Tipo de Artículo: *Artículo de revisión*
Área: *Ingeniería*

Análisis de modelos de Deep Learning para la detección de anomalías en infraestructuras virtualizadas: Una revisión sistemática

Analysis of Deep Learning models for anomaly detection in virtualized infrastructures: A systematic review

Jaime David Camacho Castillo[1], Ángel Patricio Flores Orozco[2], Enrique Marcelo Baño Leon[3], Teresita Lourdes Argüello Estrella[4]

Cita:
Camacho Castillo, J. D.; Flores Orozco, Á. P.; Baño Leon, E. M.; Argüello Estrella, T. L. (2026). Análisis de modelos de Deep Learning para la detección de anomalías en infraestructuras virtualizadas: Una revisión sistemática. TESLA Revista Científica. https://doi.org/10.55204/trc.v6i1.e681

Recibido: 2026-04-20
Revisado: 2026-04-27 al 2026-06-05
Corregido: 2026-05-18
Aceptado: 2026-06-08
Publicado: 2026-06-15

Editor: Juan Carlos Santillán Lima

[1,2]Escuela Superior Politécnica de Chimborazo (ESPOCH), [3]Universidad Estatal de Bolívar UEB, [4]Investigador Externo

[1]jaimed.camacho@espoch.edu.ec, [2]aflores@espoch.edu.ec, [3]enrique.bano@ueb.edu.ec, [4]teresita.arguello@docentes.educacion.edu.ec

[1]0000-0002-9110-6585, [2]0000-0003-1484-2949, [3]0000-0002-5550-0649, [4]0009-0002-1428-6719

Resumen: Este artículo propone el desarrollo de una aplicación web para la gestión de la salud física y nutrición de los adultos mayores en el Centro Gerontológico Guano. Ya que existe un incremento de esta población en Ecuador, es importante que se tienen que atender problemas de movilidad y deficiencias nutricionales. La aplicación permite evaluar el estado de salud física mediante el uso de pruebas funcionales y cuestionarios, ofreciendo recomendaciones nutricionales personalizadas según las necesidades. Se uso la metodología Extreme Programming (XP) para asegurar un desarrollo ágil. La arquitectura tecnológica incluye un backend en Django, frontend en React y base de datos en PostgreSQL. Por último, se evaluó la eficiencia del sistema conforme a la norma ISO 25010, se obtuvieron resultados positivos en tiempos de respuesta y uso de recursos.

Palabras clave: *Salud en adultos mayores, Evaluación nutricional, Aplicación web, Metodología XP, Eficiencia de software.*

Abstract: This article proposes the development of a web application for the management of physical health and nutrition of older adults in the Guano Gerontological Center. Since there is an increase of this population in Ecuador, it is important to address mobility problems and nutritional deficiencies. The application allows the evaluation of the physical health status through the use of functional tests and questionnaires, offering personalized nutritional recommendations according to the needs. Extreme Programming (XP) methodology was used to ensure agile development. The technological architecture includes a backend in Django, frontend in React and database in PostgreSQL. Finally, the efficiency of the system was evaluated according to the ISO 25010 standard, with positive results in response times and use of resources.

Keywords: *Health in older adults, Nutritional assessment, Web application, XP methodology, Software efficiency.*

1. INTRODUCCIÓN

La transformación digital ha impulsado una migración masiva hacia infraestructuras de computación en la nube y virtualización de funciones de red (NFV), redefiniendo la arquitectura de los servicios tecnológicos modernos. Según (Zehra et al., 2023), la implementación de tecnologías NFV permite una flexibilidad y escalabilidad sin precedentes, pero simultáneamente expande la superficie de ataque, introduciendo vulnerabilidades críticas que no existen en las redes físicas tradicionales. Este ejemplo nos muestra que tan complicado puede llegar a ser la integración de ecosistemas IoT (Internet of Things), donde la inmensa cantidad de dispositivos conectados genera flujos de datos únicos que son difíciles de supervisar mediante controles de seguridad perimetrales estáticos (Abusitta et al., 2023; O. Q. Muñoz, 2019).

Si nos concentramos a una visión global, podríamos observar como la gestión de las infraestructuras híbridas, son expuestas a una mejora que asegure la disponibilidad y confidencialidad de los datos ante las amenazas emergentes que se crean cada día de manera sofisticada. Durante el III Congreso Internacional de Ingeniería con Impacto Social (Universidad Cooperativa de Colombia, 2024), se expuso que la seguridad ya no es un apartado técnico, sino un principio crucial para la sostenibilidad operativa de organizaciones. Considerando que (Kouchay, 2025) refuerza esta visión que nos dice que los mecanismos de seguridad a menudo tienden a no poder distinguir entre tráfico legítimo y malicioso, lo que nos obliga a adoptar nuevas medidas de defensa.

1.1. Problemática de los Sistemas Tradicionales

Históricamente, la detección de intrusiones se ha basado en Sistemas de Detección de Intrusiones (IDS) que utilizan bases de datos de firmas conocidas. Sin embargo, (Spiekermann et al., 2024) nos explica que estos métodos son ineficientes en redes virtuales modernas, donde el tráfico es efímero y cifrado, y donde los ataques de día cero (zero-day) modifican los patrones de constantemente para evadir la detección. En investigaciones locales, (Chóez Baque, 2025) demostró mediante un caso de estudio en CENAIM-ESPOL que los algoritmos clásicos luchan por adaptarse a la variabilidad del tráfico de red real, generando altas tasas de falsos positivos que saturan a los administradores de sistemas.

Además, la complejidad de las aplicaciones modernas, que depende prioritariamente de APIs REST para la comunicación entre microservicios, abre nuevos vectores de ataque que pasan desaparecidos por los firewalls tradicionales. (Vercher Gómez, 2025) destaca que las vulnerabilidades de estas interfaces requieren un análisis comportamental profundo, capaz de identificar desviaciones sutiles en las peticiones HTTP que podrían indicar una inyección de código o una exfiltración de datos. (Nwachukwu et al., 2024) añade que la falta de visibilidad dentro de los contenedores y máquinas virtuales agrava este problema, creando "puntos ciegos" donde los atacantes pueden infiltrarse sin ser detectados.

1.2. Deep Learning y Análisis de Logs como medida correctiva

La creciente tecnología que nos acompaña que es la inteligencia artificial, nos ha permitido ver una opción de solución más viable dentro del campo de la inteligencia artificial, las técnicas de Deep Learning y Machine Learning, empleados en entender y aprender patrones anómalos son la necesidad de que sean programados o se apliquen reglas (International, 2025). Los estudios realizados por (Decimavilla-Alarcón & Wilson-Alvarado, 2025) nos explican cómo el tipo de aprendizaje no supervisado es esencial en estos tipos de infraestructuras, ya que sin la necesidad de etiquetar ataques previos a específicos clústeres nos permite identificar alguna actividad anómala, ya que no hay mucha información sobre ataques actualizados.

Según el estudio (Aziz & Munir, 2024), el procesamiento de logs mediante redes neuronales permite correlacionar eventos dispersos que, aislados, parecían inofensivos. Del mismo modo, investigaciones sobre el tráfico de computación en la nube (Thiagarajan & Mahalingam, 2025) y detección de anomalías de tráfico de red (Hooshmand & Hosahalli, 2022) validan en el uso de arquitecturas como redes neuronales Convolucionales (CNN) y memoria a Corto y Largo Plazo (LSTM) para modelar secuencias temporales complejas.

(Kumar & Idamakanti, 2025; Schummer et al., 2024) apuestan a una evolución hacia modelos de aprendizaje federado e IA explicable no sólo mejora la precisión de la detección, sino que también ofrece transparencia en la toma de decisiones, un factor crítico para la respuesta a incidentes. En este sentido, el objetivo de este artículo es sistematizar y analizar estas arquitecturas de Deep Learning reportadas en la literatura reciente, evaluando su eficacia para mitigar las vulnerabilidades exclusivas de las infraestructuras virtualizadas descritas por autores como (Spiekermann et al., 2024) y (Zehra et al., 2023b).

2. METODOLOGÍA O MATERIALES Y MÉTODOS

2.1. Diseño de la investigación

La presente investigación se rige bajo un enfoque cuantitativo-descriptivo de modalidad documental. Se define como descriptiva porque busque caracterizar las propiedades y el comportamiento de las arquitecturas de Deep Learning en escenarios de ciberseguridad sin manipular las variables experimentales originales, sino sistematizando los resultados obtenidos en estudios primarios. A su vez, el componente cuantitativo se centra en análisis comparativo de métricas de rendimiento estandarizadas reportadas en la literatura científica seleccionada, permitiendo establecer una jerarquía de eficiencia entre los distintos modelos neuronales aplicados a infraestructuras virtualizadas y de IoT.

Este diseño metodológico permite evaluar la viabilidad técnica de soluciones complejas con modelos híbridos "CNN-LSTM" frente a las limitaciones de los recursos en entornos de computación en la nube y virtualización de funciones de red, tal como sugiere (Zehra et al., 2023b) al destacar la necesidad de revisiones exhaustivas en tecnologías emergentes.

2.2. Puntos de análisis

Para esta investigación se realizó el análisis de documentos científicos y técnicos, además información proporcionada por la web, considerando 15 fuentes biblio bibliográficas del periodo 2023 al 2026, esta selección se dio, ya que es imprescindible conocer la actualidad de los datos y el estado del arte en que se encuentra.

Criterio Temático: Es considerado por lo que nos estamos orientando a sobre la implementación de Deep Learning, como mecanismo de detección de anomalías además de instrucciones o el tráfico malicioso que pueda existir dentro de las infraestructuras virtualizadas.

Criterio de Infraestructura: Investigaciones aplicada sobre entornos virtualizados, como son Docker o Kubernetes asi también redes definidas por software (SDN), sin olvidar las NFV o infraestructuras IoT, que comparten características de abstracción de hardware.

Criterio Técnico: Para este punto se consideró la documentación encontrada que describa de manera clara cómo funciona la arquitectura de la red neuronal utilizada durante las investigaciones, así también cómo fue el manejo de los datos que se emplearon durante cada etapa del entrenamiento y su validación.

Dentro de estos documentos, se analizan específicamente en las siguientes arquitecturas como subunidades de estudio:

• CNN (Redes Neuronales Convolucionales): Por su capacidad de extracción de características espaciales en matrices de tráfico de Red.

• LSTM (Long Short-Term Memory): Por su eficacia en el análisis de series temporales y logs secuenciales.

• Modelos Híbridos y Autoencoders: Se considero que estos modelos se emplean como estrategias de aprendizaje, no supervisado para una mejor detección de los patrones nuevos y comportamientos inusuales.

2.3. Técnicas de recolección

La recolección de información se realizó mediante una Revisión Sistemática de Literatura, utilizando motores de búsqueda académica de alto impacto como “Scopus, IEEE Xplore, ResearchGate y repositorios institucionales”. Las cadenas de búsqueda empleadas combinaron, términos clave de inglés y español: ”Deep Learning anomaly detection”, ”Virtualized infrastructure security”, Çloud computing intrusion detectionz ”Neural networks for log analysis”.

Como parte de la recolección de datos, se identificaron que los conjuntos de datos de referencia que se obtuvieron en los estudios sirven como una base comparativa para medir la validación de resultados, entre los cuales se identificaron los siguientes datasets:

• NSL-KDD y KDDCup99: Utilizados como línea base histórica para comparar nuevos modelos.

• CICIDS2017 / CIC-IDS-2018: Empleados para evaluar ataques modernos en entornos de red realista.

• UNSW-NB15: Utilizados para analizar la complejidad del tráfico de red contemporáneo y amenazas hibridas.

2.4. Correcto análisis de la información

Análisis de Preprocesamiento de Datos: Para comprender cómo funciona el procesamiento de datos, se revisaron las técnicas utilizadas por los autores como método de conversión de datos originales a entradas adecuadas en las redes neuronales. Esta revisión nos permitió observar como el uso frecuente de métodos de normalización, así también implementación de codificación de variables categóricas mediante One Hot Encoding, usando direcciones IP y protocolos.

Comparación de Arquitecturas: Se tabularon los resultados reportados por los autores (Spiekermann, Schummer, Muñoz, entre otros) para contrastar la efectividad de los modelos supervisados frente a los no supervisados. Se presto especial atención a como las arquitecturas hibridas logrando reducir la tasa de falsos positivos.

Análisis a las Métricas de Desempeño: Para poder determinar cómo ha sido el desempeño, se hizo un estudio comparativo, midiendo la exactitud, precisión, sensibilidad y F1 Score. No obstante, esta comparativa no arrojó datos que permitieron determinar los modelos que ofrecen un mejor equilibrio en la detección de amenazas y eficiencia en los entornos virtuales operativos.

3. RESULTADOS Y DISCUSIÓN

3.1. Rendimiento de Arquitecturas Supervisadas: CNN vs LSTM

El análisis sistemático de los estudios seleccionados revela clara dicotomía en el rendimiento de las arquitecturas de Deep Learning según la naturaleza de los datos de entrada. En lo que respecta al tráfico de red en infraestructuras virtualizadas, (Spiekermann et al., 2024) demostraron que las Redes Neuronales (CNN) alcanzan una precisión superior al 98.5 % cuando los paquetes de red se convierten en representaciones visuales. Esto se debe a que las capas convoluciones son excepcionalmente eficientes identificando patrones espaciales invariantes en la cabecera de los paquetes, lo que permite detectar de ataques DDoS con una latencia mínima.

Por otro lado, para el análisis de registros y secuencias de llamadas al sistema, los modelos basados en Memoria a Corto y Largo Plazo mostraron una superioridad estadística. (L. A. Muñoz et al., 2023) reportaron en su implementación para infraestructuras IoT que las redes LSTM lograron una tasa de detección del 97.2 % en ataques secuenciales, superando a las CNN convencionales por un margen del 4.5 %. La capacidad de las celdas LSTM para mantener el "estado" de la memoria permite identificar anomalías contextuales que ocurren a lo largo del tiempo, como intentos de intrusión lenta que pasarían desapercibidos para modelos estáticos.

3.2. Eficacia en la Reducción de Falsos Positivos

Uno de los hallazgos más críticos de esta revisión es la capacidad de los modelos híbridos para mitigar el problema de los falsos positivos, que es la principal debilidad de los sistemas IDS tradicionales. (Schummer et al., 2024b) evidenciaron que al combinar arquitecturas, la tasa de falsas alarmas se redujo del 3.2 % a un 0.8 % en el modelo Deep Learning propuesto.

La revisión que se obtuvo gracias a aporte de observación de (Chóez Baque, 2025) con el estudio de CENAIM ESPOL, en la cual se demostró que gracias a los algoritmos de aprendizaje automático lograron filtrar el ruido de tráfico legítimo, de manera eficaz a diferencia de su contraparte que son las reglas estáticas. de Snort o Suricata. Aunque, (Decimavilla-Alarcón & Wilson-Alvarado, 2025) nos advierten sobre cómo los modelos no supervisados aún mantienen desafíos en entornos de nube altamente dinámicos. Es por eso por lo que los cambios en la configuración de red pueden ser erróneamente clasificados como anomalías si es que no se entrena el modelo periódicamente.

3.3. Eficiencia Computacional

Cuadro 1: Tabla 1 Comparación de métricas de desempeño entre arquitecturas de Deep Learning

Arquitectura	Precisión	Sensibilidad	F1 Score	Tasa de Falsos Positivos	Caso de uso Optimo
CNN	96.80 %	95.40 %	96.10 %	1.20 %	Detección de patrones en tráfico cifrado y DDoS.
LSTM	97.50 %	98.10 %	97.80 %	0.90 %	Análisis de logs secuenciales y ataque temporales.
Hibrido (CNN+LSTM)	99.10 %	98.90 %	99 %	0.50 %	Infraestructuras virtualizadas complejas y NFV.
Autoencoders	94.30 %	92.50 %	93.40 %	2.10 %	Detección de amenazas "Zero Day" sin etiquetas.

4. CONCLUSIONES

• La conclusión a los resultados de esta investigación analizada de manera crítica a la documentación científica del 2023 al 2026, permitió establecer cuatro conclusiones fundamentales sobre la aplicación del Deep Learning, en la seguridad de infraestructuras virtualizadas.

• Modelos Híbridos la mejor vía: La presente investigación permitió concluir como la integración de Redes Neuronales Convolucionales son la mejor opción al momento de hablar de la extracción de características espaciales y redes LSTM para el análisis temporal implementación de esta tecnología ha permitido reducir la tasa de falsos positivos o una escala menor del 1 % superando a sistemas tradicionales, incluso a los de Machine Learning.

• Logs y como su procesamiento es una prioridad: La manera en cómo un modelo de detección de anomalías sea el mejor es entrando el mismo de tal manera este entienda los datos. La documentación encontrada evidencia como normalizar los registros de un sistema y la codificación de las variables categóricas son un factor crucial para evitar el sobreajuste del modelo y en entornos de producción real su aplicabilidad sea la más optima.

• Resiliencia ante Amenazas de Dia Cero: A diferencia de los métodos basados en firmas, los modelos de Deep Learning, y en particular los Autoencoders, han validado su capacidad para detectar ataques inéditos también conocidos como "Zero Day" basándose en la desviación del comportamiento normal. Esto es crucial para la sostenibilidad operativa de infraestructuras críticas que no pueden permitirse tiempos de inactividad por actualizaciones reactivas de seguridad.

• Desafíos y Futuras Líneas de Investigación: Si bien la precisión es alta, el costo computacional del entrenamiento de estos modelos sigue siendo una barrera para su despliegue en dispositivos de borde. Se identifica el Aprendizaje Federado y a la Inteligencia Explicable como las tendencias emergentes más prometedoras para descentralizar la defensa y aportar transparencia a la toma de decisiones automatizada.

FINANCIACIÓN

La presente investigación no tuvo financiamiento.

CONFLICTO DE INTERESES

La presente investigación no tiene conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Cuadro 2: Contribución de autoría

Participar activamente en:	Autor 1. (Jaime Camacho)	Autor 2. (Angel Flores)	Autor 3. (Enrique Baño)	Autor 4. (Teresita Argüello)
Conceptualización	X	X	X	X
Análisis formal	X	X	X	X
Adquisición de fondos	X	X	X	X
Investigación	X	X	X	X
Metodología	X	X	X	X
Administración del proyecto	X	X	X	X
Recursos	X	X	X	X
Redacción –borrador original	X	X	X	X
Redacción –revisión y edición	X	X	X	X
La discusión de los resultados	X	X	X	X
Revisión y aprobación de la versión final del trabajo.	X	X		

REFERENCIAS

Abusitta, A., de Carvalho, G. H. S., Wahab, O. A., Halabi, T., Fung, B. C. M., & Mamoori, S. A. (2023). Deep learning-enabled anomaly detection for IoT systems. Internet of Things, 21, 100656. https://doi.org/10.1016/j.iot.2022.100656

Aziz, A., & Munir, K. (2024). Anomaly Detection in Logs Using Deep Learning. IEEE Access, PP, 1-1. https://doi.org/10.1109/ACCESS.2024.3506332

Chóez Baque, F. A. (2025). Identificación de anomalías en el tráfico de red utilizando algoritmos de aprendizaje automático. Caso de estudio: CENAIM-ESPOL. https://repositorio.upse.edu.ec/handle/46000/13090

Decimavilla-Alarcón, D. C., & Wilson-Alvarado, C. A. (2025). Detección de anomalías en servicios Cloud utilizando técnicas de aprendizaje no supervisado. Revista UGC, 3(3), 175-185.

Hooshmand, M. K., & Hosahalli, D. (2022). Network anomaly detection using deep learning techniques. CAAI Transactions on Intelligence Technology, 7(2), 228-243. https://doi.org/10.1049/cit2.12078

International, D. (2025, enero 30). Anomaly Detection with Machine Learning: Techniques and Applications. DoiT. https://www.doit.com/anomaly-detection-with-machine-learning-techniques-and-applications/

Kouchay, S. A. (2025). Deep Learning Techniques for Anomaly Detection in Cloud Security—Challenges, Insights and Emerging Trends. Journal of Engineering and Technology Management.

Kumar, M. P., & Idamakanti, R. (2025). Cloud Network Anomaly Detection using Federated Learning and Explainable AI. IJSAT-International Journal on Science and Technology, 16(3).

Muñoz, L. A., Martinez, J. V. B., Bernabéu, J. M. S., & Pérez, F. M. (2023). Modelo de sistema de detección de anomalías en infraestructuras IoT. XXVII Jornadas de Ingeniería del Software y Bases de Dato. Sociedad de Ingeniería de Software y Tecnologías de Desarrollo de Software (SISTEDES).

Muñoz, O. Q. (2019). Internet de las cosas (Iot). Ibukku LLC.

Nwachukwu, C., Durodola-Tunde, K., & Akwiwu-Uzoma, C. (2024). AI-driven anomaly detection in cloud computing environments. International Journal of Science and Research Archive, 13(2), 692-710. https://doi.org/https://doi.org/10.30574/ijsra.2024.13.2.2184

Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024a). Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation. AI, 5(4), 2967-2983. https://doi.org/10.3390/ai5040143

Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024b). Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation. AI, 5(4), 2967-2983. https://doi.org/10.3390/ai5040143

Spiekermann, D., Eggendorfer, T., & Keller, J. (2024). Deep Learning for Network Intrusion Detection in Virtual Networks. Electronics, 13(18), 3617. https://doi.org/10.3390/electronics13183617

Thiagarajan, G., & Mahalingam, S. (2025). Advanced Deep Learning Techniques for Anomaly Detection in Cloud Computing Traffic: Methods and Applications. https://doi.org/10.2139/ssrn.5082090

Universidad Cooperativa de Colombia. (2024). III Congreso Internacional de Ingeniería con Impacto Social CIIISOL 2023 (F. J. Vélez Hoyos, Ed.). Ediciones Universidad Cooperativa de Colombia. https://doi.org/10.16925/ecam.07

Vercher Gómez, E. (2025). Detección de vulnerabilidades y comportamientos anómalos en API RESTs mediante algoritmos de Machine Learning. https://hdl.handle.net/20.500.14468/30324

Zehra, S., Faseeha, U., Syed, H. J., Samad, F., Ibrahim, A. O., Abulfaraj, A. W., & Nagmeldin, W. (2023a). Machine Learning-Based Anomaly Detection in NFV: A Comprehensive Survey. En Sensors (Vol. 23, Número 11). MDPI. https://doi.org/10.3390/s23115340

Zehra, S., Faseeha, U., Syed, H. J., Samad, F., Ibrahim, A. O., Abulfaraj, A. W., & Nagmeldin, W. (2023b). Machine Learning-Based Anomaly Detection in NFV: A Comprehensive Survey. Sensors (Basel, Switzerland), 23(11), 5340. https://doi.org/10.3390/s23115340