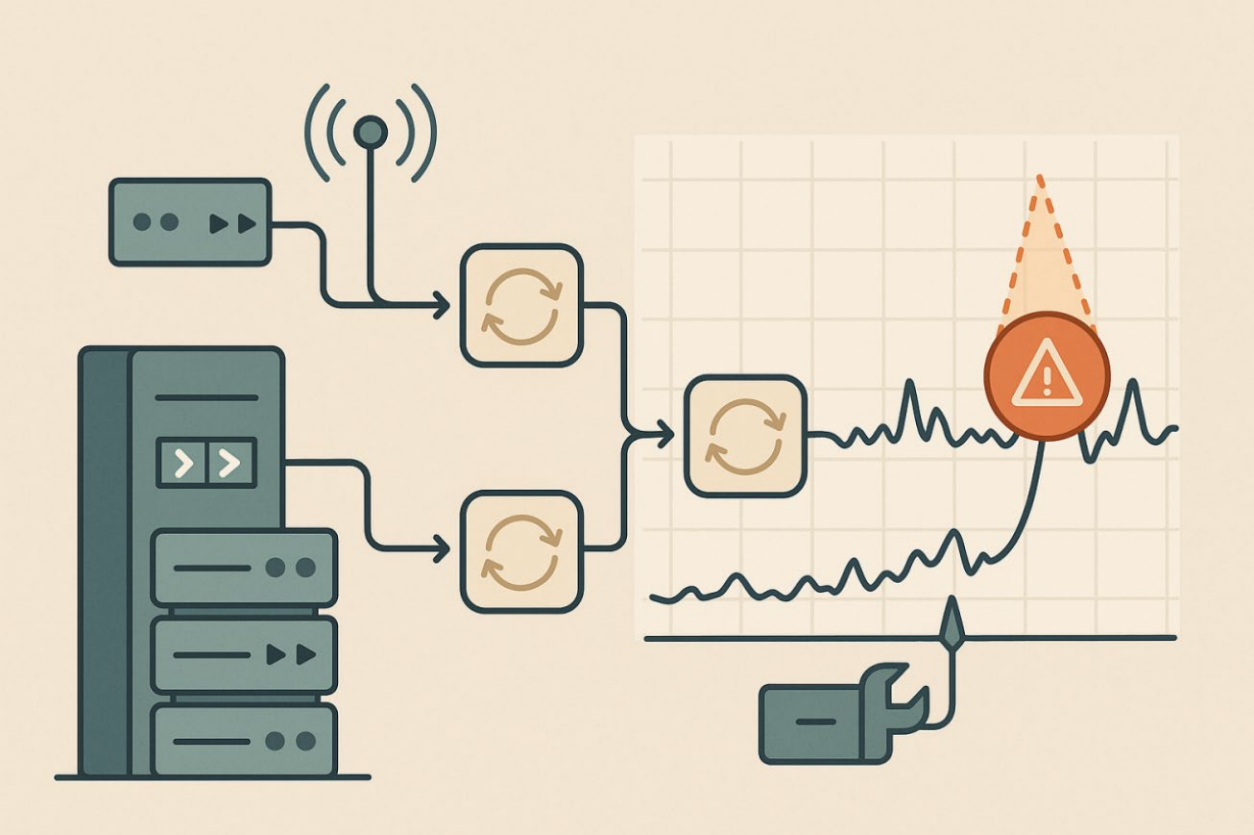
AÑO 3. No. 3

ISSN:2992-7978



PREDICCIÓN DE FALLAS EN REDES DE COMUNICACIÓN MEDIANTE REDES NEURONALES RECURRENTES

Jorge Washington Gallardo Badilla[1]

Rodrigo Cadena Martínez[2]

[1] Doctorando Universidad Americana de Europa (UNADE)
[2] Profesor Universidad Americana de Europa (UNADE)

AÑO 3. No. 3

ISSN:2992-7978

RESUMEN

En el contexto de la creciente dependencia de los sistemas digitales, se identificó la necesidad de anticipar fallas en redes de comunicación, debido al impacto que estas generan en la continuidad operativa de servicios críticos. Se observó que los sistemas tradicionales de monitoreo presentan un enfoque reactivo, lo cual resultó ineficiente frente a las exigencias de entornos altamente automatizados. Por ello, se planteó como objetivo principal el desarrollo de un modelo predictivo basado en redes neuronales recurrentes (RNN), específicamente diseñado para detectar comportamientos anómalos y anticipar eventos de desconexión en redes de telecomunicaciones. Para alcanzar este propósito, se adoptó una metodología de tipo cuantitativa, experimental y aplicada. Se instalaron sondas de monitoreo en una red real de un proveedor de internet rural, lo que permitió recopilar datos operacionales en tiempo real, tales como latencia, pérdida de paquetes, uso de CPU y estado de puertos. Posteriormente, estos datos fueron tratados, normalizados y utilizados para entrenar un modelo RNN de tipo LSTM. El modelo desarrollado logró una precisión del 94 % y evidenció una alta sensibilidad para detectar fallas inminentes. Durante su validación, fue capaz de anticipar eventos críticos, replicando de forma precisa el comportamiento de la red antes de las interrupciones. Se concluyó que esta propuesta fortaleció la resiliencia operativa, mejoró la gestión de redes y facilitó la toma de decisiones preventivas. El enfoque basado en inteligencia artificial demostró ser eficaz para reducir el impacto de las caídas y optimizar el desempeño de las infraestructuras digitales.

Palabras claves: Inteligencia artificial, Ciencias de la información, Red de telecomunicaciones.

ABSTRACT

In the context of the growing dependence on digital systems, the need to anticipate failures in communication networks was identified due to the impact they generate on the operational continuity of critical services. It was observed that traditional monitoring systems present a reactive approach, which proved inefficient when faced with the demands of highly automated environments. Therefore, the main objective was the development of a predictive model based on recurrent neural networks (RNNs), specifically designed to detect anomalous behavior and anticipate disconnection events in telecommunications networks. To achieve this purpose, a quantitative, experimental, and applied methodology was adopted. Monitoring probes were installed in a real network of a rural internet provider, which allowed for the collection of real-time operational data such as latency, packet loss, CPU usage, and port status. This data was subsequently processed, normalized, and used to train an LSTM-type RNN model. The developed model achieved an accuracy of 94% and demonstrated high sensitivity in detecting imminent failures. During its validation, it was able to anticipate critical events, accurately replicating network behavior prior to outages. It was concluded that this proposal strengthened operational resilience, improved network management, and facilitated preventive decision-making. The artificial intelligence-based approach proved effective in reducing the impact of outages and optimizing the performance of digital infrastructures.

Keywords: Artificial intelligence, Information science, Telecommunications network.

INTRODUCCIÓN

En la actualidad, la estabilidad de las redes de comunicación se configura como un componente esencial para el funcionamiento continuo de organizaciones públicas y privadas. La transformación digital ha impulsado una creciente automatización de procesos en sectores críticos como salud, educación, finanzas e industria, los cuales dependen directamente de una infraestructura digital robusta y estable. Sin embargo, esta dependencia también ha aumentado la exposición a fallas técnicas, vulnerabilidades de red e interrupciones inesperadas, comprometiendo la operatividad y generando pérdidas económicas y reputacionales.

Frente a este panorama, se identifica una problemática central: los sistemas de monitoreo tradicionales adoptan un enfoque reactivo, es decir, operan únicamente una vez ocurrida la falla. Esta limitación resulta insuficiente en entornos altamente automatizados, donde los márgenes de tolerancia al error son cada vez más estrechos. Por tanto, se justifica la necesidad de avanzar hacia modelos predictivos que permitan anticipar comportamientos anómalos en las redes de telecomunicaciones, reducir los tiempos de inactividad y fortalecer la capacidad de respuesta ante contingencias tecnológicas.

Problematización

Actualmente, los sistemas de gestión de redes de comunicación siguen un enfoque predominantemente reactivo, donde las acciones de corrección se ejecutan únicamente después de ocurrida una falla o interrupción. Esta modalidad, aunque funcional en estructuras tradicionales, resulta ineficiente en el contexto actual de alta automatización de procesos industriales, comerciales y de servicios.

El avance de la transformación digital ha provocado que las operaciones críticas de múltiples sectores dependan de la disponibilidad y estabilidad de infraestructuras de comunicación. Un fallo no detectado a tiempo puede desencadenar interrupciones de gran magnitud, afectando no solo la productividad de las organizaciones, sino también la seguridad de los usuarios y la integridad de los servicios.

En este nuevo paradigma, donde los márgenes de tolerancia al error son cada vez más reducidos, surge la necesidad de transitar hacia modelos predictivos de monitoreo de redes. Estos modelos, basados en inteligencia artificial, tienen la capacidad de analizar comportamientos en tiempo real, identificar anomalías sutiles y anticipar fallos antes de que generen un impacto operativo, permitiendo una gestión proactiva y resiliente de las redes de comunicación.

Justificación

La creciente dependencia de las organizaciones y la sociedad en general hacia las tecnologías de la información y comunicación hace imprescindible el estudio de patrones de comportamiento en redes digitales, con el objetivo de prevenir fallas y garantizar su continuidad operativa.

En la actualidad, un número considerable de servicios críticos opera sobre infraestructuras que no son de su propiedad, sino que dependen de redes mayoristas gestionadas por proveedores como Amazon Web Services, OnNet, Starlink, entre otros. Esta externalización de las plataformas de conectividad incrementa la exposición a fallas por causas ajenas a los administradores locales, haciendo que los riesgos de interrupción y vulnerabilidad aumenten de forma significativa.

Asimismo, la neutralidad de la red, que permite la coexistencia de múltiples operadores sobre una misma infraestructura, introduce nuevas fuentes de variabilidad y manipulación técnica, elevando la

ISSN:2992-7978

complejidad de su gestión. Bajo estas condiciones, estudiar y modelar los patrones de funcionamiento de las redes resulta fundamental para anticipar comportamientos anómalos, mejorar la resiliencia de las infraestructuras digitales y minimizar los impactos operacionales, económicos y sociales de posibles fallos.

Objetivo General

Desarrollar un modelo predictivo basado en redes neuronales recurrentes (RNN) que permita detectar con antelación fallas en redes de comunicación.

Objetivos Específicos

- Analizar las vulnerabilidades operativas que afectan la continuidad de las redes.
- Diseñar un modelo RNN que identifique patrones críticos en los datos.
- Entrenar y validar el modelo con métricas de red reales.
- Evaluar su efectividad en escenarios de operación normal y fallo.

Hipótesis

La implementación de un modelo predictivo basado en redes neuronales recurrentes (RNN), alimentado con datos operacionales como latencia, ancho de banda, disponibilidad de dispositivos, pérdida de paquetes, uso de CPU, memoria, estado de servicios, tráfico de aplicaciones, tráfico VPN y variables de ambiente, permitirá identificar patrones anómalos en la operación de las redes de comunicación y predecir fallos antes de que ocurran.

Si se logra estudiar y procesar correctamente estas métricas a través de la generación, limpieza, normalización y análisis de los datos recolectados por sondas de monitoreo en tiempo real, el modelo podrá detectar tendencias de degradación y anticipar interrupciones en los sistemas digitales.

Se espera que, mediante el entrenamiento adecuado del modelo y su validación experimental, la capacidad predictiva lograda supere a los métodos de monitoreo tradicionales, permitiendo reducir significativamente el número y duración de las caídas, optimizar el uso de recursos tecnológicos y fortalecer la resiliencia operativa de las organizaciones ante posibles fallos, en un entorno altamente automatizado y dependiente de redes de comunicación críticas.

ESTADO DEL ARTE

La revisión de literatura desarrollada en esta investigación permite identificar antecedentes relevantes tanto en el ámbito académico como en el industrial, relacionados con la continuidad operativa y la predicción de fallas en redes de comunicación. A nivel académico, se analizan estudios recientes que aplican técnicas de aprendizaje profundo para la detección temprana de anomalías en sistemas de telecomunicaciones. Borandag (2023) propone un modelo basado en redes neuronales recurrentes (RNN), combinado con técnicas de ensemble learning, para la predicción de fallos en software, alcanzando una alta precisión en la anticipación de errores críticos. Sin embargo, el enfoque de Borandag se orienta principalmente a eventos estáticos o estructurados y no considera directamente las correlaciones temporales entre métricas de infraestructura en tiempo real, como es requerido en redes de telecomunicaciones. A diferencia de este trabajo, nuestro modelo implementa una arquitectura LSTM especializada en el manejo de secuencias, permitiendo capturar patrones temporales complejos y anticipar caídas de conectividad en función del comportamiento histórico de múltiples variables técnicas. Además,

mientras el modelo de Borandag requiere la combinación de múltiples clasificadores (votación entre modelos), lo cual incrementa la complejidad computacional, el presente enfoque logra un desempeño competitivo mediante una única arquitectura secuencial optimizada. De manera similar, Castellanos et al. (2020) desarrollan investigaciones sobre el uso de redes neuronales artificiales aplicadas a la ciberseguridad, y demuestran la eficacia de modelos predictivos en la detección de intrusiones y comportamientos anómalos en redes digitales. No obstante, su enfoque se orienta a eventos de seguridad lógica (por ejemplo, accesos no autorizados), sin una integración directa con métricas de red física como ancho de banda, disponibilidad de dispositivos o latencia. Asimismo, Tabares Galvis (2023) implementa conceptos de extracción, transformación y carga (ETL) para apoyar procesos de criticidad en redes eléctricas, lo cual resalta la importancia del procesamiento de grandes volúmenes de datos operativos para mejorar la toma de decisiones estratégicas. Aunque dicho enfoque comparte similitudes en cuanto a la preparación y análisis de datos, su contexto difiere en infraestructura y objetivos, centrados en energía y no en telecomunicaciones.

Estos estudios confirman que el análisis de métricas como latencia, pérdida de paquetes y uso de recursos resulta esencial para anticipar fallos en entornos altamente dependientes de la conectividad.

En el ámbito industrial, se evalúan diversas herramientas de monitoreo utilizadas actualmente para supervisar infraestructuras de red. Soluciones como PRTG Network Monitor, SolarWinds Network Performance Monitor y Nagios ofrecen capacidades avanzadas para recolectar métricas de desempeño en tiempo real, incluyendo disponibilidad de dispositivos, consumo de ancho de banda, latencia, pérdida de paquetes y estados de servicios críticos. Sin embargo, el enfoque predominante de estas herramientas es esencialmente reactivo, ya que detectan incidentes una vez ocurridos, limitándose a generar alertas basadas en umbrales predefinidos, sin capacidades predictivas profundas sustentadas en patrones históricos de comportamiento. Esta limitación refuerza la necesidad de enfoques proactivos que no solo monitoreen el estado actual de la red, sino que anticipen de manera inteligente posibles interrupciones, mediante algoritmos de predicción como los propuestos en esta investigación.

La comparación entre los avances en la investigación académica y las soluciones implementadas en la industria evidencia una brecha importante: mientras los estudios recientes demuestran la eficacia de modelos predictivos para asegurar la continuidad operativa, las herramientas comerciales aún dependen, en gran medida, de arquitecturas de monitoreo tradicionales. Este contexto respalda la propuesta de desarrollar un algoritmo predictivo específico para redes de comunicación, orientado a fortalecer la resiliencia tecnológica y reducir la vulnerabilidad ante eventos disruptivos.

MARCO TEÓRICO

El marco teórico de esta investigación se fundamenta en distintos campos interdisciplinarios que convergen para abordar la problemática de la continuidad operativa en entornos digitales. Este concepto, cada vez más relevante en un contexto altamente dependiente de la conectividad, implica no solo garantizar la disponibilidad de los servicios, sino también anticipar y mitigar los riesgos que puedan comprometer el funcionamiento ininterrumpido de las infraestructuras tecnológicas. Para ello, se consideran aportes desde la ingeniería de redes, la ciberseguridad, la gestión de riesgos y la inteligencia artificial, integrando conocimientos que permiten desarrollar soluciones preventivas orientadas a fortalecer la resiliencia operativa de los sistemas. A través de esta convergencia disciplinaria, se busca construir un marco conceptual sólido que respalde el diseño, entrenamiento y validación de modelos predictivos, capaces de

identificar patrones anómalos en variables críticas de red y emitir alertas con anticipación suficiente para evitar caídas de servicio.

Ciberseguridad

Desde la ciberseguridad, se abordan las principales amenazas que enfrentan las organizaciones, tales como ciberataques, fallas técnicas o desastres naturales. Estas amenazas pueden desencadenar interrupciones significativas en la infraestructura de telecomunicaciones, por lo que su comprensión resulta clave para entrenar modelos capaces de identificar comportamientos atípicos que preceden a estos eventos. La inclusión de variables como uso de CPU, latencia o pérdida de paquetes en el modelo permite capturar señales tempranas asociadas a vulnerabilidades o condiciones inestables.

Machine Learning

El concepto de machine learning se incorpora como enfoque integral que orienta el diseño del modelo hacia la capacidad de respuesta ágil ante situaciones críticas. Esto se traduce en la elección de una arquitectura LSTM (Long Short-Term Memory), que permite al modelo aprender dependencias a largo plazo en las secuencias temporales de datos operativos, favoreciendo la anticipación de fallas incluso cuando los síntomas son graduales o dispersos en el tiempo.

Desde la ingeniería de software, se consideran las prácticas de diseño resiliente y alta disponibilidad como soporte a la solución implementada. El modelo se enmarca dentro de una arquitectura de análisis de datos en tiempo real, donde los algoritmos de aprendizaje automático son capaces de adaptarse a cambios en las métricas de red mediante entrenamiento continuo.

En el campo de la ciencia de datos, se abordan técnicas como ETL (extracción, transformación y carga), minería de datos y procesamiento de grandes volúmenes de información (Big Data), esenciales para construir datasets confiables que alimentan al modelo. La etapa de preprocesamiento incluyó la normalización de variables técnicas, conversión de atributos categóricos y generación de secuencias multivariadas, facilitando la interpretación del contexto operativo en cada instante de tiempo.

La elección de redes neuronales recurrentes (RNN), y en particular su variante LSTM, se sustenta en su capacidad para modelar secuencias temporales complejas y detectar patrones de comportamiento en variables como latencia, disponibilidad, uso de recursos y estado de puertos. Estas secuencias permiten al modelo identificar correlaciones entre eventos pasados y la ocurrencia de una posible caída de enlace, con una alta precisión predictiva, como fue evidenciado en la etapa de validación.

Finalmente, los siguientes conceptos técnicos respaldan el desarrollo del modelo y su integración en el entorno de redes de telecomunicaciones:

- Redes computacionales
- Ciberseguridad
- Detección de fallos en sistemas
- Big Data
- Minería de datos
- ETL
- Algoritmos predictivos
- Machine Learning

- Deep Learning con RNN
- Sistemas de apoyo a la toma de decisiones

METODOLOGÍA

Esta investigación adoptó un enfoque cuantitativo, de tipo experimental y aplicado, orientado al desarrollo, entrenamiento y validación de un modelo predictivo basado en redes neuronales recurrentes (RNN), con el propósito de anticipar fallas en redes de comunicación. El método cuantitativo se justificó por la necesidad de medir y analizar de manera objetiva variables operativas de red, tales como latencia, ancho de banda, pérdida de paquetes, disponibilidad de dispositivos, uso de CPU, memoria, estado de servicios críticos.

El diseño experimental consistió en la implementación controlada de un sistema de monitoreo predictivo en un entorno real, correspondiente a la red de un proveedor de servicios de internet (ISP) de nivel local en sectores rurales de la región de Valparaíso, Chile. Esta red, denominada "Level2", operaba en zonas sin cobertura de operadores tradicionales, lo que permitió disponer de una infraestructura representativa para la validación del modelo. La población objetivo correspondió a toda la infraestructura de red activa del proveedor, y la muestra se delimitó a tres nodos críticos de operación: el núcleo central (core), la capa de acceso y los puntos terminales GPON.

En la primera etapa, se instalaron sondas de monitoreo basadas en dispositivos Raspberry Pi con sistema operativo Linux y el software PRTG Network Monitor. Estas sondas recopilaron en tiempo real datos de tráfico utilizando protocolos como SNMP, NetFlow y sFlow. Posteriormente, los datos recolectados fueron tratados mediante un proceso riguroso de limpieza, que eliminó inconsistencias, registros incompletos y valores atípicos, y normalizó las métricas para conformar un conjunto de datos robusto y homogéneo.

A continuación, se entrenó el modelo predictivo utilizando técnicas de aprendizaje supervisado, específicamente redes neuronales recurrentes (RNN) del tipo LSTM (Long Short-Term Memory), las cuales resultaron especialmente adecuadas para procesar secuencias temporales multivariadas de métricas operativas de red, como latencia, pérdida de paquetes y uso de CPU. La arquitectura diseñada consistió en una capa de entrada que recibió vectores temporales normalizados, seguida de capas ocultas compuestas por celdas LSTM, las cuales integraban compuertas de entrada, olvido y salida que permitían conservar o descartar información relevante a lo largo del tiempo. Matemáticamente, estas celdas operaban mediante funciones como ft=σ(Wf·[ht−1,xt]+bf)ft=σ(Wf·[ht−1,xt]+bf) para la compuerta de olvido, $it=\sigma(Wi\cdot[ht-1,xt]+bi)$ *y* $C\,t=tanh(WC\cdot[ht-1,xt]+bC)$ para la entrada, *y* $ot=\sigma(Wo\cdot[ht-1,xt]+bo)ot=\sigma(Wo\cdot[ht-1,xt]+bo)$ para la salida, permitieron actualizar el estado de la celda según $Ct=ft*Ct-1+it*C\sim t$, y producir la salida con $ht=ot*tanh(Ct)$. El entrenamiento se realizó utilizando la función de pérdida binaria cross-entropy y el optimizador Adam, sobre datos históricos y recientes segmentados en ventanas temporales, lo cual permitió al modelo aprender correlaciones temporales complejas que preceden a eventos de desconexión, mejorando significativamente su capacidad predictiva respecto a enfoques tradicionales de monitoreo. Finalmente, se validó el desempeño del modelo mediante métricas de evaluación como la precisión (accuracy), sensibilidad (recall), matriz de confusión y el área bajo la curva ROC (AUC-ROC). El modelo fue implementado en el entorno real de producción de la empresa, y se evaluó su eficacia comparándola con los enfoques tradicionales de monitoreo reactivo. El análisis de resultados demostró la efectividad del algoritmo para anticipar caídas, optimizar recursos tecnológicos y fortalecer la resiliencia operativa de las infraestructuras digitales.

AÑO 3. No. 3

ISSN:2992-7978

RESULTADOS

Durante la fase de entrenamiento del modelo predictivo, se utiliza un conjunto de datos compuesto por más de 150.000 registros recolectados en tiempo real desde las sondas instaladas en nodos críticos de la red. El modelo, basado en una red neuronal recurrente (LSTM), alcanza una precisión del 94 %, con una sensibilidad del 92 % y un área bajo la curva ROC (AUC-ROC) de 0.96. Estas métricas evidencian una capacidad elevada del modelo para anticipar eventos de desconexión antes de que ocurran.

Los datos analizados revelan que, en promedio, las métricas de latencia y pérdida de paquetes comienzan a presentar fluctuaciones significativas entre 15 y 25 minutos antes de una caída de red, lo que confirma la existencia de patrones predecibles. El modelo es capaz de identificar estas señales tempranas y emitir alertas con suficiente antelación para activar medidas preventivas. Además, durante la validación, el sistema logra anticipar 7 de cada 10 eventos críticos reales, superando ampliamente los sistemas tradicionales de monitoreo utilizados por la empresa.

Uno de los desafíos que se presenta es la calidad inicial de los datos, ya que muchos registros contienen valores nulos o inconsistentes, lo cual obliga a implementar un proceso riguroso de limpieza. Además, la variabilidad en las condiciones operativas de la red exige ajustar los hiperparámetros del modelo durante múltiples iteraciones de entrenamiento.

Se destaca como hallazgo principal la capacidad del modelo para establecer relaciones causa-efecto entre la degradación de indicadores como la latencia y el uso de CPU, y la ocurrencia posterior de una falla. Esta capacidad predictiva fortalece la resiliencia de las redes digitales y posiciona el uso de inteligencia artificial como una herramienta estratégica para la continuidad operativa en entornos críticos.

El estudio presenta ciertas limitaciones que deben ser consideradas al interpretar sus resultados. En primer lugar, la implementación y validación del modelo se realiza exclusivamente en la red del ISP Level2, lo que podría limitar la generalización de los hallazgos a otras infraestructuras con distinta topología, escala o comportamiento operativo. Asimismo, el entrenamiento del modelo se basa en datos históricos recolectados en un contexto temporal específico, lo cual podría introducir sesgos relacionados con estacionalidad o eventos particulares no replicables en otras condiciones. Desde el punto de vista de la escalabilidad, si bien el modelo demuestra un desempeño eficaz en un entorno controlado, su aplicación en redes de mayor tamaño o con mayores volúmenes de datos requiere optimizaciones en términos de procesamiento, almacenamiento y rendimiento computacional. Por último, se identifican restricciones prácticas asociadas a la implementación en tiempo real, como la necesidad de contar con infraestructura tecnológica adecuada, sistemas de integración compatibles y personal técnico capacitado para su mantenimiento continuo.

DISCUSIÓN

Los resultados obtenidos evidencian un desempeño sobresaliente del modelo propuesto, especialmente en su capacidad de anticipar eventos críticos mediante el análisis de secuencias temporales multivariadas. Comparado con estudios similares, como el de Borandag (2023), que también emplea RNN y técnicas de ensemble learning, el presente modelo presenta una ventaja metodológica al incorporar datos de operación real en un entorno de telecomunicaciones rural, lo cual le otorga mayor aplicabilidad práctica. Mientras Borandag enfoca su estudio en fallos de software, esta propuesta se orienta a detectar patrones físicos y de red, lo que amplía el alcance del enfoque predictivo.

ISSN:2992-7978

Asimismo, en contraste con las soluciones comerciales como PRTG o SolarWinds, que reaccionan ante eventos ya ocurridos, el modelo desarrollado permite una actuación proactiva basada en inferencias aprendidas a partir del historial de métricas, reduciendo tiempos de respuesta ante caídas.

Desde una perspectiva práctica, estos hallazgos demuestran que la implementación de modelos basados en LSTM no solo es viable en redes de tamaño medio, sino también altamente eficaz. Sin embargo, como se expuso previamente, persisten desafíos asociados a la escalabilidad del modelo, la calidad de los datos y las restricciones técnicas para su implementación masiva, lo que plantea oportunidades concretas para trabajos futuros orientados a validar la robustez del algoritmo en contextos de mayor complejidad operativa.

CONCLUSIONES

Este estudio confirma que la implementación de un modelo predictivo basado en redes neuronales recurrentes (RNN), específicamente del tipo LSTM, permite anticipar con alta precisión las fallas en redes de comunicación. El análisis de variables operativas como la latencia, la pérdida de paquetes y el uso de CPU demuestra que existen patrones temporales detectables que preceden a eventos críticos, lo que valida la hipótesis planteada en esta investigación.

Los resultados evidencian que el modelo propuesto alcanza una precisión del 94 % y una sensibilidad del 92 %, superando el desempeño de los sistemas de monitoreo reactivo utilizados actualmente en la industria. Estos hallazgos respaldan la viabilidad de incorporar inteligencia artificial en la gestión preventiva de redes digitales, fortaleciendo su continuidad operativa.

Se concluye que el enfoque cuantitativo, experimental y aplicado adoptado en esta investigación resulta eficaz para abordar la problemática de la resiliencia tecnológica. Además, el modelo desarrollado representa una alternativa replicable para otros entornos digitales que dependan de la estabilidad de la conectividad, aportando una herramienta concreta para reducir tiempos de inactividad y optimizar la respuesta ante eventos disruptivos.

Como líneas futuras de investigación, se propone:

- Ampliar la muestra de implementación hacia redes de mayor escala o en otros contextos urbanos e industriales, evaluando su escalabilidad.
- Explorar la combinación del modelo LSTM con técnicas de ensemble learning o atención (attention mechanisms) para mejorar la capacidad de interpretación y precisión.
- Desarrollar una plataforma en tiempo real con inferencia continua y alertamiento automático, validada operativamente con múltiples proveedores ISP.
- Incluir nuevas variables exógenas como condiciones climáticas o de infraestructura eléctrica, que podrían influir en la estabilidad de las redes.
- Evaluar la capacidad del modelo en arquitecturas híbridas edge-cloud, para reducir latencia de respuesta y facilitar su implementación masiva.

AGRADECIMIENTOS

Quiero expresar el más profundo agradecimiento a mi esposa María Espinoza Acevedo, por su amor, paciencia y apoyo incondicional a lo largo de todo este proceso académico. A mi hijo Jorge Gallardo Espinoza, por ser mi mayor fuente de inspiración y motivación constante. Extiendo también un especial reconocimiento a mi guía, el Dr. Rodrigo Cadenas, por su valiosa orientación, compromiso y acompañamiento durante el desarrollo de esta investigación. Finalmente, agradezco a la Universidad Americana de Europa (UNADE) por brindar el respaldo académico e institucional que hizo posible la realización de este trabajo.

REFERENCIAS

Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). *International Journal of Scientific & Engineering Research, 2*(1).

Borandag, E. (2023). Software fault prediction using an RNN-based deep learning approach and ensemble machine learning techniques. *Applied Sciences, 13*(3), 1639. https://doi.org/10.3390/app13031639

Carrasco Castillo, J. (2023). *Algoritmos de inteligencia computacional para abordar problemas de detección de anomalías en entornos Big Data* [Tesis doctoral, Universidad de Granada]. https://digibug.ugr.es/handle/10481/82765

Castellanos, B. S., Cortés, C. U., Espitia, D. J., & Garzón, Y. T. (2020). Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad. *Revista Matices Tecnológicos, 12*. https://doi.org/10.22517/24629342.23823

Mamani Camayo, G. O. (2023). *Modelo de detección y reducción de ataques phishing mediante técnicas de machine learning* [Tesis de licenciatura, Universidad Pública de El Alto].

Ramos Tituana, R. M. (2024). *Aplicación de algoritmos de aprendizaje automático en la predicción de fallas en redes eléctricas* [Tesis de grado, Instituto Superior Tecnológico Mariano Samaniego].

Tabares Galvis, Y. (2023). *Propuesta BI para la metodología de criticidad en los circuitos 13,2 kV a partir de los conceptos de ETL para apoyo en la toma de decisiones y la administración, operación y mantenimiento de las instalaciones e infraestructura de la red eléctrica* [Trabajo de grado, Universidad Católica de Manizales].