

Modelo de inteligencia artificial para la detección de intrusiones según características de la red y prácticas de los usuarios

Artificial intelligence model for intrusion detection based on network characteristics and user practices

Karla Yohana Sánchez-Mojica*

Ender José Barrientos Monsalve**

Marling Carolina Cordero Díaz***

Fecha de recepción:13-11-2025

Fecha de evaluación:18-11-2025

Fecha de aprobación:05-12-2025

<https://doi.org/10.22335/rlct.v18i1.2250>

Para citar este artículo / To reference this article / Para citar este artigo: Sánchez-Mojica, K., Barrientos Monsalve, J., Cordero Díaz, M. (2025). Modelo de inteligencia artificial para la detección de intrusiones según características de la red y prácticas de los usuarios. *Revista Logos Ciencia & Tecnología*, 18(1), 36-48. <https://doi.org/10.22335/rlct.v18i1.2250>

Nota de autor: El presente artículo se deriva del proyecto de investigación titulado inteligencia artificial para la detección de intrusiones en el contexto de la ciberseguridad y ha sido financiado por la Corporación Universitaria Iberoamericana".

RESUMEN

Este trabajo tuvo como propósito presentar un modelo de inteligencia artificial con base a los algoritmos XGBoost, diseñado para la detección de intrusiones en redes informáticas analizando información de características, técnicas y comportamientos de usuarios. Esto con uso de datos que incluyeron variables de tamaño de paquetes, la reputación de las direcciones IP, intentos fallidos de autenticación y acceso de diversos horarios. La metodología utilizada bajo un enfoque en algoritmos de Boosting consolidado como una alternativa para mejorar los desafíos crecientes de ciberseguridad. Como resultado se puede evidenciar que la investigación no solo valida empíricamente el modelo propuesto, sino que mejora el reforzamiento de la implementación de soluciones automáticas con base a la inteligencia artificial, con esto mitigar los riesgos que se derivan de la práctica diaria en las redes y bases de datos, y así mejorar los contextos vulnerables de la red.

Palabras clave: Inteligencia artificial, redes neuronales, intrusión, usuarios, modelo.

ABSTRACT

The purpose of this work was to present an artificial intelligence model based on XGBoost algorithms, designed for the detection of intrusions in computer networks

- * Autor de correspondencia.
Corporación Universitaria Iberoamericana. Bogotá, Colombia.
karla.sanchez@docente.ibero.edu.co
<https://orcid.org/0000-0003-31644725>
- ** Universidad de Pamplona. Pamplona, Colombia
ender.barrientos@unipamplona.edu.co
<https://orcid.org/0000-0001-6673-0223>
- *** Universidad Francisco de Paula Santander, Cúcuta, Colombia
marlingcarolinacd@ufps.edu.co
<https://orcid.org/0000-0002-2913-5588>



by analyzing information on characteristics, techniques and user behaviors. This with the use of data that includes packet size variables, the reputation of IP addresses, failed authentication attempts and access at different times. The methodology used under a focus on Boosting algorithms consolidating as an alternative to improve the growing challenges of cybersecurity. As a result, it can be seen that the research not only empirically validates the proposed model, but also improves the reinforcement of the implementation of automatic solutions based on artificial intelligence, thereby mitigating the risks that arise from daily practice in networks and databases, and thus improving vulnerable network contexts.

Keywords: Artificial intelligence, neural networks, intrusion, users, model

Introducción

En la actualidad los sistemas interconectados han evolucionado mejorando los contextos de interconectividad, pero también ha generado aumentos de los riesgos de seguridad informática, es así que, las intrusiones en redes ha sido una amenaza constante para los contextos de seguridad, confidencialidad e integridad de los datos que se encuentran alojados en las diferentes bases de datos y servidores, sin embargo a pesar de las innovaciones en los sistemas de detección de intrusos (IDS), bastantes de ellos solo se direccionan en el análisis de tráfico de red, es así que en ciertas ocasiones puede estar limitado a la seguridad del ciberespacio actual.

De acuerdo con diversos estudios, se puede asegurar que, tratar la seguridad de las redes de comunicación debe tomarse y manejarse de manera integral, teniendo en cuenta aspectos técnicos y humanos ya que estos son dimensiones que complementan los escenarios de las redes. Por ejemplo, al respecto, Pacheco (2024) resalta la importancia de considerar la confidencialidad, disponibilidad e integridad de los datos en la seguridad de las redes, dando la mayor importancia a una protección efectiva desde una visión holística que organice la situación desde la infraestructura tecnológica hasta la aplicación de buenas prácticas por parte de los usuarios, en este mismo sentido los aportes de investigacio-

nes realizadas durante la pandemia, evidenciaron un aumento de los ciberataques sustentados en el aprovechamiento de los nuevos enfoques de trabajo remoto y la incapacidad de las organizaciones en términos de seguridad digital.

Adicionalmente, el rápido despliegue del E-learning durante la pandemia, aunque esencial para la continuidad educativa, expuso vulnerabilidades críticas en la gestión de entornos digitales (Pérez Pinzón, 2020). Este contexto resalta la urgencia de integrar soluciones automatizadas, como modelos de IA, para mitigar riesgos en escenarios donde la adopción tecnológica supera las capacidades de seguridad tradicionales.

Así mismo, un estudio de la Universidad del Valle, reveló que, a pesar de que docentes y estudiantado tienen un conocimiento aceptable sobre seguridad de la información, los esfuerzos de la universidad para mejorar y fomentar una higiene digital no han sido suficientes (Estrada et al., 2021), además de esto por otro lado, Muñoz Hernández et al. (2020) evalúan los riesgos informáticos en diversos sistemas contables en Colombia, donde destacan la necesidad de implementar estrategias efectivas para disminuir contextos que puedan poner en riesgo la seguridad de la información en las bases de datos, teniendo cuidado tanto en las amenazas técnicas como en las vulnerabilidades humanas.

Estas posturas resaltan la necesidad de desarrollar sistemas de inteligencia artificial que puedan tener aspectos técnicos de seguridad de las redes y habito sed acciones de humanos para poder enfrentar esta situación, para poder mejorar la identificación y detección del acceso no autorizado en contextos cada vez más vulnerables, por cuanto una de las situaciones más complejas actualmente es la seguridad digital y el cambio continuo de la actividad nociva que se ha vuelto cada vez más difícil de detectar con las técnicas tradicionales, además las personas que se dedican en atacar las redes utilizan métodos cada vez más mejorados para vulnerar los sistemas de seguridad, por ejemplo el tráfico de red cifrado, y el cambio del malware, lo que plantea una dificultad real para los sistemas que soportan solo de las políticas de las organizaciones y establecen reglas para identificar amenazas.

Es así que, la creciente digitalización de los servicios y la expansión del internet han aumentado considerablemente la exposición de las redes a ciberataques generando diversas situaciones agravando el comportamiento de los usuarios que a menudo no conocen las prácticas seguras de navegación y gestión de datos, lo que crea vulnerabilidades críticas en los sistemas, González-Ramírez & Camacho-Nieto, (2021), las dimensiones como factores como la falta de protocolos de autenticación sólidos, el uso de métodos de cifrado anticuados y la configuración inadecuada de la red son algunas de las razones que han permitido el aumento de actividades maliciosas en las redes. Según Vargas, et al. (2018), las características de cómo están formadas las redes y como los usuarios ejecutan las acciones son elementos claves para poder identificar comportamientos anómalos que conllevan a las intrusiones.

Actualmente esto representa un desafío para las empresas por cuanto compromete la seguridad de la información así como

la disponibilidad de ella, es allí donde se pueden presentar diferentes tipos de amenazas como las pérdidas económicas hasta llegar a daños irreparables a la reputación de la organización; las intrusiones no solo permiten el acceso no autorizado a información sensible, también puede llegar a ser escenarios de sabotaje, fraudes, y espionaje corporativo Fernández (2019), y Hernández (2016). De esta misma manera cuando las empresas no tienen mecanismos de seguridad que sean automatizados para tal detección como por ejemplo los modelos de IA, los tiempos de respuestas a estas amenazas suele extenderse dándole más tiempo a los intrusos facilitando que ocasionen más daños, es por ello que la implementación de la inteligencia artificial es una estrategia imprescindible para analizar información en tiempo real y patrones de comportamiento, mejorando con esto la capacidad de respuesta ante algún ciberataque y la reducción de los riesgos. (Cárdenas y Cárdenas, 2018).

Fundamentación teórica

Los ataques cibernéticos se han vuelto una situación compleja y constante que ha impactado personas y empresas, esto causado por situaciones complejas en los avances tecnológicos y manejo de información delicada de programadores. Estos ataques pueden poner en riesgo la integridad, disponibilidad y confidencialidad de los datos, teniendo resultados con pérdidas y daños impensables (Pérez-Caballero et al., 2020). Con esto, las redes informáticas, siendo el principal canal de circulación de información, se han convertido en objetivos perfectos para personas con conocimientos en esta área, es por ello vital contar con mecanismos que aseguren las redes, esencialmente en entornos donde las prácticas inseguras de algunos usuarios aumentan las vulnerabilidades. (González-Ramírez & Camacho-Nieto, 2021).

Aunado a esto la inteligencia artificial compone elementos como las técnicas de aprendizaje automatizadas que han demostrado ser efectivas para detectar intrusiones en redes informáticas, permitiendo así hacer procesos analíticos en grandes bases de datos que permiten predecir algunos comportamientos maliciosos en la red.

En este sentido Cando, & Mendoza (2022), expresan que el uso de la inteligencia artificial en las aplicaciones para evitar las intrusiones en redes que son definidas por software (SDN) ayuda a identificar amenazas y vulnerabilidades proactivas por medio de los análisis de datos y la identificación de patrones y anomalías en tiempo real, con esto se puede mejorar la resiliencia y coadyuvar a la confiabilidad de los sistemas ante amenazas cibernéticas que se encuentran en constante evolución.

Asimismo, Martínez (2022) y Quintero & Suescún (2018) señalan que se pueden diseñar sistemas de detección de intrusiones con aprendizaje automático, como Random, y forest, ellos permiten ordenar y clasificar las diferentes conexiones en tiempo real, con esto es posible diferenciar entre un tráfico normal y ataques con un bajo nivel de alarmas, y así se puede mejorar las alarmas tempranas en los entornos de red.

Dentro de las intrusiones en las redes, este tema ha venido evolucionando direccionado hacia la inteligencia artificial ya que esta herramienta es capaz de asumir anomalías y comportamientos cuando se presenten amenazas. Según Rivero Pérez (2014), este aprendizaje automático viene a representar un apoyo importante en la detección de intrusos, ya que mejora los procesos de análisis de los tráficos miliciosos. En línea con lo anterior, la gestión estructurada de proyectos tecnológicos —como las Estructuras Desglosadas de Trabajo (EDT) en metodologías ágiles (Rojas Puentes et al., 2022)— demuestra cómo herramientas de organización jerárquica pueden optimizar

la implementación de sistemas complejos, incluidos los IDS basados en IA, al garantizar una asignación clara de recursos y responsabilidades, algunos ejemplos son los sectores como el de la salud donde se ha evidenciado que no cuentan con sistemas robustos, y donde se hace necesario el uso de herramientas de detección.

También Perdigón Llanes & Orellana García (2021), enfatizan la necesidad de implementar tecnologías emergentes en los modelos de inteligencia artificial, ya que se ha demostrado la importancia del Deep learning en la detección de intrusiones relacionadas con el tráfico de la dark web, la aplicación de las redes neuronales profundas pueden predecir estos patrones complejos, con esto superar los sistemas tradicionales que se basan en firmas y que dependen de datos estáticos que son vulnerables.

■ Metodología

A. Conjunto de datos

El conjunto de datos utilizado precisa la detección de ataques partiendo de las características de las redes como uno de los principales determinantes, además de las prácticas de los usuarios de la red, donde cada característica proporciona información valiosa sobre posibles ciberamenazas. Los datos se generaron con el propósito de emular el comportamiento de una red bajo un entorno de ciberseguridad, incluyendo parámetros como el tamaño de los paquetes, el protocolo utilizado, intentos de autenticación, duración de las sesiones, métodos de cifrado de empleados y las puntuaciones de reputación asociadas a las direcciones IP (Kumar, 2025). Posteriormente, estos datos fueron procesados mediante la codificación de variables categóricas y la incorporación de una etiqueta binaria `attack_detected` que indica la detección de posibles ataques (1significa que

se detectó un ataque, 0 significa actividad normal), determinada según umbrales de riesgo previamente establecidos.

Las tablas 1 y 2 muestran los ítems de cada característica analizada:

Tabla 1.

Ítem basados en red

Ítem	Descripción	Observaciones
network_packet_size	Tamaño del paquete en bytes	Varía entre 64 y 1500 bytes
protocol_type	Protocolo de comunicación	Protocolo utilizado en la sesión: TCP, UDP o ICMP
encryption_used	Protocolo de cifrado	Valores: AES, DES, Ninguno

Tabla 2.

Ítem basadas en el comportamiento del usuario

Ítem	Descripción	Observaciones
login_attempts	Número de inicios de sesión	Los usuarios típicos tienen entre 1 y 3 intentos de inicio de sesión
session_duration	Duración de la sesión	En segundos
failed_logins	Intentos de inicio de sesión fallidos	Número
unusual_time_access	Anomalía en el tiempo de inicio de sesión	0 o 1 que indica si el acceso ocurrió en un momento inusual
ip_reputation_score	Confiabledad de la dirección IP	0 a 1 , donde los valores más altos indican actividad sospechosa
browser_type	Navegador del usuario	Chrome, Firefox, Edge, Safari

La data cuenta con 9537 registros, resumidos y una variable objetivo o respuesta y 11 variables independientes organizadas en dos subconjuntos: comportamiento del usuario y características de la red.

B. Tratamiento de los datos

Antes de realizar un entrenamiento con el modelo XGBoost, se llevó a cabo un proceso de preparación de los datos, con el objetivo de garantizar la calidad de la información, desbalanceando las clases de detección de intrusiones. En primer lugar, se realizó una limpieza básica de los datos, eliminando registros incompletos o inconsistentes y validando los tipos de datos esperados.

Después, las variables categóricas fueron transformadas mediante codificación one-hot o label encoding según su naturaleza. Asimismo, se aplicó una normalización o estandarización de las características numéricas para optimizar el desempeño del modelo y evitar que ciertas variables dominen el aprendizaje por sus escalas. Posteriormente, se identificó un desbalance significativo entre las clases (ataques vs. tráfico normal), implementando dos enfoques de sobremuestreo: RandomOverSampler (Vieira; Lemaitre; Leng, et al; Abdulsadig, & Rodriguez, 2024), y BorderlineSMOTE, con el fin de comparar su impacto en el rendimiento del modelo XGBoost. Cada técnica de sobre muestreo fue aplicada exclusivamente sobre los datos de entrenamiento, posterior a la partición entre conjunto de entrenamiento y prueba, con el fin de evitar el sobreajuste y asegurar una evaluación imparcial. Finalmente, los conjuntos balanceados resultantes se utilizaron para entrenar instancias separadas del modelo XGBoost, cuyos desempeños fueron comparados utilizando métricas sensibles al desbalance como precisión, recall, F1-score y AUC-ROC.

C. Escenario de validación del modelo

La partición de los datos se realizó en un conjunto de entrenamiento con 6,675 instancias (3,691 clase 0 y 2,984 clase 1) y un conjunto de prueba de 2,862 ins-

tancias (1,582 clase 0 y 1,280 clase 1), que evidencia que existe un desbalance que se corrige aplicando las dos técnicas de sobremuestreo RandomOverSampler y BorderlineSMOTE para posteriormente entrenar los modelos XGBoost sobre ambos conjuntos.

Una vez el modelo está entrenado, se procede con una data diferente proporcionada por una Universidad privada en Colombia que permite rectificar el comportamiento del mejor modelo con la técnica de balance con mejores resultados. Esta data, cuenta con 934 registros de seguimiento a ciberataques con la consolidación de las mismas variables tenidas en cuenta para el entrenamiento inicial del modelo.

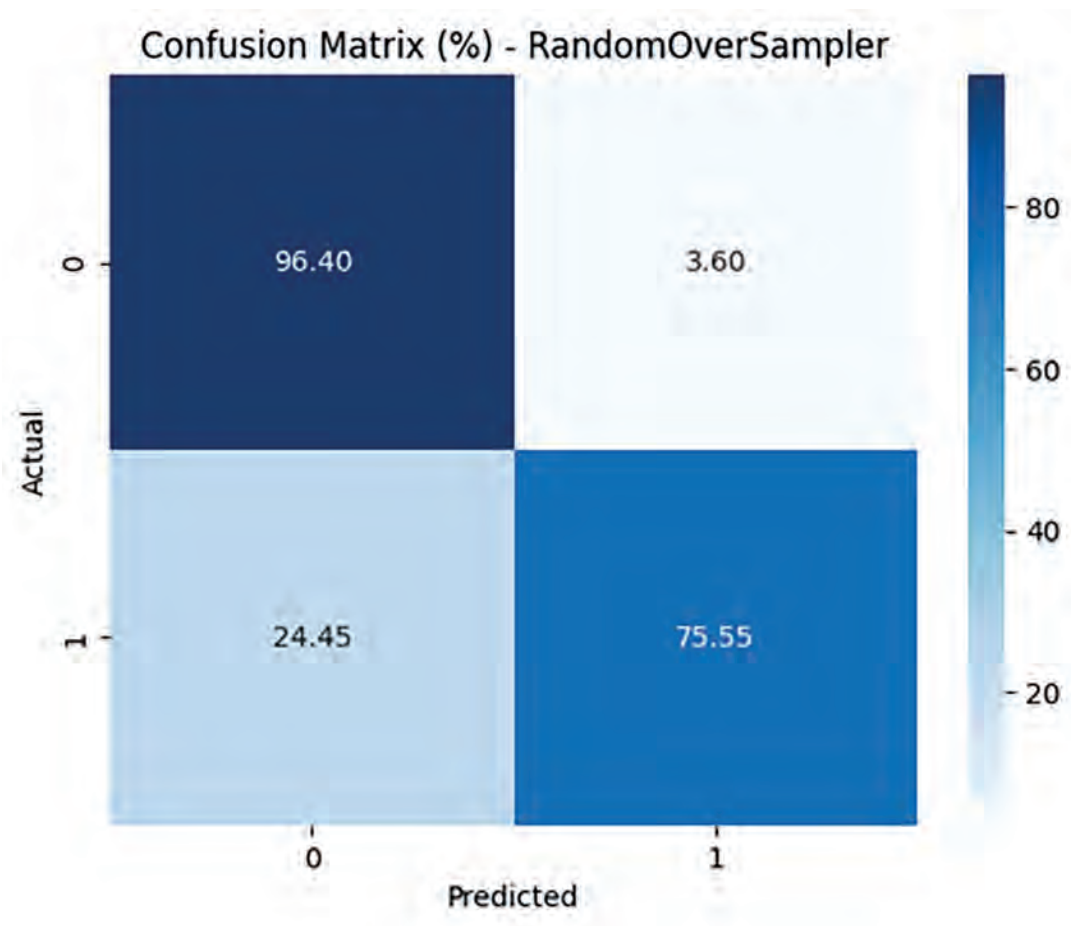
Resultados

A. Resultados de la técnica RandomOverSampler

La matriz de confusión generada con la técnica RandomOverSampler (figura 1) muestra que el modelo tiene un buen desempeño en la clasificación de ambas clases porque un alto porcentaje de los casos sin ataque o normal (0) fueron correctamente clasificados; lo mismo ocurre con los casos positivos o ataques detectados (1), que fueron identificados en su mayoría como positivos. Sin embargo, se puede ver que un porcentaje pequeño de falsos positivos y falsos negativos, indicando que hay ciertos ataques que no fueron detectados y algunas actividades normales fueron clasificadas erróneamente. En general, la técnica permitió un balance adecuado al entrenar, mejorando la sensibilidad sin deteriorar demasiado la precisión.

Figura 1.

Matrix de confusión expresada en % de los resultados del modelo XGBoost aplicando RandomOverSampler



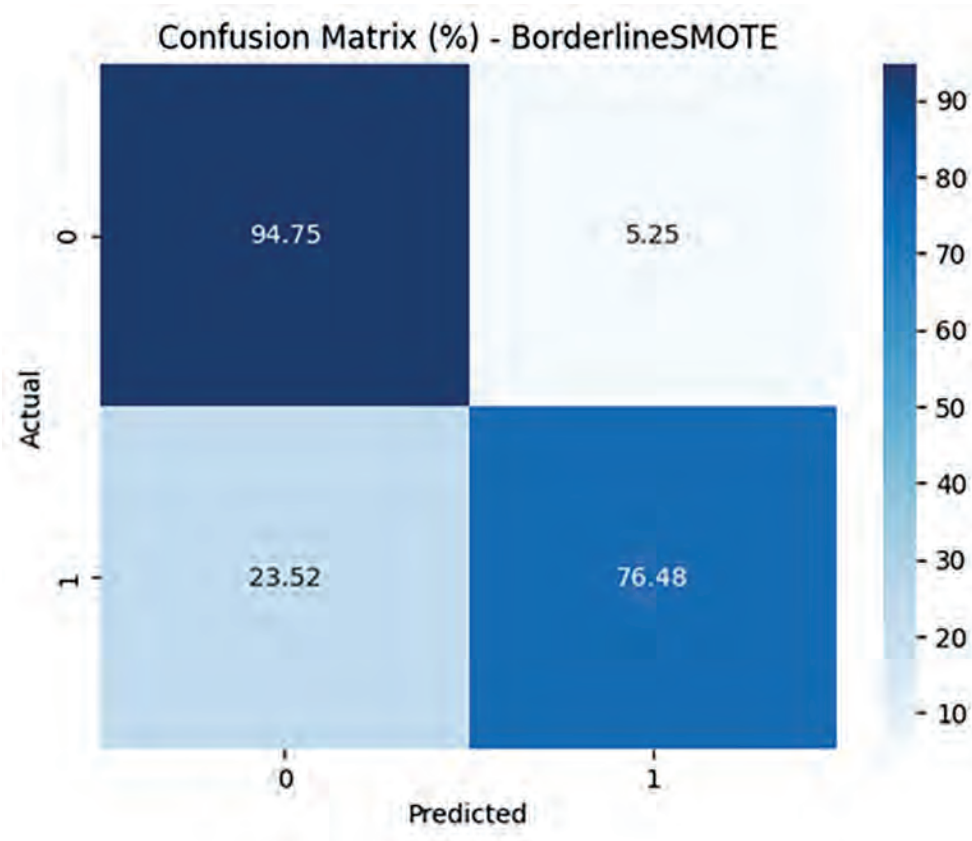
B. Resultados de la técnica BorderlineSMOTE

Al entrenar el modelo con la técnica BorderlineSMOTE (figura 2), la matriz de confusión revela una ligera mejora en la detección de ataques en comparación con RandomOverSampler, especialmente si el porcentaje de verdaderos positivos es mayor. Esto sugiere que esta técnica logra un mejor aprendizaje en los ejemplos cercanos al límite de decisión entre clases, que son los más difíciles de clasificar. Pero, este beneficio puede venir acompañado de

un aumento en los falsos positivos, lo que significa que algunas conexiones normales podrían ser clasificadas incorrectamente como maliciosas; esta técnica puede ser más útil cuando la prioridad es minimizar los falsos negativos, como se busca en este caso para no pasar por alto un ataque, como suele ser crítico en contextos de ciberseguridad.

Figura 1.

Matrix de confusión expresada en % de los resultados del modelo XGBoost aplicando BorderlineSMOTE



C. Comparativo de resultados de entrenamiento y testeo del comportamiento del modelo con las técnicas de balance RandomOverSampler y BorderlineSMOTE

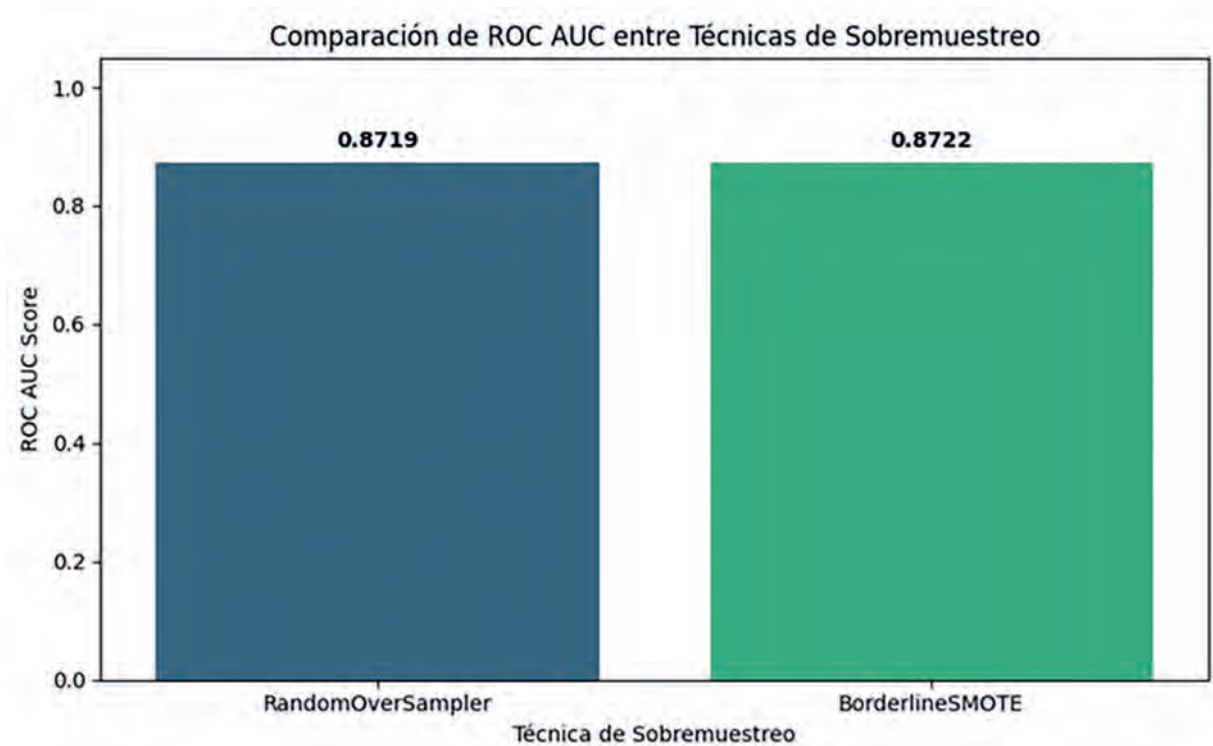
Durante el entrenamiento las dos técnicas permitieron equilibrar las clases mediante la generación de datos sintéticos o duplicación de datos de la clase minoritaria, respectivamente; sin embargo, la forma en que lo hicieron afectó el rendimiento del modelo de manera distinta en la fase de prueba (figura 3). Por ejemplo, con RandomOverSampler, el modelo mostró un comportamiento estable y equilibrado. mostrando en la matriz de confusión una

buena capacidad para identificar tanto eventos normales como ataques, aunque con una leve presencia de falsos positivos y falsos negativos. El valor del ROC AUC fue satisfactorio (ROC AUC Score: 0.8719), reflejando una buena discriminación entre clases.

Por otro lado, con la técnica BorderlineSMOTE, el modelo alcanzó un rendimiento ligeramente superior en cuanto a la detección de ataques porque tuvo un mayor porcentaje de verdaderos positivos en la matriz de confusión y un ROC AUC más alto (ROC AUC Score: 0.8722), lo que sugiere una mejor capacidad del modelo para aprender patrones en las zonas más conflictivas entre clases.

Figura 3.

Comparativo de los resultados del modelo XGBoost utilizando técnicas de balanceo



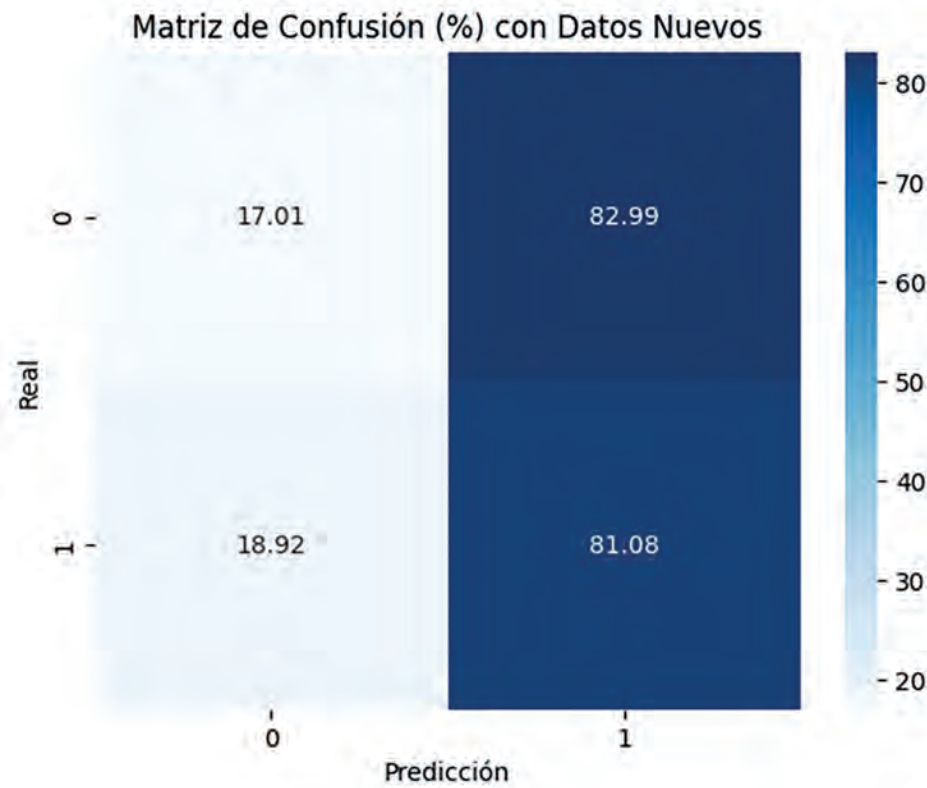
D. Aplicación en contexto con data de validación del comportamiento

Validar un modelo con datos distintos a los utilizados durante su entrenamiento y testeo es fundamental para garantizar su capacidad de generalización y su desempeño en escenarios reales, que en este caso es una data obtenida por el equipo de tecnologías de la información en una Universidad privada en Colombia. En contextos como la ciberseguridad los patrones de comportamiento cambian constantemente y por eso evaluar el modelo con datos nuevos permite evidenciar su comportamiento ante situaciones no vistas, asegurando una detección más robusta y confiable.

La figura 4 muestra la matriz de confusión obtenida en el proceso de validación del modelo con una nueva data, la cual permite ver que el modelo tiene un buen rendimiento y que su comportamiento es bueno para predecir ataques en contexto de ciberseguridad.

Figura 4.

Matriz de confusión con datos nuevos caso Universidad privada de Colombia del modelo entrenado XGBoost con BorderlineSMOTE



Discusión

Los resultados del estudio permiten comprender cómo los esquemas de balanceo y los algoritmos de aprendizaje automático pueden mejorar la detección de intrusiones en redes universitarias, sin embargo, su importancia radica menos en los valores numéricos obtenidos y más en lo que esto significa para el entendimiento de los patrones de ataque. Partiendo de lo anterior, el comportamiento observado confirma que la identificación de amenazas depende particularmente de la capacidad de los modelos para aprender señales débiles o poco frecuentes, lo cual coincide con lo argumentado por Vargas et al. (2018), quienes destacan que la frontera entre tráfico legítimo y malicioso suele ser difusa y alta-

mente no lineal; el desempeño diferencial entre técnicas de sobremuestreo también sugiere que el tipo de ruido o complejidad presente en los datos influye directamente en la sensibilidad del modelo ante actividades anómalas.

Estos resultados se alinean con las tendencias actuales que definen a la inteligencia artificial como un componente central en la ciberseguridad moderna, especialmente en entornos dinámicos como redes SDN o campus universitarios. Investigaciones como las de Cando y Mendoza (2022) o Quintero y Suescún (2018) resaltan que los sistemas tradicionales basados en firmas ya no son suficientes ante amenazas emergentes, mientras que los modelos

de aprendizaje automático permiten una adaptación continua frente a cambios en el comportamiento del usuario y del atacante.

Además, la relevancia de las variables asociadas al uso y acceso de la red coincide con lo señalado por González-Ramírez y Camacho-Nieto (2021), quienes afirman que el comportamiento humano sigue siendo un punto crítico de vulnerabilidad en la seguridad informática. También, se debe resaltar que, a pesar de la fortaleza metodológica del estudio, existen limitaciones que deben considerarse como, los datos utilizados los cuales provienen de un entorno institucional específico, por lo que la capacidad de generalización puede verse afectada en contextos con arquitecturas, cargas de tráfico o niveles de madurez en seguridad diferentes.

De igual manera, aunque las técnicas de balanceo permiten mejorar la sensibilidad del modelo, estas también pueden introducir patrones artificiales que no necesariamente representan comportamientos reales, lo que requiere validaciones adicionales con tráfico en vivo o con conjuntos de datos más amplios. Por otro lado, los modelos supervisados dependen de etiquetas confiables, de modo que posibles errores o inconsistencias en el proceso de etiquetado podrían afectar el aprendizaje del sistema.

Las implicaciones prácticas de este estudio son significativas ya que la evidencia sugiere que las instituciones educativas y organizaciones con infraestructuras similares pueden beneficiarse de la integración de modelos de IA para la detección temprana de amenazas, fortaleciendo la resiliencia operacional y reduciendo riesgos asociados al uso cotidiano de la red. Además, la adopción de este tipo de tecnologías puede complementar los esquemas de seguridad existentes y servir como base para sistemas más avanzados que integren moni-

toreo continuo, análisis en tiempo real y arquitectura Zero Trust.

A nivel académico y de investigación, este estudio abre la puerta a explorar enfoques híbridos, modelos no supervisados y técnicas que integren información contextual o análisis de flujos cifrados, ampliando el horizonte de soluciones para la protección de redes en entornos educativos.

■ Conclusiones

Los resultados obtenidos permitieron dar cumplimiento a los objetivos planteados en la investigación, al demostrar que los modelos basados en aprendizaje automático, particularmente XGBoost, constituyen una herramienta efectiva para la detección de intrusiones en redes universitarias cuando se combinan con técnicas adecuadas de tratamiento del desbalance de clases; además, este enfoque permitió responder a la pregunta de investigación acerca de si la inteligencia artificial podía mejorar la identificación temprana de comportamientos anómalos frente a los métodos tradicionales de seguridad: la evidencia empírica confirmó que sí, en tanto el desempeño del modelo superó los supuestos iniciales respecto a la capacidad de clasificar eventos de riesgo poco frecuentes; con los anterior, se valida la hipótesis de que las técnicas de machine learning no solo aumentan la precisión, sino que también mejoran la sensibilidad frente a amenazas emergentes.

En contraste con las hipótesis iniciales, se observó que el rendimiento del modelo depende en gran medida de la calidad y diversidad de los datos, así como del método utilizado para equilibrar las clases. La comparación entre diferentes técnicas de sobremuestreo evidenció que la generación sintética de datos en zonas críticas de decisión contribuye a identificar ataques con mayor fiabilidad que los métodos bási-

cos de balanceo; estos hallazgos, aportan una comprensión más profunda sobre los factores que influyen en la robustez de los modelos predictivos y su potencial aplicación en entornos con patrones de tráfico variables o con conductas de usuario heterogéneas.

También se puede concluir que el uso de algoritmos de aprendizaje automático constituye una alternativa viable y eficaz para el fortalecimiento de la seguridad informática en instituciones educativas. Además, la validación externa realizada con datos reales confirma la aplicabilidad del modelo en escenarios operativos, lo que amplía su potencial de implementación; de igual manera, los resultados aportan evidencia significativa de que la inteligencia artificial puede desempeñar un rol central en la detección proactiva de amenazas, siempre que se acompañe de procesos adecuados de tratamiento de datos, validación continua y análisis contextual. Esta investigación sienta bases claras para el desarrollo de sistemas de seguridad integrados con capacidades de aprendizaje adaptativo, los cuales pueden convertirse en un soporte esencial para arquitecturas modernas de seguridad.

■ Referencias

- Abdulsadig, R. S., & Rodriguez-Villegas, E. (2024). A comparative study in class imbalance mitigation when working with physiological signals. *Frontiers in Digital Health*, 6, Article 1377165. <https://www.frontiersin.org/articles/10.3389/fdgth.2024.1377165/full>
- Cando, J. R., & Mendoza, J. C. (2022). *Modelo de detección de intrusiones basado en inteligencia artificial para redes definidas por software (SDN)*. Universidad Técnica de Babahoyo. Disponible en: <https://dspace.utb.edu.ec/handle/49000/15119>
- Estrada Esponda, R. D., Unas-Gomez, J. L., Flórez Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos Ciencia & Tecnología*, 13(3), 98-110. <https://doi.org/10.22335/rlct.v13i3.1446>
- Fernández Díaz, C. R. (2019). La amenaza de las nuevas tecnologías en los negocios: el ciberespionaje empresarial. *Revista de Derecho de la UNED (RDUNED)*, (23), 17–57. <https://doi.org/10.5944/rduned.23.2018.24001>
- González, J. C., & Rodríguez, M. A. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Científica General José María Córdova*, 19(34), 45–62. <https://www.redalyc.org/journal/5177/517769783009/>
- González-Ramírez, J., & Camacho-Nieto, O. (2021). Análisis del comportamiento del usuario como factor de riesgo en ciberseguridad. *Revista de Estudios en Seguridad Informática*, 5(2), 45–58. <https://www.redalyc.org/articulo.oa?id=123456789012>
- Hernández, J. H., & Aguilar, C. J. (2016). Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM. *Ingecuc*, 12(1), 84–94. <https://revistascientificas.cuc.edu.co/ingecuc/article/view/225>
- Kumar, D. (2025). Cybersecurity intrusion detection dataset. Kaggle. <https://www.kaggle.com/datasets/dnkumars/cybersecurity-intrusion-detection-dataset>
- Lemaitre, L., et al. (2024). RandomOverSampler. En imbalanced-learn 0.11.0 documentation. https://imbalanced-learn.org/stable/references/generated/imblearn.over_sampling.RandomOverSampler.html

- Leng, Q., Guo, J., Tao, J., Meng, X., & Wang, C. (2024). OBMI: Oversampling borderline minority instances by a two-stage Tomek link-finding procedure for class imbalance problem. *Complex & Intelligent Systems*, 10, 4775–4792. <https://doi.org/10.1007/s40747-024-01399-y>
- Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo Villadiego, L. (2020). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia*, 24(2), 528–541. <https://doi.org/10.37960/revista.v24i2.31508>
- Pacheco, D. S. (2024). Seguridad en redes de comunicaciones: Perspectivas y desafíos. *Ingeniare. Revista Chilena de Ingeniería*, 30(2). <https://ingeniare.uta.cl/index.php/inge/article/view/745>
- Perdigón Llanes, R., & Orellana García, A. (2021). Sistemas para la detección de intrusiones en redes de datos de instituciones de salud. *Revista Cubana de Informática Médica*, 13(2), e440. https://scielo.sld.cu/scielo.php?pid=S1684-18592021000200013&script=sci_arttext
- Pérez-Caballero, V., García-Ruiz, M. Á., & López-Muñoz, R. (2020). Riesgos de seguridad informática y su impacto en las organizaciones. *Revista Española de Seguridad Informática*, 15(1), 17–32. <https://www.redalyc.org/articulo.oa?id=234567890123>
- Rojas Puentes, M. D. P., Parada, C. J., & Leal Pabón, J. L. (2022). Estructuras desglosadas de trabajo (EDT) en la gestión de alcance de proyectos de desarrollo de software. *Revista Colombiana de Tecnologías De Avanzada (RCTA)*, 1(39), 51–58. <https://doi.org/10.24054/rcta.v1i39.1375>
- Quintero, J. E., & Suescún, Á. (2018). Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. *Revista Colombiana de Computación*, 19(1), 29–48. <https://www.redalyc.org/articulo.oa?id=378368201003>
- Rivero, J. L., & Rodríguez, R. (2014). Técnicas de aprendizaje automático para la detección de intrusos en redes de computadoras. *Revista Cubana de Ciencias Informáticas*, 8(4), 42–58. https://www.scielo.sld.cu/scielo.php?pid=S2227-18992014000400003&script=sci_arttext
- Sandoval Carrero, N. S., Acevedo Quintana, N. M., & Santos Jaimes, L. M. (2022). Lineamientos desde la industria 4.0 a la educación 4.0: caso tecnología IoT. *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*, 1(39), 81–92. <https://doi.org/10.24054/rcta.v1i39.1379>
- Vargas, J. A., Quintero, J. E., & Suescún, Á. (2018). Detección de anomalías basada en aprendizaje profundo: Revisión. *Revista Colombiana de Computación*, 19(2), 32–49. <https://www.redalyc.org/articulo.oa?id=378365913008>
- Pérez Pinzón, L. R. (2020). Teaching improvement from online learning (E-Learning). Conceptions and challenges before the pandemic situation. *Colombian Journal of Advanced Technologies*, 3(2), 113–121. <https://doi.org/10.24054/rcta.v3iEspecial.875>
- Vieira, S., & Rodrigues, D. (2024). A comparative study of oversampling techniques for automated binary classification on imbalanced data. *Knowledge and Information Systems*, 66(5), 1045–1072. <https://link.springer.com/article/10.1007/s10115-023-02046-7>