Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 1.1
Edición Especial I 2026

ANÁLISIS CUANTITATIVO Y CUALITATIVO DE LA PERTINENCIA DEL PROGRAMA DE MAESTRÍA EN CIBERSEGURIDAD APLICADA A LA INTELIGENCIA ARTIFICIAL EN EL CONTEXTO ECUATORIANO

QUANTITATIVE AND QUALITATIVE ANALYSIS OF THE RELEVANCE OF THE MASTER'S PROGRAM IN CYBERSECURITY APPLIED TO ARTIFICIAL INTELLIGENCE IN THE ECUADORIAN CONTEXT

Autores: [1]Danny Velasco Silva, [2]Fernando Molina Granja, [3]Alejandra del Pilar Pozo Jara y [4]Lidia Castro Cepeda.

[1]ORCID ID: https://orcid.org/0000-0003-0396-4086
[2]ORCID ID: https://orcid.org/0000-0003-2486-894X
[3]ORCID ID: https://orcid.org/0000-0001-9854-8098
[4]ORCID ID: https://orcid.org/0000-0002-0471-2879
[1]E-mail de contacto: dvelasco@unach.edu.ec
[2]E-mail de contacto: fmolina@unach.edu.ec
[3]E-mail de contacto: apozo@unach.edu.ec
[4]E-mail de contacto: lidia.castro@unach.edu.ec
Afiliación: [1*2*3*4*]Universidad Nacional de Chimborazo, (Ecuador).
Articulo recibido: 2 de Enero del 2026
Articulo revisado: 7 de Enero del 2026
Articulo aprobado: 12 de Enero del 2026
[1]Ingeniero en Sistemas graduado de la Escuela Superior Politécnica de Chimborazo, (Ecuador). Magíster en Interconectividad de Redes graduado de la Escuela Superior Politécnica de Chimborazo, (Ecuador).
[2]Maestría en Educación a Distancia. Doctorado en Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, (Perú). Posdoctorado en Ciencias de la Informática con especialidad en Preservación de Evidencias Digitales.
[3]Ingeniero en Sistemas graduado de la Escuela Superior Politécnica de Chimborazo, (Ecuador). Magíster en Interconectividad de Redes graduado de la Escuela Superior Politécnica de Chimborazo, (Ecuador).
[4]Máster Universitario en Ingeniería Matemática y Computación graduada de la Universidad Internacional de La Rioja, (España).

Resumen

El estudio tuvo como propósito analizar la pertinencia académica, social y productiva de la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial en el contexto ecuatoriano, considerando la demanda estudiantil y los requerimientos del sector empleador frente al incremento de amenazas cibernéticas y la adopción de tecnologías basadas en inteligencia artificial. Se aplicó un enfoque mixto, con un diseño descriptivo y analítico. Se emplearon encuestas estructuradas dirigidas a profesionales de áreas afines y a empleadores de sectores estratégicos, complementadas con entrevistas a expertos. El análisis cuantitativo se realizó mediante estadística descriptiva, mientras que la información cualitativa permitió interpretar percepciones, expectativas y necesidades del mercado laboral. Los resultados evidenciaron una alta intención de cursar estudios de posgrado en ciberseguridad, con preferencia por modalidades en línea y enfoques prácticos. Desde el sector empleador, se identificó un alto impacto de los ciberataques y una creciente demanda de profesionales con competencias en programación avanzada, análisis de datos, gestión de riesgos y ciberseguridad con el uso de inteligencia artificial, particularmente en sectores como el financiero, gubernamental y de salud. Asimismo, se detectaron barreras relacionadas con la falta de talento especializado y limitaciones presupuestarias. Se concluyó que la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial presentó una alta pertinencia académica y profesional, al responder a las necesidades reales del entorno productivo y contribuir al fortalecimiento del talento humano especializado en el contexto ecuatoriano.

Palabras clave: Pertinencia académica, Ciberseguridad, Inteligencia artificial.

Abstract

The purpose of this study was to analyze the academic, social, and productive relevance of the Master's Degree in Cybersecurity Applied

to Artificial Intelligence in the Ecuadorian context, considering student demand and employer requirements in the face of increasing cyber threats and the adoption of artificial intelligence-based technologies. A mixed-methods approach was used, with a descriptive and analytical design. Structured surveys were administered to professionals in related fields and employers in strategic sectors, complemented by interviews with experts. Quantitative analysis was performed using descriptive statistics, while qualitative data allowed for the interpretation of perceptions, expectations, and needs of the labor market. The results showed a high intention to pursue postgraduate studies in cybersecurity, with a preference for online modalities and practical approaches. From the employer sector, a high impact of cyberattacks was identified, along with a growing demand for professionals with skills in advanced programming, data analysis, risk management, and cybersecurity using artificial intelligence, particularly in sectors such as finance, government, and healthcare. Furthermore, barriers related to a lack of specialized talent and budgetary limitations were identified. It was concluded that the Master's Program in Cybersecurity Applied to Artificial Intelligence demonstrated high academic and professional relevance, responding to the real needs of the productive environment and contributing to the strengthening of specialized human talent in the Ecuadorian context.

Keywords: Academic relevance, Cybersecurity, Artificial intelligence.

Sumário

O objetivo deste estudo foi analisar a relevância acadêmica, social e produtiva do Mestrado em Cibersegurança Aplicada à Inteligência Artificial no contexto equatoriano, considerando a demanda estudantil e as exigências do mercado de trabalho diante do aumento das ameaças cibernéticas e da adoção de tecnologias baseadas em inteligência artificial. Utilizou-se uma abordagem mista, com delineamento descritivo e analítico. Questionários estruturados foram aplicados a profissionais de áreas afins e a empregadores de setores estratégicos, complementados por entrevistas com especialistas. A análise quantitativa foi realizada por meio de estatística descritiva, enquanto os dados qualitativos permitiram a interpretação das percepções, expectativas e necessidades do mercado de trabalho. Os resultados demonstraram uma alta intenção de cursar pós-graduação em cibersegurança, com preferência por modalidades online e abordagens práticas. Do lado dos empregadores, identificou-se um alto impacto dos ataques cibernéticos, juntamente com uma crescente demanda por profissionais com habilidades em programação avançada, análise de dados, gestão de riscos e cibersegurança utilizando inteligência artificial, particularmente em setores como finanças, governo e saúde. Além disso, foram identificadas barreiras relacionadas à falta de profissionais especializados e às limitações orçamentárias. Concluiu-se que o Programa de Mestrado em Cibersegurança Aplicada à Inteligência Artificial demonstrou alta relevância acadêmica e profissional, respondendo às reais necessidades do ambiente produtivo e contribuindo para o fortalecimento do talento humano especializado no contexto equatoriano.

Palavras-chave: Relevância acadêmica, Cibersegurança, Inteligência artificial.

Introducción

La acelerada transformación digital que experimentan las sociedades contemporáneas ha propiciado una expansión sin precedentes del uso de la inteligencia artificial (IA) en sectores estratégicos como la administración pública, la industria, la salud, las finanzas y las infraestructuras críticas. Si bien la IA ha permitido optimizar procesos, automatizar decisiones y mejorar la eficiencia operativa (**Nicoletti et al., 2024**), su adopción masiva también ha ampliado de manera significativa la superficie de ataque y la complejidad de los riesgos cibernéticos (**Fernández, 2024**). En este contexto, la ciberseguridad emerge no solo

como un componente técnico, sino como un eje estratégico para garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de los sistemas inteligentes. Los ciberataques actuales han evolucionado hacia modelos más sofisticados, persistentes y automatizados, incorporando técnicas avanzadas como aprendizaje automático, suplantación de identidades mediante modelos generativos, ataques dirigidos a modelos de IA y explotación de vulnerabilidades en arquitecturas híbridas que integran datos y servicios en la nube (**Sánchez Díaz, 2024**). Estas amenazas superan las capacidades de los enfoques tradicionales de seguridad, demandando profesionales altamente especializados capaces de diseñar, implementar y gestionar soluciones de ciberseguridad apoyadas en inteligencia artificial, análisis avanzado de datos y automatización defensiva (**Campos, 2025**).

El análisis de la pertinencia de una Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial en el contexto ecuatoriano requiere, por tanto, un enfoque cuantitativo y cualitativo sustentado en experiencias internacionales, modelos curriculares innovadores y evidencias empíricas sobre alineación con el entorno productivo y social. Desde una perspectiva pedagógica, Buríachok y Sokolov (2020) analizan la implementación del aprendizaje activo en programas de maestría en ciberseguridad, demostrando que metodologías basadas en problemas, estudios de caso y simulaciones incrementan significativamente el desarrollo de competencias técnicas y analíticas. Este enfoque resulta relevante para el análisis cualitativo de la pertinencia, ya que evidencia la necesidad de programas de posgrado orientados no solo a la transmisión de conocimientos, sino al fortalecimiento de capacidades prácticas, críticas y de toma de decisiones, competencias esenciales para enfrentar amenazas cibernéticas apoyadas en IA. A nivel académico y formativo, esta realidad plantea un desafío crítico para las instituciones de educación superior: la necesidad de desarrollar programas de posgrado que respondan de manera pertinente, actualizada y prospectiva a las demandas del entorno tecnológico, laboral y normativo, con las mejores prácticas internacionales en la formación de especialistas en ciberseguridad, dado el impulso que cobrará el proceso de transformación y formación de la sociedad mundial de la información (Buríachok y Sokolov, 2020).

Por su parte, de Jager et al. (2026) proponen un enfoque transdisciplinario para integrar la ciberseguridad a lo largo del currículo en programas de computación a nivel internacional. Aunque su estudio se centra en el nivel de pregrado, aporta elementos clave para el diseño de programas de posgrado, al destacar la importancia de articular conocimientos técnicos con aspectos legales, éticos y organizacionales, lo que es pertinente para el contexto ecuatoriano, donde la ciberseguridad vinculada a la IA demanda profesionales capaces de interactuar con marcos normativos, políticas públicas y necesidades institucionales, reforzando así la dimensión cualitativa de la pertinencia académica y social (Dávila, 2023). En el ámbito de la alineación con el mercado laboral, Ekqvist et al. (2025) examinan la educación en ciberseguridad en universidades de ciencias aplicadas, destacando la correspondencia entre la formación académica y las necesidades del sector productivo. Mediante indicadores cuantitativos de empleabilidad y competencias requeridas, los autores evidencian que los programas exitosos son aquellos que se construyen a partir de diagnósticos del entorno laboral, lo que resulta clave para el análisis cuantitativo de la

pertinencia del programa propuesto en Ecuador, donde la demanda de especialistas en ciberseguridad e IA en sectores como gobierno electrónico, banca, telecomunicaciones y servicios críticos es creciente (Lucio, 2024). En particular, la formación avanzada en ciberseguridad aplicada a la inteligencia artificial se posiciona como un campo emergente de alto valor estratégico, al integrar conocimientos de seguridad informática, ciencia de datos, aprendizaje automático, gestión de riesgos, normativas y gobernanza digital (Reznik, 202; Coronel, 2022).

En países en vías de desarrollo y economías emergentes, como el Ecuador y la región latinoamericana, esta necesidad se intensifica debido al incremento de incidentes cibernéticos en instituciones públicas y privadas, la digitalización de servicios gubernamentales, y la limitada disponibilidad de talento humano especializado en ciberseguridad avanzada. Asimismo, los marcos regulatorios y las políticas públicas en educación superior exigen que los programas de posgrado respondan a las expectativas y necesidades de la sociedad, a la planificación nacional, y al régimen de desarrollo, a la prospectiva de desarrollo científico, humanístico y tecnológico mundial, y a la diversidad cultural(Ley Orgánica de Educación Superior [LOES], s. f.), alineándose con las disposiciones de la Ley Orgánica de Educación Superior (LOES), las regulaciones del Consejo de Educación Superior (CES), promoviendo la articulación de las funciones sustantivas; Docencia, Investigación y Vinculación con la sociedad.(Consejo de Educación Superior [CES], 2022; Calle, 2024). El artículo examina la posibilidad y el enfoque práctico de combinar los estándares de educación superior con las mejores prácticas internacionales en la formación de especialistas en ciberseguridad, dado el impulso que cobrará el proceso de transformación y formación de la sociedad mundial de la información, tiene como objetivo realizar un análisis cuantitativo y cualitativo de la pertinencia del programa de Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial en el contexto ecuatoriano, integrando indicadores de demanda académica, necesidades del mercado laboral, tendencias tecnológicas y criterios normativos. A través de este enfoque metodológico mixto, se busca aportar evidencia científica que respalde la viabilidad y relevancia del programa, contribuyendo a la toma de decisiones en el ámbito de la educación superior y al fortalecimiento de la formación de talento humano especializado para la protección de los sistemas inteligentes y la soberanía digital del país.

Materiales y Métodos

La investigación se desarrolló bajo un enfoque metodológico mixto, integrando métodos cuantitativos y cualitativos con el propósito de evaluar de manera integral la pertinencia académica, social y productiva del programa de Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial. Este enfoque permitió contrastar datos empíricos medibles con análisis interpretativos, garantizando una comprensión holística de las necesidades formativas y del entorno profesional en el contexto ecuatoriano. El diseño de la investigación fue no experimental, descriptivo y analítico, con alcance transversal, dado que la recolección de datos se realizó en un período determinado sin manipulación de variables. Asimismo, se adoptó un carácter prospectivo, orientado a identificar tendencias emergentes en ciberseguridad e inteligencia artificial relevantes para la planificación académica de programas de posgrado. A continuación, se presentan las fases del proceso metodológico aplicado.

Figura 1. *Fases del proceso metodológico*

En la primera fase se realizó una revisión sistemática de literatura científica y técnica relacionada con ciberseguridad, inteligencia artificial y formación de posgrado, priorizando fuentes indexadas en bases de datos académicas de alto impacto. Paralelamente, se analizó el marco normativo nacional vigente, incluyendo la Ley Orgánica de Educación Superior (LOES), las regulaciones y lineamientos del Consejo de Educación Superior (CES) y documentos estratégicos vinculados a transformación digital, seguridad de la información y desarrollo tecnológico. Este análisis permitió establecer los criterios normativos, académicos y científicos que sustentan la pertinencia del programa, así como identificar brechas formativas y tendencias relevantes para el diseño curricular a través de métodos atractivos y sostenibles (Nisar y Shankar, 2025). La fase 2, correspondiente a la determinación de la demanda estudiantil (análisis cuantitativo), la demanda estudiantil potencial fue evaluada mediante la aplicación de instrumentos cuantitativos, principalmente encuestas estructuradas dirigidas a profesionales de áreas afines como tecnologías de la información, ingeniería informática, telecomunicaciones, sistemas, seguridad de la información y ciencia de datos. Los instrumentos incluyeron variables relacionadas con interés académico, motivaciones para cursar estudios de posgrado, expectativas profesionales y disponibilidad para formación especializada en ciberseguridad aplicada a la IA.

Los datos recolectados fueron procesados mediante técnicas de estadística descriptiva, permitiendo identificar patrones de interés, niveles de aceptación del programa y proyecciones de matrícula potencial. Para este propósito, se estableció una muestra no probabilística por conveniencia, debido a la necesidad de identificar participantes que cumplieran con características específicas y pertinentes para el análisis, en este caso, profesionales del área de tecnologías de la información y disciplinas afines. El instrumento fue aplicado a un total de 218 graduados y consta de 10 preguntas cerradas enfocadas al interés de los graduados en elegir estudiar un máster en ciberseguridad. En la fase 3 correspondiente al análisis de la demanda ocupacional y empleabilidad, la evaluación de la demanda ocupacional se desarrolló a partir de un análisis cuantitativo y cualitativo del mercado laboral, considerando ofertas de empleo, perfiles profesionales requeridos y competencias demandadas en los sectores público y privado. Se revisaron informes institucionales, estudios sectoriales y bases de datos laborales, complementados con entrevistas semiestructuradas a expertos y empleadores del ámbito tecnológico y de la ciberseguridad. Esta fase permitió identificar los roles profesionales emergentes, las competencias técnicas y transversales más requeridas, así como las oportunidades de inserción laboral y proyección profesional de los futuros graduados del programa. Al igual que en el apartado anterior, se estableció una muestra no probabilística por conveniencia, la cual permitió la aplicación del instrumento a expertos y empleadores del área, conformada

por un total de 17 participantes. El instrumento consta de 6 preguntas enfocadas a su ocupación, nivel de experiencia y el uso de tecnologías emergentes, desafíos, usos y habilidades en el campo de la ciberseguridad.

En la fase 4 asociada al análisis cualitativo de pertinencia académica y tecnológica, con el objetivo de profundizar en la pertinencia académica y tecnológica del programa, se desarrollaron entrevistas a informantes clave, incluyendo académicos, investigadores, gestores de tecnología y responsables de seguridad de la información. El análisis cualitativo se orientó a evaluar la coherencia del programa con las tendencias internacionales, la innovación curricular, la integración de inteligencia artificial en la ciberseguridad y la capacidad del programa para responder a desafíos reales del entorno ecuatoriano. La información cualitativa fue analizada mediante técnicas de codificación temática, permitiendo identificar categorías y subcategorías relevantes para la evaluación de pertinencia. Para este apartado se desarrolló un instrumento que consta de 18 pregunta enfocadas al análisis de metodologías educativas, competencias específicas, uso de nuevas tecnologías y principales desafíos, se aplicó a una muestra de 12 de expertos con amplia experiencia en ciberseguridad, IA y docencia en educación superior.

Resultados y Discusión

Resultados de la Fase 1: Análisis documental y normativo

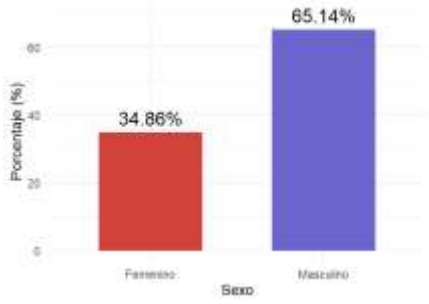
El análisis documental evidenció una alta convergencia entre las tendencias globales en ciberseguridad e inteligencia artificial y las directrices académicas internacionales para la formación de posgrado. La revisión de literatura especializada mostró un crecimiento sostenido de investigaciones orientadas a la seguridad de modelos de aprendizaje automático, detección inteligente de amenazas, automatización de respuestas a incidentes y gobernanza de la IA, lo que confirma la consolidación de este campo como una línea estratégica de desarrollo científico y tecnológico. Desde el punto de vista normativo, se identificó una alineación directa del programa propuesto con los principios establecidos en la Ley Orgánica de Educación Superior, en los artículos 12, 13, 93, 97 y específicamente en el artículo 107, particularmente en lo referente a las necesidades de desarrollo local, regional y nacional, a la innovación y diversificación de profesiones y grados académicos, a las tendencias del mercado ocupacional local, regional y nacional, a las tendencias demográficas locales, provinciales y regionales; a la vinculación con la estructura productiva actual y potencial de la provincia y la región, y a las políticas nacionales de ciencia y tecnología (Ley Orgánica de Educación Superior [LOES], s. f.). Asimismo, los lineamientos del Consejo de Educación Superior destacan la necesidad de programas de cuarto nivel que respondan a problemáticas emergentes de acuerdo con las necesidades de la sociedad; asegurando el cumplimiento de los principios y derechos consagrados en la Constitución, la LOES y demás normativa aplicable (Consejo de Educación Superior [CES], 2022). Estos resultados permitieron establecer una base conceptual y regulatoria sólida que respalda la viabilidad académica del programa.

Resultados de la Fase 2: Demanda estudiantil

Los resultados de las encuestas aplicadas a profesionales de áreas afines evidenciaron una alta aceptación e interés por el programa de maestría. Un porcentaje significativo de los encuestados manifestó intención de cursar estudios de posgrado en ciberseguridad, destacando como principales motivaciones el

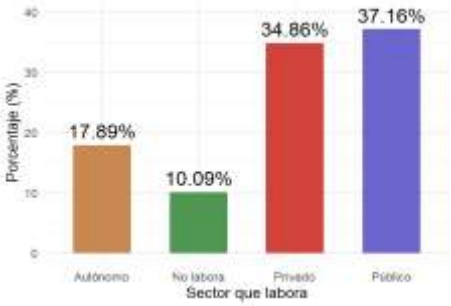
fortalecimiento de competencias técnicas avanzadas, la mejora de oportunidades laborales y la especialización en tecnologías emergentes basadas en IA. Asimismo, se identificó que una mayoría de los participantes percibe la ciberseguridad aplicada a la inteligencia artificial como un campo con alta proyección profesional, tanto a nivel nacional como internacional. Los datos también reflejaron una preferencia por programas que integren formación práctica, investigación aplicada y resolución de problemas reales del entorno institucional y empresarial.

Figura 2. *Distribución de los individuos según el género*



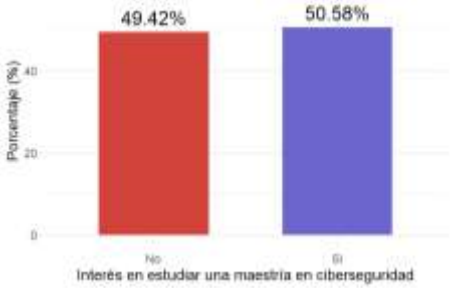
Los resultados obtenidos permiten caracterizar el perfil de los potenciales aspirantes y analizar la pertinencia del programa de Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial en el contexto ecuatoriano, considerando variables sociodemográficas, laborales, académicas y de expectativas formativas. En relación con el sexo, se evidencia una mayor participación del género masculino (65,14%) frente al femenino (34,86%). Esta distribución es consistente con tendencias históricas en áreas vinculadas a tecnologías de la información y ciberseguridad, donde persiste una brecha de género. No obstante, la participación femenina superior al 30% refleja una progresiva incorporación de mujeres en programas de posgrado tecnológicos, lo que sugiere oportunidades para fortalecer políticas de equidad e inclusión en la oferta académica.

Figura 3. *Distribución de los individuos según el sector que labora*



Respecto al sector laboral, la mayoría de los encuestados se desempeña en el sector público (37,16%) y privado (34,86%), seguidos por trabajadores autónomos (17,89%). Este resultado evidencia una demanda transversal desde distintos ámbitos productivos, lo que refuerza la pertinencia del programa frente a los retos de ciberseguridad en instituciones estatales, empresas privadas y emprendimientos independientes. El 10,09% que no labora actualmente representa un segmento potencialmente interesado en fortalecer su empleabilidad mediante formación especializada.

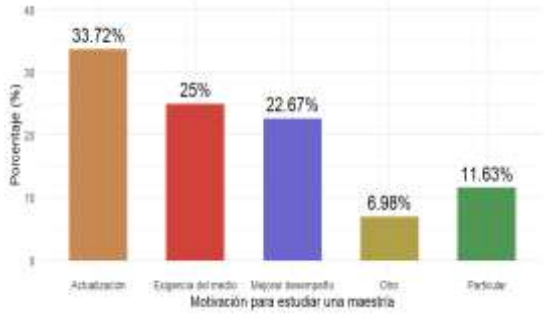
Figura 4. *Interés en estudiar una maestría en ciberseguridad*



En cuanto a la continuidad de estudios de posgrado, un porcentaje significativo (78,90%) manifiesta su intención de continuar estudios, lo cual evidencia una alta predisposición hacia la formación avanzada. Este dato constituye un indicador clave de viabilidad académica y

social del programa, alineado con las políticas nacionales de fortalecimiento del talento humano especializado.

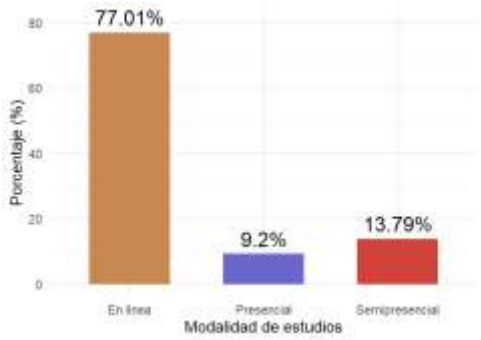
Figura 5. *Motivación para estudiar una maestría*



Las motivaciones para cursar una maestría se concentran principalmente en la actualización de conocimientos (33,72%), seguida de exigencias del medio laboral (25,00%) y mejoramiento del desempeño profesional (22,67%). Estos resultados reflejan un contexto dinámico, caracterizado por la rápida evolución tecnológica y el incremento de amenazas cibernéticas, además de la necesidad de contar con profesionales con competencias actualizadas y especializadas.

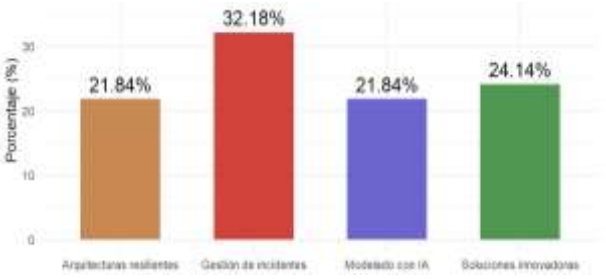
El análisis de los factores determinantes para estudiar una maestría, evaluados en una escala de importancia, muestra que el título que ofrece el programa es altamente valorado, con un 91,9% en el nivel máximo.

Figura 6. *Modalidad de estudios*



Asimismo, el personal docente (70,3%) y la modalidad de estudio (66,9%) alcanzan valoraciones elevadas, lo que subraya la importancia de contar con docentes especializados y modalidades flexibles. La infraestructura y otros factores, aunque relevantes, presentan valoraciones moderadas, lo que sugiere que la calidad académica y la flexibilidad superan a los recursos físicos como criterios decisivos. En relación con el interés específico en una maestría en ciberseguridad, los resultados muestran una distribución casi equilibrada, con un 50,58% de respuestas afirmativas. Este hallazgo indica un interés significativo, pero también revela la necesidad de estrategias de difusión y sensibilización que destaquen el valor diferencial del enfoque aplicado a la inteligencia artificial dentro del contexto ecuatoriano. Entre quienes manifestaron interés, la modalidad de estudio preferida es mayoritariamente en línea (77,01%), seguida por la modalidad semipresencial (13,79%) y presencial (9,20%). Este resultado evidencia una clara preferencia por esquemas flexibles, compatibles con la actividad laboral, lo cual refuerza la pertinencia de una oferta virtual para programas de cuarto nivel en áreas tecnológicas.

Figura 7. *Habilidades del programa de Ciberseguridad*



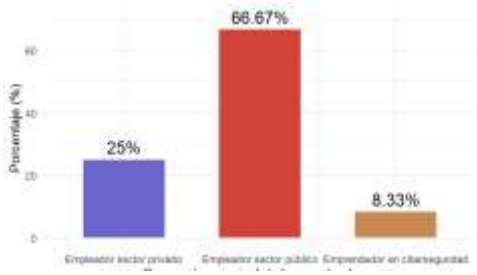
Finalmente, las habilidades consideradas más relevantes dentro del programa se concentran en la gestión de incidentes (32,18%), seguida por soluciones innovadoras (24,14%), modelado con inteligencia artificial (21,84%) y arquitecturas resilientes (21,84%). Estas preferencias evidencian una orientación

práctica y aplicada del perfil de egreso, alineada con las necesidades reales del mercado laboral y los desafíos actuales en ciberseguridad, donde la respuesta a incidentes y la innovación tecnológica resultan competencias críticas. Estos resultados confirman la pertinencia académica, social y profesional de la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial, destacando la demanda de formación especializada, la preferencia por modalidades flexibles y la necesidad de competencias orientadas a la gestión de riesgos, innovación y resiliencia digital en el contexto ecuatoriano. Las respuestas abiertas de los encuestados reforzaron la percepción de una brecha formativa existente en el país, señalando la escasa oferta de programas especializados que integren ciberseguridad e IA de manera estructurada. Este hallazgo cualitativo complementa los resultados cuantitativos y fortalece el argumento de pertinencia académica del programa.

Resultados de la Fase 3: Demanda ocupacional y empleabilidad

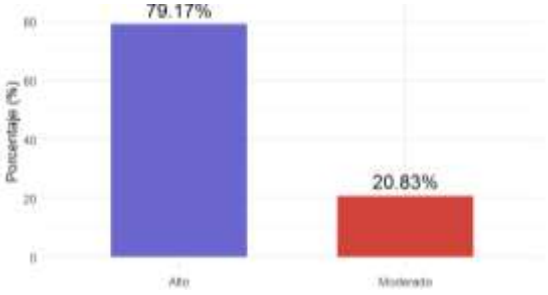
El análisis de la información recolectada del sector de empleadores permite identificar las necesidades reales del mercado laboral y su correspondencia con la propuesta académica de la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial, constituyéndose en un insumo clave para evaluar la pertinencia profesional y productiva del programa en el contexto ecuatoriano, lo que evidenció un incremento sostenido en la demanda de perfiles profesionales especializados en ciberseguridad avanzada, particularmente aquellos con conocimientos en análisis de datos, automatización, inteligencia artificial y gestión de riesgos digitales. Se identificaron roles emergentes como analista de ciberseguridad con enfoque en IA, arquitecto de seguridad inteligente, especialista en detección de amenazas avanzadas y gestor de seguridad en infraestructuras críticas Los datos recopilados muestran que estos perfiles presentan altos niveles de empleabilidad y una proyección favorable en sectores como banca, telecomunicaciones, industria tecnológica, servicios digitales y administración pública.

Figura 8. *Ocupación principal de los empleadores*



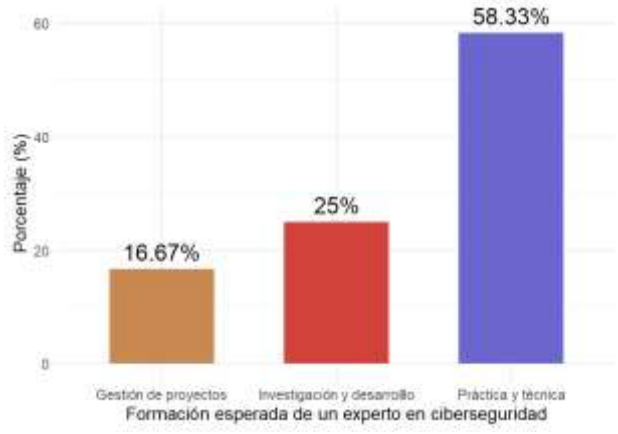
En cuanto a la ocupación de los participantes, se observa una predominancia del sector privado (66,67%), seguido del sector público (25,00%) y, en menor proporción, de emprendedores vinculados a la ciberseguridad (8,33%). Esta distribución evidencia que la demanda de especialistas en ciberseguridad con competencias en inteligencia artificial se concentra principalmente en organizaciones privadas, donde la transformación digital y la protección de activos de información son prioridades estratégicas. No obstante, la participación del sector público refleja la creciente preocupación institucional por la seguridad de la información y la protección de infraestructuras críticas del Estado.

Figura 9. *Impacto de ciberataques en su lugar de trabajo*



Respecto al impacto de los ciberataques, los resultados son contundentes: el 79,17% de los empleadores considera que el impacto es alto y el 20,83% lo califica como moderado, sin registros en los niveles bajo o no relevante. Este hallazgo confirma la alta exposición de las organizaciones a amenazas cibernéticas y refuerza la necesidad urgente de contar con profesionales altamente capacitados, capaces de prevenir, detectar y responder a incidentes de seguridad mediante el uso de tecnologías avanzadas, incluida la inteligencia artificial. En relación con la formación esperada de un experto en ciberseguridad, los empleadores priorizan una formación práctica y técnica (58,33%), seguida de competencias en investigación y desarrollo (25,00%) y, en menor medida, en gestión de proyectos (16,67%). Estos resultados sugieren que el mercado laboral ecuatoriano demanda perfiles con un fuerte enfoque aplicado, orientados a la resolución de problemas reales y a la implementación de soluciones tecnológicas, sin descuidar las capacidades de innovación y gestión necesarias para liderar proyectos estratégicos de seguridad de la información.

Figura 9. *Formación esperada de un experto en ciberseguridad*



El análisis de las tecnologías emergentes relevantes muestra que el machine learning (37,50%) y el deep learning (29,17%) son consideradas prioritarias por los empleadores, seguidas por blockchain (20,83%). Este resultado evidencia una clara alineación con el enfoque del programa propuesto, el cual integra la inteligencia artificial como eje transversal para la detección de amenazas, el análisis predictivo y la automatización de procesos de seguridad, fortaleciendo así su pertinencia tecnológica.

Figura 9. *Tecnologías emergentes relevantes*

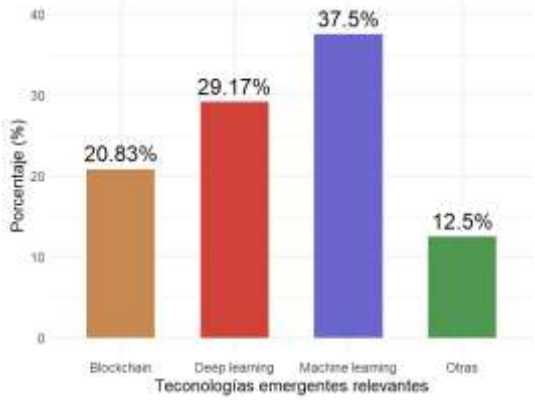
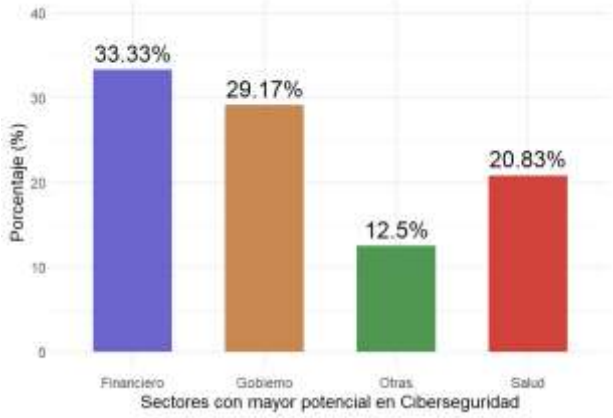


Figura 10. *Sectores con mayor potencial en cyberseguridad*



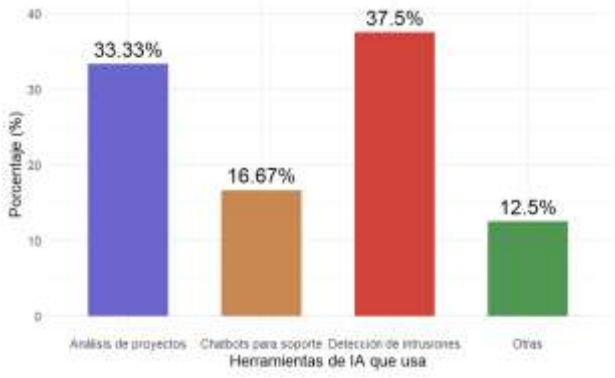
En cuanto a los sectores con mayor potencial de aplicación, el sector financiero lidera con el 33,33%, seguido del sector gubernamental (29,17%) y el sector salud (20,83%). Estos sectores se caracterizan por el manejo de información sensible y regulada, lo que demanda altos estándares de seguridad. Este resultado refuerza la necesidad de formar profesionales especializados capaces de

responder a los requerimientos específicos de sectores estratégicos para el desarrollo económico y social del país.

Figura 11. *Habilidades necesarias en profesionales de ciberseguridad*

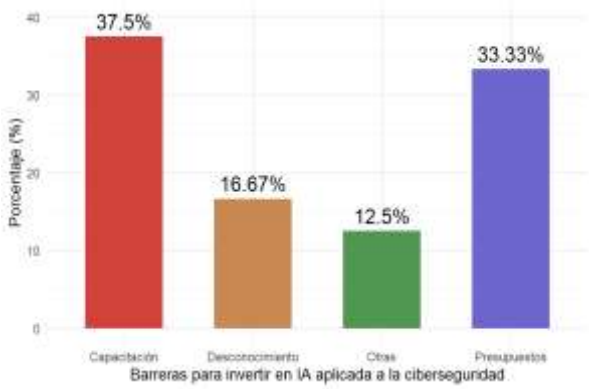
Respecto a las habilidades más demandadas en profesionales de ciberseguridad, los empleadores destacan la programación avanzada (37,50%), el análisis de datos (29,17%) y la gestión de riesgos (25,00%). Estas competencias reflejan la convergencia entre ciberseguridad e inteligencia artificial, donde la capacidad de programar, analizar grandes volúmenes de datos y gestionar riesgos se vuelve fundamental para anticipar y mitigar amenazas complejas.

Figura 12. *Herramientas de IA que usa*



En relación con las herramientas de inteligencia artificial utilizadas, se evidencia un mayor uso de sistemas de detección de intrusiones basados en IA (37,50%) y de análisis predictivo (33,33%), mientras que los chatbots para soporte presentan una adopción menor (16,67%). Este patrón sugiere que las organizaciones priorizan soluciones de IA directamente vinculadas a la protección de sistemas y la toma de decisiones, lo que respalda la inclusión de estos contenidos en la malla curricular del programa. El análisis de las barreras para invertir en inteligencia artificial aplicada a la ciberseguridad revela que el principal obstáculo es el presupuesto ineficiente (41,67%), seguido por la falta de personal capacitado (29,17%) y el desconocimiento de herramientas (20,83%). Lo que evidencia una brecha significativa de talento humano especializado y refuerza la pertinencia social y económica del programa de maestría como mecanismo para fortalecer las capacidades nacionales y reducir la dependencia de soluciones externas. Las entrevistas a empleadores y expertos del sector confirmaron que existe una escasez de talento humano especializado en ciberseguridad aplicada a la IA en el contexto ecuatoriano. Los informantes clave señalaron que los profesionales con formación avanzada en este campo poseen una ventaja competitiva significativa, especialmente para liderar procesos de transformación digital segura y gestión de incidentes complejos.

Figura 12. *Barreras para invertir en IA aplicada a la ciberseguridad*



Resultados de la Fase 4: Análisis cualitativo de pertinencia académica y tecnológica

El análisis de las entrevistas a informantes clave permitió identificar una alta valoración del enfoque interdisciplinario del programa, destacándose la integración de ciberseguridad, inteligencia artificial, análisis de datos y gestión estratégica. Los expertos coincidieron en que este enfoque responde de manera adecuada a las tendencias internacionales y a las necesidades reales del entorno tecnológico nacional. Asimismo, se evidenció consenso en torno a la necesidad de que el programa incorpore componentes de investigación aplicada, laboratorios especializados, simulación de ciberataques y análisis de casos reales, lo que refuerza su pertinencia académica y tecnológica. Las categorías emergentes del análisis cualitativo incluyeron innovación curricular, actualización tecnológica, impacto institucional y contribución al desarrollo de capacidades nacionales en seguridad digital. Los resultados del análisis documental y normativo evidencian una alta correspondencia entre el programa propuesto y los lineamientos nacionales e internacionales sobre formación avanzada en tecnologías emergentes. Este hallazgo coincide con estudios previos que señalan que los programas de posgrado en ciberseguridad deben evolucionar hacia enfoques interdisciplinarios, incorporando inteligencia artificial, análisis de datos y automatización defensiva. Desde la perspectiva normativa, la alineación con la LOES y los criterios del CES refuerza la legitimidad académica del programa, dado que estos organismos priorizan la pertinencia social, la innovación curricular y la contribución al desarrollo productivo. En este sentido, la maestría analizada cumple con los principios de calidad, relevancia y prospectiva exigidos para programas de cuarto nivel. Los resultados de la demanda estudiantil confirman una alta aceptación del programa, lo que refleja una necesidad formativa insatisfecha en el sistema de educación superior ecuatoriano. Este comportamiento es consistente con tendencias regionales que evidencian un creciente interés por especializaciones en ciberseguridad avanzada, especialmente aquellas que integran inteligencia artificial como herramienta estratégica.

Los resultados de la Fase 2 evidencian una alta pertinencia del programa de Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial, en concordancia con las necesidades formativas y profesionales de los potenciales aspirantes en el contexto ecuatoriano. La elevada intención de continuar estudios de posgrado y la clara orientación hacia la actualización de conocimientos y el fortalecimiento de competencias técnicas avanzadas confirman la existencia de una demanda real por programas especializados en áreas tecnológicas emergentes, particularmente aquellas que integran ciberseguridad e inteligencia artificial. La preferencia mayoritaria por modalidades de estudio en línea se alinea con transformaciones recientes en la educación superior, donde la flexibilidad, el acceso y la compatibilidad con la actividad laboral se han convertido en factores determinantes para la elección de programas de cuarto nivel. Este hallazgo respalda la viabilidad académica y social de una oferta virtual, especialmente en un país con brechas geográficas y necesidades de formación continua como Ecuador. Por otra parte, la valoración prioritaria del título, del cuerpo docente y de la modalidad por encima de la infraestructura física sugiere un cambio en los criterios tradicionales de selección de programas de posgrado, donde la calidad académica, la especialización del profesorado y la aplicabilidad de los contenidos adquieren

mayor relevancia. De igual forma, la orientación práctica y aplicada de las habilidades demandadas, la innovación y el uso de inteligencia artificial confirma la necesidad de un perfil de egreso alineado con la resolución de problemas reales y los desafíos actuales de la ciberseguridad.

El análisis del mercado laboral evidencia una demanda sostenida de perfiles especializados en ciberseguridad aplicada a la IA, lo que confirma la relevancia productiva del programa. La identificación de roles emergentes coincide con estudios internacionales que destacan la escasez global de talento en ciberseguridad avanzada y la creciente valorización de competencias en análisis inteligente de amenazas. Los resultados del análisis del sector empleador evidencian una clara correspondencia entre las necesidades actuales del mercado laboral ecuatoriano y la propuesta académica de la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial. La identificación de roles emergentes vinculados a la ciberseguridad avanzada y al uso de inteligencia artificial confirma una transformación progresiva de los perfiles profesionales requeridos, marcada por la automatización, el análisis de datos y la gestión integral de riesgos digitales. La alta concentración de empleadores del sector privado, junto con la participación del sector público, refleja que la ciberseguridad se ha consolidado como una prioridad estratégica tanto en organizaciones orientadas al mercado como en instituciones estatales responsables de la protección de infraestructuras críticas. Esta tendencia es consistente con el elevado impacto percibido de los ciberataques, el cual es considerado alto o moderado por la totalidad de los participantes, lo que refuerza la urgencia de contar con profesionales altamente especializados y con capacidad de respuesta ante amenazas complejas. La preferencia de los empleadores por una formación predominantemente práctica y técnica, complementada con competencias en investigación y gestión, sugiere la necesidad de programas de posgrado con un enfoque aplicado, orientados a la resolución de problemas reales del entorno organizacional. Este hallazgo respalda el diseño curricular de la maestría, que integra la formación técnica especializada con la innovación y la investigación aplicada como ejes fundamentales.

Asimismo, la priorización de tecnologías emergentes como machine learning, deep learning y blockchain evidencia la convergencia entre ciberseguridad e inteligencia artificial como una tendencia consolidada, especialmente en sectores estratégicos como el financiero, gubernamental y de salud. Esta convergencia demanda profesionales capaces de diseñar e implementar soluciones inteligentes que fortalezcan la seguridad de la información y la resiliencia digital de las organizaciones. Las habilidades más demandadas confirman la necesidad de un perfil de egreso integral, con capacidades técnicas avanzadas y una visión estratégica de la seguridad digital. Del mismo modo, el uso predominante de herramientas de IA orientadas a la detección de intrusiones y al análisis predictivo pone de manifiesto que las organizaciones priorizan soluciones que permitan anticipar y mitigar amenazas, más que aplicaciones de soporte operativo. Las barreras identificadas para la inversión en inteligencia artificial aplicada a la ciberseguridad, particularmente la falta de presupuesto eficiente y de personal capacitado, evidencian una brecha estructural de talento humano especializado en el país. Esta situación, corroborada por las entrevistas a empleadores y expertos, refuerza la pertinencia social, económica y académica del programa de maestría como una respuesta

estratégica para fortalecer las capacidades nacionales, mejorar la empleabilidad y reducir la dependencia de soluciones externas. El análisis cualitativo revela un consenso entre los informantes clave respecto a la pertinencia del enfoque interdisciplinario del programa. La integración de ciberseguridad, inteligencia artificial, gestión de riesgos y análisis de datos se identifica como un elemento diferenciador frente a otras ofertas académicas existentes. Estos resultados se alinean con la literatura que sostiene que los programas de posgrado en áreas tecnológicas deben incorporar investigación aplicada, laboratorios especializados y metodologías activas para garantizar su pertinencia y sostenibilidad.

Conclusiones

El análisis cuantitativo y cualitativo realizado en el presente estudio permite concluir que el programa de Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial presenta una alta pertinencia académica, social, productiva y tecnológica en el contexto ecuatoriano. La integración de evidencia empírica, análisis normativo y revisión científica confirma la necesidad de una formación avanzada que responda a los desafíos emergentes derivados de la transformación digital y del uso intensivo de inteligencia artificial en sistemas críticos. Desde la perspectiva académica, los resultados evidencian que el programa se alinea de manera consistente con las tendencias internacionales en ciberseguridad e inteligencia artificial, así como con los principios de calidad, innovación y pertinencia establecidos por la Ley Orgánica de Educación Superior (LOES) y las regulaciones del Consejo de Educación Superior (CES). La propuesta curricular, sustentada en un enfoque interdisciplinario y aplicado, responde a las exigencias actuales de formación de cuarto nivel orientadas a la investigación aplicada y a la solución de problemáticas reales del entorno.

En relación con la demanda estudiantil, el estudio demuestra la existencia de un interés significativo por parte de profesionales de áreas afines, quienes identifican la ciberseguridad aplicada a la inteligencia artificial como un campo estratégico para su desarrollo profesional y empleabilidad. Este hallazgo confirma la presencia de una brecha formativa en la oferta académica nacional y respalda la viabilidad del programa desde una perspectiva de sostenibilidad académica. Asimismo, el análisis de la demanda ocupacional y la empleabilidad evidencia una necesidad creciente de talento humano especializado en ciberseguridad avanzada, particularmente en perfiles que integren competencias en inteligencia artificial, análisis de datos y gestión de riesgos digitales. Los sectores público y privado coinciden en la escasez de profesionales con estas capacidades, lo que posiciona al programa como una respuesta pertinente a las demandas del mercado laboral y a los procesos de transformación digital segura del país. Desde el enfoque cualitativo, la valoración de expertos e informantes clave refuerza la pertinencia tecnológica y estratégica del programa, destacando su potencial para fortalecer capacidades institucionales, mejorar la protección de infraestructuras críticas y contribuir a la soberanía digital. La convergencia de estos resultados, validada mediante procesos de triangulación, otorga solidez y confiabilidad a las conclusiones del estudio. En conclusión, la Maestría en Ciberseguridad Aplicada a la Inteligencia Artificial se configura como una propuesta académica viable, necesaria y alineada con las necesidades actuales y futuras del Ecuador. Su implementación contribuirá al fortalecimiento del sistema de educación superior, al desarrollo

de talento humano altamente calificado y a la consolidación de capacidades nacionales para enfrentar los desafíos de la seguridad digital en entornos inteligentes, constituyéndose en un aporte estratégico para el desarrollo científico, tecnológico y productivo del país.

Referencias Bibliográficas

Buríachok, V., & Sokolov, V. (2020). Implementation of active learning in the master's program on cybersecurity. *Advances in Intelligent Systems and Computing*, 938, 610–624. https://www.scopus.com/pages/publications/85064552966

Calle, M. (2024). Pertinencia social y normativa de los programas de posgrado tecnológicos en el Ecuador. *Revista Andina de Educación*, 8(1), 1–14. https://doi.org/10.32719/26312816.2024.8.1.1

Campos, J. (2025). Automatización defensiva y aprendizaje automático en ciberseguridad organizacional. *Ingeniería y Competitividad*, 27(1), 1–12. https://doi.org/10.25100/iyc.v27i1.13245

Consejo de Educación Superior. (2022). Reglamento de régimen académico. https://www.ces.gob.ec/wp-content/uploads/2022/08/Reglamento-de-Re%CC%81gimen-Acade%CC%81mico-vigente-a-partir-del-16-de-septiembre-de-2022.pdf

Coronel-Suárez, M. (2022). Gobernanza digital y ciberseguridad en sistemas inteligentes: una perspectiva latinoamericana. *Revista Ciencia, Tecnología y Sociedad*, 17(50), 97–112. https://doi.org/10.22201/cts.2022.50.978

Dávila-Morán, R. (2023). Formación en ciberseguridad y competencias digitales avanzadas en la educación superior latinoamericana. *Formación Universitaria*, 16(6), 73–84. https://doi.org/10.4067/S0718-50062023000600073

de Jager, M., Heymann, R., & Greeff, J. (2026). A transdisciplinary approach to embedding cybersecurity across the curriculum of an undergraduate computing degree program in South Africa. *IFIP Advances in Information and Communication Technology*, 742, 49–63. https://www.scopus.com/pages/publications/105012920642

Ekqvist, J., Kämppi, P., & Rajamäki, J. (2025). Cybersecurity education in Finnish universities of applied sciences: Workforce alignment. *European Conference on Information Warfare and Security*, 735–744. https://www.scopus.com/pages/publications/105014923363

Fernández, A. (2024). Inteligencia artificial y ciberseguridad: riesgos emergentes en la transformación digital del sector público latinoamericano. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (48), 1–15. https://doi.org/10.17013/risti.48.1-15

Ley Orgánica de Educación Superior. (s. f.). https://www.lexis.com.ec

Lucio-Vásquez, L. (2024). Demanda laboral de profesionales en ciberseguridad e inteligencia artificial en economías emergentes. *Revista Venezolana de Gerencia*, 29(106), 214–230. https://doi.org/10.37960/rvg.v29i106.41287

Nicoletti, L., Scannapieco, M., Sorella, M., & Centenaro, M. (2024). Governing artificial intelligence systems: Aspects of cybersecurity. *Mondo Digitale*. https://www.scopus.com/pages/publications/105013261562

Nisar, K., & Chowdhry, B. S. (2025). The role of cybersecurity and big data in digital twinning: A review, challenges, and opportunities. En *Digital twinning for discrete manufacturing*. 48–52. *CRC Press*. https://www.scopus.com/pages/publications/105025266825

Reznik, L. (2021). Intelligent security systems: How artificial intelligence, machine learning and data science work for and against computer security. Wiley. https://www.scopus.com/pages/publications/85149428746

Sánchez, M. (2024). Amenazas cibernéticas basadas en inteligencia artificial: desafíos

para la seguridad de la información en América Latina. *Revista Latinoamericana de Ingeniería de Software*, 12(2), 45–59. https://doi.org/10.18294/relais.2024.2489