LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, Asunción, Paraguay.
ISSN en línea: 2789-3855, 2025, Volumen VI

El papel de la inteligencia artificial en la detección del phishing: un enfoque descriptivo sobre su impacto en la ciberseguridad

The role of artificial intelligence in phishing detection: A descriptive approach to its impact on cybersecurity

Javier Rubén León Naranjo
Javier.leon@educacion.gob.ec
https://orcid.org/0000-0002-6411-7879
Ministerio de Educación. Distrito Educativo 09D19
Daule – Ecuador

Marjorie Monserrate Oleas Morán
marjorieoleas@gmail.com
https://orcid.org/0009-0006-4149-4547
Ministerio de Educación. Distrito Educativo 09D19
Nobol – Ecuador

Karen Zullay Pimentel Salazar
Karen.pimentel@educacion.gob.ec
https://orcid.org/0009-0004-6900-1201
Ministerio de Educación. Distrito Educativo 09D19
Daule – Ecuador

DOI: https://doi.org/10.56712/latam.v6i4.4437

Artículo recibido: 27 de mayo de 2025
Aceptado para pub licación: 29 de agosto de 2025.
Conflictos de Interés: Ninguno que declarar.

Redilat
Red de Investigadores Latinoamericanos

NÚMERO 4

DOI: https://doi.org/10.56712/latam.v6i4.4437

El papel de la inteligencia artificial en la detección del *phishing*: un enfoque descriptivo sobre su impacto en la ciberseguridad

The role of artificial intelligence in phishing detection: A descriptive approach to its impact on cybersecurity

Javier Rubén León Naranjo
Javier.leon@educacion.gob.ec
https://orcid.org/0000-0002-6411-7879
Ministerio de Educación. Distrito Educativo 09D19
Daule – Ecuador

Marjorie Monserrate Oleas Morán
marjorieoleas@gmail.com
https://orcid.org/0009-0006-4149-4547
Ministerio de Educación. Distrito Educativo 09D19
Nobol – Ecuador

Karen Zullay Pimentel Salazar
Karen.pimentel@educacion.gob.ec
https://orcid.org/0009-0004-6900-1201
Ministerio de Educación. Distrito Educativo 09D19
Daule – Ecuador

Artículo recibido: 27 de mayo de 2025. Aceptado para publicación: 29 de agosto de 2025.
Conflictos de Interés: Ninguno que declarar.

Resumen

Este estudio analiza el uso de la inteligencia artificial (IA) para la detección y prevención del phishing, un delito cibernético que afecta la seguridad de datos personales y recursos económicos. Se empleó un enfoque mixto, combinando métodos cuantitativos y cualitativos. La recolección de datos se realizó mediante encuestas aplicadas a 95 comerciantes y profesionales de Daule, Ecuador, quienes respondieron preguntas sobre su experiencia con correos fraudulentos, mensajes sospechosos y llamadas telefónicas relacionadas con phishing. Además, se realizó una revisión documental para complementar y contextualizar los hallazgos. Los resultados indicaron que el 87% de los encuestados ha recibido correos fraudulentos, el 86% mensajes sospechosos y el 74% ha sido víctima o conoce a alguien afectado por phishing telefónico. En cuanto a la percepción sobre la IA, el 59% la considera una herramienta confiable y el 68% se siente más seguro cuando una plataforma la utiliza para proteger sus datos. El análisis estadístico descriptivo mostró una media de 3,82 con baja dispersión, reflejando una tendencia general hacia la aceptación de la IA como solución. Se concluye que, aunque la IA es una herramienta valiosa, es necesario fomentar la educación digital y aumentar la confianza en estas tecnologías para mejorar la ciberseguridad.

Palabras clave: inteligencia artificial, phishing, ciberseguridad, seguridad informática

Abstract

This study analyzes the use of artificial intelligence (AI) for the detection and prevention of phishing, a cybercrime that affects the security of personal data and economic resources. A mixed-method

approach was used, combining quantitative and qualitative methods. Data collection was conducted through surveys of 95 merchants and professionals in Daule, Ecuador, who answered questions about their experience with fraudulent emails, suspicious messages, and phishing-related phone calls. A document review was also conducted to complement and contextualize the findings. The results indicated that 87% of respondents have received fraudulent emails, 86% have received suspicious messages, and 74% have been a victim or know someone affected by phone phishing. Regarding perceptions of AI, 59% consider it a trustworthy tool, and 68% feel more secure when a platform uses it to protect their data. Descriptive statistical analysis showed a mean of 3.82 with low dispersion, reflecting a general trend toward acceptance of AI as a solution. The conclusion is that, although AI is a valuable tool, it is necessary to promote digital education and increase trust in these technologies to improve cybersecurity.

Keywords: artificial intelligence, phishing, cybersecurity, computer security

Cómo citar: León Naranjo, J. R., Oleas Morán, M. M., & Pimentel Salazar, K. Z. (2025). El papel de la inteligencia artificial en la detección del phishing: un enfoque descriptivo sobre su impacto en la ciberseguridad. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 6 (4), 2330 – 2340. https://doi.org/10.56712/latam.v6i4.4437*

INTRODUCCIÓN

El phishing es una forma de delito informático que afecta de manera considerable a tres aspectos esenciales: la reputación de las marcas, la privacidad de los datos personales y los recursos económicos de los usuarios. Cervieri, V. & Pavón, C. (2025). La información digital se ha transformado en un recurso de alto valor dentro del entorno criminal. Los ciberdelincuentes no solo la sustraen, sino que también la comercializan y la utilizan con fines ilícitos, obteniendo beneficios económicos y facilitando otras formas de delito. Además, las amenazas híbridas impulsadas por actores maliciosos encuentran sustento en esta economía delictiva basada en datos. Estas observaciones forman parte de las conclusiones centrales del informe IOCTA, elaborado por Europol para analizar la evolución y las tendencias actuales en el ámbito de la ciberdelincuencia.

Durante los años 2024 y 2025, se llevaron a cabo diversas operaciones internacionales, lideradas por Europol y otras entidades de seguridad, que lograron desmantelar importantes plataformas vinculadas al cibercrimen. Una de ellas fue LabHost32, un sitio que ofrecía kits de phishing, servicios de alojamiento e interacción directa con las víctimas mediante una suscripción mensual, y que estaba asociado a más de 40,000 dominios fraudulentos y aproximadamente 10,000 usuarios en todo el mundo. De forma paralela, se observó un notable auge en el comercio ilegal de accesos a sistemas comprometidos, actividad protagonizada por los llamados Corredores de Acceso Inicial (IAB), cuyos precios aumentaron cerca de un 50 %. Asimismo, en enero de 2025 se logró desactivar los foros Cracked y Nulled, considerados dos de las plataformas más influyentes en la distribución de datos robados y herramientas para ciberataques. Ambas ofrecían servicios respaldados por inteligencia artificial y acumulaban millones de usuarios, generando ingresos significativos a través de actividades delictivas.

El fraude digital, en particular la modalidad conocida como phishing, ha evolucionado significativamente con el avance de las tecnologías digitales. En este contexto, la inteligencia artificial (IA) se destaca como un factor transformador, que, aunque puede ser utilizada para fortalecer la ciberseguridad, también es explotada por los delincuentes cibernéticos para optimizar, ampliar y sofisticar sus métodos fraudulentos. El phishing implica el uso de técnicas de ingeniería social con el objetivo de engañar a los usuarios para obtener datos sensibles, como credenciales y datos bancarios, a través de correos electrónicos, mensajes o sitios web falsificados.

La inteligencia artificial comprende un conjunto de tecnologías que emulan procesos cognitivos humanos, como el aprendizaje y la toma de decisiones, utilizando modelos avanzados de aprendizaje automático y generativos. En el ámbito del phishing, la IA posibilita la automatización de ataques mediante la creación de mensajes altamente personalizados, multilingües y contextualmente adecuados en tiempos muy breves. Además, mejora las técnicas de ingeniería social mediante el análisis de grandes cantidades de datos personales, lo que hace que los mensajes fraudulentos sean más convincentes y están dirigidos a objetivos específicos. Esta tecnología también facilita la escalabilidad de los ataques, permitiendo su ejecución masiva con mínima intervención humana, y ayuda a evadir los sistemas de detección al modificar continuamente los mensajes para evitar los filtros de spam y otros mecanismos de seguridad tradicionales.

El objetivo de la presente investigación es analizar la relación entre el uso de técnicas de inteligencia artificial en campañas de phishing y la efectividad de estos fraudes digitales, con el fin de identificar patrones y factores que influyen en su éxito. En este contexto, es relevante llevar a cabo un análisis correlacional que permita identificar la relación estadística entre el uso de la inteligencia artificial en campañas de phishing y la efectividad de estos fraudes digitales. Este enfoque cuantitativo posibilita medir el impacto real de la IA en las tasas de éxito del phishing, descubrir patrones y tendencias emergentes, y anticipar la evolución de ataques más sofisticados. De igual forma, los resultados

obtenidos pueden contribuir al diseño de estrategias de prevención y detección adecuadas a los retos que plantea la evolución tecnológica.

METODOLOGÍA

La investigación adoptó un enfoque mixto, el abordaje cualitativo consistió en una revisión cuidadosa y profunda de diversas fuentes secundarias. Se consultaron textos de tesis y artículos científicos relacionados con el Phishing o fraude digital, y de qué forma representa una amenaza real y constante para nuestra seguridad en internet. También se revisaron estudios recientes sobre el papel de la inteligencia artificial en la detección del phishing: y construir un marco conceptual sólido y conectado con la realidad actual. Además, se incorporó un componente cuantitativo, basado en el análisis descriptivo e inferencial de los datos obtenidos a través de una encuesta a comerciantes y profesionales de Daule, Ecuador 2025.

La presente investigación es del tipo aplicada, ya que busca resolver un problema práctico como es la detección y prevención de ataques de phishing a través de la IA; el estudio corresponde a un diseño no experimental del tipo descriptivo y posee un enfoque mixto. El estudio tiene corte transversal debido a que los datos se recolectaron en un solo momento, sin realizar seguimiento a lo largo del tiempo. Este tipo de estudio nos permitió describir situaciones y relaciones entre las variables, también permitió obtener una visión general del estudio sin analizar su evolución temporal. El alcance descriptivo permitió analizar el rol de la inteligencia artificial en la detección del phishing para caracterizar y detallar cómo se emplea la IA al identificar este tipo de ataques cibernéticos, se describe la frecuencia con la que las personas han sido víctimas de phishing, las modalidades más comunes detectadas por sistemas de IA, las herramientas utilizadas, así como la percepción y conocimientos de los usuarios sobre la efectividad de estas tecnologías.

Las fuentes de datos primarias se obtuvieron de la encuesta a los participantes para conocer de parte de comerciantes y profesionales de Daule, Ecuador, 2025. Las fuentes de datos secundarias fueron obtenidas de tesis y artículos científicos sobre las variables de estudio y permitieron elaborar el marco teórico de este trabajo. Se optó por el uso de un cuestionario como instrumento principal para la recolección de datos, el cual fue aplicado a estudiantes de la carrera de Ingeniería en software, con el propósito de conocer su apreciación sobre la detección del Phishing, consideradas como la variable dependiente. El cuestionario está formado por 12 preguntas con cinco alternativas en la escala de Likert: Totalmente de acuerdo (5), De acuerdo (4), ni de acuerdo ni en desacuerdo (3), en desacuerdo (2) y totalmente en desacuerdo (1). La elaboración del cuestionario estuvo a cargo del investigador, quien asumió plenamente esta responsabilidad.

En cuanto a la técnica empleada, se utilizó la encuesta, un método de investigación ampliamente usado para obtener información de una muestra representativa del grupo estudiado. Según Hernández Sampieri (2018), las encuestas son herramientas frecuentes en estudios de enfoque cuantitativo, ya que permiten recolectar y organizar datos de manera eficiente y rápida, incluso cuando se trata de grandes volúmenes de personas. Se aseguró que todos los participantes comprendieran el propósito del estudio y consientan su participación de manera informada; se garantizó la confidencialidad y anonimato de los datos recopilados, y se tomaron medidas para minimizar cualquier potencial riesgo o inconveniente para los participantes. Además, se proporcionó a los participantes la opción de retirar su consentimiento y dejar de participar en cualquier momento sin repercusiones.

Se realizó un análisis descriptivo e inferencial; el análisis descriptivo se aplicó a los datos recolectados del cuestionario aplicado, y tuvo como objetivo organizar y resumir la información mediante estadísticas como frecuencias, porcentajes, promedios y gráficos. El análisis inferencial se aplicó a los datos cuantitativos obtenidos de la muestra, con el fin de hacer generalizaciones o predicciones sobre una población más amplia. La población total fue 125 comerciantes de la zona urbana de Daule, los

cuales ejercen su actividad comercial con la venta de artículos varios (ropa, calzado, celulares, electrométricos, camas, colchones, entre otros). La gran mayoría ha recibido alguna vez correos, mensajes y llamadas sospechosas.

En la presente investigación se utilizó una muestra probabilística, debido a que la población es grande (más de 100). La muestra representativa correspondió a 95 comerciantes. Con un nivel de confianza del 95%, y un margen de error del 5%. Para el cálculo se aplicó la fórmula para una población finita.

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{e^2 \cdot (N-1) + Z^2 \cdot p \cdot (1-p)}$$

$$n = \frac{125 \cdot (1.96)^2 \cdot 0.5 \cdot 0.5}{(0.05)^2 \cdot (125-1) + (1.96)^2 \cdot 0.5 \cdot 0.5}$$

$$n = \frac{125 \cdot 3.8416 \cdot 0.25}{0.0025 \cdot 124 + 0.9604}$$

$$n = \frac{120.05}{0.31 + 0.9604} = \frac{120.05}{1.2704} \approx 94.5$$

Tabla 1

Total de comerciantes

		F	%
Válido	Hombres	57	60
	Mujeres	38	40
	Total	95	100

Fuente: Asociación de comerciantes del Cantón Daule.

RESULTADOS

Pregunta 1: ¿He escuchado sobre el uso de inteligencia artificial para detectar correos electrónicos maliciosos?

Tabla 2

Uso de la IA para detectar correos maliciosos

		F	%
Válido	Totalmente en desacuerdo	10	11
	En desacuerdo	15	16
	Ni de acuerdo ni en desacuerdo	21	22
	De acuerdo	28	29
	Totalmente de acuerdo	21	22
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

La mayoría de los encuestados (51%) indicó estar de acuerdo o totalmente de acuerdo con la afirmación “He escuchado sobre el uso de inteligencia artificial para detectar correos electrónicos

maliciosos", lo que refleja un nivel general de conocimiento o familiaridad con esta aplicación de la IA. Sin embargo, un 27% expresó desacuerdo y un 22% se mantuvo en una posición neutral, lo que sugiere que, aunque existe una tendencia positiva hacia el reconocimiento de esta tecnología, aún hay una proporción considerable de personas que no están informadas o no tienen una postura clara al respecto.

Pregunta 2: ¿Considero que las herramientas de IA pueden identificar patrones sospechosos mejor que los humanos?

Tabla 3

IA para identificar patrones

		F	%
Válido	Totalmente en desacuerdo	15	16
	En desacuerdo	14	15
	Ni de acuerdo ni en desacuerdo	24	25
	De acuerdo	20	21
	Totalmente de acuerdo	22	23
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 44% de los encuestados cree que las herramientas de IA identifican patrones sospechosos mejor que los humanos, mostrando una percepción positiva moderada. Sin embargo, un 31% no está de acuerdo y un 25% se mantiene neutral, lo que indica dudas y falta de claridad sobre el tema. Esta división sugiere la necesidad de mayor información y formación sobre el potencial de la IA en la detección de amenazas.

Pregunta 3: ¿Conozco que existen sistemas automáticos que bloquean intentos de phishing gracias a algoritmos de IA?

Tabla 4

Sistemas automáticos que bloquean el phishing

		F	%
Válido	Totalmente en desacuerdo	14	15
	En desacuerdo	15	16
	Ni de acuerdo ni en desacuerdo	25	26
	De acuerdo	19	20
	Totalmente de acuerdo	22	23
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 43% de los encuestados está de acuerdo o totalmente de acuerdo en conocer sistemas automáticos basados en IA para bloquear phishing, indicando un nivel moderado de familiaridad con esta tecnología. Sin embargo, el 31% no está de acuerdo y un 26% permanece neutral, lo que refleja que una parte importante de la población no está suficientemente informada o no tiene una postura clara sobre el tema. Esto resalta la necesidad de fortalecer la difusión y educación sobre las capacidades de la inteligencia artificial en la prevención de ataques de phishing.

Pregunta 4: ¿He recibido correos electrónicos que intentaban engañarme para que proporcione datos personales?

Tabla 5

Correos electrónicos engañosos

		F	%
Válido	Totalmente en desacuerdo	1	1
	En desacuerdo	1	1
	Ni de acuerdo ni en desacuerdo	10	11
	De acuerdo	36	38
	Totalmente de acuerdo	47	49
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

La gran mayoría de los encuestados (87%) está de acuerdo o totalmente de acuerdo en haber recibido correos electrónicos que intentaban engañarlos para obtener información personal, lo que evidencia que este tipo de intentos de phishing son muy frecuentes. Solo un 2% negó haber recibido estos correos y un 11% se mostró neutral, lo que indica que casi todos los participantes han tenido experiencia con este tipo de amenaza. Esto subraya la importancia de aumentar la conciencia y las medidas de protección contra correos maliciosos.

Pregunta 5: ¿He recibido mensajes sospechosos por SMS o WhatsApp con enlaces dudosos?

Tabla 6

Mensajes sospechosos

		F	%
Válido	Totalmente en desacuerdo	2	2
	En desacuerdo	2	2
	Ni de acuerdo ni en desacuerdo	9	9
	De acuerdo	36	38
	Totalmente de acuerdo	46	48
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 86% de los encuestados está de acuerdo o totalmente de acuerdo en haber recibido mensajes sospechosos con enlaces dudosos a través de SMS o WhatsApp, indicando que esta forma de intento de fraude es muy común. Solo un 4% negó haber recibido estos mensajes y un 9% se mostró neutral, lo que refleja que la mayoría de los participantes han sido expuestos a este tipo de amenazas digitales, subrayando la necesidad de fortalecer la educación y las precauciones en el uso de plataformas de mensajería.

Pregunta 6: ¿He sido víctima o conozco a alguien que ha sido víctima de phishing por una llamada telefónica?

Tabla 7

Víctima de Phishing

		F	%
Válido	Totalmente en desacuerdo	3	3
	En desacuerdo	4	4
	Ni de acuerdo ni en desacuerdo	18	19
	De acuerdo	34	36
	Totalmente de acuerdo	36	38
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 74% de los encuestados está de acuerdo o totalmente de acuerdo en haber sido víctima o conocer a alguien que lo ha sido a través de phishing telefónico, lo que indica que esta modalidad de fraude es bastante frecuente y afecta a una gran parte de la población. Un 7% negó esta experiencia y un 19% se mostró neutral, reflejando que, aunque la mayoría ha tenido contacto con este tipo de casos, todavía hay personas que no están seguras o no lo han experimentado directamente. Esto resalta la importancia de promover mayor conciencia y prevención contra el phishing por llamadas.

Pregunta 7: ¿La inteligencia artificial es una herramienta confiable para prevenir ataques de phishing?

Tabla 8

IA Herramienta confiable

		F	%
Válido	Totalmente en desacuerdo	5	5
	En desacuerdo	8	8
	Ni de acuerdo ni en desacuerdo	26	27
	De acuerdo	29	31
	Totalmente de acuerdo	27	28
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 59% de los encuestados considera que la inteligencia artificial es una herramienta confiable para prevenir ataques de phishing, al estar de acuerdo o totalmente de acuerdo con la afirmación. Esto refleja una percepción mayormente positiva sobre la capacidad de la IA en ciberseguridad. Sin embargo, un 27% de los participantes se mantiene neutral y un 13% expresa desacuerdo, lo cual indica que aún hay cierto nivel de desconocimiento o escepticismo respecto al papel de la IA en este ámbito. Estos resultados sugieren que, si bien existe una aceptación creciente, es necesario seguir fortaleciendo la confianza a través de información, formación y evidencia práctica del uso efectivo de estas tecnologías.

Pregunta 8: ¿Me siento seguro(a) si una plataforma usa inteligencia artificial para proteger mis datos?

Tabla 9

Seguridad en plataforma con IA

		F	%
Válido	Totalmente en desacuerdo	1	1
	En desacuerdo	1	1
	Ni de acuerdo ni en desacuerdo	29	31
	De acuerdo	31	33
	Totalmente de acuerdo	33	35
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 68% de los encuestados se siente seguro al saber que una plataforma utiliza inteligencia artificial para proteger sus datos, lo que refleja una confianza mayoritaria en la IA aplicada a la seguridad digital. Solo un 2% expresó desconfianza y un 31% se mantuvo neutral, lo que indica que, aunque la percepción es positiva en general, hay un grupo significativo de usuarios que aún no tiene una postura clara o no comprende del todo el funcionamiento de estas tecnologías. Esto sugiere que fortalecer la comunicación sobre cómo la IA protege los datos personales puede contribuir a mejorar la percepción de seguridad entre los usuarios.

Pregunta 9: ¿Las soluciones de ciberseguridad actuales deberían integrar más tecnologías de IA?

Tabla 10

Ciberseguridad con IA

		F	%
Válido	Totalmente en desacuerdo	3	3
	En desacuerdo	6	6
	Ni de acuerdo ni en desacuerdo	32	34
	De acuerdo	25	26
	Totalmente de acuerdo	29	31
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 57% de los encuestados está de acuerdo o totalmente de acuerdo en que las soluciones de ciberseguridad deberían integrar más tecnologías de inteligencia artificial, lo que indica una actitud mayoritariamente favorable hacia el fortalecimiento de la ciberseguridad mediante IA. Sin embargo, un 34% se mantiene neutral y un 9% está en desacuerdo, lo que sugiere que, aunque hay aceptación, una parte considerable de la población aún no tiene una postura definida o desconoce los beneficios concretos de esta integración. Esto resalta la necesidad de mayor información y evidencia práctica sobre el aporte real de la IA en los sistemas de seguridad actuales.

Pregunta 10: ¿Desde que usó herramientas con inteligencia artificial, he notado menos intentos de phishing?

Tabla 11

Herramientas con IA

		F	%
Válido	Totalmente en desacuerdo	4	4
	En desacuerdo	7	7
	Ni de acuerdo ni en desacuerdo	31	33
	De acuerdo	25	26
	Totalmente de acuerdo	28	29
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 55% de los encuestados está de acuerdo o totalmente de acuerdo en que ha notado una reducción en los intentos de phishing desde que utiliza herramientas con inteligencia artificial, lo que refleja una percepción mayoritariamente positiva sobre su efectividad. Sin embargo, un 33% se mantiene neutral y un 11% expresa desacuerdo, lo que indica que una parte significativa aún no percibe cambios claros o no tiene certeza sobre el impacto real de estas herramientas. Estos datos sugieren que, aunque la IA es vista como útil por la mayoría, es necesario seguir promoviendo su uso y demostrar con mayor claridad sus beneficios en la prevención del phishing.

Pregunta 11: ¿Creo que el uso de IA ha reducido el riesgo de ser víctima de ataques cibernéticos?

Tabla 12

Uso de IA y reducción de riesgo

		F	%
Válido	Totalmente en desacuerdo	6	6
	En desacuerdo	7	7
	Ni de acuerdo ni en desacuerdo	32	34
	De acuerdo	26	27
	Totalmente de acuerdo	24	25
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 52% de los encuestados está de acuerdo o totalmente de acuerdo en que el uso de inteligencia artificial ha reducido su riesgo de ser víctima de ataques cibernéticos, lo que indica una percepción moderadamente positiva sobre su efectividad en la protección digital. Sin embargo, un 34% se mantiene neutral y un 13% no está de acuerdo, lo que refleja que una parte importante aún no tiene una opinión clara o no percibe beneficios directos. Esto sugiere que, si bien más de la mitad confía en el impacto positivo de la IA, aún es necesario fortalecer la comunicación y evidencia sobre cómo la IA contribuye a la ciberseguridad personal.

Pregunta 12: ¿Considero que las empresas que implementan IA están mejor protegidas contra el phishing?

Tabla 13

Implementación de la IA

		F	%
Válido	Totalmente en desacuerdo	5	5
	En desacuerdo	8	8
	Ni de acuerdo ni en desacuerdo	34	36
	De acuerdo	26	27
	Totalmente de acuerdo	22	23
	Total	95	100

Nota: Análisis estadístico Microsoft Excel.

El 50% de los encuestados está de acuerdo o totalmente de acuerdo en que las empresas que usan inteligencia artificial están mejor protegidas contra el phishing, lo que refleja una percepción positiva moderada sobre el impacto de la IA en la ciberseguridad empresarial. No obstante, un 36% se mantiene neutral y un 13% está en desacuerdo, lo que indica que una parte importante de los participantes aún no tiene una postura clara o confía poco en la efectividad de la IA en este contexto. Esto sugiere la necesidad de mayor difusión de casos reales y evidencia concreta del valor de la IA en la protección empresarial frente a amenazas cibernéticas como el phishing.

Tabla 14

La IA en la detección del Phishing

Nota: Estadístico Descriptivo SPSS.

Estadísticos Descriptivos

	N	Media	Desv Std	Mínimo	Máximo
IA	95	3,82	,31	NI DE ACURDO NI DESACUERDO	4,25
N Válido (listwise)	96				
Missing N (listwise)	1				

El estudio descriptivo de la variable IA, basado en una muestra válida de 95 personas, muestra una media de 3,82 y una desviación estándar de 0,31, lo que indica una tendencia general al acuerdo por parte de los encuestados. El valor mínimo registrado corresponde a una postura neutral ("Ni de acuerdo ni en desacuerdo") y el máximo alcanzó 4,25, lo que sugiere que las respuestas se ubicaron mayormente en los niveles más altos de la escala, con poca dispersión entre ellas. La baja variabilidad en las respuestas sugiere una percepción común entre los participantes en relación con la IA. En resumen, se evidencia una actitud mayoritariamente positiva frente a la temática evaluada, lo cual podría ser un punto de partida para futuros estudios comparativos o análisis más profundos por subgrupos.

DISCUSIÓN

Los resultados de este estudio indican que la inteligencia artificial (IA) está empezando a convertirse en una solución relevante para la guerra contra el phishing, pero aún persisten la falta de conocimiento y la percepción del usuario. En primer lugar, más de la mitad (51%) de los encuestados afirma ser consciente del uso de la IA en la monitorización del correo electrónico malicioso, lo que muestra un entendimiento razonable del tema en general. Por el contrario, el 27% no está de acuerdo y el 22% ni

está de acuerdo ni en desacuerdo, lo que deja mucho margen para garantizar una mayor comprensión y promoción de esta tecnología y sus usos.

Sobre la cuestión de la capacidad de la IA para detectar patrones sospechosos, el 44% dice que puede hacerlo de manera más efectiva que los humanos, mientras que el 31% dice que no puede y el 25% no está seguro. Esta distribución nos advierte contra confiar completamente en dicha tecnología o asumir que su valor es evidente por sí mismo y nos recuerda la importancia de la formación y la confianza en los sistemas automáticos, incluso cuando están respaldados por probabilidades estadísticas, o más probablemente en parte debido a que lo están.

Con respecto a los sistemas automáticos que previenen el phishing, el 43% indica que los conoce, el 31% no y el 26% es neutral. Esto es consistente con nuestro objetivo principal de evaluar el nivel de conocimiento y sugiere la ausencia de información suficiente entre los usuarios finales, a pesar del aumento de la exposición a estos sistemas.

Por otro lado, los datos indican que el phishing es una amenaza frecuente que la mayoría de los visitantes han experimentado. El 87% dijo haber recibido correos electrónicos fraudulentos y el 86% sospecha de mensajes de SMS o WhatsApp. Un similar 74% ha sido víctima o conoce a alguien afectado por el phishing a través de una llamada telefónica. Esto respalda lo que destacamos anteriormente en el contexto: que Ecuador es uno de los países con el mayor número de este tipo de delitos en la región.

El 59% cree que la IA es una herramienta efectiva contra el phishing y el 68% está menos preocupado al utilizar plataformas que emplean IA de esta manera. Si bien estas cifras son prometedoras, la presencia de valores intermedios en las respuestas (entre el 27% y el 34% en los diferentes ítems) nos advierte que existe una brecha entre la utilización de la IA y el impacto real que tiene, lo cual consideramos importante abordar para aumentar la efectividad de estos dispositivos.

Es más, el 57% desearía que sus soluciones de ciberseguridad incluyeran tecnologías de IA de manera más generalizada, lo que indica una aceptación generalmente positiva de su inclusión, y el 55% ha visto una disminución en los intentos de phishing al utilizar herramientas potenciadas por IA. No obstante, entre el 11% y el 13% de los encuestados no observa beneficios directos de la IA, por lo que existe la posibilidad de que la IA se confirme como una solución tangible y efectiva en la experiencia del usuario.

El cincuenta por ciento dice que las empresas con IA están mejor equipadas para defenderse contra el phishing, mientras que el 36% no está seguro. Estos datos confirman la percepción ambivalente de la efectividad en el mundo corporativo, donde los empleados conocen la IA, pero carecen de una comprensión profunda del poder real de la IA en los negocios.

En resumen, los resultados están en línea con el objetivo general del estudio: que la IA es efectiva para combatir el phishing y es vista de manera positiva por muchos usuarios. Pero también subrayan cómo la información, la confianza y la conciencia sobre su utilidad, ya sea personal o profesional, podrían mejorarse. Por lo tanto, es necesario construir educación digital, fomentar historias de éxito y facilitar el acceso a herramientas de IA que protejan al usuario común, en consonancia con este contexto y la urgencia de fortalecer la ciberseguridad para enfrentar los ataques cada vez más frecuentes en Ecuador y en el mundo.

CONCLUSIONES

Los resultados obtenidos en nuestra investigación nos permiten suponer que la inteligencia artificial (IA) jugará un papel muy significativo en la identificación y prevención de ataques de phishing, incluyendo no solo la seguridad individual, sino también la organizacional. La mayoría de los encuestados reportan haber experimentado intentos de phishing y, en general, responden

positivamente hacia la IA en la lucha contra ellos. Sin embargo, también existen importantes brechas en el entendimiento, percepción y confianza en cómo realmente funcionan y lo hacen de manera eficiente.

Aunque más de la mitad es consciente del papel de la IA en la detección de correos electrónicos maliciosos, y una proporción similar cree que tiene un impacto directo en su seguridad digital, muchos no están impresionados o son cínicos. Esta conclusión deja claro cuánto trabajo tenemos que hacer en términos tanto de cultura mediática computacional como del conocimiento público sobre por qué la IA puede detener el phishing, no solo como software, sino como un aliado estratégico, no solo en el trabajo.

Otro dato interesante es que el phishing sigue siendo una amenaza significativa en Ecuador y requiere una buena medida tecnológica para enfrentarlo. Aunque la invasión de la IA está más extendida y el impacto de la IA no es aún claro para todos, es importante avanzar tanto en la implementación como en la concienciación y poder cristalizar los beneficios percibidos.

En resumen, este documento apoya la misión última de examinar el papel de la IA en la ciberseguridad: que su éxito depende no solo de las habilidades técnicas, sino también de la confianza, el entendimiento y la adopción por parte de los usuarios finales. Para impulsar un mundo digital más seguro, deberán promoverse métodos de formación, reforzarse la protección digital y garantizarse un acceso justo a los recursos basados en IA que realmente protejan a los usuarios contra ataques de ingeniería social inteligente.

REFERENCIAS

Becerril, A. A. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DEPUEBLA, MÉXICO, 48. Recuperado el 20 de Mayo de 2025, de https://revistaius.com/index.php/ius/article/view/705/794

Benavides, E. et al (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura https://doi.org/10.18779/cyt.v13i1.357

Bolaño García, M., & Duarte Acosta, N. (2024). Una revisión sistemática del uso de la inteligencia artificial en la educación. Revista Colombiana de Cirugía, 39(1), 51-63. https://doi.org/10.30944/20117582.2365

Castro, J. (28 de Julio de 2022). Corponet. Recuperado el 20 de Mayo de 2025, de Corponet: https://blog.corponet.com/ciberseguridad-concepto-tipos-amenazas-estrategias

Cervieri, V. & Pavón, C. (2025). El Phishing como Delito de Triple Impacto: Marcas, Datos Personales y Afectación del Patrimonio. https://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/30902/27411

EL COMERCIO. (15 de Abril de 2024). El Comercio. Recuperado el 19 de Mayo de 2025, de El Comercio: https://www.elcomercio.com/tecnologia/enlaces-falsos-phising-estafas-internet-ayuda.html

Elternativa, D. D. M. (2021). Historia de la inteligencia artificial: Origen y auge de la IA. www.elternativa.com. https://www.elternativa.com/historia-inteligencia-artificial/

Europol, Robar, negociar y repetir - Cómo los ciberdelincuentes comercian y explotan sus datos - Evaluación de la amenaza de la delincuencia organizada en Internet, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2025. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

Forero Corba, W., & Negre Bennásar, F. (2024). Técnicas y aplicaciones del Machine Learning e inteligencia artificial en educación: Una revisión sistemática. RIED. Revista iberoamericana de educación a distancia. https://doi.org/10.5944/ried.27.1.3749

Franganillo, J. (2023). La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos. methaodos.revista de ciencias sociales, 11(2), m231102a10. http://dx.doi.org/10.17502/mrcs.v11i2.710

IBM. (12 de Agosto de 2024). IBM. Recuperado el 20 de Mayo de 2025, de IBM: https://www.ibm.com/es-es/security

Kosinski, M. (17 de Mayo de 2024). IBM. Recuperado el 20 de Mayo de 2025, de IBM: https://www.ibm.com/es-es/think/topics/phishing

López Blanco, M. (2023). Inteligencia artificial en los medios periodísticos. https://hdl.handle.net/20.500.14352/3345

Ocaña-Fernández, Y., Valenzuela-Fernández, L. A., & Garro-Aburto, L. L. (2019). Inteligencia artificial y sus implicaciones en la educación superior. Propósitos y Representaciones, 7(2), 536-568. https://doi.org/10.20511/pyr2019.v7n2.274

PRIMICIAS. (7 de Noviembre de 2023). Primicias. Recuperado el 19 de Mayo de 2025, de Primicias: https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-

phishing/#:~:text=En%20toda%20Am%C3%A9rica%20Latina%2C%20Ecuador,un%20ciberdelincuente%20dedicado%20al%20phishing.&text=Ecuador%20sigue%20acechado%20por%20los,datos%20sensibles%20de%20

Redia. (17 de Junio de 2024). REDiA. Recuperado el 20 de Mayo de 2025, de REDiA: https://rediai.org/john-mccarthy-origen-de-la-ia

Regulación de la Inteligencia Artificial, ¿Compatibilidad con la Protección de Datos Personales? (s. f.). Recuperado 4 de julio de 2024, https://www.dentons.com/es/insights/articles/2024/february/16/regulacion-de-la inteligencia-artificial

Rosero, L. (2021). El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático. http://dspace.ups.edu.ec/handle/123456789/21699

Rouse, M. (2021). ¿Qué es Inteligencia artificial o IA? - Definición en Computer Weekly. ComputerWeekly.es. artificial-o-IA https://www.computerweekly.com/es/definicion/Inteligencia

Takeyas, B. L. (2007). INTRODUCCIÓN A LA INTELIGENCIA ARTIFICIAL. Instituto Tecnológico de Nuevo Laredo, 3. Recuperado el 20 de Mayo de 2025, de https://d1wqtxts1xzle7.cloudfront.net/95659120/ARTICULO_Introduccion_a_la_Inteligencia_Artificial_1_-libre.pdf?1670872226=&response-content-disposition=inline%3B+filename%3DARTICULO_Introduccion_a_la_Inteligencia.pdf&Expires=1747761457&Signature=VHM1OQg~q

UNESCO. (2022). Recomendación sobre la ética de la inteligencia artificial. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Valenzuela, P. R., & Fernández, N. A. D. (2024). Estudios sobre la inteligencia artificial como herramienta del diseño gráfico: Una investigación documental. Artificio. https://revistas.uaa.mx/index.php/artificio/article/view/4772

Vidovic López, J. F., & Villasmil Espinoza, J. J. (2024). Reflexiones esenciales sobre las implicaciones éticas de uso de la inteligencia artificial en la elaboración de artículos científicos de alto impacto. Multiverso https://doi.org/10.46502/issn.2792-3681/2024.6.0