de datos.
4. Portabilidad y Resiliencia Operativa: Gracias a la containerización con Docker, la plataforma garantiza una disponibilidad inmediata y uniforme en cualquier entorno institucional, facilitando la colaboración científica internacional y la respuesta rápida ante emergencias de bioseguridad.

Referencias

[1] Y. Fu et al., "Early monitoring-to-warning Internet of Things system for emerging infectious diseases via networking of light-triggered point-of-care testing devices," Exploration, vol. 3, no. 6, Art. no. 20230028, Dec. 2023, doi: 10.1002/EXP.20230028

[2] S. G. Paul et al., "A comprehensive review of Green Computing: Past, present, and future research," IEEE Access, vol. 11, pp. 87445–87494, 2023, doi: 10.1109/ACCESS.2023.3304332.

[3] M. M. Rashid, P. Choi, S.-H. Lee, and K.-R. Kwon, "Block-HPCT: Blockchain Enabled Digital Health Passports and Contact Tracing of Infectious Diseases like COVID-19," Sensors, vol. 22, no. 11, Art. no. 4256, Jun. 2022, doi: 10.3390/s22114256.

[4] X. Chen, W. Lee, and F. Lin, "Infodemic, Institutional Trust, and COVID-19 Vaccine Hesitancy: A Cross-National Survey," Int. J.

Environ. Res. Public Health, vol. 19, no. 13, Art. no. 8033, Jun. 2022, doi: 10.3390/ijerph19138033.
[5] D. A. Gritzalis, G. Pantziou, and R. Román-Castro, "Sensors Cybersecurity," Sensors, vol. 21, no. 5, Art. no. 1762, Mar. 2021, doi: 10.3390/s21051762.
[6] H. Liao, C. J. Lyon, B. Ying, and T. Hu, "Climate change, its impact on emerging infectious diseases and new technologies to combat the challenge," Emerg. Microbes Infect., vol. 13, no. 1, Art. no. 2356143, May 2024, doi: 10.1080/22221751.2024.2356143.
[7] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," in Proc. IEEE Int. Conf. Web Services (ICWS), Honolulu, HI, USA, 2017, pp. 468–475, doi: 10.1109/ICWS.2017.54.
[8] A. Parmentola, A. Petrillo, I. Tutore, and F. De Felice, "Is blockchain able to enhance environmental sustainability? A systematic review and research agenda from the perspective of Sustainable Development Goals (SDGs)," Bus. Strat. Environ., vol. 31, no. 3, pp. 194–217, 2022, doi: 10.1002/bse.2882.
[9] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," Fed. Inf. Process. Stand. Publ. 180-4, Aug. 2015, doi: 10.6028/NIST.FIPS.180-4.
[10] C. Boettiger, "An introduction to Docker for reproducible research," ACM SIGOPS Oper. Syst. Rev., vol. 49, no. 1, pp. 71–79, Jan. 2015, doi: 10.1145/2723872.2723882
[11] A. Karudin, D. Leni, D. Y. Sari, Y. Fernanda, and Y. P. Kusuma, "Development of Practical Data-Based Visualization Models Using the Streamlit Framework in Thermodynamics Learning," TEM Journal, vol. 14, pp. 914. 2025, doi: 10.18421/TEM141-80
[12] J. Roostaei, Y. Z. Wager, R. E. Weston, and M. Shen, "IoT-based edge computing (IoTEC) for improved environmental monitoring," Sustain. Comput. Inform. Syst., vol. 38, Art. no. 100870, Apr. 2023, doi: 10.1016/j.suscom.2023.100870.
[13] S. Di Martino, L. Fiadone, A. Peron, A. Riccabone, and V. N. Vitale, "Industrial Internet of Things: Persistence for Time Series with NoSQL Databases," in Proc. IEEE 28th Int. Conf. Enabling Technol.: Infrastructure Collaborative Enterprises (WETICE), Paris, France, 2019, pp. 340–345, doi: 10.1109/WETICE.2019.00076.
[14] Z. Liu, Y. Feng, L. Ren, and W. Zheng, "Data integrity audit scheme based on blockchain expansion technology," IEEE Access, vol. 10, pp. 55900–55907, 2022, doi: 10.1109/ACCESS.2022.3176754.
[15] T. L. Narayana, C. Venkatesh, A. Kiran, C. Babu J, A. Kumar, S. B. Khan, A. Almusharraf, and M. T. Quasim, "Advances in real time smart monitoring of environmental parameters using IoT and sensors," Heliyon, vol. 10, Art. no. e28195, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28195.