UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración

Carrera de Ingeniería en Ciencias de la Computación

LA INTELIGENCIA ARTIFICIAL EN ATAQUE Y DEFENSA CIBERNÉTICA: UNA REVISIÓN SISTEMÁTICA DE LITERATURA

Trabajo de titulación previo a la obtención del grado de Ingeniera en Ciencias de la Computación

Autora:
Anahí Dennisse Silva Campoverde

Director:
Paúl Esteban Crespo Martínez

Cuenca – Ecuador

2025

DEDICATORIA

A Dios, por la vida, la sabiduría y la fortaleza que me concedió para llegar hasta aquí. Por guiarme en cada paso, darme luz en los momentos de duda y enseñarme que todo esfuerzo tiene su recompensa.

A mis padres, por su amor incondicional, su paciencia y su apoyo en cada etapa de mi formación. Sus palabras de aliento, su entusiasmo y su orgullo en cada paso de este proceso me han hecho sentir acompañada, como si este logro también les perteneciera. Gracias por estar siempre presentes, por creer en mí y por impulsarme a poner mis metas y mi crecimiento personal como prioridad.

A mi familia, a mis tíos, tías, primos y primas, por su cariño, por acompañarme con palabras de ánimo y por celebrar cada pequeño logro conmigo. Cada muestra de afecto ha sido un recordatorio de que nunca he estado sola en este camino.

De manera muy especial, a mi abuelo, quien me enseñó que el mejor camino siempre será el más difícil, pero también el que más fortalece el alma. Sus palabras —que nunca debo rendirme y que siempre debo luchar por lo que sueño— se han convertido en una guía constante y en fuente de inspiración en mi vida. Gracias por inspirarme a no rendirme, por recordarme que los sueños se alcanzan con esfuerzo, y por inculcarme el valor del trabajo, la perseverancia y la fe en un futuro mejor.

Y, finalmente, a mí misma, por no rendirme, por mantener la disciplina y la responsabilidad aun cuando todo parecía cuesta arriba. Por confiar en mi capacidad, creer en mis metas y seguir adelante a pesar de las inseguridades, la soledad y los miedos. Me dedico este logro porque sé cuánto esfuerzo, coraje y determinación puse para alcanzarlo, y porque hoy puedo reconocer que soy capaz de más de lo que alguna vez imaginé.

AGRADECIMIENTO

A la Universidad del Azuay y a la Facultad de Ciencias de la Administración, por brindarme el conocimiento, la orientación y las herramientas necesarias para mi formación profesional.

A mi director de tesis, Magíster Esteban Crespo Martínez, por su guía, paciencia y apoyo constante durante todo este proceso. Agradezco su disposición, sus enseñanzas y el entusiasmo con el que siempre compartió sus conocimientos.

A la Magíster María Inés Acosta, por su acompañamiento en la parte metodológica, su orientación precisa y su constante disposición para ayudarme con amabilidad y compromiso. Su apoyo fue fundamental para el desarrollo técnico y estructural de este trabajo.

A mis docentes en general, por motivarme a seguir aprendiendo con pasión, dedicación y compromiso, y por contribuir significativamente a mi crecimiento académico y personal.

A mis compañeros y amigos, por compartir conmigo esta etapa llena de aprendizajes, desafíos y buenos momentos. Gracias por su amistad, por las ideas compartidas y por el apoyo mutuo que hizo más llevadero cada ciclo.

Asimismo, deseo agradecer a todas las personas que he conocido a lo largo de mi carrera universitaria, quienes, de una u otra manera, han formado parte de este camino. He aprendido mucho de cada experiencia compartida y me quedo con gratos recuerdos que conservaré siempre.

Finalmente, agradezco también a los funcionarios y al personal administrativo de la universidad que me brindaron la oportunidad de participar en proyectos que fortalecieron mi aprendizaje y me permitieron desarrollarme tanto a nivel académico como profesional.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

La Inteligencia Artificial en Ataque y Defensa Cibernética: Una Revisión Sistemática de Literatura

RESUMEN

La incorporación de la inteligencia artificial (IA) en la ciberseguridad ha transformado tanto la defensa como el ataque, pero la literatura se encuentra fragmentada y carece de revisiones integrales que analicen ambas perspectivas. Con el fin de responder a esta problemática, se realizó una revisión sistemática de literatura siguiendo el protocolo PRISMA 2020, complementada con análisis lexicométrico mediante IRaMuTeQ. A partir de 646 registros iniciales, se seleccionaron 222 estudios pertinentes, que fueron organizados y clasificados en clústeres temáticos. El hallazgo más relevante revela tres ejes centrales: el uso de IA en detección y prevención de intrusiones (IDS/NIDS), la explotación ofensiva de técnicas como adversarial machine learning y backdoors, y la emergencia de tendencias que integran modelos generativos y aprendizaje federado en escenarios de defensa y ataque. En conclusión, este estudio sistematiza un campo en rápida evolución, identifica brechas metodológicas y proyecta líneas de investigación orientadas a fortalecer defensas robustas y anticipar amenazas cada vez más sofisticadas.

Palabras clave: ciberataques, ciberseguridad, inteligencia artificial, machine learning, revisión sistemática de la literatura.

Artificial Intelligence in Cyber Attack and Defense: A Systematic Literature Review

ABSTRACT

The incorporation of artificial intelligence (AI) into cybersecurity has transformed both defense and offense, but the literature remains fragmented and lacks comprehensive reviews that analyze both perspectives. To address this issue, a systematic literature review was conducted following the PRISMA 2020 protocol, complemented with lexicometric analysis using IRaMuTeQ. From an initial 646 records, 222 relevant studies were selected and classified into thematic clusters. The most relevant finding reveals three central axes: the use of AI in intrusion detection and prevention (IDS/NIDS), the offensive exploitation of techniques such as adversarial machine learning and backdoors, and the emergence of trends that integrate generative models and federated learning in both defense and attack scenarios. In conclusion, this study systematizes a rapidly evolving field, identifies methodological gaps, and projects research lines aimed at strengthening robust defenses and anticipating increasingly sophisticated threats.

Keywords: artificial intelligence, cyberattacks, cybersecurity, machine learning, systematic literature review.