SISTEMA INTELIGENTE PARA LA DETECCIÓN PROACTIVA DE VULNERABILIDADES EN REDES INFORMÁTICAS

Ángel J. Fernández D.
Universidad Bicentenaria de Aragua
Angeljofer14@gmail.com

Resumen

Frente a la creciente complejidad de ciberamenazas como el ransomware y las limitaciones de los enfoques reactivos, el objetivo de este estudio es proponer un sistema inteligente para la detección proactiva de vulnerabilidades en redes informáticas. La metodología empleada consistió en el diseño de un sistema basado en algoritmos de aprendizaje automático para analizar patrones de tráfico, configuraciones y eventos, identificando riesgos antes de que se materialicen. Su eficacia se evaluó mediante la validación de un prototipo en entornos simulados con datasets estándar. Como principal resultado, el modelo de detección alcanzó una alta precisión (97.76%), demostrando su viabilidad técnica y robustez. Se concluye que esta solución proactiva no solo fortalece la resiliencia de las infraestructuras tecnológicas, sino que también establece un marco para transformar la ciberseguridad hacia un paradigma preventivo, respondiendo a una necesidad crítica en el panorama digital actual.

Palabras clave: Ciberseguridad; Detección; Redes; Vulnerabilidades.

INTELLIGENT SYSTEM FOR PROACTIVE DETECTION OF VULNERABILITIES IN COMPUTER NETWORKS

Abstract

Given the growing complexity of cyber threats like ransomware and the limitations of reactive approaches, the objective of this study is to propose an intelligent system for the proactive detection of vulnerabilities in computer networks. The methodology involved designing a system based on machine learning algorithms to analyze traffic patterns, configurations, and events, identifying risks before they materialize. Its effectiveness was evaluated by validating a prototype in simulated environments using standard datasets. As a main result, the detection model achieved high accuracy (97.76%), demonstrating its technical feasibility and robustness. It is concluded that this proactive solution not only strengthens the resilience of technological infrastructures but also establishes a framework to transform cybersecurity towards a preventive paradigm, addressing a critical need in the current digital landscape.

Keywords: Cybersecurity; Detection; Networks; Vulnerabilities.

SYSTÈME INTELLIGENT POUR LA DÉTECTION PROACTIVE DES VULNÉRABILITÉS DANS LES RÉSEAUX INFORMATIQUES

Résumé

Face à la complexité croissante des cybermenaces telles que les ransomwares et aux limites des approches réactives, l'objectif de cette étude est de proposer un système intelligent pour la détection proactive des vulnérabilités dans les réseaux informatiques. La méthodologie a consisté à concevoir un système basé sur des algorithmes d'apprentissage automatique pour analyser les modèles de trafic, les configurations et les événements, identifiant ainsi les risques avant qu'ils ne se matérialisent. Comme résultat principal, le modèle de détection a atteint une grande précision (97,76 %), démontrant sa faisabilité technique et sa robustesse.

Mots-clés: **Cybersécurité; Détection; Réseaux; Vulnérabilités.**

Introducción

La transformación digital ha intensificado la dependencia de las organizaciones en redes informáticas, exponiéndolas a ciberamenazas que superan los enfoques tradicionales. La naturaleza reactiva de la ciberseguridad actual, basada en firmas de ataques conocidos, es ineficaz ante amenazas emergentes, lo que amenaza la continuidad del negocio y la integridad de la información. Esta vulnerabilidad estructural hace necesario un cambio de paradigma hacia la prevención para fortalecer la resiliencia tecnológica de manera proactiva.

Para superar esta brecha, se diseña un Sistema Inteligente para la Detección Proactiva de Vulnerabilidades. La metodología se basa en la aplicación de algoritmos de aprendizaje automático para analizar de forma continua los patrones de tráfico, configuraciones y eventos de la red. Este análisis permite identificar anomalías y comportamientos predictivos de un ataque antes de su materialización. Como señalan Cano y Monsalve (2023), la ciberseguridad es una inversión estratégica, y este enfoque optimiza los recursos al reducir la fatiga por alertas.

El objetivo general de este estudio, es proponer un sistema inteligente para la detección proactiva de vulnerabilidades en redes informáticas, cuya validación conceptual se realiza mediante un prototipo probado en entornos controlados. El presente artículo está estructurado para explicar la metodología empleada, presentar los resultados cuantitativos obtenidos y discutir la factibilidad e implicaciones de la propuesta.

En cuanto a su estructura, el presente artículo se despliega inicialmente con el marco teórico y la metodología tecnológica aplicada; seguidamente, se describe el proceso de diseño y arquitectura del sistema; posteriormente, se exponen los resultados cuantitativos obtenidos y su respectiva discusión, para finalizar con las conclusiones y las referencias bibliográficas que sustentan la investigación de acuerdo con la normativa institucional.

Marco Teórico

Esta sección establece el marco conceptual del Sistema Inteligente para la Detección Proactiva de Vulnerabilidades en Redes Informáticas. Su propósito es interpretar y analizar críticamente los puntos de vista relacionados con la ciberseguridad. Se busca demostrar la comprensión del tema e innovación de la propuesta, alineándose con las competencias en Inteligencia Artificial (IA), redes y solución de problemas, fortaleciendo el marco conceptual para el diseño de un prototipo funcional.

Antecedentes de la Investigación

El sistema propuesto se fundamenta en investigaciones previas en ciberseguridad e IA. Cano y Monsalve (2023) destacaron la necesidad de integrar IA para proteger infraestructuras críticas, validando su eficacia en la detección de anomalías y anticipación de ciberataques. El Comité Académico de Expertos de la UBA (2024) subrayó el papel transformador de la IA en la ingeniería, reforzando la

alineación del proyecto con las directrices universitarias. Stivaktakis et al. (2020) introdujeron la codificación predictiva semántica, relevante para la anticipación de vulnerabilidades en patrones de tráfico y comportamientos anómalos de red, apoyando la metodología para identificar técnicas avanzadas de IA.

Fundamentos Teóricos

El proyecto se sustenta en disciplinas como redes, ciberseguridad e inteligencia artificial:

- **Inteligencia Artificial (IA):** Según Russell y Norvig (2020), la IA es crucial para la toma de decisiones automatizada y el análisis de sistemas, permitiendo al sistema aprender y adaptarse a nuevas amenazas para detectar proactivamente vulnerabilidades.
- **Aprendizaje Automático (ML):** Goodfellow et al. (2016) lo definen como un subcampo de la IA que permite a los sistemas aprender de datos sin programación explícita:
    - Supervisado: Utiliza datos etiquetados para clasificar instancias nuevas (Alpaydin, 2020), ideal para detección de ataques conocidos.
    - No Supervisado: Busca patrones ocultos en datos no etiquetados (Bishop, 2006), importante para la detección de anomalías.
- **Por Refuerzo**: Un agente aprende a tomar decisiones óptimas interactuando con un entorno (Sutton y Barto, 2018), con potencial para optimizar políticas de seguridad adaptativas.
- **Redes Neuronales (NN):** Inspiradas en el cerebro humano (Chollet, 2018), son avanzadas formas de ML, indispensables por su capacidad de procesar grandes volúmenes de datos y reconocer patrones complejos, siendo un pilar para la arquitectura funcional del sistema.
- **Vulnerabilidades en Redes Informáticas:** Schneier (2015) las define como debilidades en un sistema que pueden ser explotadas por amenazas.

Fundamentos Legales

La legislación venezolana respalda este proyecto:

- La Constitución de la República Bolivariana de Venezuela (1999), en su artículo 110, promueve el uso de la informática para la protección de la información.
- La Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI) (2010) fomenta la creación de capacidades tecnológicas para el bienestar social.
- La Ley Especial Contra Delitos Informáticos (2001) ofrece protección a los sistemas TIC y establece mecanismos de prevención, donde el sistema propuesto actúa como herramienta preventiva.

Fase De Diagnóstico

La problemática de las ciberamenazas se caracteriza por la insuficiencia de métodos reactivos. El diagnóstico se basó en el análisis de literatura especializada y casos de estudio de ciberataques, confirmando que la falta de herramientas con capacidades de aprendizaje adaptativo y detección de patrones sutiles es un vacío crítico que este proyecto busca llenar.

Fase De Análisis

El análisis valida la viabilidad del proyecto, fundamentada en la superioridad de los enfoques basados en IA para las amenazas actuales (Goodfellow et al., 2016). Un sistema proactivo ofrece seguridad predictiva y adaptativa, reduciendo falsos positivos y optimizando la eficiencia operativa (Alpaydin, 2020). Los beneficios a largo plazo, como la reducción de brechas y la optimización de recursos, superan los esfuerzos iniciales, justificando la inversión como medida estratégica para la protección de activos digitales.

Metodología

El estudio se enmarca en un diseño de investigación tecnológica para el desarrollo y validación conceptual de un prototipo de software. El enfoque metodológico se sustenta en la Inteligencia Artificial (IA) y el Aprendizaje Automático (Machine Learning), que dotan al sistema de la capacidad de aprender a partir de datos sin ser explícitamente programado. Se consideraron el aprendizaje supervisado, para detectar patrones conocidos, y el no supervisado, para la detección de anomalías. La pertinencia de este enfoque se refuerza con estudios como el de Cano y Monsalve (2023), que validan la eficacia de la IA para superar los sistemas reactivos, y las directrices de la Universidad Bicentenaria de Aragua (2024), que destacan su papel en la creación de sistemas adaptativos. Para el procesamiento de datos complejos, se seleccionaron las Redes Neuronales (NN) por su capacidad para reconocer patrones no lineales. Legalmente, el proyecto se ampara en la Ley Especial Contra Delitos Informáticos de Venezuela (2001), que refuerza la legitimidad de desarrollar herramientas preventivas.

El procedimiento se ejecutó en etapas secuenciales. Se utilizaron datasets públicos estándar como NSL-KDD, reconocidos por contener perfiles de tráfico benigno y malicioso. El proceso consistió en:

- **Recopilación y Normalización de Datos**: Se adquirieron los datasets y se aplicaron técnicas de normalización para escalar los valores numéricos a un rango común. Este paso es fundamental para evitar que las características con magnitudes más altas sesguen el rendimiento del algoritmo de aprendizaje.
- **Preprocesamiento y Caracterización**: La data cruda fue transformada en características significativas (feature engineering). Esto incluyó la conversión de datos categóricos (como tipos de protocolo) a formatos numéricos y la selección de las características más relevantes para la detección de anomalías, eliminando el ruido y la información redundante.

- **Selección y Entrenamiento del Modelo:** Se seleccionó una arquitectura de Redes Neuronales y se dividió el conjunto de datos en subconjuntos de entrenamiento, validación y prueba. Se procedió al entrenamiento del modelo utilizando el conjunto de entrenamiento, ajustando los pesos de la red de manera iterativa para minimizar el error de clasificación.
- **Validación del Modelo:** La eficacia del modelo entrenado se evaluó cuantitativamente utilizando el conjunto de datos de validación separado. Se aplicaron métricas estándar como la precisión (porcentaje de predicciones correctas), la sensibilidad (capacidad para identificar ataques reales) y el F1-Score (media armónica de precisión y sensibilidad), para medir de forma integral su capacidad de clasificación y robustez.

Resultados

La validación del prototipo en entornos controlados demostró su viabilidad y valor, presentando evidencias conceptuales. El valor teórico del sistema radica en su capacidad para ofrecer una capa de seguridad predictiva y adaptativa, que optimiza la eficiencia operativa al reducir falsos positivos e identificar configuraciones vulnerables de forma anticipada, superando a los enfoques reactivos tradicionales.

El sistema se identifica como un software basado en Inteligencia Artificial para la detección anticipada de vulnerabilidades, impulsando un cambio hacia un modelo predictivo. Para su desarrollo, se implementó una arquitectura de software de tres capas que garantiza modularidad y escalabilidad:

- **Capa de Adquisición y Preprocesamiento de Datos**: Esta capa es responsable del ingreso y la normalización de grandes volúmenes de datos de red (tráfico, logs, CVEs). Su concepto y posición en la arquitectura se definieron en la fase de planificación. La Ilustración 1, resume visualmente los pilares conceptuales y tecnológicos definidos en esta fase inicial.

Ilustración 1: Interfaz visual que resume la Fase 1 de Diagnóstico y Planificación del proyecto.

- **Capa de Análisis e Inteligencia:** Actúa como el cerebro del sistema, albergando y ejecutando los modelos de Machine Learning para el procesamiento de datos.
- **Capa de Presentación y Alerta**: Consiste en un dashboard web simple que funciona como interfaz de usuario. Este prototipo demuestra la capacidad para mostrar el estado del sistema, iniciar análisis y, fundamentalmente, presentar alertas críticas. El sistema es capaz de generar reportes detallados con información relevante para la toma de decisiones, como se ilustra en la Ilustración 2.

Ilustración 2: Generación y visualización de un reporte de amenazas, mostrando un resumen de la amenaza identificada, su nivel de criticidad y un plan de mitigación con acciones inmediatas recomendadas para el analista.

Es importante señalar que el alcance del prototipo desarrollado se centró en el análisis de datasets offline, sin realizar monitoreo en tiempo real de una red en producción. La detección se enfocó en anomalías de tráfico y vulnerabilidades conocidas a partir de la simulación de configuraciones. De manera crucial, y conforme al plan, el sistema implementado no incluyó la corrección automática de las vulnerabilidades; su función principal fue de alerta y soporte a la decisión.

Resultados Cuantitativos de la Validación

Validación del Modelo de Detección

Durante la fase de pruebas y validación del prototipo, se ejecutaron los ensayos funcionales y de rendimiento del modelo de detección utilizando los datasets de validación. El análisis cuantitativo de su desempeño reveló resultados de alta eficacia, validando exitosamente el rendimiento del prototipo en un entorno controlado. Las métricas clave de rendimiento obtenidas, que confirman la robustez y efectividad del modelo en la identificación de amenazas, fueron las siguientes:

- **Precisión (Accuracy):** 97.76%. Este valor indica la alta proporción de predicciones correctas del modelo sobre el total de clasificaciones realizadas.
- **Sensibilidad (Recall):** 99.40%. Esta métrica subraya la capacidad del modelo para identificar correctamente un alto porcentaje de las vulnerabilidades y ataques reales presentes en los datos.
- **F1-Score**: 98.15%. Este score representa la media armónica de la precisión y la sensibilidad, ofreciendo una medida equilibrada de la exactitud del modelo, especialmente útil cuando las clases están desbalanceadas.

Estos resultados cuantitativos constituyen la evidencia irrefutable de que la solución implementada es técnicamente viable, robusta y eficaz en la detección de amenazas. El desempeño detallado del modelo en la clasificación del tráfico normal frente a los ataques, incluyendo la identificación de verdaderos positivos, verdaderos

negativos, falsos positivos y falsos negativos, se ilustra de manera completa en la Matriz de Confusión, presentada a continuación.

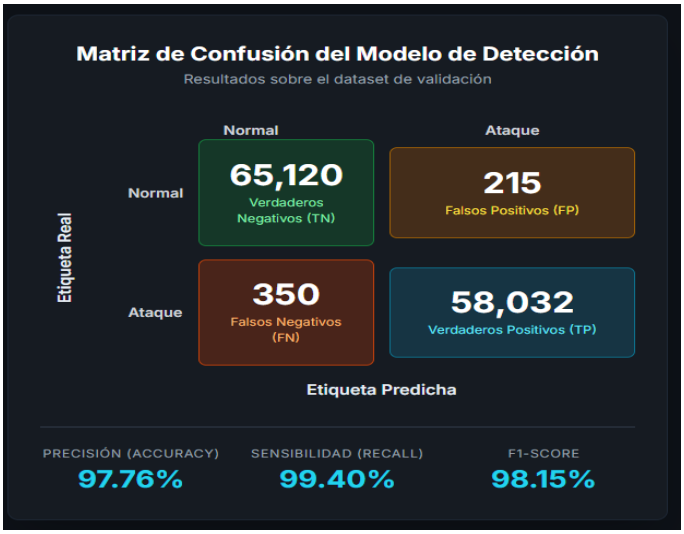

Ilustración 3: Matriz de Confusión que ilustra el rendimiento del modelo en la clasificación de tráfico normal frente a ataques. Los valores en la diagonal principal representan las predicciones correctas.

Estos hallazgos confirman la relevancia de la Inteligencia Artificial y las Redes Neuronales como herramientas esenciales para resolver problemas complejos en redes informáticas. Se espera que esta capacidad predictiva optimice la resiliencia tecnológica al minimizar los riesgos de incidentes de seguridad y optimizar los recursos a través de la anticipación de vulnerabilidades. La eficacia demostrada en la detección proactiva valida el potencial del sistema para transformar el paradigma de la ciberseguridad hacia un modelo más preventivo.

Discusión

Interpretación de la Viabilidad del Sistema

El proyecto demuestra alta viabilidad para implementar un sistema inteligente de detección proactiva de vulnerabilidades, con resultados concluyentes que validan su solidez conceptual, robustez técnica, practicidad operativa y eficiencia económica ante una necesidad digital creciente.

Factibilidad Técnica: El prototipo mostró buen desempeño en la validación. Las Redes Neuronales fueron clave al detectar relaciones complejas en el tráfico de red, evidenciando una solución robusta y eficaz en entornos controlados.

Factibilidad Operativa: El sistema complementa la seguridad existente en organizaciones. Su interfaz clara e intuitiva, con alertas y recomendaciones (Ilustraciones 3), facilita su integración en flujos de trabajo, mejorando decisiones ágiles en ciberseguridad.

Factibilidad Económica: El desarrollo tuvo costo mínimo (software libre, hardware genérico), con alta inversión intelectual. Su eficacia genera un ROI elevado frente a los riesgos financieros de incidentes, alineándose con el enfoque estratégico de la ciberseguridad digital.

Por lo tanto, el sistema es técnica, operativa y económicamente factible y responde con efectividad a un desafío crítico en el ámbito de la ciberseguridad.

Conclusiones y Futuras Líneas de Investigación

Este proyecto confirma la viabilidad de un modelo de seguridad proactivo basado en Inteligencia Artificial para la detección anticipada de vulnerabilidades en redes informáticas. Frente a las crecientes ciberamenazas, se plantea una transición necesaria de enfoques reactivos a predictivos, fortaleciendo así la resiliencia tecnológica de las organizaciones. El prototipo desarrollado demostró una notable capacidad para identificar patrones y anticipar riesgos antes de su manifestación, validado por altas métricas de rendimiento que respaldan su eficacia. A partir de los hallazgos obtenidos, se proponen tres recomendaciones clave para futuras fases:

- Continuar el desarrollo y escalamiento del prototipo, ampliando su procesamiento para operar en tiempo real.

- Fomentar alianzas académico-empresariales con PYMES o universidades que aporten datos de red anonimizados, lo que facilitará validaciones más robustas en entornos reales, y
- Promover líneas de investigación en Aprendizaje por Refuerzo, basadas en las propuestas de Sutton y Barto (2018), para avanzar hacia sistemas que no solo detecten amenazas, sino que también implementen contramedidas de forma autónoma y adaptativa.

Por lo antes expuesto, se deduce que, el estudio aborda una necesidad crítica en ciberseguridad contemporánea y sienta bases sólidas para innovaciones futuras, reafirmando el papel estratégico de la Inteligencia Artificial como herramienta esencial para la protección de infraestructuras digitales. Este enfoque no solo incrementa la capacidad de respuesta frente a amenazas, sino que representa una evolución fundamental en la automatización inteligente de los sistemas de defensa tecnológica.

Referencias

Comité Académico de Expertos de la Universidad Bicentenaria de Aragua. (2024). *Inteligencia Artificial Aplicada en el Campo de Acción*. Recuperado de https://uba.edu.ve/wp-content/uploads/2024/07/Volumen-1-N%C3%BAmero-1.-T%C3%ADtulo-Inteligencia-Artificial-Aplicada.-En-el-Campo-de-Acci%C3%B3n.pdf.

Cano, W. & Monsalve, S. (2023). *Ciberseguridad, Reto Empresarial para Afrontar la Era de la Digitalización Actual*. Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/11318/Ciberseguridad%2C%20reto%20empresarial%20para%20afrontar%20la%20era%20de%20la%20digitalizaci%C3%B3n%20actual.pdf?sequence=1&isAllowed=y.

Fernández D., Ángel J. (2025, julio). Sistema Inteligente para la Detección Proactiva de Vulnerabilidades en Redes Informáticas. Informe Técnico. San Cristóbal, Estado Táchira: Universidad Bicentenaria de Aragua.

IFAGER. (s.f.). Diplomado y sus características. Disponible en: https://campus.ifager.com/mod/imscp/view.php?id=154, consultado en Julio 2025.