Vulnerabilidad de estudiantes ante ataques de Phishing

Vulnerability of students to phishing sttacks

Rebeca del Carmen Molina Hernández
https://orcid.org/0009-0002-7479-8310
rebeca.molina@ucn.edu.ni
Universidad Central de Nicaragua. Nicaragua

Hilder Amílcar Olivas Doña
https://orcid.org/0009-0006-1378-7625
hilder.olivas@ucn.edu.ni
Universidad Central de Nicaragua. Nicaragua

DOI: https://doi.org/10.61454/88z0zw71

Resumen

El uso de medios digitales por estudiantes universitarios ha incrementado su susceptibilidad de exposición de su información personal y académica. Este estudio tuvo como finalidad determinar la vulnerabilidad de los estudiantes de la Universidad Central de Nicaragua durante 2025 ante ataques de phishing por correo electrónico y mensajes de texto, además se analizó su posible asociación con variables sociodemográficas como edad, sexo, año académico y carrera mediante un enfoque cuantitativo de tipo correlacional. Se planteó como hipótesis la existencia de una proporción significativo de vulnerabilidad frente a ataques de phishing (p=0.5), con asociaciones con las variables mencionadas con anterioridad. La población estuvo conformada por 700 estudiantes de diversas carreras, y mediante muestreo aleatorio simple, con un nivel de confianza del 95% y un margen de error del 5%, se seleccionó una muestra de 249 estudiantes con correo electrónico registrado en la base de datos institucional. Los datos se analizaron mediante frecuencias, porcentaje e intervalos de confianza. Para determinar asociaciones se aplicó la prueba de chi-cuadrado de independencia; cuando no se cumplieron los supuestos, se recurrió al método de Monte Carlo y la prueba exacta de Fisher. El 36,9% resultó vulnerable, con proporción ligeramente mayor en mujeres, sin asociaciones significativas con variables sociodemográficas. Los estudiantes más jóvenes y de primeros años presentaron mayor cantidad de casos de vulnerabilidad. Esto destaca la necesidad de implementar estrategias de concientización y formación en ciberseguridad, así como explorar nuevas variables que permitan comprender mejor los factores que influyen en la susceptibilidad ante ataques de phishing.

Palabras Clave

ciberseguridad, seguridad de los datos, Ciberataque, Phishing, Ingeniería social, correo electrónico

Abstract

The use of digital media by university students has increased their susceptibility to the exposure of their personal and academic information. This study aimed to determine the vulnerability of students at the Central University of Nicaragua during 2025 to phishing attacks via email and text messages. It also analyzed the potential association of these attacks with sociodemographic variables such as age, sex, academic year, and major using a quantitative correlational approach. The hypothesis was that a significant proportion of students would be vulnerable to phishing attacks (p=0.5), with associations to the aforementioned variables. The population consisted of 700 students from various majors. Using

simple random sampling, with a 95% confidence level and a 5% margin of error, a sample of 249 students with email addresses registered in the institutional database was selected. Data were analyzed using frequencies, percentages, and confidence intervals. The chi-square test of independence was applied to determine associations; when the assumptions were not met, the Monte Carlo method and Fisher's exact test were used. 36.9% of students were found to be vulnerable, with a slightly higher proportion among women, and no significant associations with sociodemographic variables. Younger students and first-year students showed a higher number of cases of vulnerability. This highlights the need to implement cybersecurity awareness and training strategies, as well as to explore new variables that allow for a better understanding of the factors that influence susceptibility to phishing attacks.

Keywords
cybersecurity, data security, cyberattack, phishing, social engineering, electronic mail

Recepción: 30 de septiembre de 2025
Aceptación: 8 de diciembre de 2025

Introducción

En la era digital, los estudiantes universitarios se encuentran cada vez más expuestos a amenazas cibernéticas que comprometen su información personal y académica. Entre estas amenazas, el phishing se destaca como una de las más prevalentes, la cual utiliza técnicas de ingeniería social que explotan factores humanos tales como la confianza, urgencias o falta de conocimiento digital de forma que las personas se vean inducidas a comportamientos que comprometan la seguridad de su información. La vulnerabilidad digital entendida como susceptibilidad de ser afectado por amenazas cibernéticas, aumenta ya que los discentes universitarios por el uso frecuente de plataformas instituciones y herramientas en línea sin la información suficiente en ciberseguridad.

Estudios previos han mostrado la magnitud de esta problemática, entre ellos; Okokpujie et al., (2023), quienes encontraron que el 70.6% de los estudiantes de una universidad nigeriana fueron susceptibles a ataques de phishing, principalmente por desconocimiento en ciberseguridad. Kennet et al., (2023), demostraron que, aunque un porcentaje menor cayó en la trampa, persistía una baja preparación frentes a ataques de ingeniería social. Asimismo, Diaz et al., (2020) evidencian que los usuarios en comunidades académicas muestran patrones específicos de susceptibilidad y comportamiento ante phishing, lo que refuerza la necesidad de educación en ciberseguridad. Du et al., (2024) identifican determinantes de comportamiento que influyen en la adopción de medidas de seguridad entre estudiantes. Asiri et al., (2023) y Blažič y Blažič, (2024) señalan la necesidad de combinar soluciones tecnológicas inteligentes con la educación en ciberseguridad para reducir estos riesgos.

Otros estudios pertinentes como el de Alqahtani et al., (2025) y Morrow, (2024) destacan que la población universitaria es un grupo de riesgo debido a la exposición a plataformas digitales y el poco hábito de verificación de correos electrónicos; Dubovecka, (2024) afirma que la edad y el nivel académico no siempre predicen la vulnerabilidad ante phishing, pero identifica tendencias descriptivas de mayor susceptibilidad en estudiantes jóvenes; Kavvadias et al., (2024) y Abroshan (2021) coinciden en que pese a que las diferencias por sexo no son significativas, las mujeres pueden mostrar una vulnerabilidad mayor. Molina-Granja et al., (2025), Jiménez Sánchez et al., (2025), Rama et al., (2025) y Aguilar Ojeda et al., (2024) enfatizan la importancia de la formación en ciberseguridad y estrategias de concientización estructuradas reducen la vulnerabilidad estudiantil.

En otro aspecto Alsharif et al., (2022) y Armas y Taherdoost, (2025) destacan cómo los errores, falta de conciencia y malas prácticas, contribuyen a la ciberseguridad débil, así como el estudio de Yoro et al., (2023) y Ahmead et al., (2024), quienes investigan los comportamientos de las personas en líneas de riesgo y sugieren la urgente necesidad de educación, capacitación y conciencia en ciberseguridad en instituciones universitarias.

De aquí, que el presente estudio tiene como objetivo analizar y caracterizar el grado de vulnerabilidad digital de los estudiantes de la Universidad Central de Nicaragua, sede Jinotepe, frente a ataques de phishing durante el año 2025. Se busca identificar la relación entre vulnerabilidad y variables sociodemográficas como sexo, carrera y edad, así como evaluar la efectividad de la concienciación en ciberseguridad como factor protector.

La importancia de esta investigación radica en que sus resultados permitirán diseñar estrategias de prevención adaptadas al contexto universitario, fomenta la resiliencia digital, es decir, la capacidad de los estudiantes de protegerse y recuperarse ante incidentes cibernéticos, y contribuyendo a la formación de ciudadanos capaces de desenvolverse de manera segura en entornos virtuales.

Diseño y método

El presente estudio adoptó un enfoque cuantitativo de alcance correlacional, en donde el interés central fue cuantificar la proporción de estudiantes vulnerables ante ataques de phishing de la Universidad Central de Nicaragua, sede Jinotepe y evaluar su asociación con factores sociodemográficos como el sexo, por rango de edades y carrera. La vulnerabilidad fue determinada mediante simulaciones de diversos ataques por correo electrónico, entre los que se destacan phishing por correo electrónico y por mensajes de texto.

La población de estudio estuvo compuesta por 700 estudiantes de la modalidad cuatrimestral de las carreras de Ingeniería en sistemas, Banca y Finanzas, Administración de empresas, Contabilidad Pública y Auditoría, Mercadotecnia, Farmacia, Relaciones Internacionales y Comercio Exterior, Administración Turismo y Hotelería, de los cuales, con un nivel de confianza del 95% y un margen de error de 5% se seleccionaron a 249 estudiantes que tuviesen correo electrónico registrado en la base de datos de la universidad. El método de muestreo empleado fue el muestreo aleatorio simple, y los participantes debían contar con una dirección de correo electrónico registrada en la base de datos de la universidad.

Las simulaciones de ataques se realizaron por medio de Ngrok, Zphisher, Kali Linux y Nmap. con el objetivo de crear escenarios realistas sin afectar sistemas externos. Se diseñaron correos electrónicos y mensajes de texto (SMS) simulados que replicaban becas académicas, una técnica común en ingeniería social. Estos mensajes se enviaron a los correos y números de teléfonos registrados por los estudiantes, además se utilizó un dominio temporal controlado por el equipo de investigación, lo que garantizó que se no emplearan cuentas institucionales reales ni se suplantara la identidad de la universidad.

El procedimiento consistió en la preparación del entorno seguro en Kali Linux, el despliegue de dominios temporales mediante Ngrok y enlaces simulados con Zphisher, que dirigían a páginas de prueba donde únicamente se resgistró la interacción con el usuario, es decir, al hacer click en el enlace, sin recopilar información personal. Nmap se empleó para la verificar la conectividad y seguridad del

entorno antes de cada simulación, lo que garantizó que el entorno estuviese disponible y aislados de sistemas externos.

Las simulaciones se realizaron durante dos semanas en horarios de 10:00 am-11:00am y 0400pm-08:00pm, lo que permitió que lo estudiantes pudiesen participar en condiciones reales de conectividad y disponibilidad tecnológica. Se registró como vulnerables a los estudiantes que hicieron click en los enlaces, tras la finalización de las simulaciones, se realizó un proceso de retroalimentación para informar a los participantes sobre la naturaleza del estudio y fomentar la concientización en ciberseguridad. El estudio se desarrolló bajo principios éticos de consentimiento informado, confidencialidad y no daño, con la aprobación del director de investigación.

Por último, para analizar la vulnerabilidad de los estudiantes frente a estos ataques se aplicó un análisis comparativo por grupos de sexo, carrera y por rangos etarios lo que permitió detectar tendencias relacionadas a la vulnerabilidad de los estudiantes. Para el análisis estadístico inferencial se utilizó SPSS v27, se aplicó la prueba binomial para contrastar si la proporción de estudiantes vulnerables ante ataques de phishing difería del valor teórico de 0.5, posteriormente se empleó la prueba de chi-cuadrado de independencia para examinar la relación entre la vulnerabilidad y variables sociodemográficos, en caso de no cumplirse con los supuestos de la prueba chi-cuadrado se utilizó la prueba de Fisher y Prueba de Monte Carlo, de acuerdo al cumplimiento de los supuestos de cada prueba.

Resultado

Los resultados se organizan según las variables evaluadas, incluyendo la vulnerabilidad global, y se describen las frecuencias y porcentajes correspondientes, desagregados por sexo, edad, año académico y carrera. Asimismo, se incorporan tablas y gráficos que facilitan la interpretación y comparación de la información.

De los 249 estudiantes evaluados, 95 (38,2%) resultaron vulnerables ante los ataques simulados, mientras que 154 (61,8%) no lo fueron. Esto se ve reflejado en la Tabla 1, en donde también según los intervalos de confianza al 95% para la proporción de vulnerables se ubicaron se encuentra entre los 32.5% y 44.2%. La simulación de muestreo basada en 1000, mostró un sesgo de 0.0 y un error estándar de 3.1%. La proporción acumulada indicó que el 100% de los discentes se clasificaron en alguna de las dos categorías.

Tabla 1: *vulnerabilidad de estudiantes*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado	Simulación de muestreo para Porcentaje[a]			
						Sesgo	Error estándar	Intervalo de confianza al 95%	
								Inferior	Superior
Válido	si	95	38,2	38,2	38,2	,0	3,1	32,5	44,2
	no	154	61,8	61,8	100,0	,0	3,1	55,8	67,5
	Total	249	100,0	100,0		,0	,0	100,0	100,0

a. A menos que se indique lo contrario, los resultados de la simulación de muestreo se basan en 1000 muestras de simulación de muestreo

La Tabla 2 muestra una diferencia estadísticamente significativa respecto a la proporción teórica con una significancia (p<.001), lo que indica que el número de estudiantes no vulnerables (62%) fue significativamente mayor a los vulnerables (38%).

Tabla 2: *prueba binomial*

		Categoría	N	Prop. observada	Prop. de prueba	Significación exacta (bilateral)
vulnerabilidad	Grupo 1	no	154	,62	,50	,000
	Grupo 2	si	95	,38		
	Total		249	1,00		

En la Tabla 3 se observa que la mayoría de los participantes mostraron una mayor vulnerabilidad ante ataques de phishing por correo electrónico (E-mail), con una frecuencia de 85 casos, lo que representa el 89,5% del total. En contraste, únicamente 10 participantes (10,5%) resultaron vulnerables ante intentos de phishing por mensajes de texto (SMS).

El análisis de simulación de muestreo, basado en 1000 muestras, indica que el intervalo de confianza al 95% para la vulnerabilidad por SMS se ubica entre 5,3% y 16,8%, mientras que para la vulnerabilidad por E-mail oscila entre 83,2% y 94,7%. El error estándar fue de aproximadamente 3,1% en ambas categorías, y el sesgo fue mínimo (±0,1), lo cual sugiere estabilidad en las estimaciones obtenidas

Tabla 3: *medio utilizado*

						Simulación de muestreo para Porcentaje[a]			
								Intervalo de confianza al 95%	
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado	Sesgo	Error estándar	Inferior	Superior
Válido	SMS	10	10,5	10,5	10,5	,1	3,1	5,3	16,8
	E-MAIL	85	89,5	89,5	100,0	-,1	3,1	83,2	94,7
	Total	95	100,0	100,0		,0	,0	100,0	100,0

a. A menos que se indique lo contrario, los resultados de la simulación de muestreo se basan en 1000 muestras de simulación de muestreo

Al analizar la vulnerabilidad por sexo (Tabla 4), se observó que 37 de 101 estudiantes masculinos (36,6%) y 58 de 148 estudiantes femeninas (39.2%) resultaron vulnerables. La prueba de chi-cuadrado de Pearson (Tabla 5) indicó $\chi^2 = 0,166$, gl = 1, p = 0,684 y la prueba exacta de Fisher p = 0,693,

Tabla 4: ***v****ulnerabilidad por sexo*

			vulnerabilidad		
			si	**no**	**Total**
Sexo	Masculino	Recuento	37	64	101
		% dentro de Sexo	36,6%	63,4%	100,0%
	Femenino	Recuento	58	90	148
		% dentro de Sexo	39,2%	60,8%	100,0%
Total		Recuento	95	154	249
		% dentro de Sexo	38,2%	61,8%	100,0%

Tabla 5: *chi-cuadrado -vulnerabilidad por sexo*

	Valor	gl	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	,166[a]	1	,684		
Corrección de continuidad[b]	,075	1	,783		
Razón de verosimilitud	,166	1	,683		
Prueba exacta de Fisher				,693	,393
Asociación lineal por lineal	,165	1	,684		
N de casos válidos	249				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 38,53.
b. Sólo se ha calculado para una tabla 2x2

En la (Tabla 6) se observa la distribución de la vulnerabilidad ante intentos de phishing según el rango de edades de los participantes. La mayoría de los casos vulnerables se concentraron en el grupo de 17 a 22 años (69,5%), seguido de los grupos de 23 a 28 años (15,8%) y 29 a 34 años (7,4%).

En contraste, los grupos de mayor edad (35 años o más) presentaron frecuencias más bajas de vulnerabilidad (Tabla5). En general, de los 249 participantes, 95 (38,2%) fueron clasificados como vulnerables y 154 (61,8%) como no vulnerables.

La prueba de chi-cuadrado de Pearson (Tabla 7) indicó $\chi^2 = 6{,}104$, gl = 4, p = ,192 y debido a que el 20% de las casillas presentaron valores esperados menores a cinco, se aplicó la prueba exacta de Fisher y la simulación de Monte Carlo mostraron resultados de p= 0.184 y p=0.196

Tabla 6- *Vulnerabilidad *rango de edades*

		vulnerabilidad		
		si	**no**	**Total**
Rango de edades	17-22 años	66	103	169
	23-28 años	15	24	39
	29-34 años	7	13	20
	35-40 años	1	10	11
	41-49 años	6	4	10
Total		95	154	249

Tabla 7- chi-cuadrado -Vulnerabilidad * rango de edades

				Sig. Monte Carlo (bilateral)			Sig. Monte Carlo (unilateral)		
					Intervalo de confianza al 99%			Intervalo de confianza al 99%	
	Valor	gl	Significación asintótica (bilateral)	Significación	Límite inferior	Límite superior	Significación	Límite inferior	Límite superior
Chi-cuadrado de Pearson	6,104[a]	4	,192	,196[b]	,186	,207			
Razón de verosimilitud	6,927	4	,140	,158[b]	,149	,168			
Prueba exacta de Fisher-Freeman-Halton	6,129			,184[b]	,174	,194			
Asociación lineal por lineal	,059[c]	1	,809	,857[b]	,848	,866	,434[b]	,421	,447
N de casos válidos	249								

a. 2 casillas (20,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 3,82.

b. Se basa en 10000 tablas de muestras con una semilla de inicio 617149054.

c. El estadístico estandarizado es ,242.

Al considerar la variable carrera se observa en la Tabla 8 que la carrera con mayor porcentaje de afectación fue Psicología y Farmacia con un 13.7% de estudiantes que presentaron mayor vulnerabilidad, seguidas de Derecho, Administración de empresas e Ingeniería en sistemas. La prueba de chi-cuadrado de Pearson Tabla 9 indicó $\chi^2 = 10,853$, gl = 9, p = ,286y debido tres casillas presentaron valores esperados menores a cinco, se aplicó la prueba exacta de Fisher-Freeman-Halton (p = 0,310) y la simulación de Monte Carlo (p = 0,282; IC99% = 0,271–0,294)

Tabla 8: *Vulnerabilidad *carrera*

		Vulnerabilidad		
		Si	**No**	**Total**
Carrera que cursa	Ingenieria en Sistemas	10	24	34
	Administración	11	17	28
	Psicología	13	18	31
	Derecho	11	22	33
	Farmacia	13	25	38
	Contabilidad Pública y Auditoría	7	20	27
	Mercadotecnia	11	14	25
	Banca y Finanzas	2	0	2
	Relaciones Internacionales y Comercio Exterior	11	9	20
	Administración Turismo y Hotelería	6	5	11
Total		95	154	249

Tabla 9: *chi-cuadrado -Vulnerabilidad * rango de edades*

				Sig. Monte Carlo (bilateral)			Sig. Monte Carlo (unilateral)		
					Intervalo de confianza al 99%			Intervalo de confianza al 99%	
	Valor	gl	Significación asintótica (bilateral)	Significación	Límite inferior	Límite superior	Significación	Límite inferior	Límite superior
Chi-cuadrado de Pearson	10,853[a]	9	,286	,282[b]	,271	,294			
Razón de verosimilitud	11,476	9	,244	,282[b]	,271	,294			
Prueba exacta de Fisher-Freeman-Halton	10,333			,310[b]	,298	,322			
Asociación lineal por lineal	3,901[c]	1	,048	,049[b]	,043	,054	,023[b]	,019	,027
N de casos válidos	249								

a. 3 casillas (15,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,76.
b. Se basa en 10000 tablas de muestras con una semilla de inicio 1335104164.
c. El estadístico estandarizado es -1,975.

Según la Tabla 10 los años con mayor proporción de estudiantes vulnerables fueron Primer Año (35,8%) y Segundo Año (38%), mientras que los años superiores presentaron porcentajes menores. Las pruebas estadísticas confirmaron que no existía asociación significativa (Tabla 11) entre el año cursado y la vulnerabilidad: Chi-cuadrado de Pearson $\chi^2 = 4,192$; gl = 5; p = 0,522, Razón de verosimilitud $\chi^2 = 4,815$; gl = 5; p = 0,439, y Prueba exacta de Fisher-Freeman-Halton p = 0,589.

Tabla 10: *año que cursa*vulnerabilidad*

			vulnerabilidad		
			si	**no**	**Total**
Año que cursa	Primer Año	Recuento	34_a	61_a	95
		% dentro de Año que cursa	35,8%	64,2%	100,0%
	Segundo Año	Recuento	19_a	31_a	50
		% dentro de Año que cursa	38,0%	62,0%	100,0%
	Tercer Año	Recuento	16_a	15_a	31
		% dentro de Año que cursa	51,6%	48,4%	100,0%
	Cuarto Año	Recuento	11_a	22_a	33
		% dentro de Año que cursa	33,3%	66,7%	100,0%
	Quinto Año	Recuento	15_a	23_a	38
		% dentro de Año que cursa	39,5%	60,5%	100,0%
	Sexto Año	Recuento	0_a	2_a	2
		% dentro de Año que cursa	0,0%	100,0%	100,0%
Total		Recuento	95	154	249
		% dentro de Año que cursa	38,2%	61,8%	100,0%

Cada letra del subíndice denota un subconjunto de vulnerabilidad categorías cuyas proporciones de columna no difieren de forma significativa entre sí en el nivel ,05

Tabla 11: *chi-cuadrado: edad * vulnerabilidad*

				Sig. Monte Carlo (bilateral)			Sig. Monte Carlo (unilateral)		
			Significación asintótica (bilateral)		Intervalo de confianza al 99%			Intervalo de confianza al 99%	
	Valor	gl		Significación	Límite inferior	Límite superior	Significación	Límite inferior	Límite superior
Chi-cuadrado de Pearson	4,192[a]	5	,522	,544[b]	,531	,557			
Razón de verosimilitud	4,815	5	,439	,513[b]	,500	,526			
Prueba exacta de Fisher-Freeman-Halton	3,771			,594[b]	,581	,606			
Asociación lineal por lineal	,021[c]	1	,884	,896[b]	,888	,904	,458[b]	,446	,471
N de casos válidos	249								

a. 2 casillas (16,7%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,76.
b. Se basa en 10000 tablas de muestras con una semilla de inicio 957002199.
c. El estadístico estandarizado es -,145.

Discusión

Los resultados muestran que un porcentaje significativos de los estudiantes se clasificaron como vulnerables, lo que demuestra el cumplimiento de la hipótesis de que la población universitaria es susceptible a fraude digital, lo que coincide con investigaciones de Alqahtani et al., (2025), Dubovecka, (2024), Morrow, (2024) Okokpujie et al., (2023) que destacan la exposición de estudiantes a plataformas digitales y la verificación de correos electrónicos. La contribución principal de este estudio radica en la caracterización de la vulnerabilidad en un contexto universitario latinoamericano específico mediante simulaciones controladas, lo que permite replicar escenarios reales sin comprometer la seguridad de la información de los estudiantes.

También se ha evidenciado que, aunque no todos los estudiantes caen en la trampa, la preparación frente a ataques de ingeniería social es insuficiente, lo que sugiere que la vulnerabilidad está más relacionada con hábitos digitales y formación en ciberseguridad que con características sociodemográficas (Kennet et al., 2023).

Respecto al medio utilizado, se observó que la mayoría de los estudiantes vulnerables respondieron a correos electrónicos fraudulentos, mientras que solo una minoría reaccionó ante mensajes de texto (SMS). Esta diferencia señala que, aunque ambos canales son explotados por atacantes, el correo electrónico es el vector más efectivo para ataques de phishing. La comparación directa entre E-mail y SMS mediante simulaciones controladas constituye un aporte novedoso del estudio, ya que permite identificar cuáles canales representan mayor riesgo y orientar estrategias de concienciación más focalizadas. Esta tendencia coincide con estudios previos que señalan que el correo electrónico es el medio más explotado por los atacantes debido a su uso masivo y a la apariencia de legitimidad que pueden adquirir los mensajes, así como principios de persuasión para engañar a los usuarios (Khadka et al., 2025; Dubovecka, 2024).

En cuanto a las variables sociodemográficas, aunque descriptivamente las mujeres y los estudiantes más jóvenes mostraron una mayor proporción de vulnerabilidad, las pruebas estadísticas no evidenciaron diferencias significativas, lo cual coincide con estudios previos como los de Duvobecka, (2024), Abroshan, (2021), Du et al., (2024) y Kavvadias, et al., (2024) que señalan que factores como sexo, edad o nivel académico por sí solos no determinan necesariamente un mayor nivel de conciencia o precaución ante intentos de phishing. No obstante, las tendencias descriptivas identificadas sugieren que programas de concienciación en ciberseguridad deberían abarcar a toda la población estudiantil, con énfasis en subgrupos potencialmente más vulnerables.

Respecto a la carrera académica, aunque las diferencias no fueron estadísticamente significativas, se observó mayor vulnerabilidad en estudiantes de Farmacia y Psicología, seguidos de Derecho y Administración de Empresas. Esta distribución podría estar relacionada con la alfabetización digital y la frecuencia de uso de herramientas tecnológicas, apoyado por el estudio de Díaz et al., (2018) y Alsharif et al., (2022) sobre la influencia del conocimiento tecnológico en la capacidad de detección de fraudes digitales

Una aportación importante de este estudio es la validación de los resultados mediante simulaciones controladas y métodos estadísticos robustos, como la Prueba exacta de Fisher y la simulación de Monte Carlo, ya que garantiza la confiabilidad de los datos incluso cuando algunas frecuencias esperadas son bajas, y respalda su aplicabilidad en otros entornos universitarios con características similares.

En términos de educación y prevención, los resultados confirman que la vulnerabilidad ante phishing no depende exclusivamente del nivel académico, sino de la formación específica en ciberseguridad y la alfabetización digital tal como señala Jiménez Sánchez et al., (2025), Molina-Granja et al., (2025), y Rama et al., (2025). Esto enfatiza la importancia de incorporar estrategias educativas desde los primeros niveles de la universidad, que incluyan simulaciones de phishing, identificación de señales de riesgo y fortalecimiento de una cultura de ciberseguridad transversal a toda la comunidad estudiantil. El nivel educativo no mostró una relación significativa, lo que da a entender que tener estudios superiores no garantiza una mejor defensa contra el phishing, esto es respaldado por Abroshan, (2021), Alsharif et al., (2022) y Duvobecka, (2024), y quienes afirman que, si no se cuenta con formación específica en ciberseguridad, los es estudiantes son más vulnerables.

Tanto la investigación sobre los principios de persuasión en ataques de phishing como los estudios sobre educación en ciberseguridad y mitigación de ataques en estudiantes universitarios coinciden en que la formación específica y práctica en ciberseguridad es clave para reducir la vulnerabilidad, independientemente del nivel educativo formal (Khadka, et al., 2025; Molina-Granja et al., 2025).

Además, la combinación de soluciones tecnológicas inteligentes y educación en ciberseguridad resulta fundamental para reducir riesgos, lo cual refuerza la necesidad de programas de concienciación estructurados y simulaciones prácticas que permitan a los estudiantes desarrollar habilidades efectivas de detección de phishing (Asiri et al., 2023; Blažič y Blažič, 2024).

Este estudio muestra que la vulnerabilidad al phishing entre estudiantes pone de manifiesto la necesidad de estrategias de concienciación diferenciadas, tal como propone Armas, (2025), Aguilar-Ojeda et al., (2024), Ahmead et al., (2024), Rama et al., (2025) y Yoro et al., (2023). Los cuales han desarrollado marcos conceptuales de concienciación y capacitación en ciberseguridad para la

educación superior, que buscan mejorar de manera sistemática el conocimiento y la preparación de los estudiantes frente a amenazas digitales

Finalmente, este estudio amplía la comprensión del fenómeno del phishing en contextos universitarios latinoamericanos y proporciona evidencia empírica sobre tendencias de vulnerabilidad que pueden ser aplicables en otras instituciones de educación superior. La metodología utilizada y los hallazgos obtenidos representan una mejora respecto a estudios anteriores, al combinar simulaciones controladas, análisis estadístico robusto y la identificación de patrones descriptivos relevantes para la prevención de ataques digitales.

Conclusión

Los datos revelaron que las variables sociodemográficas tales como: sexo, edad, año académico y carrera no presentaron una relación estadísticamente significativa con la vulnerabilidad. Esto destaca la importancia de orientar las estrategias preventivas hacia los comportamientos de los estudiantes, el fortalecimiento de la alfabetización digital y la capacitación especializada en ciberseguridad.

Referencias

Abroshan, H., Devos, J., Poels, G., y Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of H investigan los comportamientos de las personas en líneas de riesgo y sugieren la urgente necesidad de educación, capacitación y conciencia en ciberseguridad en instituciones universitarias.uman Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access, 9*, 44928 - 44949. https://doi.org/10.1109/ACCESS.2021.3066383

Aguilar-Ojeda, C. E., Hernández-Omaña, T. H., y Soto-Ortíz, S. I. (2024). Buenas prácticas de ciberseguridad en educación superior. *South Florida Journal of Development, 5*(12), e4879. https://doi.org/10.46932/sfjdv5n12-080

Ahmead, M., Sharif, N. E., y Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science, 13*(29). https://doi.org/10.1186/s40163-024-00230-w

Alqahtani, S., Nanda, P., y Mohanty, M. (2025). Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors, and Mitigating Strategies on Phishing Attack Perception. *Web Information Systems Engineering–WISE 2024 PhD Symposium, Demos and Workshops. WISE 2024.* Springer: Singapore. https://doi.org/10.1007/978-981-96-1483-7_27

Alsharif, M., Mishra, S., y AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering, 40*(3), 1153-1166. https://doi.org/10.32604/csse.2022.019938

Armas, R., y Taherdoost, H. (2025). Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information, 16*(5), 336. https://doi.org/10.3390/info16050336

Asiri, S., y Alzahrani, Y. X. (2024). Towards Improving Phishing Detection System Using Human in the Loop Deep Learning Model. *ACMSE '24: Proceedings*

of the 2024 ACM Southeast Conference (pp. 77-85). New York: NY,USA. https://doi.org/10.1145/3603287.3651193

Blažič, A. J., y Blažič, B. J. (2024). Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. *Education and Information Technologies, 30*, 9093-9120. https://doi.org/10.1007/s10639-024-13155-3

Diaz, A., Sherman, A. T., y Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia, 44*(1), 53-67. https://doi.org/10.1080/01611194.2019.1623343

Du, J., Kalafut, A., y Schymik, G. (2024). The health belief model and phishing: determinants of preventative security behaviors. *Journal of Cybersecurity, 10*(Issue 1), tyae012. https://doi.org/10.1093/cybsec/tyae012

Dubovecka, K. (2024). Vulnerability of Students of Masaryk University to Two Different Types of Phishing. *Applied Cybersecurity & Internet Governance (ACIG), 3*(2), 268-285. https://doi.org/10.60097/ACIG/190268

Jiménez-Sánchez, V. G., Tipanluisa-Masabanda, R. I., y León-Espinoza, C. J. (2025). Ciberseguridad en la educación superior: evaluación y estrategias de formación. *Technology Rain Journal, 4*(2). https://doi.org/10.55204/trj.v4i1.e94

Kavvadias, A., y Kotsilieris, T. (2025). Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review. *Applied Sciences, 14*(4), 2236. https://doi.org/10.3390/app15042236

Kenneth, A., Hayashi, B. B., Lionardi, J., y Richie, S. (9 Agosto 2023). Phishing Attack Awareness Among College Students. *3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS).* https://www.researchgate.net/publication/376442564_Phishing_Attack_Awareness_Among_College_Students

Khadka, K., Ullah, A. B., y Marroquin, E. M. (2025). Unmasking persuasion in phishing: a content analysis of principles of persuasion in emails and subject lines. *Information and Computer Security*. https://doi.org/10.1108/ICS-12-2024-0321

Molina-Granja, F., Cabezas-Heredia, E., Castelo, L. E., y Guambo-Vallejo, D. C. (2025). Ciberataques y rendimiento académico en educación superior: efectos psicoeducativos y estrategias de mitigación en contextos digitales latinoamericanos. *Tesla Revista Científica, 5*(1), e497. https://doi.org/10.55204/trc.v5i1.e497

Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior, 158*, 108274. https://doi.org/10.1016/j.chb.2024.108274

Okokpujie, K., Kennedy, C. G., Nnodu, K., y Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *International Journal of Sustainable Development and Planning, 18*(1), 255-263. https://doi.org/10.18280/ijsdp.180127

Rama, P., Marx, B., y Smith, R. (2025). Cybersecurity awareness among accounting students at a South African public university. *South African*

Journal of Information Management, 27(1), a1948. https://doi.org/10.4102/sajim.v27i1.1948

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., y Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engi, 13*(2), 1943-1953. https://doi.org/10.11591/ijece.v13i2.pp1943-1953