

**FACTIBILIDAD DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL PARA
IDENTIFICAR VULNERABILIDADES EN REDES INALÁMBRICAS
FEASIBILITY OF ARTIFICIAL INTELLIGENCE TOOLS FOR IDENTIFYING
VULNERABILITIES IN WIRELESS NETWORKS**

Autores: ¹Walter Javier Maldonado De La Cruz, ²Carlos Alberto Chacón Terán.

¹ORCID ID: <https://orcid.org/0000-0002-4725-0870>

²ORCID ID: <https://orcid.org/0009-0003-3939-9725>

¹E-mail de contacto: wmaldonado@euroamericano.edu.ec

²E-mail de contacto: cchacon@euroamericano.edu.ec

Afiliación: ^{1*2}Instituto Superior Tecnológico EuroAmericano, (Ecuador).

Artículo recibido: 8 de Septiembre del 2026.

Artículo revisado: 15 de Septiembre del 2026.

Artículo aprobado: 15 de Septiembre del 2026.

¹Ingeniero en Sistemas Computacionales, graduado de la Universidad de Guayaquil, (Ecuador). Magíster en Gerencia Educativa, graduado de la Universidad Metropolitana, (Ecuador). Vicerrector Académico, docente e investigador del Instituto Superior Tecnológico Universitario EuroAmericano, con más de 20 años de experiencia.

²Ingeniero en Sistemas Computacionales, graduado de la Universidad de Guayaquil, (Ecuador). Máster Universitario en Diseño y Gestión de Proyectos Tecnológicos, graduado de la Universidad Internacional de La Rioja, (España). Docente investigador del Instituto Superior Tecnológico Universitario EuroAmericano, con 9 años de experiencia laboral.

Resumen

La creciente dependencia de redes inalámbricas en instituciones educativas ha incrementado la exposición a vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de la información. La inteligencia artificial (IA) ofrece oportunidades para fortalecer la ciberseguridad mediante la detección temprana de amenazas y el análisis automatizado de tráfico. Este estudio evaluó la factibilidad técnica e institucional de implementar herramientas basadas en IA para identificar vulnerabilidades en la red inalámbrica del Instituto Superior Tecnológico Universitario EuroAmericano. Se aplicó un enfoque mixto con diseño no experimental de corte transversal: se encuestó a 45 docentes y se entrevistó a 5 informantes clave vinculados con la gestión tecnológica y administrativa. Los resultados revelan una percepción altamente favorable ($\geq 86\%$ de acuerdo) respecto al potencial de la IA para mejorar el monitoreo, el análisis de tráfico y la detección de anomalías. Sin embargo, se identificaron brechas significativas en infraestructura tecnológica, capacitación especializada y asignación presupuestaria que limitan la adopción inmediata. Se concluye que, aunque existe disposición institucional, se requiere una inversión estratégica en actualización tecnológica y formación para materializar los

beneficios de la IA en la seguridad de la red inalámbrica. El estudio aporta un diagnóstico preliminar y criterios para futuras implementaciones en contextos educativos similares.

Palabras clave: Inteligencia artificial, Ciberseguridad, Redes inalámbricas, Vulnerabilidades, Amenazas cibernéticas.

Abstract

The increasing reliance on wireless networks in educational institutions has heightened exposure to vulnerabilities that compromise the confidentiality, integrity, and availability of information. Artificial intelligence (AI) offers opportunities to strengthen cybersecurity through early threat detection and automated traffic analysis. This study evaluated the technical and institutional feasibility of implementing AI-based tools to identify vulnerabilities in the wireless network of the Instituto Superior Tecnológico Universitario EuroAmericano. A mixed-methods approach with a non-experimental cross-sectional design was applied: 45 faculty members were surveyed and 5 key informants related to technology and administrative management were interviewed. Results reveal a highly favorable perception ($\geq 86\%$ agreement) regarding AI's potential to enhance monitoring, traffic analysis, and anomaly detection.

However, significant gaps in technological infrastructure, specialized training, and budget allocation were identified that limit immediate adoption. It is concluded that, although institutional willingness exists, strategic investment in technological upgrading and training is required to realize AI's benefits in wireless network security. This study provides a preliminary diagnosis and criteria for future implementations in similar educational contexts.

Keywords: Artificial intelligence, Cybersecurity, Wireless networks, Vulnerabilities, Cyber threats.

Sumário

A crescente dependência de redes sem fio em instituições educativas tem aumentado a exposição a vulnerabilidades que comprometem a confidencialidade, a integridade e a disponibilidade da informação. A inteligência artificial (IA) oferece oportunidades para fortalecer a cibersegurança por meio da detecção precoce de ameaças e da análise automatizada de tráfego. Este estudo avaliou a viabilidade técnica e institucional de implementar ferramentas baseadas em IA para identificar vulnerabilidades na rede sem fio do Instituto Superior Tecnológico Universitario EuroAmericano. Aplicou-se uma abordagem mista com desenho não experimental de corte transversal: pesquisaram-se 45 docentes e entrevistaram-se 5 informantes-chave vinculados à gestão tecnológica e administrativa. Os resultados revelam uma percepção altamente favorável ($\geq 86\%$ de concordância) quanto ao potencial da IA para melhorar o monitoramento, a análise de tráfego e a detecção de anomalias. No entanto, identificaram-se lacunas significativas em infraestrutura tecnológica, capacitação especializada e alocação orçamentária que limitam a adoção imediata. Conclui-se que, embora exista disposição institucional, é necessário um investimento estratégico em atualização tecnológica e formação para materializar os benefícios da IA na segurança da rede sem fio. O estudo contribui com um diagnóstico preliminar e critérios para futuras

implementações em contextos educativos semelhantes.

Palavras-chave: Inteligência artificial, Cibersegurança, Redes sem fio, Vulnerabilidades, Ameaças cibernéticas.

Introducción

La digitalización de la educación superior ha incrementado de manera significativa la dependencia de las instituciones respecto de las infraestructuras tecnológicas y de conectividad. Las redes inalámbricas constituyen actualmente un recurso fundamental para las actividades académicas, administrativas y de investigación, debido a que permiten el acceso permanente de estudiantes, docentes y personal institucional a plataformas educativas, sistemas de información, repositorios, servicios en la nube y aplicaciones institucionales. No obstante, esta expansión de la conectividad también incrementa la exposición frente a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

A diferencia de las redes cableadas, las redes inalámbricas transmiten información mediante un medio abierto, lo que amplía las posibilidades de interceptación, accesos no autorizados, ataques de suplantación y explotación de configuraciones deficientes. La seguridad de una WLAN depende no solamente del protocolo de cifrado utilizado, sino también de la configuración de los puntos de acceso, los mecanismos de autenticación, los dispositivos conectados, la segmentación de la red y el monitoreo permanente de su funcionamiento. En este sentido, el National Institute of Standards and Technology establece que la protección de las redes inalámbricas debe contemplarse durante todo su ciclo de vida, desde su diseño y configuración hasta su mantenimiento, evaluación y supervisión continua (Souppaya y Scarfone, 2012). La existencia de una infraestructura inalámbrica no

garantiza, por sí sola, condiciones adecuadas de seguridad. Las configuraciones débiles, las contraseñas vulnerables, la utilización de mecanismos de autenticación insuficientes y la ausencia de procedimientos periódicos de evaluación pueden facilitar el acceso no autorizado. Arteaga et al. (2024) al realizar pruebas sobre diez redes Wi-Fi, reportaron que siete de los ataques ejecutados fueron exitosos en menos de cinco minutos y que una parte importante de las redes examinadas presentaba configuraciones de seguridad inadecuadas. Estos resultados ponen de manifiesto que las debilidades asociadas a la configuración y a las prácticas de seguridad pueden aumentar considerablemente la exposición de las redes inalámbricas frente a posibles amenazas.

Las vulnerabilidades más frecuentes en las redes institucionales pueden relacionarse con configuraciones débiles de autenticación, protocolos de seguridad insuficientes, servicios innecesariamente expuestos, ausencia de segmentación y deficiencias en los mecanismos de supervisión. Jinez y Rochina (2024) analizaron una red universitaria y determinaron un nivel de seguridad medio, identificando debilidades relevantes en las contraseñas utilizadas para la autenticación. González (2024), por su parte, sostiene que la evaluación sistemática de las infraestructuras tecnológicas facilita la identificación de fallos relacionados con el cifrado, la segmentación y la configuración de dispositivos, elementos indispensables para prevenir incidentes y reducir la superficie de ataque.

El contexto ecuatoriano confirma la necesidad de fortalecer estos mecanismos. Cajamarca et al. (2023) al evaluar la seguridad informática en instituciones de educación superior del Ecuador, identificaron deficiencias relacionadas con la adopción de políticas,

controles y marcos referenciales de seguridad, señalando que la ausencia de mecanismos institucionales suficientemente estructurados puede incrementar el impacto de posibles incidentes. De manera similar, Derenzin-Martinez (2024) advierte que las instituciones de educación superior ecuatorianas se encuentran expuestas a diferentes formas de ciberataques y plantea la necesidad de fortalecer los mecanismos institucionales de prevención, monitoreo y respuesta.

En este escenario, los métodos tradicionales de evaluación y vigilancia presentan limitaciones cuando deben analizar grandes volúmenes de información generados continuamente por las redes. La revisión manual de registros, las evaluaciones periódicas y los sistemas basados exclusivamente en reglas predefinidas pueden resultar insuficientes para identificar comportamientos nuevos o variaciones sutiles en los patrones de tráfico. Por esta razón, los sistemas de detección de intrusiones se han convertido en un componente relevante de las arquitecturas contemporáneas de ciberseguridad. Kumar y Kumar (2023) señalan que estos sistemas permiten identificar diferentes clases de ataques en redes inalámbricas, aunque su funcionamiento está condicionado por aspectos como la infraestructura disponible, los recursos computacionales y el tipo de mecanismo de detección utilizado.

Ante la evolución y complejidad de las amenazas, la inteligencia artificial y, particularmente, las técnicas de aprendizaje automático han adquirido una creciente relevancia para la identificación de comportamientos anómalos. A diferencia de los mecanismos sustentados únicamente en firmas previamente conocidas, los modelos de aprendizaje automático pueden procesar

conjuntos extensos de datos y establecer patrones que permitan diferenciar comportamientos normales de actividades potencialmente maliciosas. Ali et al. (2024) destacan que los sistemas de detección de intrusiones basados en *machine learning* y *deep learning* ofrecen posibilidades importantes para mejorar la identificación de ataques, especialmente cuando se requiere analizar grandes cantidades de tráfico y reconocer patrones complejos. No obstante, estos sistemas todavía enfrentan desafíos relacionados con los falsos positivos, la calidad de los conjuntos de datos, la detección de nuevas amenazas y la capacidad de generalización de los modelos.

Dentro de estas alternativas se encuentran algoritmos supervisados como árboles de decisión, *Random Forest*, máquinas de vectores de soporte y XGBoost, así como técnicas de aprendizaje profundo y modelos de detección de anomalías. Estos algoritmos pueden utilizar diferentes características del tráfico para clasificar comportamientos, identificar accesos sospechosos y generar alertas ante patrones que se desvían del funcionamiento habitual de la infraestructura. Estudios recientes han mostrado, además, aplicaciones de XGBoost en modelos orientados a la detección de intrusiones en redes inalámbricas, confirmando el interés actual por combinar análisis automatizado y técnicas de aprendizaje automático para fortalecer las capacidades de supervisión (Wu, 2024).

En esta línea, Toasa et al. (2024) destacan que las herramientas basadas en análisis automatizado pueden contribuir a mejorar la identificación de vulnerabilidades y apoyar los procesos de evaluación técnica de redes. De manera complementaria, Sánchez et al. (2026) presentaron un modelo basado en XGBoost para la detección de intrusiones, evidenciando

la capacidad de este tipo de algoritmos para procesar grandes volúmenes de información e identificar patrones potencialmente anómalos. Estas aproximaciones reflejan una transición desde mecanismos predominantemente reactivos hacia esquemas de vigilancia con mayores capacidades de anticipación y apoyo automatizado a la toma de decisiones.

Cari (2023) aplicó analítica de datos para detectar anomalías en la red Wi-Fi de un campus universitario, identificando picos críticos de utilización y comportamientos irregulares. Los resultados permitieron establecer umbrales dinámicos y formular recomendaciones relacionadas con la gestión del ancho de banda y los mecanismos de autenticación. Este tipo de enfoque evidencia que el análisis automatizado del tráfico no solamente puede apoyar la identificación de vulnerabilidades, sino también proporcionar información útil para comprender el comportamiento de la infraestructura y anticipar situaciones que podrían comprometer su rendimiento o seguridad.

Sin embargo, la incorporación de inteligencia artificial en ciberseguridad no puede valorarse exclusivamente a partir del rendimiento de los algoritmos. Su aplicación implica también considerar la infraestructura tecnológica disponible, la calidad y cantidad de los datos, la capacidad de procesamiento, la interoperabilidad con los sistemas existentes, la formación del personal responsable y los mecanismos de supervisión humana. Ambali Parambil et al. (2024), en una revisión centrada en ciberseguridad e inteligencia artificial en educación superior, concluyen que estas tecnologías ofrecen posibilidades para mejorar la detección de amenazas, la autenticación y la protección de la información, pero su implementación requiere atender

simultáneamente aspectos técnicos, éticos, de privacidad, transparencia y robustez. Este planteamiento resulta particularmente importante porque la incorporación de tecnologías inteligentes no elimina la necesidad de los controles tradicionales de seguridad. Por el contrario, la evidencia reciente apunta hacia modelos complementarios en los que la inteligencia artificial amplía las capacidades de identificación y análisis, mientras que los mecanismos convencionales continúan desempeñando funciones esenciales en autenticación, control de acceso, cifrado, segmentación, protección de dispositivos y gestión de incidentes. Por tanto, la utilidad de una herramienta basada en inteligencia artificial depende en gran medida de su integración dentro de una estrategia institucional de ciberseguridad y no de su implementación como una solución aislada.

En las instituciones de educación superior, la dimensión organizacional adquiere especial relevancia debido a que la ciberseguridad implica coordinación entre infraestructura tecnológica, normativas, recursos humanos y procedimientos internos. Mahmood et al. (2024) identificaron entre las estrategias relevantes para fortalecer la ciberseguridad universitaria la actualización de políticas y procedimientos, la incorporación de nuevas soluciones tecnológicas, la capacitación del personal, el establecimiento de alianzas y el monitoreo continuo de las medidas de seguridad. Estos elementos demuestran que la capacidad de respuesta frente a amenazas depende tanto de la tecnología disponible como del aprendizaje y de la capacidad organizacional para utilizarla de manera adecuada. En consecuencia, la factibilidad de incorporar soluciones basadas en inteligencia artificial debe abordarse desde una perspectiva multidimensional. Una solución puede

demostrar elevada precisión en un entorno experimental y, aun así, resultar poco viable para una institución si requiere infraestructura de alto costo, capacidades técnicas inexistentes, grandes volúmenes de datos de entrenamiento o procesos de mantenimiento que exceden los recursos disponibles. Las barreras para la adopción de sistemas de inteligencia artificial aplicados a ciberseguridad pueden incluir la complejidad tecnológica, la insuficiencia de personal especializado, las limitaciones presupuestarias, el respaldo institucional y las exigencias regulatorias, aspectos que deben considerarse al evaluar una posible implementación (Ali & Shah, 2024).

Estas consideraciones adquieren mayor relevancia en instituciones educativas de países en desarrollo, donde la innovación tecnológica puede coexistir con limitaciones en infraestructura, presupuesto, actualización de equipos y disponibilidad de especialistas. La evidencia producida en Ecuador ha identificado precisamente dificultades relacionadas con la disponibilidad de profesionales especializados y con la consolidación de capacidades institucionales en ciberseguridad. Por ello, estudiar una herramienta únicamente desde su desempeño técnico puede generar una visión incompleta; también es necesario valorar si la institución posee condiciones económicas, tecnológicas, humanas y organizacionales para adoptarla de manera sostenible.

El concepto de factibilidad utilizado en este estudio comprende, por tanto, dos dimensiones interrelacionadas. La factibilidad técnica se refiere a la disponibilidad de infraestructura, compatibilidad tecnológica, capacidad de procesamiento, calidad de los datos, herramientas existentes y requerimientos para la implementación y mantenimiento de soluciones basadas en inteligencia artificial. Por su parte,

la factibilidad institucional comprende elementos relacionados con recursos económicos, competencias del personal, políticas de seguridad, disposición hacia la innovación, capacidad de gestión y posibilidades de incorporar nuevas tecnologías dentro de los procedimientos existentes. Esta distinción permite analizar la adopción tecnológica desde una perspectiva más cercana a las condiciones reales de funcionamiento de una institución de educación superior.

En el Instituto Superior Tecnológico Universitario EuroAmericano, el crecimiento de la utilización de la red inalámbrica ha incrementado la importancia de disponer de mecanismos adecuados para supervisar su seguridad. El aumento de dispositivos, usuarios y servicios conectados genera mayores volúmenes de tráfico y, simultáneamente, amplía los puntos que requieren supervisión. La ausencia de un modelo consolidado que integre análisis automatizado del tráfico y mecanismos inteligentes de generación de alertas sugiere que la identificación de vulnerabilidades depende principalmente de procedimientos tradicionales y revisiones periódicas, lo que puede limitar la capacidad institucional para reconocer oportunamente comportamientos anómalos frente a amenazas dinámicas.

En este contexto se identifica un vacío práctico y de investigación relacionado con la diferencia entre la disponibilidad teórica de herramientas basadas en inteligencia artificial y las condiciones reales para implementarlas en instituciones tecnológicas de educación superior. Una parte importante de la literatura se concentra en comparar algoritmos mediante indicadores como precisión, sensibilidad, especificidad, tasa de falsos positivos o tiempo de procesamiento. Aunque estos parámetros son indispensables para conocer el desempeño

técnico de los modelos, resultan insuficientes para determinar si una institución específica dispone de las condiciones necesarias para incorporarlos de manera eficiente, segura y sostenible. Por ello, la presente investigación no se limita a determinar si existen técnicas de inteligencia artificial capaces de identificar vulnerabilidades o anomalías en redes inalámbricas, sino que analiza la correspondencia entre dichas alternativas y las condiciones institucionales del Instituto Superior Tecnológico Universitario EuroAmericano. Esta orientación permite vincular la investigación tecnológica con la toma de decisiones institucional, evitando plantear la adopción de herramientas avanzadas únicamente desde sus capacidades algorítmicas y considerando también sus requerimientos operativos, humanos y económicos.

Ante este escenario, la pregunta de investigación que guía el presente estudio es: ¿cuál es la factibilidad técnica e institucional de implementar herramientas digitales basadas en inteligencia artificial para la identificación de vulnerabilidades en la red inalámbrica del Instituto Superior Tecnológico Universitario EuroAmericano? Para dar respuesta a esta interrogante se plantearon como objetivos describir las herramientas digitales basadas en inteligencia artificial utilizadas para el análisis de seguridad en redes inalámbricas; identificar las principales vulnerabilidades presentes en las redes inalámbricas institucionales; y determinar el grado de factibilidad y disposición institucional para su adopción. De esta manera, la investigación busca generar evidencia que contribuya a orientar la toma de decisiones en materia de inversión tecnológica, fortalecimiento de la infraestructura, capacitación del talento humano y desarrollo progresivo de capacidades institucionales de ciberseguridad.

Materiales y Métodos

El estudio se desarrolló bajo un enfoque mixto de investigación, que combinó estrategias cuantitativas y cualitativas con el propósito de obtener una visión integral del fenómeno analizado. El alcance fue descriptivo, orientado a caracterizar el estado actual de la red inalámbrica institucional y las percepciones sobre la inteligencia artificial, sin establecer relaciones causales entre variables. El diseño fue no experimental de corte transversal, ya que los datos se recolectaron en un único momento sin manipular las variables de estudio.

La población objetivo estuvo conformada por 45 docentes del Instituto Superior Tecnológico Universitario EuroAmericano, quienes utilizan de manera habitual la red inalámbrica para el desarrollo de sus actividades académicas. Se aplicó un muestreo censal que incluyó a la totalidad de este grupo, eliminando el error de selección. Del total de participantes, el 58% fueron hombres y el 42% mujeres, con edades entre 25 y 55 años (media = 38,2; DE = 7,5). Se seleccionaron, además, 5 informantes clave mediante muestreo intencional, con base en su rol estratégico dentro de la gestión tecnológica, administrativa y de redes de la institución.

Para la recolección de información cuantitativa se diseñó un cuestionario estructurado de 10 ítems en escala Likert de cinco puntos (1 = totalmente en desacuerdo; 5 = totalmente de acuerdo). Los ítems evaluaron cuatro dimensiones: percepción sobre la utilidad de la IA en seguridad de redes, identificación de vulnerabilidades, monitoreo y análisis de tráfico, e infraestructura y disposición institucional. Para el componente cualitativo se elaboró una guía de entrevista semiestructurada con categorías predefinidas: herramientas actuales de monitoreo, ventajas percibidas de la IA, recursos necesarios para su

implementación, vulnerabilidades frecuentes en la red y estrategias de mejora. Las encuestas se administraron en formato digital mediante un formulario en línea, garantizando el anonimato de las respuestas. Las entrevistas se realizaron de manera presencial, con una duración promedio de 30 minutos cada una, y fueron registradas en audio con el consentimiento de los participantes para su posterior transcripción y análisis. Las entrevistas se programaron en horarios acordados con los informantes clave y se llevaron a cabo en las instalaciones institucionales.

El análisis de los datos cuantitativos se realizó mediante estadística descriptiva, calculando frecuencias absolutas y relativas para cada ítem del cuestionario. Los datos cualitativos se analizaron mediante análisis temático, siguiendo un proceso de codificación abierta y axial para identificar patrones y categorías emergentes a partir del discurso de los entrevistados. Se aplicó triangulación metodológica para contrastar ambas fuentes de información y fortalecer la validez de los hallazgos. La investigación cumplió con los estándares éticos establecidos para estudios con seres humanos. Se obtuvo el consentimiento informado de todos los participantes, quienes fueron debidamente informados sobre los propósitos del estudio, la naturaleza voluntaria de su participación y su derecho a retirarse en cualquier momento sin consecuencias. Se garantizó la confidencialidad de las respuestas y el anonimato en el tratamiento de los datos. En ningún momento los participantes estuvieron expuestos a riesgos físicos o psicológicos durante el desarrollo de la investigación.

Resultados y Discusión

A continuación, se presentan los hallazgos obtenidos a partir de las encuestas aplicadas a los 45 docentes. El cuestionario, compuesto por

10 ítems en escala Likert, permitió evaluar la percepción docente sobre la inteligencia artificial, la identificación de vulnerabilidades,

el monitoreo de la red y la disposición institucional.

Tabla 1. *Distribución de respuestas al cuestionario sobre percepción docente (N=45).*

Ítem	TD	D	N	DA	TA
1. Mejora del análisis de seguridad mediante herramientas tecnológicas	0%	2,2%	6,7%	44,4%	46,7%
2. Monitoreo automatizado de la red inalámbrica	0%	2,2%	8,9%	48,9%	40,0%
3. Análisis eficiente de grandes volúmenes de tráfico de red	0%	2,2%	11,1%	46,7%	40,0%
4. Detección de anomalías en el comportamiento de la red	0%	2,2%	8,9%	51,1%	37,8%
5. Infraestructura institucional para implementar IA	2,2%	8,9%	17,8%	42,2%	28,9%
6. Vulnerabilidades por configuraciones débiles o accesos no autorizados	0%	2,2%	11,1%	48,9%	37,8%
7. Prevención de incidentes mediante identificación temprana	0%	0%	4,4%	40,0%	55,6%
8. Monitoreo constante para detectar fallas de seguridad	0%	2,2%	6,7%	46,7%	44,4%
9. Protección de la información mediante detección oportuna	0%	0%	4,4%	37,8%	57,8%
10. Disposición institucional para invertir en herramientas de IA	2,2%	6,7%	13,3%	44,4%	33,4%

Fuente: Elaboración propia.

Los resultados evidencian una percepción altamente favorable hacia la incorporación de inteligencia artificial en la seguridad de redes. Los ítems 7 y 9 alcanzaron el mayor nivel de acuerdo, con un 95,6% de los docentes manifestando estar de acuerdo o totalmente de acuerdo en ambos casos: la identificación temprana de vulnerabilidades y su contribución a la protección de la información institucional se valoran como aspectos críticos para la prevención de incidentes. Los ítems 1, 2, 4 y 8 superaron, de manera similar, el 88% de acuerdo, lo que indica que los docentes reconocen el potencial de las herramientas automatizadas para mejorar el monitoreo, el análisis de tráfico y la detección de anomalías. El ítem 6, referido a la existencia de vulnerabilidades por configuraciones débiles o accesos no autorizados, alcanzó un 86,7% de acuerdo, hallazgo particularmente relevante porque evidencia que la comunidad académica es consciente de los riesgos asociados a la infraestructura inalámbrica, un punto de partida favorable para implementar medidas correctivas. En contraste, los ítems 5 y 10

presentaron los niveles de acuerdo más bajos, con 71,1% y 77,8% respectivamente. El ítem 5, relacionado con la infraestructura institucional para incorporar herramientas de IA, mostró un 11,1% de desacuerdo y un 17,8% de indecisos, lo que sugiere que una parte significativa del profesorado no percibe que la institución cuente con las condiciones técnicas óptimas para una adopción inmediata, posiblemente por obsolescencia parcial de equipos, falta de actualización de software especializado y ausencia de políticas claras de inversión.

El ítem 10, sobre la disposición institucional para invertir en IA, acumuló un 8,9% de desacuerdo y un 13,3% de indecisos; aunque la mayoría respalda la inversión, un grupo no menor de docentes cautelosos refleja la necesidad de fortalecer la comunicación institucional sobre los planes de modernización. El análisis conjunto revela una tensión productiva entre dos fuerzas. Por un lado, emerge una percepción ampliamente favorable hacia la IA, respaldada por el reconocimiento de su utilidad para el monitoreo, el análisis de tráfico y la detección de anomalías,

acompañada de conciencia generalizada sobre las vulnerabilidades existentes. Por otro, este entusiasmo conceptual encuentra un contrapeso en las dudas sobre las condiciones reales para la implementación, reflejando una evaluación realista de las limitaciones técnicas y presupuestarias. La institución se encuentra así en un punto de inflexión: la aceptación generalizada de la IA coexiste con la percepción

de brechas estructurales, lo que desafía a las autoridades a traducir el respaldo conceptual en acciones tangibles. Las entrevistas a los 5 informantes clave (E1-E5) permitieron profundizar en aspectos técnicos y organizacionales que complementan la información cuantitativa, organizados en las categorías temáticas de la Tabla 2.

Tabla 2. Síntesis de la categorización cualitativa.

Categoría	Cita representativa	Interpretación
Herramientas actuales	"Utilizamos los logs de los controladores, pero todo requiere revisión manual" (E1)	Dependencia de procesos manuales, limitada para entornos complejos
Ventajas percibidas de la IA	"Lo más valioso sería anticiparnos, encontrar algo raro antes de que se convierta en un incidente grave" (E1)	Consenso en el valor preventivo y la necesidad de automatización
Eficiencia operativa	"Muchas veces las alertas son falsas y perdemos tiempo; con IA eso podría mejorar" (E5)	La IA optimiza la precisión y agiliza la reacción ante incidentes
Recursos necesarios	"No se puede pensar en IA si los equipos no están actualizados" (E2)	Modernización tecnológica y formación especializada son requisitos indispensables
Asignación presupuestaria	"Sin un presupuesto asignado, cualquier iniciativa queda en el aire" (E1)	La disponibilidad de recursos financieros condiciona la viabilidad
Vulnerabilidades frecuentes	"Seguimos viendo contraseñas como '123456' o nombres de usuarios" (E3)	Persisten debilidades de credenciales inseguras y configuraciones incorrectas
Obsolescencia y monitoreo	"Hay equipos viejos que ya no reciben actualizaciones"; "el monitoreo no es 24/7" (E4, E2)	La obsolescencia y la ausencia de supervisión continua incrementan los riesgos
Estrategias de mejora	"Si el sistema nos avisa automáticamente cuando algo está fuera de lo normal, podemos actuar rápido" (E3)	Consenso sobre la necesidad de supervisión permanente y alertas automatizadas

Fuente: Elaboración propia.

Los informantes coinciden en que las herramientas actuales dependen de la revisión manual de registros, un método que se vuelve impracticable cuando el volumen de tráfico aumenta. Todos valoran el potencial preventivo de la IA para anticipar incidentes y reducir falsas alertas, pero condicionan su implementación a la modernización de equipos, la capacitación especializada y la asignación de un presupuesto específico. En cuanto a

vulnerabilidades, señalan de forma recurrente contraseñas débiles, configuraciones incorrectas y equipos sin actualizaciones, agravados por la ausencia de monitoreo continuo las 24 horas. La Tabla 3 sintetiza la relación entre los hallazgos cuantitativos y cualitativos en las principales dimensiones analizadas.

Tabla 3. Triangulación de hallazgos.

Dimensión	Docentes (encuesta)	Informantes (entrevistas)	Relación
Potencial de la IA	≥88% de acuerdo en monitoreo, análisis de tráfico y detección de anomalías	Detección temprana de amenazas y optimización de tiempos de respuesta	Convergencia
Vulnerabilidades existentes	86,7% reconoce configuraciones débiles y accesos no autorizados	Contraseñas frágiles, equipos desactualizados, monitoreo no continuo	Convergencia
Condiciones para implementar	71,1% de acuerdo en infraestructura; mayor neutralidad y desacuerdo del estudio	Obsolescencia de equipos, falta de capacitación, insuficiencia presupuestaria	Discrepancia
Disposición institucional	77,8% de acuerdo en invertir en IA	Necesidad reconocida, pero condicionada a presupuesto asignado	Matización
Estrategias de mejora	No indagado directamente en la encuesta	Monitoreo continuo, alertas automáticas, segmentación de red	Aporte exclusivo cualitativo

Fuente: Elaboración propia.

Existe una convergencia clara entre la percepción docente y la visión de los informantes clave respecto al potencial de la IA para fortalecer la seguridad de la red: las encuestas reflejan una aceptación mayoritaria hacia su capacidad de mejorar el monitoreo, y las entrevistas profundizan en ventajas específicas como la detección temprana de amenazas. Ambos componentes coinciden, además, en señalar la existencia de vulnerabilidades significativas, lo que refuerza la idea de que las debilidades identificadas no son producto de percepciones subjetivas, sino de una realidad institucional compartida por distintos actores.

La triangulación evidencia, sin embargo, una discrepancia entre la aceptación conceptual de la IA y la percepción sobre las condiciones reales para su implementación: mientras las encuestas muestran un apoyo mayoritario, los informantes clave identifican barreras estructurales concretas. Esta tensión revela que el entusiasmo hacia la IA no se acompaña necesariamente de una evaluación realista de los recursos disponibles, lo que podría generar expectativas desajustadas respecto a los plazos de adopción. Finalmente, ambas fuentes convergen en un consenso tácito sobre la necesidad de avanzar hacia un modelo de seguridad más automatizado y preventivo, lo que sugiere un terreno común sobre el cual construir una hoja de ruta realista.

La percepción favorable hacia la inteligencia artificial como herramienta de seguridad coincide con lo señalado por Borrero y Ponce (2023), quienes destacan que los sistemas de detección basados en comportamiento superan a los enfoques tradicionales en entornos dinámicos. Esta coincidencia sugiere que la comunidad académica ha internalizado, al menos de forma intuitiva, las ventajas de la IA

para el monitoreo y la detección de amenazas. La conciencia sobre vulnerabilidades en la red inalámbrica, manifestada por docentes e informantes clave, encuentra respaldo en el trabajo de Sánchez et al. (2026), quienes desarrollaron un modelo basado en XGBoost que demuestra que el análisis de características de la red y prácticas de usuario permite identificar intrusiones con alta precisión. La coincidencia entre esta evidencia técnica y la percepción institucional refuerza la necesidad de implementar soluciones basadas en datos.

Las limitaciones operativas de las herramientas actuales de monitoreo, reportadas por los entrevistados, se alinean con los hallazgos de Gutiérrez y Granda (2025), quienes evidenciaron que la detección temprana en redes empresariales mejora cuando se emplean modelos capaces de reconocer patrones complejos de comportamiento. La brecha entre las capacidades actuales y las necesidades operativas constituye un punto crítico para la modernización de la infraestructura de seguridad.

En el contexto de redes 5G y entornos de alta densidad, Bravo y Zambrano (2024) subrayan que la identificación de vectores de amenaza exige mecanismos adaptativos, planteamiento consistente con las barreras identificadas en el Instituto, donde la obsolescencia de equipos y la falta de monitoreo continuo limitan la capacidad de anticipación. La convergencia entre ambos diagnósticos sugiere que la institución enfrenta desafíos comunes a otras organizaciones educativas. La aplicación de analítica de datos para la detección de anomalías, propuesta por Cari (2023) en el contexto de una universidad, permitió establecer umbrales de alerta dinámicos y recomendaciones para la gestión del ancho de banda. Este enfoque práctico coincide con las

estrategias de mejora sugeridas por los informantes clave, como el monitoreo continuo y las alertas automáticas, aunque su replicabilidad en el Instituto depende de superar las brechas de infraestructura y capacitación identificadas. Chinchay et al. (2022) enfatizan, por último, que el control de acceso mediante protocolos de autenticación robustos es

fundamental para mitigar riesgos, principio que se alinea con la percepción docente sobre la necesidad de fortalecer los mecanismos de autenticación y segmentación. La Tabla 4 sintetiza la relación entre los hallazgos propios y los antecedentes citados a lo largo de esta discusión.

Tabla 4. Vinculación de los hallazgos con la literatura.

Hallazgo propio	Literatura	Relación
Los sistemas basados en comportamiento superan los enfoques tradicionales	Borrero y Ponce (2023)	Converge
Modelos supervisados detectan intrusiones con alta precisión	Sánchez et al. (2026)	Converge
La detección temprana mejora con reconocimiento de patrones complejos	Gutiérrez y Granda (2025)	Converge
Entornos de alta densidad exigen mecanismos adaptativos	Bravo y Zambrano (2024)	Converge
La analítica de datos habilita umbrales de alerta dinámicos	Cari (2023)	Converge
La autenticación robusta es clave para mitigar riesgos	Chinchay et al. (2022)	Converge

Fuente: Elaboración propia.

La consistencia entre la literatura y los hallazgos empíricos valida el diagnóstico institucional, aunque conviene señalar que el estudio no incorporó deliberadamente posturas críticas sobre los límites de la IA en ciberseguridad institucional, lo que constituye una limitación interpretativa a considerar en futuras investigaciones. El Instituto se encuentra, en definitiva, en una transición hacia un modelo de seguridad más automatizado y preventivo: las percepciones favorables y las propuestas de mejora coinciden con las tendencias documentadas, aunque las barreras estructurales exigen un abordaje gradual y planificado que combine inversión tecnológica, formación continua y una cultura organizacional orientada a la prevención.

Conclusiones

El presente estudio evaluó la factibilidad técnica e institucional de implementar herramientas basadas en inteligencia artificial para la identificación de vulnerabilidades en la red inalámbrica del Instituto Superior Tecnológico Universitario EuroAmericano. A partir del análisis integrado de las percepciones

docentes y la visión de los informantes clave, existe una base favorable para la adopción de estas tecnologías, aunque su materialización efectiva depende de superar barreras estructurales significativas en infraestructura, capacitación y presupuesto.

Los modelos de aprendizaje automático supervisado, como XGBoost, y las técnicas de analítica de datos para detección de anomalías son las aproximaciones más prometedoras y documentadas en la literatura reciente; la comunidad institucional reconoce su valor para el procesamiento automatizado de grandes volúmenes de tráfico y la generación de alertas tempranas, capacidades que superan ampliamente los métodos de monitoreo tradicionales basados en revisión manual de registros. El estudio constató la persistencia de debilidades críticas coincidentes con la literatura para contextos educativos: contraseñas débiles, configuraciones incorrectas en puntos de acceso, obsolescencia de equipos sin actualizaciones de seguridad, y ausencia de segmentación adecuada y de monitoreo continuo, factores que incrementan la superficie de ataque. La conciencia

generalizada sobre estos riesgos, manifestada por docentes e informantes, constituye un activo institucional que facilita la sensibilización y el respaldo a futuras intervenciones.

En cuanto a la factibilidad y disposición institucional, se evidencia una tensión productiva entre dos fuerzas: una disposición altamente favorable, con porcentajes de acuerdo que superan el 86% en la mayoría de las dimensiones evaluadas, y brechas concretas en infraestructura, capacitación especializada y asignación presupuestaria que limitan la factibilidad inmediata. Esta discrepancia entre la aceptación conceptual y las condiciones reales implica que la implementación requiere una planificación progresiva y un acompañamiento institucional sostenido, y no una adopción inmediata.

Se recomienda a las autoridades diseñar una hoja de ruta por fases: una primera etapa centrada en la actualización de la infraestructura de red y la capacitación básica del personal técnico; una segunda etapa de implementación piloto de herramientas de IA en entornos controlados, escalando progresivamente según los resultados; y el establecimiento de políticas claras de ciberseguridad que integren la segmentación de la red y el fortalecimiento de los protocolos de autenticación. Quedan abiertas líneas de investigación futura orientadas a la evaluación comparativa de herramientas específicas de IA aplicadas a redes educativas, estudios longitudinales que midan el impacto real de estas tecnologías en la reducción de incidentes, y la réplica de este diseño metodológico en otras instituciones de educación superior de la región, con el fin de construir un cuerpo de conocimiento más robusto sobre la factibilidad de la IA en contextos con restricciones presupuestarias y tecnológicas similares.

Referencias Bibliográficas

- Ali, A., Charfeddine, M., Ammar, B., Ben Hamed, B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. *Frontiers in Computer Science*, 6, 1387354. <https://doi.org/10.3389/fcomp.2024.1387354>
- Ali, A., & Shah, M. (2024). What hinders adoption of artificial intelligence for cybersecurity in the banking sector. *Information*, 15(12), 760. <https://doi.org/10.3390/info15120760>
- Ambali, M., Rustamov, J., Ahmed, S., Rustamov, Z., Awad, A., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, 7, 100327. <https://doi.org/10.1016/j.caeai.2024.100327>
- Arteaga, H., Obregón, J., & Núñez, F. (2024). Análisis de la seguridad de redes inalámbricas y las posibilidades de explotación mediante herramientas de seguridad informática. *Revista Científica Multidisciplinar G-Nerando*, 5(2), 513. <https://doi.org/10.60100/rcmg.v5i2.284>
- Borrero, J., & Ponce, J. (2023). Impacto en la seguridad de las redes inalámbricas. *Journal TechInnovation*, 2(1), 62–71. <https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.62-71>
- Bravo, Y., & Zambrano, D. (2024). Seguridad y privacidad en las redes 5G: Una revisión sistemática de la literatura. *Revista Científica Multidisciplinar G-Nerando*, 5(2), 116–144. <https://doi.org/10.60100/rcmg.v5i2.259>
- Cajamarca, G., Ron, M., Chamorro, P., & Genovez, C. (2023). Evaluación del nivel de seguridad informática desplegado en las instituciones de educación superior de la red RIT II. *Conectividad*, 4(1), 38–49. <https://doi.org/10.37431/conectividad.v4i1.49>
- Cari, A. (2025). *Aplicación de analítica de datos para la detección de anomalías y fortalecimiento de la seguridad en la red*

- WiFi del campus universitario de la Universidad Nacional del Altiplano* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2601.00798>
- Chinchay, K., Peña, V., Carrión, G., Fuentes, D., Delgado, A., & Yeckle, R. (2022). Control de acceso a redes inalámbricas por medio de protocolos de autenticación de usuarios. *Colloquium*. <https://colloquiumbiblioteca.com/index.php/web/article/view/140>
- Derenzin, F. (2024). ¿Están los institutos universitarios en Ecuador preparados para los ciberataques? *593 Digital Publisher CEIT*, 9(6), 1220–1232. <https://doi.org/10.33386/593dp.2024.6.2864>
- González, R. (2024). *Análisis de seguridad mediante técnicas de ciberseguridad en redes inalámbricas 802.11* [Tesis, Universidad Estatal Península de Santa Elena]. Repositorio Institucional UPSE. <https://repositorio.upse.edu.ec/handle/46000/11843>
- Gutiérrez, A., & Granda, A. (2025). *Desarrollo de detección de amenazas cibernéticas en redes empresariales usando algoritmos supervisados* [Tesis, Universidad Politécnica Salesiana]. Repositorio Institucional de la Universidad Politécnica Salesiana. <http://dspace.ups.edu.ec/handle/123456789/31552>
- Jínez, J., & Rochina, M. (2024). *Análisis y evaluación de la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo* [Tesis, Universidad Nacional de Chimborazo]. Repositorio Digital UNACH. <http://dspace.unach.edu.ec/handle/51000/12979>
- Kumar, Y., & Kumar, V. (2023). A systematic review on intrusion detection system in wireless networks: Variants, attacks, and applications. *Wireless Personal Communications*, 133, 395–452. <https://doi.org/10.1007/s11277-023-10773-x>
- Mahmood, S., Chadhar, M., & Firmin, S. (2024). Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. *Information*, 15(2), 106. <https://doi.org/10.3390/info15020106>
- Sánchez, K., Barrientos, E., & Cordero, M. (2026). 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). <https://doi.org/10.22335/rlct.v18i1.2250>
- Souppaya, M. P., & Scarfone, K. A. (2012). *Guidelines for securing wireless local area networks (WLANs)* (NIST Special Publication 800-153). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-153>
- Toasa, R., Urdaneta, M., & Villacís, B. (2024). *Análisis de vulnerabilidades basado en técnicas de inteligencia artificial para la seguridad informática en redes de área local* [Tesis, Universidad Tecnológica Israel]. Repositorio Institucional de la Universidad Tecnológica Israel. <https://repositorio.uisrael.edu.ec/handle/47000/4140>
- Wu, H. (2024). Intrusion detection model for wireless sensor networks based on FedAvg and XGBoost algorithm. *International Journal of Distributed Sensor Networks*, 2024, 5536615. <https://doi.org/10.1155/2024/5536615>



Esta obra está bajo una licencia de Creative Commons Reconocimiento-No Comercial 4.0 Internacional. Copyright © Walter Javier Maldonado de la Cruz y Carlos Alberto Chacón Terán.

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT) Walter Javier Maldonado de la Cruz: conceptualización de la investigación, formulación del problema y objetivos, revisión bibliográfica, diseño metodológico, coordinación del proceso investigativo, análisis e interpretación de los resultados, redacción del borrador original y supervisión general del estudio. Carlos Alberto Chacón Terán: apoyo en el diseño metodológico y componente tecnológico de la investigación, análisis de requerimientos técnicos, revisión de soluciones basadas en inteligencia artificial y redes de comunicación, organización y análisis de la información, interpretación de resultados, revisión crítica del contenido científico y edición del manuscrito.
Declaración de conflicto de intereses Los autores declaran que no existen conflictos de intereses relacionados con la investigación, la autoría ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales ni de organizaciones sin fines de lucro.
Declaración del editor No aplica en la versión presentada por los autores. Esta declaración corresponde al equipo editorial de la revista una vez concluido el proceso de evaluación y publicación del manuscrito.
Declaración de los revisores No aplica en la versión presentada por los autores. Esta declaración corresponde a la revista una vez finalizado el proceso de revisión por pares.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios de integridad científica, confidencialidad y protección de la información institucional utilizada durante el estudio. La información recopilada fue empleada exclusivamente con fines académicos y científicos. En los casos en que participaron personas en la recopilación de información, su participación fue voluntaria y los datos obtenidos fueron tratados de manera confidencial, garantizando el respeto a los participantes y la protección de su identidad.
Declaración sobre el uso de inteligencia artificial Los autores declaran que las herramientas de inteligencia artificial utilizadas en el contexto de la investigación fueron objeto de análisis como parte del estudio sobre su factibilidad para la identificación de vulnerabilidades en redes inalámbricas. En caso de haberse empleado herramientas de inteligencia artificial como apoyo durante la elaboración del manuscrito, su utilización se limitó a tareas técnicas de organización de información, revisión del lenguaje o mejora de la claridad del texto. La interpretación de los resultados, las decisiones metodológicas y la responsabilidad intelectual sobre el contenido corresponden exclusivamente a los autores.
Disponibilidad de datos Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando los principios de confidencialidad, seguridad de la información y protección de los datos institucionales establecidos durante el estudio.

