

**SERVICIO NACIONAL DE APRENDIZAJE SENA**

**Inteligencia artificial aplicada a la ciberseguridad**

**Entrenamiento para una inteligencia artificial que detecta malware en computadores de empresas.**

**Jaider Sebastian Moreno Quintero**

**Juan Sebastian Martinez Pinto**

**Nicolas Martinez Valenzuela**

**Michael Stiven Salamanca Martin**

**Paula Andrea Cassiani Castillo**

**Ficha 2996150**

**Daniela Alejandra Cuenca Sacristan**

**26/11/2024**

**Introducción**

En la actualidad, la ciberseguridad se enfrenta a desafíos cada vez más complejos debido al crecimiento exponencial de las amenazas cibernéticas, incluyendo ataques de malware, ransomware y otras formas de software malicioso. El malware, en particular, ha evolucionado tanto en cantidad como en sofisticación, adoptando técnicas avanzadas para evadir los métodos tradicionales de detección basados en firmas y reglas predefinidas. En este contexto, la inteligencia artificial (IA) ha emergido como una herramienta crucial para la protección de los sistemas informáticos, revolucionando la manera en que las organizaciones identifican y neutralizan estas amenazas.

La aplicación de la IA en ciberseguridad ha permitido el desarrollo de sistemas más robustos y adaptativos, capaces de analizar grandes volúmenes de datos en tiempo real y detectar patrones anómalos que podrían pasar desapercibidos para los métodos convencionales. Estas capacidades son especialmente relevantes en la detección de malware de día cero, donde el código malicioso no ha sido previamente catalogado. La IA utiliza técnicas avanzadas como el aprendizaje supervisado, no supervisado y profundo, que emplean algoritmos para procesar características complejas de archivos o redes, identificar comportamientos maliciosos y predecir posibles vectores de ataque futuros.

Además, los avances en el entrenamiento de modelos de IA han permitido la integración de datasets más representativos y balanceados, mejorando la precisión y reduciendo los falsos positivos, un problema común en las soluciones tradicionales. Este enfoque también facilita la creación de sistemas capaces de aprender y adaptarse a nuevas amenazas, ofreciendo una solución dinámica frente a un panorama de ciberamenazas en constante evolución.

Este informe explora el diseño de técnicas de entrenamiento específicas para sistemas de inteligencia artificial enfocados en la detección de malware. El objetivo principal es optimizar su desempeño mediante el uso de datasets enriquecidos, estrategias de validación y metodologías de evaluación avanzadas. Asimismo, se aborda el impacto de estas tecnologías en la reducción de riesgos cibernéticos, la mejora en la eficiencia operativa de los equipos de seguridad y la protección de infraestructuras críticas.

En un mundo cada vez más interconectado, donde la seguridad informática es esencial para garantizar la continuidad de los negocios y la confianza de los usuarios, la implementación de soluciones basadas en IA no solo representa una ventaja estratégica, sino también una necesidad imperativa. Este proyecto busca aportar al desarrollo de tecnologías que no solo respondan al presente, sino que también se anticipen a las amenazas del futuro.

**Antecedentes**

En los últimos años, el aumento en la sofisticación de los ciberataques ha evidenciado las limitaciones de las soluciones tradicionales de ciberseguridad, como los antivirus basados en firmas. Diversos estudios han explorado el uso de aprendizaje automático y redes neuronales en la detección de malware, destacando enfoques como el análisis estático y dinámico de archivos, el procesamiento de datos de red y la clasificación basada en vectores de características. Sin embargo, persisten desafíos relacionados con el entrenamiento en datasets balanceados y representativos, a continuación se exponen dichos desafíos.

1. **Adopción de redes neuronales para detección binaria**: Métodos como MalConv utilizan directamente las secuencias de bytes de un archivo para clasificar su naturaleza maliciosa mediante redes neuronales convolucionales, integrando capas densamente conectadas y algoritmos de aprendizaje en conjunto como Random Forest para mejorar la precisión de detección​(Solis, 2023)
2. **Aplicación del aprendizaje profundo**: Sistemas como los de McAfee incorporan aprendizaje profundo, que utiliza redes neuronales multicapa para identificar patrones de comportamiento malicioso en tiempo real, adaptándose incluso a amenazas de día cero​(Chamorro Fernández, n.d.)
3. **Detección basada en comportamientos heurísticos**: Los sistemas avanzados emplean heurísticas para analizar comportamientos anómalos, combinando aprendizaje supervisado y aprendizaje automático en múltiples capas para aumentar la precisión de detección​(Solis, 2023)
4. **Mitigación del error humano**: La inteligencia artificial ayuda a reducir errores asociados con la supervisión manual, automatizando tareas complejas y permitiendo que los equipos de ciberseguridad se enfoquen en problemas estratégicos​(Chamorro Fernández, n.d.)
5. **Datos de entrenamiento y limitaciones**: Uno de los desafíos para la IA en ciberseguridad es la falta de datos de entrenamiento completos y actualizados, lo cual afecta la efectividad de los modelos en entornos con amenazas evolutivas​(Chamorro Fernández, n.d.).
6. **IBM Watson for Cybersecurity**: Este sistema aplica aprendizaje automático para analizar grandes volúmenes de datos de eventos y vulnerabilidades, mejorando la capacidad de respuesta contra ataques avanzados​(Vishnu Varadaraj, 2024).
7. **Enfoque de aprendizaje conjunto**: Se combinan múltiples modelos de aprendizaje para crear sistemas más robustos, mejorando la detección con menos errores y aumentando la precisión ante amenazas dinámicas​.(Chamorro Fernández, n.d.)
8. **Impacto del aprendizaje supervisado**: Este método ha demostrado ser eficaz al asociar entradas específicas con salidas deseadas, desarrollando algoritmos que predicen comportamientos maliciosos con mayor exactitud​(Solis, 2023)
9. **Modelos adaptativos de IA**: Los sistemas modernos pueden aprender y adaptarse continuamente, analizando datos históricos y actuales para prever comportamientos futuros de malware​.(Vishnu Varadaraj, 2024)
10. **Amenazas de ataques adversarios**: Los ciberdelincuentes diseñan malware que busca evadir defensas basadas en IA, lo que motiva el desarrollo de modelos más sofisticados para anticipar y contrarrestar estas tácticas​(Vishnu Varadaraj, 2024)

**Planteamiento del problema**

El malware evoluciona constantemente para evadir sistemas de seguridad. Aunque existen soluciones basadas en IA, estas enfrentan problemas como:

* Insuficiencia de datos reales etiquetados para entrenamiento.
* Alta tasa de falsos positivos que genera alertas irrelevantes.
* Escalabilidad limitada para identificar variantes desconocidas.

**Pregunta de investigación**: ¿Qué técnicas de entrenamiento pueden optimizar la capacidad de una inteligencia artificial para detectar malware de manera precisa y eficiente durante el periodo 2024-2025-1 en Bogotá?

**Hipótesis**

Si se diseñan y aplican técnicas de entrenamiento basadas en datasets enriquecidos, estrategias de oversampling y algoritmos adaptativos, entonces la IA mejorará su precisión en la detección de malware, reduciendo falsos positivos y elevando su capacidad de adaptación a nuevas amenazas.

**Justificación**

La ciberseguridad es una prioridad global en un mundo altamente digitalizado. La implementación de sistemas de IA robustos puede revolucionar la manera en que las organizaciones prevenir ciberataques. Este proyecto no solo contribuirá a fortalecer la seguridad informática, sino que también optimizará costos y reducirá riesgos asociados a brechas de seguridad.

**Objetivos**

**General**

Diseñar y evaluar técnicas de entrenamiento para una IA que detecte malware con alta precisión y bajo índice de falsos positivos.

**Específicos**

1. Crear un dataset balanceado y representativo de malware y software legítimo.
2. Implementar modelos de aprendizaje supervisado y no supervisado.
3. Evaluar el rendimiento de los modelos en términos de precisión, recall y tiempo de respuesta.

**Resultados y productos**

**Resultados esperados:**

Un modelo entrenado con precisión superior al 95% en detección de malware.

Informe técnico sobre las técnicas de entrenamiento aplicadas y su impacto.

Dataset documentado y estructurado para futuras investigaciones.

**Productos entregables:**

Repositorio en GitHub

Código fuente del modelo de IA.

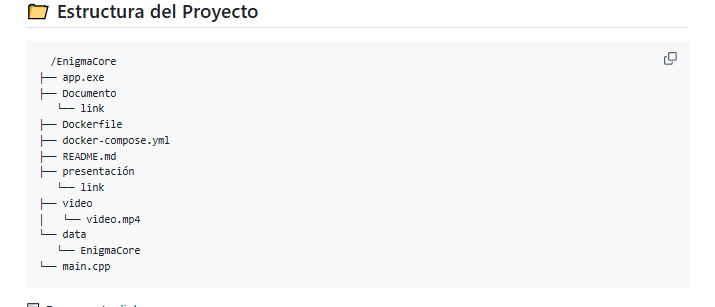
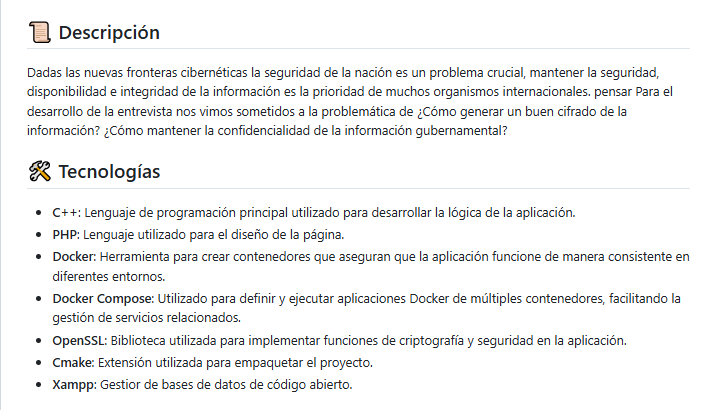
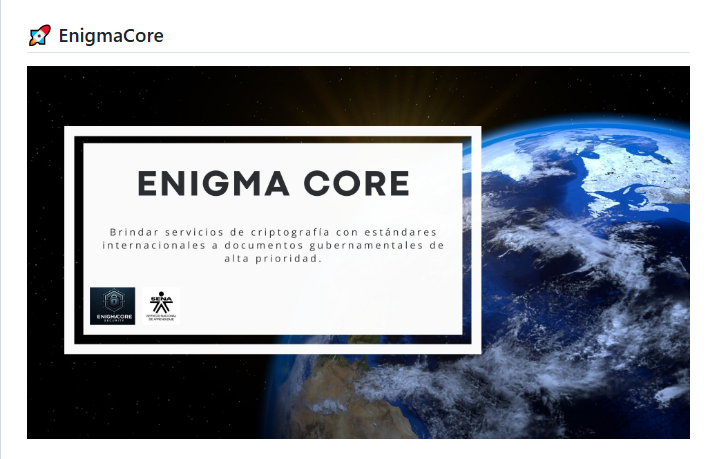
Manual de implementación.

Publicación académica en conferencias especializadas.

**Repositorio:**

<https://github.com/JaiderSe/EnigmaCore>

*Link 1 Repositorio de la inteligencia artificial*



*Imagen 1 Repositorio en GitHub*

**Cronograma de ejecución**

| **Fase** | **Mes 1** | **Mes 2** | **Mes 3** | **Mes 4** | **Mes 5** | **Mes 6** |
| --- | --- | --- | --- | --- | --- | --- |
| **Recolección de datos** | **X** |  |  |  |  |  |
| **Preprocesamiento** |  | **X** |  |  |  |  |
| **Desarrollo del modelo** |  | **X** | **X** |  |  |  |
| **Pruebas y validación** |  |  | **X** | **X** |  |  |
| **Documentación y entrega** |  |  |  |  | **X** | **X** |

*Tabla 1 cronograma*

**Presupuesto**

| **Recurso** | **Cantidad** | **Costo en COP (Aprox.)** | **Subtotal en COP** |
| --- | --- | --- | --- |
| **Equipo de cómputo** | **2** | **13,335,750 COP** | **26,671,500 COP** |
| **Licencias de software** | **-** | **4,445,250 COP** | **4,445,250 COP** |
| **Servicios de nube** | **500 horas** | **2,222.625 COP/hora** | **1,111,312.5 COP** |
| **Investigación y capacitación** | **-** | **8,890,500 COP** | **8,890,500 COP** |
| **Total estimado** |  |  | **41,118,562.5 COP** |

*Tabla 2 Presupuesto*

**Referencias**

Solis, D. C. (2023, June 9). *Uso de Inteligencia Artificial y Machine Learning en ciberseguridad*. OpenWebinars.net. <https://openwebinars.net/blog/uso-de-inteligencia-artificial-y-machine-learning-en-ciberseguridad/>

Chamorro Fernández, A. (n.d.). Malware Detection with Machine Learning. Retrieved December 2, 2024, from <https://ddd.uab.cat/pub/tfg/2020/tfg_285427/MalwareDetection-Informe-final.pdf>

Vishnu Varadaraj. (2024, April 2). Todo sobre la IA y la detección de amenazas | Blog de McAfee. Blog de McAfee. <https://www.mcafee.com/blogs/es-es/internet-security/todo-sobre-la-ia-y-la-deteccion-de-amenazas/>

¿Qué es la inteligencia artificial para la ciberseguridad? | Seguridad de Microsoft. (2024). Microsoft.com. <https://www.microsoft.com/es-co/security/business/security-101/what-is-ai-for-cybersecurity>

Ciberseguridad con inteligencia artificial (IA) | IBM. (2024). Ibm.com. <https://www.ibm.com/mx-es/ai-cybersecurity>

Conzultek. (2024). La importancia de la Inteligencia Artificial en la ciberseguridad. Conzultek.com. <https://blog.conzultek.com/ciberseguridad/inteligencia-artificial-en-la-ciberseguridad>

‌

‌

‌