UNIVERSIDAD CENTRAL DE NICARAGUA

FACULTAD DE INGENERÍA EN SISTEMAS

SEDE-JINOTEPE

INFORME DE INVESTIGACIÓN

Título:

Vulnerabilidad de estudiantes universitarios en la Universidad Central de Nicaragua ante ataques de phishing, Jinotepe, 2025

Autores:

Lic. Rebeca del Carmen Molina Hernández

Ing. Hilder Amílcar Olivas Doña

Instituciones:

Universidad Central de Nicaragua

Fecha de presentación:

06 de mayo de 2025

Resumen

El creciente uso de medios digitales en el ámbito universitario ha incrementado la exposición de los estudiantes a ataques de phishing, poniendo en riesgo su información personal y académica. Este estudio tuvo como objetivo analizar el grado de vulnerabilidad de los estudiantes de la Universidad Central de Nicaragua, sede Jinotepe, frente a ataques de phishing durante el I cuatrimestre 2025. Se empleó un enfoque cuantitativo, descriptivo-correlacional, evaluando la vulnerabilidad frente a correos electrónicos simulados y su relación con sexo, edad, año académico y carrera. La muestra incluyó 249 estudiantes, y los datos se analizaron mediante frecuencias, porcentajes y pruebas de chi-cuadrado.

Los resultados mostraron que 36,9% de los estudiantes fueron vulnerables, sin asociaciones significativas con las variables sociodemográficas, aunque los estudiantes jóvenes y de primeros años presentaron mayor cantidad absoluta de casos. Esto, evidencian riesgos digitales en la población universitaria y resaltan la necesidad de estrategias de concientización y formación en ciberseguridad, así como la exploración de otras variables en futuras investigaciones.

Palabras Claves: *Ciberseguridad, Seguridad de los datos, Ciberataque, Phishing, Ingeniería social, correo electrónico.*

Abstract

The increasing use of digital media in the university environment has raised students' exposure to phishing attacks, putting their personal and academic information at risk. This study aimed to analyze the degree of vulnerability of students at the Central University of Nicaragua, Jinotepe campus, to phishing attacks during the first semester of 2025. A quantitative, descriptive-correlational approach was used, evaluating vulnerability to simulated phishing emails and its relationship with sex, age, academic year, and major. The sample included 249 students, and data were analyzed using frequencies, percentages, and chi-square tests.

Results showed that 36.9% of students were vulnerable, with no significant associations with sociodemographic variables, although younger students and those in early academic years had the highest absolute number of vulnerable cases. These findings highlight digital risks among the university population and emphasize the need for awareness and cybersecurity training, as well as the exploration of additional variables in future research.

Keywords: *Cybersecurity, Data security, Cyberattack, Phishing, Social engineering, Electronic mail*

Índice

Índice de Tablas

Índice de Figuras

Introducción

Antecedentes y Contexto del Problema

Antecedentes Internacionales

Okokpujie et al., (2023), en su estudio titulado Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University), tuvieron como objetivo investigar la susceptibilidad de los estudiantes a los ataques de phishing con el fin de promover un uso sostenible y seguro del correo electrónico en el entorno académico. Para ello, se llevaron a cabo dos pruebas de phishing mediante correos electrónicos simulados, con el propósito de observar cómo reaccionaban los estudiantes ante estos mensajes fraudulentos.

Además, se evaluó la respuesta grupal cuando todos los integrantes de un equipo recibían el mismo correo de phishing, y posteriormente se aplicaron cuestionarios que midieron el nivel de conciencia y conocimiento sobre este tipo de ataques. Los resultados revelaron que el 70.6% de los estudiantes evaluados fueron susceptibles al phishing, principalmente por falta de conciencia o desconocimiento. El estudio concluye con una serie de recomendaciones orientadas a fortalecer la seguridad en la comunidad académica y en las infraestructuras tecnológicas, con el objetivo de lograr un entorno más seguro y sostenible para el uso del correo electrónico.

Asiri et al., (2023), en su artículo *A* Survey of Intelligent Detection Designs of HTML URL Phishing Attacks, realizaron una revisión exhaustiva sobre los ataques de phishing basados en HTML y URL, así como sobre los métodos inteligentes para su detección. El estudio adopta un enfoque de revisión sistemática, en el cual se analizan modelos de aprendizaje automático y profundo de última generación. Los métodos de detección fueron clasificados en tres categorías

principales: los basados en URL, que examinan únicamente las características de las direcciones; los basados en contenido, que analizan elementos del contenido de la página como texto, imágenes y código HTML; y los enfoques híbridos, que integran ambas fuentes de información. Entre los modelos evaluados destacan las Redes Neuronales Convolucionales (CNN) y Recurrentes (RNN), los cuales superan en precisión y reducción de falsos positivos a técnicas tradicionales como las Máquinas de Vectores de Soporte (SVM) y Random Forest.

Los autores concluyen que, debido a la constante evolución de las tácticas de los atacantes, es necesario desarrollar sistemas de detección más adaptativos que integren múltiples fuentes de datos. En este contexto, se resalta la importancia de considerar enfoques tecnológicos que complementen la formación en ciberseguridad de los estudiantes. El estudio ofrece un valioso soporte teórico y técnico para fortalecer la capacidad de identificar intentos de phishing, mediante una combinación de concienciación y herramientas digitales automatizadas o asistidas.

Natalia et al., (2023), en su estudio Gamification Design as Learning Media to Motivate Students to Increase Cyber Security Awareness towards Phishing, exploran el uso del diseño de gamificación como medio de aprendizaje para aumentar la conciencia sobre ciberseguridad en estudiantes universitarios, específicamente frente a los ataques de phishing. Utilizando un enfoque cuantitativo y diseño experimental, se desarrolló un juego educativo interactivo centrado en la prevención del phishing. A través de esta actividad lúdica, los estudiantes aprendieron a identificar señales de phishing, reconocer técnicas comunes de ataque y practicar comportamientos seguros en línea.

Se aplicaron cuestionarios antes y después de la intervención, y los resultados fueron analizados mediante pruebas estadísticas, como la prueba t de diferencia de medias. Los

hallazgos mostraron un aumento significativo en la habilidad de los estudiantes para identificar correos electrónicos de phishing y una mejora en su actitud hacia la ciberseguridad. La investigación concluye que la gamificación es una herramienta eficaz para elevar la conciencia sobre amenazas digitales, promoviendo un aprendizaje activo, motivador y centrado en el estudiante. Este enfoque resulta relevante para investigaciones que buscan reducir la vulnerabilidad de los estudiantes frente al phishing, permitiendo diseñar intervenciones basadas en características demográficas o niveles previos de conciencia.

Kenneth et al.,(2023), en su estudio Phishing Attack Awareness Among College Students, evaluaron la conciencia de los estudiantes universitarios frente a los ataques de phishing mediante un experimento de simulación real. Utilizaron una técnica de phishing por correo electrónico, enviando mensajes que solicitaban a los estudiantes cambiar la contraseña de su cuenta institucional. Esta metodología, de enfoque cuantitativo, permitió observar directamente el comportamiento de los estudiantes ante un intento de ataque.

Los resultados revelaron que un pequeño porcentaje de estudiantes cayó en la trampa, lo cual evidenció una falta de preparación y conciencia sobre los riesgos asociados a este tipo de ciberataques basados en ingeniería social. A partir de estos hallazgos, los autores concluyen que es urgente implementar campañas educativas y programas de sensibilización sobre phishing, ya que aún existe una significativa vulnerabilidad entre los estudiantes universitarios. Este estudio resulta especialmente pertinente para investigaciones orientadas a identificar los factores que inciden en la vulnerabilidad de los estudiantes ante el phishing, destacando el rol clave de la conciencia cibernética.

Antecedentes Nacionales

Según la literatura existente no se muestran evidencias de estudios realizados en Nicaragua sobre esta temática

Contexto del Problema

En la era digital, los ataques de phishing se han convertido en una de las principales amenazas a la seguridad de la información en todo el mundo. Este tipo de ciberataque, que consiste en engañar a las personas para que revelen información confidencial mediante correos electrónicos, mensajes de texto o sitios web falsos, ha mostrado un crecimiento sostenido en frecuencia, sofisticación y daño potencial. De acuerdo con el Cyber Threat Landscape Report *2023* de INTERPOL (2023), los delitos cibernéticos como el phishing, el ransomware y el robo de datos se incrementaron considerablemente, generando pérdidas financieras y afectaciones psicológicas en las víctimas.

A nivel europeo, el *IOCTA 2024* de Europol identificó al phishing como el vector de ataque más común en esquemas de fraude digital, observando un uso intensificado de métodos como smishing (mensajes de texto) y vishing (llamadas telefónicas) para engañar a las personas (Europol, 2024).

En América Latina, esta tendencia se refleja con fuerza, especialmente en el sector educativo, que se muestra particularmente vulnerable debido al uso masivo de plataformas digitales, la constante interacción por medios electrónicos y la variabilidad en los niveles de conciencia digital entre los estudiantes. Según la Organización de los Estados Americanos (OEA), la región experimentó 137 mil millones de intentos de ciberataques en el primer semestre de 2022, lo que refleja un aumento significativo en la actividad cibernética maliciosa (OEA, 2022).

Además, según datos de la Cybersecurity & Infrastructure Security Agency (CISA, 2020), el 32% de las violaciones de datos en instituciones públicas de EE. UU. estuvieron relacionadas con el phishing, y en el 78% de los incidentes de ciberespionaje, este tipo de ataque fue el punto de entrada. A nivel global, el X-Force Threat Intelligence Index 2025 de IBM destacó el creciente uso de inteligencia artificial generativa para diseñar correos de phishing más convincentes, lo que ha permitido a los atacantes evadir sistemas tradicionales de detección y aumentar su tasa de éxito (IBM, 2025).

En el ámbito educativo, una encuesta realizada por ESET Latinoamérica reveló que el 67% de las instituciones educativas, incluyendo universidades, han sufrido al menos un incidente de seguridad, lo que subraya la vulnerabilidad de este sector ante ataques cibernéticos (ESET, 2018).

Particularmente en México, Kaspersky reportó un incremento del 220% en los ataques de phishing entre 2022 y 2023, con más de 118 millones de intentos bloqueados en 2023. Estos ataques han evolucionado, incorporando técnicas avanzadas como la inteligencia artificial generativa, geofiltering y deepfakes, lo que los hace más difíciles de detectar y prevenir (Kaspersky, 2023).

Aunque no existen estadísticas específicas para Nicaragua, la creciente digitalización de la educación superior en el país, sumada a la falta de formación en ciberseguridad entre los estudiantes, los hace susceptibles a caer en engaños de phishing. Estos ataques pueden resultar en el robo de información personal y académica, afectando la integridad de los sistemas educativos y la privacidad de los estudiantes. Esta situación destaca la necesidad urgente de implementar

programas de concienciación y formación en ciberseguridad en las universidades, con el fin de mitigar los riesgos asociados al phishing y fortalecer la seguridad digital en el ámbito académico.

El impacto del phishing en los estudiantes universitarios puede derivar en el robo de datos personales, usurpación de identidad, pérdida de acceso a plataformas académicas, daño a la reputación digital e incluso chantaje. La falta de protocolos claros de respuesta institucional y la insuficiente conciencia sobre el tema contribuyen a una cultura de vulnerabilidad latente en los entornos universitarios.

En este contexto, la presente investigación tiene como objetivo analizar y caracterizar el nivel de vulnerabilidad de los estudiantes universitarios ante ataques de phishing, considerando variables como el sexo, la carrera y la condición económica. A través de este estudio, se pretende generar datos empíricos que sirvan como base para diseñar estrategias de concienciación y formación preventiva, contribuyendo tanto al ámbito académico como a la formulación de políticas internas de ciberseguridad en las instituciones de educación superior del país.

Asimismo, la investigación busca evaluar de manera profunda el grado de vulnerabilidad de los estudiantes universitarios frente a diferentes tipos de ataques de phishing. A través de un enfoque experimental, se examinarán los factores individuales y contextuales que influyen en la susceptibilidad de los estudiantes a caer en trampas de phishing. El objetivo es proporcionar información valiosa que sirva para el diseño de estrategias de prevención y concienciación efectivas, con el fin de reducir los riesgos asociados a estas amenazas cibernéticas, mejorando la seguridad digital de los estudiantes y, por ende, de la comunidad universitaria en su conjunto.

Objetivos

General

Analizar el grado de vulnerabilidad de los estudiantes de Universidad Central de Nicaragua de la sede Jinotepe, frente a ataques de phishing durante el I semestre 2025.

Específicos

1. Determinar el nivel de vulnerabilidad de los estudiantes de la UCN sede Jinotepe frente a ataques de phishing durante el I semestre 2025.
2. Analizar la vulnerabilidad de los estudiantes frente a ataques de phishing según sexo y carrera.
3. Evaluar la vulnerabilidad de los estudiantes frente a ataques de phishing según rangos de edad.

Pregunta de Investigación

¿Cuál es el nivel de vulnerabilidad de los estudiantes de la UCN sede Jinotepe frente a ataques de phishing durante el I semestre 2025, según sexo, edad y carrera?

Preguntas Específicas

1. ¿Qué proporción de estudiantes responde a un correo simulado de phishing?
2. ¿Cómo se distribuye la vulnerabilidad según el sexo de los estudiantes?
3. ¿Cómo se distribuye la vulnerabilidad según los rangos de edad de los estudiantes?
4. ¿Cómo se distribuye la vulnerabilidad según la carrera de los estudiantes?

Justificación

En la era digital, los estudiantes universitarios están cada vez más expuestos a riesgos cibernéticos que pueden comprometer su información personal, académica y financiera. Uno de los ataques más comunes es el phishing, una técnica de ingeniería social que busca engañar a los usuarios para obtener información confidencial. La falta de formación en seguridad digital y el conocimiento superficial sobre estos riesgos hacen que los estudiantes sean especialmente vulnerables. Por ello, esta investigación tiene como propósito identificar el nivel de conocimiento de los estudiantes sobre el phishing y los factores asociados a su vulnerabilidad ante este tipo de amenazas.

Este proyecto es importante porque permitirá generar información útil para las instituciones de educación superior en Nicaragua, orientándolas en la implementación de estrategias preventivas y formativas que protejan a sus estudiantes. Además, aporta datos empíricos que caracterizan la brecha de conocimiento sobre seguridad digital en la comunidad universitaria, un aspecto clave en el entorno educativo actual, donde el uso de plataformas digitales es indispensable.

El estudio beneficiará directamente a los estudiantes universitarios, al fomentar una mayor conciencia sobre los riesgos digitales y las medidas de prevención, y a las universidades, que podrán fortalecer sus programas de formación en competencias digitales y ciberseguridad. Esta iniciativa se alinea con el Plan Nacional de Lucha contra la Pobreza y para el Desarrollo Humano de Nicaragua, que promueve la inclusión digital como pilar del desarrollo sostenible. Prevenir el phishing protege datos y contribuye a la equidad y justicia digital, evitando que estudiantes de sectores vulnerables sufran daños por falta de información y protección.

Asimismo, se articula con la Estrategia Nacional de Educación de Nicaragua, que reconoce la importancia de preparar a los estudiantes para enfrentar los desafíos de la sociedad digital mediante una educación integral, inclusiva y segura. Fomentar la alfabetización digital crítica y responsable es esencial para formar ciudadanos capaces de desenvolverse de manera ética y segura en entornos virtuales.

La investigación aborda una problemática real y actual, con un enfoque metodológico riguroso. Para ello, se aplicaron ataques de correos electrónicos simulados un instrumento diseñado específicamente para medir el grado de vulnerabilidad de los estudiantes ante ataques de phishing en los estudiantes.

Limitaciones

Dificultad para Interpretar las Razones del Comportamiento Observado

Al no contar con reacciones auto-reportadas o entrevistas posteriores, no será posible comprender con profundidad por qué los estudiantes cayeron o no en los ataques simulados (por ejemplo, si fue por desconocimiento, descuido, o exceso de confianza).

Resultados Limitados a un Momento Específico

La evaluación se hace en un contexto puntual y no permite observar si el comportamiento de los estudiantes cambia con el tiempo, lo que limita el análisis del aprendizaje o la adaptación a futuras amenazas.

Posibles Reacciones Atípicas por Factores Externos no Controlados

Variables como el estrés académico, campañas institucionales previas o rumores entre estudiantes pueden modificar la forma en que interactúan con los mensajes de phishing, afectando la naturalidad de la simulación.

Sesgo por Cobertura Tecnológica y Acceso

Aunque se asume acceso a correo y teléfono, no todos los estudiantes revisan con la misma frecuencia sus mensajes o tienen el mismo nivel de exposición digital, lo cual podría influir en los resultados sin que sea parte del diseño experimental.

Hipótesis

Hipótesis General de Investigación

Se espera que exista un nivel observable de vulnerabilidad frente a ataques de phishing entre los estudiantes de la UCN sede Jinotepe durante el I cuatrimestre 2025, con diferencias según sexo, edad y carrera.

Hipótesis Nula y Alternativa Generales

Hipótesis Nula (Ho). No se espera un nivel observable de vulnerabilidad entre los estudiantes, ni diferencias significativas según sexo, edad o carrera.

Representación matemática. Si P = proporción de estudiantes que responde al correo simulado $H_0: P = 0.5$

Hipótesis Alternativa (H_1). Se espera que exista un nivel observable de vulnerabilidad frente a ataques de phishing, con diferencias según sexo, edad y carrera.

Representación matemática: $H_1: P \neq 0.5$

Hipótesis por Subgrupos

Tabla 1: **Hipótesis por subgrupos**

Variable	Hipótesis nula (H_0)	Hipótesis alternativa (H_1)
Sexo	$P_{hombres}=P_{mujeres}=0.5$	$P_{hombres}\neq P_{mujeres}$
Edad	$P_{edad1}=P_{edad2}=\cdots=P_{edadn}=0.5$	$P_{edad1}\neq P_{edad2}\neq\ldots\neq P_{edadn}$
Carrera	$P_{carrera1}=P_{carrera2}=\cdots=P_{carreran}=0.5$	$P_{carrera1}\neq P_{carrera2}\neq\ldots\neq P_{carreran}$

Variables

El estudio sobre la vulnerabilidad de los estudiantes de la UCN sede Jinotepe frente a ataques de phishing incluye una variable dependiente y varias variables independientes, que permiten caracterizar y analizar los patrones de respuesta ante la simulación de correos electrónicos.

Variable Dependiente

Vulnerabilidad Frente a Ataques de Phishing. Esta es la variable principal del estudio y representa la propensión de los estudiantes a responder a un correo simulado de phishing. Se midió a través del registro de respuestas (sí/no) a los correos enviados durante la simulación. La vulnerabilidad se pudo analizar en términos de proporciones y frecuencias, lo que permitió determinar el nivel general y compararlo entre grupos. Esta variable se considera dependiente porque su comportamiento puede asociarse a características sociodemográficas de los estudiantes.

Variables Independientes

Sexo. Se refiere al género del estudiante (masculino o femenino). Se analizaron diferencias en la vulnerabilidad entre hombres y mujeres mediante comparación de proporciones.

Edad. Corresponde a los rangos de edad de los estudiantes. Con esta variable se exploró la relación entre la edad y la vulnerabilidad, mediante análisis correlacional.

Carrera. Indica la carrera universitaria del estudiante. Permite comparar la vulnerabilidad entre diferentes programas académicos, utilizando análisis comparativo de proporciones. ***Ver operacionalización de variables en anexo 1 pág. # 57***

Marco Contextual

La presente investigación se desarrolla en la Universidad Centroamericana (UCN), sede Jinotepe, durante el I cuatrimestre del año 2025**,** con el propósito de evaluar la vulnerabilidad de los estudiantes frente a ataques de phishing mediante una simulación de correos electrónicos. Las carreras ofertadas durante este período fueron Ingeniería en Sistemas, Farmacia, Psicología, Derecho, Administración de empresas, Mercadotecnia, Contabilidad Pública y Auditoría, Relaciones Internacionales y Comercio Exterior, Administración Turismo y Hotelería además de Banca y Finanzas.

En cuanto a la edad de los participantes, predominan los estudiantes jóvenes entre 17 y 19 años, representando más de la mitad de la muestra (29 estudiantes de 17 años, 15,8%; 24 de 18 años, 13%; 25 de 19 años, 13,6%). Sin embargo, la muestra también incluyó estudiantes de mayor edad, hasta 49 años, lo que refleja la diversidad etaria de la población universitaria de la sede.

El contexto académico y tecnológico de la institución fue determinante para la investigación, ya que los estudiantes interactúan diariamente con plataformas virtuales, correos electrónicos y herramientas digitales que podrían exponerlos a riesgos de seguridad informática. Esta realidad hizo pertinente observar cómo los estudiantes reaccionan ante correos simulados de

phishing, así como la comparación de su vulnerabilidad según variables sociodemográficas como sexo, edad y carrera.

Asimismo, el marco temporal del estudio, el primer cuatrimestre de 2025, coincide con un período académico activo, lo que garantizó una participación representativa de los estudiantes y refleja su comportamiento real frente a correos electrónicos en un entorno habitual de estudio. De forma que, las condiciones del contexto, como el acceso a la tecnología, el uso frecuente de correo y la diversidad de la población estudiantil, proporcionaron la base para interpretar los resultados de manera objetiva y relevante, situando la investigación dentro de un escenario real y aplicable a futuras estrategias de concienciación y prevención frente al phishing.

Marco Teórico

Revisión de Literatura

La revisión de literatura de esta investigación se llevó a cabo mediante una búsqueda exhaustiva en bases de datos académicas reconocidas, como ERIC, Springer Link, Nature, Web of Science, Scopus, IEEE Xplore y Google Scholar. Se seleccionaron estudios que abordaran la vulnerabilidad de los estudiantes universitarios frente a ataques de phishing, así como los factores individuales y contextuales que influyen en dicha vulnerabilidad.

Durante la revisión, se identificaron cuatro investigaciones principales que aportaron información valiosa al estudio:

Entre los estudios revisados se encuentran investigaciones como Hable et al. (2025), que examina la susceptibilidad al phishing en entornos organizacionales; Alqahtani et al. (2025), cuyo trabajo Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors,

and Mitigating Strategies on Phishing Attack *Perception* analiza cómo el comportamiento de los estudiantes y las estrategias de mitigación influyen en la percepción de los ataques.

El estudio de Cabezas-Molina y Fiallos-Aguilar (2024) *titulado* Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial. Un enfoque práctico para mejorar la resiliencia organizacional, que evalúa la efectividad de simulaciones y programas de concienciación en entornos corporativos; y finalmente, Dubovecka (2024), quien investigó la vulnerabilidad de estudiantes de la Universidad Masaryk frente a ataques de phishing genéricos y dirigidos.

Además en las Teorías y Conceptos Asumidos se abordaron tema como:

1. **Ingeniería Social y Phishing**: Phishing como técnica de ingeniería social.
2. **Vulnerabilidad del Usuario**: Susceptibilidad influida por factores personales y contextuales.
3. **Conciencia y Comportamiento Seguro**: Educación y capacitación reducen la vulnerabilidad.
4. **Tipos de Ataques y Perfil de Riesgo**: Ataques genéricos y dirigidos; perfil del usuario determina riesgo.
5. **Marco Contextual Académico**: Entorno universitario y uso de plataformas digitales como factores determinantes.

Estado del Arte

En la actualidad, los ataques de phishing representan una de las amenazas más frecuentes y efectivas en entornos digitales, afectando tanto a usuarios individuales como a comunidades académicas. Los estudiantes universitarios constituyen un grupo particularmente vulnerable debido a la combinación de factores personales, como la edad, la experiencia tecnológica y la

familiaridad con los entornos digitales, junto con factores contextuales, como la disponibilidad de recursos tecnológicos y la cultura institucional de seguridad informática.

Diversas investigaciones han buscado identificar los perfiles de usuarios más susceptibles, analizar la efectividad de los ataques de phishing y proponer estrategias preventivas en entornos educativos y organizacionales. Comprender tanto los factores individuales como los contextuales permite abordar de manera más integral la vulnerabilidad de los estudiantes ante estas amenazas y orientar el diseño de programas de concienciación y estrategias de protección.

Tal como señala Hable et al.,(2025) examinó la susceptibilidad al phishing en entornos organizacionales, explorando cómo los factores contextuales influyen en el procesamiento cognitivo y la toma de decisiones de los usuarios frente a ataques cibernéticos. El estudio evidenció que la vulnerabilidad de los individuos no depende únicamente de características personales como la edad o la familiaridad con la tecnología, sino también del entorno organizacional, la cultura institucional de seguridad informática y el acceso a recursos digitales.

Los resultados indicaron que los usuarios en entornos con alta concienciación sobre seguridad presentaban menor probabilidad de caer en ataques de phishing, y que la disponibilidad de recursos tecnológicos y la capacitación continua son determinantes críticos para reducir la vulnerabilidad. Sin embargo, la investigación se centró en contextos corporativos, sin explorar específicamente la vulnerabilidad de estudiantes universitarios ni las diferencias entre plataformas de comunicación, como correo electrónico institucional versus redes sociales o formularios en línea, y tampoco consideró factores individuales como estilo de aprendizaje o nivel de alfabetización digital (Hable et al., 2025).

Este estudio aportó a la investigación sobre vulnerabilidad de estudiantes ante ataques de phishing al resaltar la importancia del contexto organizacional e institucional en la adopción de medidas preventivas, sugiriendo que la educación en ciberseguridad, junto con la disponibilidad de recursos seguros y una cultura institucional sólida, puede disminuir significativamente la probabilidad de ser víctima de phishing en entornos académicos.

La investigación de Alqahtani et al., (2025), titulada Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors, and Mitigating Strategies on Phishing Attack Perception detallaron cómo el comportamiento de los estudiantes, los factores percibidos y las estrategias de mitigación influyen en la percepción de los ataques de phishing en entornos académicos. El objetivo del estudio fue determinar qué aspectos humanos y de percepción aumentan o disminuyen la vulnerabilidad frente a phishing y cómo las estrategias de mitigación pueden reforzar la seguridad de los usuarios.

El estudio utilizó un enfoque cuantitativo transversal. Se recopilaron datos de 715 estudiantes universitarios mediante cuestionarios estructurados que midieron: comportamiento del usuario, factores percibidos de riesgo y estrategias de mitigación aplicadas. Posteriormente, se realizaron análisis de regresión múltiple para identificar el efecto de estas variables en la percepción del phishing y la susceptibilidad de los estudiantes a los ataques.

Los hallazgos indicaron que la falta de conciencia y la falta de verificación de la autenticidad de las comunicaciones aumentan significativamente la vulnerabilidad al phishing. El análisis de regresión mostró que el comportamiento estudiantil, los factores percibidos y las estrategias de mitigación explican colectivamente el 47% de la varianza en la percepción del phishing, con todas las variables predictoras mostrando relaciones positivas y significativas.

Los autores concluyeron que depender únicamente de soluciones tecnológicas no es suficiente; la educación del usuario y las estrategias preventivas son clave para reducir la vulnerabilidad. Además, se recomendó implementar programas educativos integrales que enseñen a los estudiantes a verificar fuentes de información y actualizar regularmente sus sistemas para fortalecer la ciberseguridad.

Similarmente, el estudio titulado “Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial. Un enfoque práctico para mejorar la resiliencia organizacional” de Cabezas-Molina y Fiallos-Aguilar (2024) aborda la problemática de la vulnerabilidad de los empleados ante ataques de phishing en entornos corporativos. El objetivo principal fue evaluar la efectividad de simulaciones de phishing y programas de concienciación en la reducción de la susceptibilidad a ataques cibernéticos.

En cuanto a la metodología, se empleó un enfoque experimental con 100 empleados de una pequeña empresa. La investigación se desarrolló en varias etapas: primero, se aplicó una simulación inicial de phishing para medir la vulnerabilidad de los participantes. Posteriormente, se implementó un programa de formación y concienciación sobre seguridad digital, incluyendo buenas prácticas para identificar correos fraudulentos y gestionar información sensible. Finalmente, se aplicaron nuevas simulaciones de phishing para evaluar los cambios en el comportamiento de los participantes. Los datos fueron recolectados mediante registros de interacción con correos simulados, cuestionarios de percepción de riesgo y análisis estadístico de tasas de clics y tiempos de respuesta.

Los resultados mostraron que, antes de la intervención, aproximadamente el 65% de los participantes hacía clic en enlaces maliciosos, mientras que después de la formación esta cifra

descendió al 20%, demostrando una mejora significativa en la detección de correos fraudulentos y en la resiliencia ante ataques. Además, se observó un incremento en la conciencia sobre técnicas de ingeniería social y en la adopción de buenas prácticas de seguridad digital.

A pesar de su relevancia, este estudio presenta algunos vacíos respecto a poblaciones fuera del ámbito empresarial, especialmente en contextos académicos. No se abordó cómo factores como edad, nivel de alfabetización digital, uso de plataformas académicas y exposición a correos institucionales podrían influir en la vulnerabilidad de estudiantes universitarios ante phishing. Tampoco se exploró la combinación de simulaciones con la educación continua adaptada a entornos educativos.

En relación con este estudio sobre la vulnerabilidad de estudiantes ante ataques de phishing aporta evidencia sobre la efectividad de intervenciones de concienciación y simulaciones prácticas para reducir la susceptibilidad ante ataques cibernéticos. Sus hallazgos sugieren que estrategias similares podrían adaptarse a estudiantes universitarios, considerando sus características específicas, para mejorar la detección de phishing y promover hábitos seguros en el uso de correos electrónicos y plataformas digitales.

Dubovecka (2024) investigó la vulnerabilidad de los estudiantes de la Universidad Masaryk frente a dos tipos de ataques de phishing: genéricos y dirigidos (spear-phishing). La autora implementó dos simulaciones reales para evaluar la susceptibilidad de los estudiantes, midiendo la apertura de correos electrónicos y la interacción con enlaces fraudulentos. Los resultados mostraron que los ataques dirigidos lograron una tasa de éxito del 71 %**,** significativamente mayor que los ataques genéricos, que alcanzaron solo un 18 % (Dubovecka, 2024).

Además, se identificaron diferencias de género y perfil académico: las mujeres presentaron una mayor propensión a interactuar con los correos electrónicos dirigidos (81 %) en comparación con los hombres (63 %). El perfil más vulnerable correspondió a estudiantes de 21–25 años, en tercer año de estudios de Relaciones Internacionales, utilizando Windows y navegadores como Google Chrome (Dubovecka, 2024). Esto evidencia que la vulnerabilidad al phishing no depende únicamente de la exposición tecnológica, sino de factores cognitivos, conductuales y contextuales**.**

Vacíos identificados:

1. El estudio se limita a una sola universidad y a carreras específicas, por lo que no refleja la vulnerabilidad de estudiantes de otras disciplinas o instituciones (Dubovecka, 2024).
2. No se evaluó la efectividad de estrategias de concienciación o formación en la reducción de la vulnerabilidad.
3. Carece de análisis sobre factores socioeconómicos, nivel de alfabetización digital y uso de dispositivos móviles, que podrían influir en la susceptibilidad al phishing.

Este estudio proporcionó evidencia empírica sobre la mayor efectividad de ataques dirigidos frente a genéricos, lo que permite focalizar las medidas preventivas en escenarios más sofisticados, además por medio de él se identificaron perfiles de estudiantes con mayor riesgo**,** ayudando a diseñar programas educativos y campañas de concienciación más efectivas. Resaltó la necesidad de integrar herramientas de monitoreo y educación digital en las universidades, lo que es directamente aplicable a estudios sobre vulnerabilidad estudiantil en contextos como el de Nicaragua.

Teorías y Conceptos Asumidos

Concepto de Phishing

Definición general y Evolución Histórica. Gupta et al., (2017) definen el phishing como un engaño digital en el que los atacantes intentan robar credenciales mediante correos electrónicos falsos, sitios web fraudulentos o ambos, señalando su evolución en paralelo al auge del internet y el comercio electrónico.

Tipos de phishing

Arshad et al. (2021) presentan una clasificación de variantes relevantes:

- **Spear phishing**: ataques dirigidos personalizados.
- **Email spoofing** y **manipulación de correo**: técnicas para forjar remitentes o contenidos.
- **Phone phishing**: equivalente al vishing (Arshad et al., 2021)

Además, fuentes de ciberseguridad detallan otras variantes:

- **Smishing**: uso de SMS falsos con enlaces o números suplantados (TREND MICRO, 2025)
- **Vishing**: llamadas fraudulentas donde se suplanta la identidad de una entidad legítima

Diferencia entre phishing y otros ataques cibernéticos

Gupta et al. enfatizan que el phishing se distingue por su base en la ingeniería social—es decir, el engaño psicológico—en lugar de vulnerar fallos técnicos, lo que lo diferencia de malware, hacking directo o inyección de código (Gupta et al., 2021)

Vulnerabilidad en Usuarios Digitales

Factores que incrementan la vulnerabilidad. Baki y Verma (2021) en su meta-análisis encuentran que la relación entre edad y vulnerabilidad al phishing no es uniforme: algunos estudios muestran mayor susceptibilidad en personas mayores, otros lo contrario; también hallan que las mujeres suelen ser más susceptibles que los hombres, y que el entrenamiento reduce la vulnerabilidad.

Comportamiento Humano Frente a Correos Sospechosos. El análisis de Baki y Verma destaca el papel clave de la formación en la detección de phishing: los usuarios entrenados mejoran significativamente su capacidad de evitar ataques

Factores de Riesgo Específicos en Estudiantes Universitarios

Estudio en Comunidad Académica. Diaz et al., (2018) realizaron un experimento enviando correos phishing a estudiantes universitarios. Hallaron que estudiantes con mayor conocimiento del término “phishing” mostraron mayor susceptibilidad al ataque (≈59 % hicieron clic; entre quienes respondieron también, hasta el 70 %) comparado con quienes sólo estaban conscientes o lo ignoraban. También observaron que variables como afiliación académica, año de estudio, formación en ciberseguridad e integración en comunidades relacionadas disminuían la vulnerabilidad

Relevancia. Este hallazgo refuerza que el conocimiento superficial no garantiza protección, y que la involucración activa en entornos ciber-educativos puede servir como factor protector.

Técnicas utilizadas por atacantes

Ingeniería Social y Manipulación Psicológica. Fuentes periodísticas como El País (2024) señalan que los ciberdelincuentes aprovechan la inteligencia artificial para replicar la voz de un familiar en estafas de vishing, generando presiones emocionales y sensación de urgencia. Asimismo es necesario destacar que, en el phishing, el factor humano es la principal vulnerabilidad, y que los ataques suelen usar ofertas atractivas o personalizadas para manipular emocionalmente a la víctima

Enlaces Falsos, Suplantación de Identidad y Archivos Maliciosos. Trend Micro (2025) explica que el **s**mishing emplea SMS fraudulentos con enlaces que imitan servicios legítimos y buscan la descarga de malware o captura de datos personales.

La entrevista realizada a Ana Collado, experta en fraude e inteligencia de seguridad en Statistical Analysis System, aporta elementos esenciales para comprender el panorama actual del fraude digital en España. La especialista señala que los tipos más comunes de ataques son el phishing, smishing y vishing, todos ellos basados en la ingeniería social y en la manipulación de la confianza del usuario (Collado, 2024). Esta perspectiva resulta relevante porque, desde su posición en una empresa dedicada al análisis avanzado de datos, evidencia cómo los ciberdelincuentes han perfeccionado sus técnicas mediante el uso de inteligencia artificial y big data, lo que incrementa la sofisticación de los engaños.

El testimonio de Collado también enfatiza la vulnerabilidad del sector financiero, donde aproximadamente el 39 % de los fraudes logra evadir las medidas de seguridad, generando pérdidas millonarias (Collado, 2024). Este señalamiento no solo muestra la magnitud del problema en el ámbito bancario, sino que también permite reflexionar sobre la urgencia de

reforzar la educación y la concienciación de los usuarios, quienes continúan siendo el eslabón más débil frente a estos ataques. En este sentido, la entrevista cobra valor como fuente directa que conecta la visión de la industria con la necesidad de fortalecer políticas de prevención y cooperación interinstitucional.

Medidas de Prevención y Mitigación

Buenas Prácticas de Seguridad Digital. BBVA (2025) aconseja:

1. No proporcionar información sensible por correo o llamada.
2. No responder nunca demandas de contraseñas o claves desde correos o mensajes inesperados.
3. Verificar siempre a través de canales oficiales (Castillo, 2024)

Educación y Concienciación Digital. El País (2024) y López (2024) subrayan la importancia de educar con mensajes simples, llamativos y socialmente inclusivos para fortalecer la conciencia de seguridad y contrarrestar la ingeniería social

Políticas Institucionales y Normativas Nacionales. Las Políticas Institucionales y Normativas Nacionales hacen referencia al conjunto de lineamientos internos de una organización (como universidades, empresas o instituciones públicas) y a las leyes del país que regulan la seguridad informática, la protección de datos y el uso adecuado de la tecnología.

En el caso de Nicaragua, la principal normativa relacionada es la Ley No. 1042, “Ley Especial de Ciberdelitos”, aprobada en octubre de 2020. Esta ley establece el marco legal para prevenir, investigar, perseguir y sancionar delitos cometidos a través de medios informáticos, de comunicación y redes digitales.

Algunos puntos clave de la Ley de Ciberdelitos establecida por la (Asamblea Nacional de la República de Nicaragua, (2020) son:

1. ***Protección de Datos y Sistemas Informáticos***. Penaliza el acceso indebido a computadoras, redes, correos electrónicos o bases de datos sin autorización.
2. ***Fraudes Electrónicos y Phishing***. Sanciona el uso de engaños digitales, correos falsos o suplantación de identidad para obtener información personal, financiera o académica.
3. ***Difusión de Información Falsa o Dañina.*** Regula la publicación de datos que afecten la reputación, integridad o seguridad de las personas.
4. ***Seguridad Nacional y Ciberterrorismo.*** Considera delitos graves los ataques cibernéticos contra infraestructuras críticas o con fines de desestabilización.
5. ***Responsabilidad Institucional***. Las universidades y organizaciones deben implementar políticas internas de seguridad informática (contraseñas, filtros de correos, capacitaciones) para proteger a su personal y estudiantes de amenazas digitales.

Supuestos asumidos sobre la relación entre características del estudiante y susceptibilidad al phishing.

1. Cuanto mayor sea la percepción de gravedad y vulnerabilidad, más motivado estará el estudiante para evitar ataques.
2. Factores demográficos (edad, formación digital, experiencia previa) influyen directamente en la tasa de respuesta a phishing (Diaz et al., 2018).
3. Intervenciones educativas y normativas institucionales pueden fortalecer la defensa del estudiante, según el modelo Teoría de la Motivación de Protección y Teoría de la Evitación de Amenazas Tecnológicas.

El análisis de la vulnerabilidad de los estudiantes universitarios ante ataques de phishing requiere comprender los factores psicológicos, contextuales y educativos que influyen en su comportamiento digital. Desde una perspectiva teórica, se asumen diversos enfoques que permiten explicar por qué ciertos individuos son más propensos a ser víctimas de este tipo de ataques.

En primer lugar, la Teoría de la Motivación de Protección, propuesta por Rogers (1975), proporciona una base sólida para analizar el comportamiento de los usuarios ante amenazas de seguridad. Esta teoría sostiene que las personas responden a situaciones de riesgo en función de la percepción de la severidad del daño, su vulnerabilidad personal, la eficacia de la respuesta y su capacidad para enfrentarla. En el contexto de los ataques de phishing, esta teoría ayuda a entender cómo los estudiantes evalúan los correos o mensajes sospechosos y qué tan motivados están para protegerse.

Asimismo, el phishing se enmarca dentro de las estrategias de ingeniería social, entendida como el conjunto de técnicas que buscan manipular psicológicamente a los individuos para que realicen acciones perjudiciales sin percatarse. Jakobsson y Myers (2006) destacan que el phishing no solo implica aspectos técnicos, sino también sociales y cognitivos, ya que explota la confianza, el desconocimiento o la urgencia emocional de las víctimas. Esta perspectiva permite analizar cómo los atacantes diseñan sus mensajes y cómo los estudiantes interpretan estos estímulos, lo cual es clave para el diseño del instrumento de evaluación.

Por otro lado, se reconoce la importancia del concepto de vulnerabilidad digital, el cual hace referencia a la propensión de los usuarios a enfrentar riesgos en entornos virtuales debido a la falta de conocimientos o competencias digitales. Sheng et al. (2010) identificaron que

variables como la edad, el género, la formación académica, el tipo de carrera y la familiaridad con la tecnología afectan directamente la probabilidad de ser víctima de phishing. Estos factores individuales y contextuales son relevantes para establecer relaciones entre las características de los estudiantes y su nivel de exposición a los ataques.

Desde un enfoque educativo, el conocimiento sobre ciberseguridad y la alfabetización digital crítica constituyen competencias fundamentales para reducir la vulnerabilidad. Hadlington (2017) argumenta que los usuarios con bajo nivel de conciencia en seguridad tienden a comportarse de manera más impulsiva y arriesgada en internet, lo que incrementa la posibilidad de caer en fraudes digitales. En este sentido, la evaluación del conocimiento mediante un cuestionario estructurado permite identificar brechas formativas en los estudiantes.

Herramientas y Técnicas de Ciberseguridad

Ngrok: Túneles Seguros para Exposición de Servicios Locales. Ngrok es una herramienta de código abierto que permite exponer aplicaciones locales a Internet mediante la creación de túneles seguros. Es ampliamente utilizada en desarrollo de software y pruebas de penetración para simular accesos remotos a servicios internos. Sin embargo, su uso indebido ha sido documentado en actividades maliciosas, como la instalación de servidores RDP o VPN accesibles desde Internet, lo que facilita el control remoto no autorizado de sistemas comprometidos (Hammond, 2021).

A pesar de sus aplicaciones legítimas, Ngrok ha sido objeto de análisis de seguridad debido a su potencial para ser explotado en ataques. Investigaciones han identificado su uso en la creación de túneles para exfiltración de datos y control remoto de sistemas infectados,

destacando la necesidad de monitorear y detectar actividades sospechosas asociadas a esta herramienta.

Nmap: Exploración y Auditoría de Redes. Nmap (Network Mapper) es una herramienta de código abierto para la exploración de redes y auditoría de seguridad. Permite descubrir hosts y servicios en una red mediante el envío de paquetes y el análisis de las respuestas obtenidas. Es ampliamente utilizada tanto por administradores de sistemas para evaluar la seguridad de sus redes como por atacantes para identificar vulnerabilidades en sistemas remotos.

La versatilidad de Nmap se debe a su capacidad para realizar escaneos de puertos, detectar servicios y sistemas operativos, y adaptarse a condiciones de red variables. Además, su motor de scripts permite realizar detección avanzada de servicios y vulnerabilidades, lo que lo convierte en una herramienta esencial en pruebas de penetración y auditorías de seguridad.

ZPhisher: Automatización de Ataques de Phishing. ZPhisher es una herramienta de código abierto diseñada para automatizar la creación de páginas de phishing que imitan sitios web legítimos, con el objetivo de capturar credenciales de usuarios desprevenidos. Utiliza plantillas predefinidas para diversos servicios en línea, facilitando la ejecución de campañas de ingeniería social (V y Selvi, 2024)

Aunque su uso está destinado a fines educativos y de concienciación en seguridad, ZPhisher ha sido identificado como una herramienta utilizada en ataques maliciosos. Estudios han analizado su funcionamiento y han discutido las implicaciones éticas y legales de su uso, destacando la importancia de emplear tales herramientas de manera responsable y dentro de un marco legal adecuado (V y Selvi, 2024).

Kali Linux: Plataforma Integral para Pruebas de Penetración. Kali Linux es una distribución basada en Debian diseñada para pruebas de penetración y auditoría de seguridad. Incluye una amplia gama de herramientas preinstaladas, como Nmap, Metasploit, Wireshark y Burp Suite, que permiten realizar evaluaciones de seguridad exhaustivas en sistemas y redes.

Su entorno de trabajo está optimizado para profesionales de la seguridad, ofreciendo un sistema robusto y flexible que facilita la realización de pruebas de penetración y la identificación de vulnerabilidades en infraestructuras tecnológicas.

Métodos

Tipo de Investigación

El presente estudio adopta un enfoque cuantitativo, dado que el interés central radica en obtener datos numéricos sobre la vulnerabilidad de los estudiantes frente a ataques de phishing. La cuantificación de respuestas a correos simulados permite analizar proporciones, identificar patrones de comportamiento y realizar comparaciones entre grupos, cumpliendo con los objetivos de determinar niveles generales de vulnerabilidad y evaluar diferencias según sexo, edad y carrera.

Se emplea un diseño descriptivo-correlacional, ya que el propósito del estudio es caracterizar la vulnerabilidad de los estudiantes y explorar posibles asociaciones entre variables observables. La utilización de correos electrónicos simulados como instrumento de recolección de datos no implica manipulación experimental de variables, sino la creación de un escenario controlado que permite observar la reacción natural de los participantes. Este diseño resulta adecuado para los objetivos planteados, porque posibilita describir tendencias, comparar grupos y examinar relaciones sin asumir causalidad.

En cuanto al alcance, el estudio es principalmente descriptivo, porque se centra en identificar el nivel de vulnerabilidad y los patrones de respuesta de los estudiantes. Además, tiene un alcance comparativo y correlacional al evaluar diferencias entre sexo y carrera, así como la relación entre edad y vulnerabilidad. Sin embargo, se aclara que los resultados reflejan únicamente observaciones y asociaciones, sin permitir inferencias causales, lo cual garantiza la pertinencia del estudio al nivel descriptivo planteado.

Población y Selección de la Muestra

La población de estudio está compuesta por 700 estudiantes de la modalidad cuatrimestral de la UCN, con sede en Jinotepe que se encuentren matriculados durante el año 2025, y que tengan acceso a correo electrónico registrados en la base de datos de la universidad. Con el fin de obtener una muestra representativa de la población, se empleó un muestreo aleatorio simple. Este tipo de muestreo garantizó que todos los estudiantes tengan la misma probabilidad de ser seleccionados, lo que minimizó cualquier sesgo en la selección de participantes y mejora la generalización de los resultados.

Para asegurar la precisión en los resultados, se fijó un nivel de confianza del 95% y un margen de error del 5%, lo que implicó que el tamaño de la muestra debe ser de 249 estudiantes. De esta manera, se aseguró que los participantes sean adecuados para recibir los ataques de phishing simulados a través de correos electrónicos, garantizando la validez interna y externa del estudio, lo que permitió evaluar la eficacia para obtener datos personales sensibles.

Tabla 2: Criterios de inclusión

Criterio	Descripción
Acceso a correo	El estudiante debe tener acceso a un correo electrónico registrado en la base de datos de la universidad.
Ser estudiante de la modalidad cuatrimestral	Debe ser un estudiante matriculado en la universidad durante el primer cuatrimestre 2025.

Tabla 3: Criterios de exclusión

Criterio	Descripción
Estudiantes que no usan correo	Si un estudiante no utiliza su correo para fines académicos, no será considerado.
Estudiantes de la modalidad semestral	Estudiantes de medicina, enfermería y medicina veterinaria.

Técnicas e Instrumentos de Recolección de Datos

Objetivo 1. determinar el nivel de vulnerabilidad de los estudiantes de la UCN sede Jinotepe frente a ataques de phishing durante el I semestre 2025.

Instrumentos y Herramientas

Las simulaciones se realizaron utilizando las siguientes herramientas y entornos tecnológicos:

- **Ngrok. P**ara desplegar dominios temporales y exponer servicios locales de manera segura.
- **Zphisher.** Para generar automáticamente páginas de phishing simuladas y correos electrónicos educativos.
- **Kali Linux y Nmap.** Para crear un entorno controlado de pruebas, identificando puertos y dispositivos conectados y evitando impacto sobre sistemas externos.

Procedimiento

1. Preparación del entorno seguro en Kali Linux y despliegue de dominios mediante Ngook.
2. Creación de ataques de phishing simulados con Zphisher, replicando escenarios comunes de ingeniería social.

3. Envío de correos simulados a los participantes durante dos semanas, en los horarios programados:

- 10:00 am – 11:00 am
- 4:00 pm – 8:00 pm

4. Registro de las respuestas de los estudiantes sin recolectar datos personales ni información sensible, únicamente identificando si cada participante caía en la trampa o detectaba correctamente el intento de phishing.

Consideraciones legales y éticas

1. Todas las simulaciones se realizaron en estricto cumplimiento de la Ley de Ciberdelitos de Nicaragua, evitando comprometer información personal real de los estudiantes.
2. Los participantes fueron informados sobre la naturaleza académica y segura de las pruebas, garantizando el respeto a la ética y confidencialidad.
3. Los datos recolectados no incluyeron información sensible; solo se registró el comportamiento frente a los correos simulados, con fines de análisis académico y mejora de estrategias preventivas.

Registro y Análisis de Resultados

1. Los resultados se registraron en una base de datos segura, indicando únicamente si los estudiantes interactuaron con los ataques simulados o los detectaron correctamente.
2. Se evaluó la vulnerabilidad según variables como carrera, sexo, y edad con una base de datos ya existente.
3. Los hallazgos permitieron identificar patrones de comportamiento y diseñar estrategias educativas para promover la ciberseguridad de los estudiantes.

Objetivo 2. Analizar la vulnerabilidad de los estudiantes frente a ataques de phishing según sexo y carrera.

Técnica: Se aplicó un análisis comparativo de grupos por sexo y carrera, dado que estas variables pueden influir en la respuesta frente a los ataques. Esta técnica facilita identificar patrones o diferencias entre subgrupos.

Instrumento: Se empleó el registro de interacciones de los ataques simulados combinado con la base de datos demográficos existente, que contiene información sobre sexo y carrera de los estudiantes. A partir de la disponibilidad de estos datos se segmentaron los resultados de manera precisa, evitando la necesidad de recopilar información adicional y aumentando la confiabilidad del análisis.

Objetivo 3. Evaluar la vulnerabilidad de los estudiantes frente a ataques de phishing según rangos de edad.

Técnica: Se realizó un análisis comparativo por rangos etarios, considerando que la edad puede influir en la experiencia tecnológica y la capacidad de identificar correos maliciosos. Esta técnica permite detectar tendencias relacionadas con la vulnerabilidad según la etapa académica de cada estudiante.

Instrumento: Se utilizó el registro de interacciones de los correos simulados junto con los datos de edad ya disponibles en la base de datos demográficos, lo que posibilita clasificar la información por rangos etarios y realizar un análisis más preciso y eficiente.

Confiabilidad y Validez de los Instrumentos (formulación y validación)

La formulación y validación de los instrumentos empleados en la investigación se enfocó en garantizar que las mediciones de vulnerabilidad frente a ataques de phishing fueran precisas, consistentes y representativas del fenómeno de estudio. El instrumento principal consistió en los ataques simulados de phishing mediante correo electrónico, cuyo diseño se basó en escenarios reales y adaptados al contexto académico de los estudiantes de la UCN sede Jinotepe. La construcción de los escenarios consideró posibles estrategias de phishing que los estudiantes podrían enfrentar, asegurando que el instrumento midiera efectivamente la susceptibilidad ante este tipo de ataques.

La validez de contenido fue asegurada mediante la revisión y juicio de expertos en ciberseguridad y educación, quienes evaluaron la pertinencia, claridad y realismo de los correos simulados, así como la capacidad del instrumento para reflejar los comportamientos esperados frente a los ataques. Además, la disponibilidad de la base de datos demográficos existente (sexo, carrera, edad) permitió segmentar los resultados de manera significativa y objetiva, reforzando la validez del análisis sin necesidad de recopilar información adicional.

La confiabilidad del instrumento se centró en la consistencia de las mediciones obtenidas a través de los registros de interacción ante los correos simulados. La naturaleza binaria del registro (1 = cayó en la trampa; 0 = no cayó) permitió una evaluación objetiva y repetible, minimizando la subjetividad en la interpretación de los resultados. La combinación del diseño estandarizado de los ataques simulados y la utilización de la base de datos demográficos previamente validada fortalece la confiabilidad del instrumento, garantizando que los resultados reflejen de manera precisa el nivel de vulnerabilidad de los estudiantes.

Procedimientos para el Procesamiento y Análisis de Datos

Una vez recolectada la información a través de los ataques simulados de phishing, los datos fueron organizados y preparados para su análisis. Cada registro de interacción fue vinculado con los datos demográficos existentes de los estudiantes, incluyendo sexo, carrera, edad y año académico, lo que permitió una segmentación precisa y evitó la recopilación de información adicional, garantizando eficiencia y fiabilidad en el manejo de los datos.

Fines Educativos y de investigación

Los correos electrónicos utilizados en este estudio fueron simulados únicamente con fines educativos y de investigación, con el propósito de evaluar la vulnerabilidad de los estudiantes ante posibles ataques de phishing, en ningún momento se accedió a cuentas reales ni se recopilaron contraseñas u otra información personal sensible, ya que se enfatizó en generar evidencia para fortalecer la alfabetización digital y la conciencia en ciberseguridad dentro de la comunidad estudiantil.

En otro aspecto todas las acciones se realizaron de manera controlada, esto porque los enlaces de simulación de ataques estuvieron disponibles únicamente durante 40 minutos y fue exclusivo para estudiantes que formaron parte de la muestra, de forma que, al compartir el enlace con otros compañeros, éste no tenía ningún acceso, esta medida garantizó la protección de los datos de los participantes y respetando las normativas legales vigentes en Nicaragua sobre delitos informáticos y protección de información.

El procesamiento de los datos incluyó la depuración de registros duplicados, incompletos o inconsistentes, y la codificación de las variables: la vulnerabilidad se registró de manera binaria, mientras que las variables demográficas fueron categorizadas según los grupos

correspondientes (sexo: masculino/femenino; carrera: Ingeniería en Sistemas, Administración, Psicología, Derecho, etc.; edad: rangos etarios predefinidos; año académico: primero a sexto). Se especificó cómo se manejaron valores faltantes para asegurar consistencia en el análisis.

Para el análisis estadístico se utilizó SPSS v27, aplicando técnicas descriptivas y comparativas. Se calcularon frecuencias, porcentajes, medias y distribuciones de vulnerabilidad general, así como de cada grupo segmentado por sexo, carrera, edad y año académico. Posteriormente, se realizaron pruebas de asociación como chi-cuadrado para variables categóricas y prueba z para proporciones, utilizando un nivel de significancia de $p < 0,05$. Esto permitió determinar si existían relaciones significativas entre la vulnerabilidad y las variables sociodemográficas de los estudiantes.

Los resultados se visualizaron mediante tablas y gráficos, lo que facilitó la interpretación de los patrones de vulnerabilidad y la identificación de subgrupos con mayor riesgo. La replicabilidad del estudio se aseguró mediante la documentación detallada del procesamiento de datos y la configuración de variables en SPSS v27.

Finalmente, se garantizaron las consideraciones éticas y de confidencialidad, de forma que los datos fueron tratados de manera anónima y los correos simulados fueron utilizados únicamente con fines educativos, sin comprometer información sensible de los participantes. Esto respaldó la validez de los hallazgos y su aplicabilidad en el diseño de estrategias de prevención frente a ataques de phishing.

Resultados

En esta sección se presentan los hallazgos obtenidos a partir del análisis de los datos recolectados en el estudio sobre la vulnerabilidad de los estudiantes universitarios ante ataques de phishing. 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, 92 (36,9%) resultaron vulnerables ante los ataques simulados, mientras que 157 (63,1%) no lo fueron. Comparando esta proporción con la hipótesis nula ($P = 0,5$) mediante prueba z para proporciones, se obtuvo un valor de $z = -4,13$ ($p < 0,05$), lo que indica que existe un nivel observable de vulnerabilidad en la muestra, confirmando la hipótesis general planteada.

Al analizar la vulnerabilidad por sexo, se observó que 35 de 101 estudiantes masculinos (34,7%) y 57 de 148 estudiantes femeninas (38,5%) resultaron vulnerables. La prueba de chi-cuadrado de Pearson indicó $\chi^2 = 0,384$, $gl = 1$, $p = 0,535$, y la prueba exacta de Fisher $p = 0,593$, lo que confirma que no existen diferencias significativas entre hombres y mujeres. Esto evidencia que la vulnerabilidad ante phishing no depende del sexo en esta muestra.

La distribución por edad mostró que la mayor proporción de estudiantes vulnerables se encuentra en el grupo de 17 a 22 años. Al examinar cada edad individualmente, se observan algunas variaciones, pero la prueba chi-cuadrado indicó $\chi^2 = 25,599$, $gl = 28$, $p = 0,595$, mientras que la razón de verosimilitud arrojó $p = 0,224$ y la asociación lineal por lineal $p = 0,518$, lo que evidencia que las diferencias entre edades no son estadísticamente significativas.

Al analizar la vulnerabilidad por año académico, se encontró que los primeros años concentraban la mayor cantidad absoluta de casos vulnerables (32/95 = 33,7%), seguidos de los terceros años (16/31 = 51,6%) y quintos años (14/38 = 36,8%). La prueba chi-cuadrado de independencia indicó $\chi^2 = 4,677$, gl = 5, p = 0,457, mostrando que las diferencias observadas entre años no son significativas.

Respecto a la carrera, las proporciones de vulnerabilidad fueron: Ingeniería en Sistemas 10/34 (29,4%), Administración 11/28 (39,3%), Psicología 13/31 (41,9%), Derecho 11/33 (33,3%), Farmacia 12/38 (31,6%), Contabilidad Pública y Auditoría 6/27 (22,2%), Mercadotecnia 11/25 (44%), Banca y Finanzas 2/2 (100%), Relaciones Internacionales y Comercio Exterior 10/20 (50%), Administración Turismo y Hotelería 6/11 (54,5%). La prueba chi-cuadrado indicó $\chi^2 = 11,27$, gl = 9, p = 0,258, evidenciando que no hay diferencias significativas entre carreras.

Los resultados muestran que existe un nivel observable de vulnerabilidad frente a ataques de phishing entre los estudiantes de la UCN sede Jinotepe durante el I cuatrimestre 2025. Sin embargo, las variables sociodemográficas analizadas como el sexo, edad, año académico y carrera, no presentaron asociaciones significativas con la vulnerabilidad, lo que sugiere que otros factores podrían influir en la susceptibilidad, como hábitos digitales, experiencia previa con incidentes de seguridad o exposición a capacitaciones en ciberseguridad. Además, futuros estudios podrían incluir variables adicionales como nivel de conocimiento en seguridad informática, frecuencia de uso del correo institucional o comportamiento en redes sociales.

Tabla 4: Pruebas de hipótesis

Variable	Hipótesis nula (H_0)	Prueba	Estadístico	p	Resultado
General	P = 0,5	Z-proporciones	-4,13	<0,05	H_0 rechazada
Sexo	Phombres=Pmujeres=0,5	Chi-cuadrado de Pearson	0,384	0,535	H_0 no rechazada
Edad	P17−22=P23−28=…=P49=0,5	Chi-cuadrado	25,599	0,595	H_0 no rechazada
Año académico	P1=P2=…=P6=0,5	Chi-cuadrado	4,677	0,457	H_0 no rechazada
Carrera	PIng.Sist=PAdm=…=PAdm.Tur=0,5	Chi-cuadrado	11,27	0,258	H_0 no rechazada

Discusión

Los hallazgos muestran que aproximadamente un 36,9% de los estudiantes fueron vulnerables ante ataques simulados de phishing, evidenciando que una proporción considerable de la población estudiantil está expuesta a riesgos digitales. Esto confirma la hipótesis general y resalta la importancia de implementar estrategias de concientización y formación en ciberseguridad en el entorno universitario.

Aunque se observaron diferencias absolutas por sexo, edad, año académico y carrera, las pruebas estadísticas indicaron que ninguna de estas variables sociodemográficas presentó asociaciones significativas con la vulnerabilidad. Esto sugiere que los factores sociodemográficos no son determinantes para predecir la susceptibilidad al phishing, y que otras variables como hábitos digitales, experiencia previa y nivel de conocimiento en seguridad informática podrían tener mayor relevancia.

Los estudiantes más jóvenes (17–22 años) presentaron la mayor cantidad absoluta de vulnerables, probablemente debido a menor experiencia en la detección de correos fraudulentos y hábitos digitales aún en formación. Sin embargo, la significancia estadística no respalda una relación causal, por lo que se recomienda que futuras investigaciones incluyan variables adicionales que puedan explicar la vulnerabilidad.

En cuanto al año académico y la carrera, no se identificaron patrones claros ni significativos, lo que indica que la vulnerabilidad frente al phishing es transversal a todos los niveles académicos y áreas de estudio. Esto refuerza la necesidad de estrategias educativas generales en ciberseguridad, más que intervenciones específicas por grupo.

Estos resultados aportan evidencia sobre la vulnerabilidad de los estudiantes universitarios y destacan la necesidad de programas educativos que fortalezcan la alfabetización digital y la capacidad de detección de correos fraudulentos. Aunque no se encontraron relaciones significativas con las variables sociodemográficas, el estudio tiene valor al evidenciar que un porcentaje considerable de estudiantes puede ser susceptible a ataques de phishing, justificando la continuidad de investigaciones y la implementación de políticas de concientización en ciberseguridad dentro del entorno universitario.

Conclusión

El estudio sobre la vulnerabilidad de los estudiantes universitarios ante ataques de phishing en la UCN sede Jinotepe durante el I cuatrimestre de 2025 evidenció que un 36,9% de los participantes resultaron vulnerables a los correos simulados. Este hallazgo confirmó que una proporción considerable de la población estudiantil estuvo expuesta a riesgos digitales y subraya la importancia de fortalecer la seguridad y conciencia en el uso de herramientas electrónicas. Además, resalta la necesidad de desarrollar políticas institucionales orientadas a la prevención de incidentes de phishing y otras amenazas cibernéticas dentro del entorno universitario.

El análisis de las variables sociodemográficas como el sexo, edad, año académico y carrera indicó que ninguna presentó asociaciones significativas con la vulnerabilidad ($p > 0,05$). Esto evidenció que estas características no fueron determinantes para predecir la susceptibilidad al phishing en la muestra estudiada y sugiere que la vulnerabilidad no se concentra en grupos específicos. Por lo tanto, factores como hábitos digitales, experiencia previa con incidentes de seguridad y nivel de conocimiento en ciberseguridad podrían ser más relevantes para explicar la exposición de los estudiantes a este tipo de ataques.

Aunque los estudiantes más jóvenes y algunos años académicos presentaron mayor número absoluto de casos vulnerables, los resultados estadísticos confirmaron que estas diferencias no fueron significativas. Esto sugiere que la vulnerabilidad fue transversal a todos los niveles y carreras, afectando por igual a la comunidad estudiantil. El patrón observado refuerza la necesidad de implementar programas educativos generales en ciberseguridad, que incluyan estrategias preventivas y formación en detección de correos fraudulentos para toda la población estudiantil.

En consecuencia, se destacó la importancia de promover la alfabetización digital y fortalecer la capacidad de identificación de riesgos en entornos virtuales, a fin de reducir la exposición de los estudiantes a ataques de phishing. Asimismo, los hallazgos justificaron la realización de investigaciones futuras que incluyan variables adicionales, como nivel de conocimiento en seguridad informática, hábitos de uso de correo institucional y comportamiento en redes sociales, con el objetivo de comprender mejor los factores que influyen en la vulnerabilidad ante estas amenazas.

Referencias

Alqahtani, S., Nanda, P., & 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. Lecture Notes in Computer Science*, *15463.* Springer, Singapore. https://doi.org/https://doi.org/10.1007/978-981-96-1483-7_27

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. (2021). A Systematic Literature Review on Phishing and Anti-Phishing Techniques. *Pakistan Journal of Engineering and Technology, PakJET, 4*(1), 163-168. https://doi.org/https://doi.org/10.48550/arXiv.2104.01255

Asamblea Nacional de la República de Nicaragua. (2020). *LEY N°. 1042, LEY ESPECIAL DE CIBERDELITOS.* http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/803E7C7FBCF44D7706258611007C6D87

Asiri, S., Xiao, Y., Alzahrani, S., Li, S., & Li, T. (18 de January de 2023). A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks. *IEEE Access, 11*, 6421 - 6443. https://doi.org/https://doi.org/10.1109/ACCESS.2023.3237798

Baki, S., & Verma, R. (2015). Sixteen Years of Phishing User Studies: What. *JOURNAL OF LATEX CLASS FILES, 14*(8). https://doi.org/https://doi.org/10.48550/arXiv.2109.04661

Cabezas-Molina, E. M., & Fiallos-Aguilar, H. C. (2024). Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial – Un enfoque práctico para

mejorar la resiliencia. *INNOVA Research Jorunal, 9*(4). https://doi.org/https://doi.org/10.33890/innova.v9.n4.2024.2678

Castillo, C. (30 de Octubre de 2024). *BBVA*. BBVA: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Collado, A. (11 de Septiembre de 2024). *Computing.es.* Computing.es: https://www.computing.es/seguridad/tipos-comunes-fraude-espana-phishing-smishing-vishing/

Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Counter-Phishing Recommendations for Federal Agencies.* Washington, D.C., EE. UU.: U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Counter-Phishing_Recommendations_for_Federal_Agencies.pdf

Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *arXiv*. https://doi.org/https://doi.org/10.48550/arXiv.1811.06078

Dubovecka, K. (2024). Vulnerability of Students of Masaryk University to Two Different Types of Phishing. *ACIG, 3*(2). https://doi.org/https://doi.org/10.60097/ACIG/190268

El País. (2024). *El País*. El País: https://elpais.com/tecnologia/2024-08-17/no-es-tu-prima-es-un-estafador-y-quiere-vaciar-tu-cuenta-corriente-asi-funciona-el-vishing.html

ESET Latinoamérica. (2018). *Instituciones educativas aseguran sufrir incidentes de seguridad.* Buenos Aires, Argentina: ESET Latinoamérica. https://www.welivesecurity.com/la-es/2018/05/11/instituciones-educativas-aseguran-sufrir-incidentes-seguridad/

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024.* La Haya, Países Bajos: Europol. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2021). Defending against Phishing Attacks: Taxonomy of Methods, Current. *arXiv, 1*. https://doi.org/https://doi.org/10.48550/arxiv.org/abs/1705.09819

Hable, F., Schirrmacher, N.-B., & Hooff, B. v. (2025). *Phishing Attacks in Context: Organizational Factors Shaping Phishing Susceptibility Phishing Susceptibility.* https://core.ac.uk/reader/658474400

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). https://doi.org/https://doi.org/10.1016/j.heliyon.2017.e00346

Hammond, J. (16 de march de 2021). *HUNTRESS*. HUNTRESS: https://www.huntress.com/blog/abusing-ngrok-hackers-at-the-end-of-the-tunnel

IBM Security. (2025). *X-Force Threat Intelligence Index 2025.* Armonk, Nueva York, EE. UU.: IBM Corporation. https://www.ibm.com/reports/threat-intelligence

INTERPOL. (2023). *Annual Report.* INTERPOL. https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft.* Wiley: IEEE Press. https://doi.org/10.1002/0470086106

Kaspersky. (2023). *Kaspersky LATAM Threat Report 2023.* Kaspersky. https://latam.kaspersky.com

Kenneth, A., Hayashi, B. B., & Lionardi, J. (2023). Phishing Attack Awareness Among College Students. *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS).* Yogyakarta, Indonesia : IEEE. https://doi.org/10.1109/ICE3IS59323.2023.10335412

Kosinski, M. (17 de mayo de 2024). *IBM*. IBM: https://www.ibm.com/es-es/think/topics/phishing

Lizarraga, J. R., Hernández, J. A., Garay, M. A., Navarro, A. F., & Espinoza, D. E. (2019). PROTOCOLO PARA LA PREVENCIÓN DE ATAQUES DE PHISHING. *ReDTIS, 3*(1). https://www.redtis.org/index.php/Redtis/article/view/34

Natalia, M. C., Cayhono, S., Purwoko, R., & Putra, I. G. (2023). Gamification Design as Learning Media to Motivate Students to Increase Cyber Security Awareness towards Phishing. *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS).* akarta Selatan, Indonesia : IEEE. https://doi.org/https://doi.org/10.1109/ICIMCIS60089.2023.10349069

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (January de 2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for. *IIETA, 18*(1), 255-263. https://doi.org/https://doi.org/10.18280/ijsdp.180127

Organización de los Estados Americanos (OEA). (2022). *Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades.* Washington, D.C., EE. UU.: Organización de los Estados Americanos (OEA). https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

Rogers, R. W. (2010). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology, 9*. https://doi.org/https://doi.org/10.1080/00223980.1975.9915803

Sheng, S., Holbrook, M., Kumaraguru, P., & Lorrie Cranor, J. D. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010).* Atlanta, GA, Estados Unidos: ACM (Association for Computing Machinery). https://doi.org/https://doi.org/10.1145/1753326.1753383

TREND MICRO. (2025). *TREND MICRO*. TREND MICRO: https://www.trendmicro.com/es_es/what-is/phishing/types-of-phishing.html

V, V., & Selvi, D. S. (2024). ZPHISHER TOOL IN CYBER SECURITY. *International Research Journal of Modernization in Engineering Technology and Science, 6*(12). https://www.irjmets.com/uploadedfiles/paper/issue_12_december_2024/65449/final/fin_irjmets1734768076.pdf

Verizon. (2025). *2025 Data Breach Investigations Report.* Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/

Anexos

Anexo 1: Operacionalización de Variables

Tabla 5: Operacionalización de variables

Variable	Dimensión	Indicador	Instrumento	Escala	Tipo de análisis
Vulnerabilidad frente a ataques de phishing	Nivel de vulnerabilidad	Respuesta al correo simulado (sí/no)	Registro de respuestas a correos simulados	Nominal (0 = No, 1 = Sí)	Descriptivo (proporciones, frecuencias)
Sexo	-	Sexo del estudiante	Base de datos existente	Nominal (1 = Masculino, 2 = Femenino)	Comparativo (frecuencias, proporciones)
Edad	-	Rango de edad del estudiante	Base de datos existente	Ordinal (18–20, 21–23, 24–26, etc.)	Correlacional (coeficiente de asociación)
Carrera	-	Carrera del estudiante	Base de datos existente	Nominal (Ingeniería en Sistemas, etc.)	Comparativo (frecuencias, proporciones)

Anexo 2: Tablas de Frecuencias y Gráficos Estadísticos

Tabla 6: Vulnerabilidad de estudiantes ante ataques de phising

	N	%
Si	92	36,9%
No	157	63,1%

Figura 1: vulnerabilidad de estudiantes ante ataques de phising

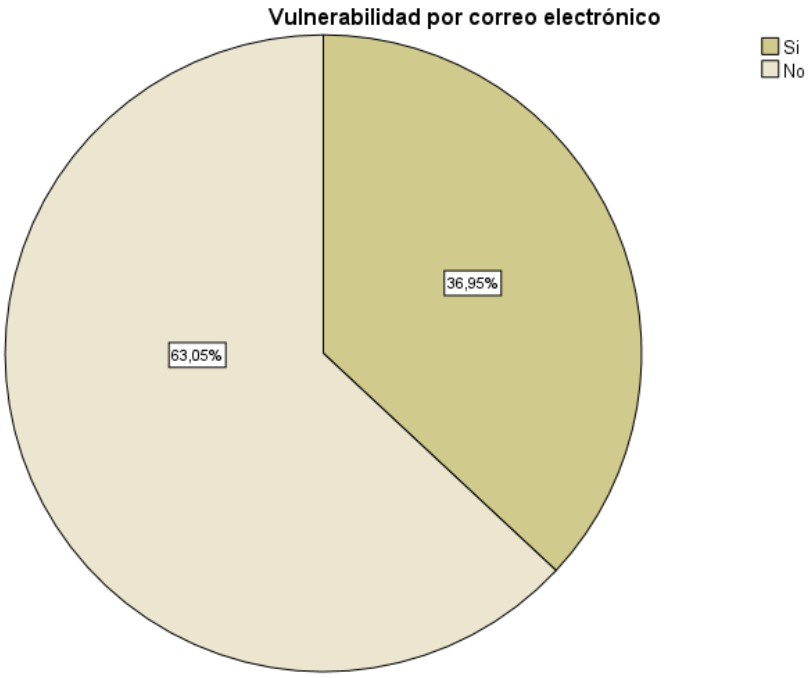


Tabla 7: Sexo*Vulnerabilidad

		Vulnerabilidad por correo electrónico		
		Si	No	Total
Sexo	Masculino	35	66	101
	Femenino	57	91	148
Total		92	157	249

Figura 2: sexo*vulnerabilidad

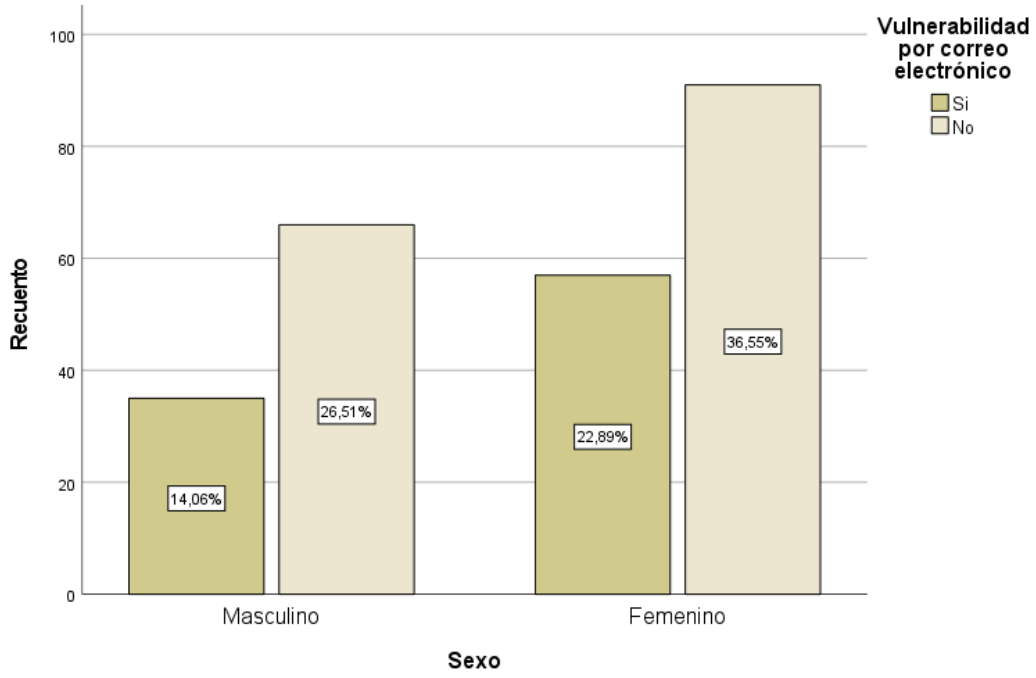


Tabla 8: edad*Vulnerabilidad

		Vulnerabilidad por correo electrónico		Total
		Si	No	
Rango de edades	17-22 años	65	104	169
	23-28 años	14	25	39
	29-34 años	6	14	20
	35-40 años	1	10	11
	41-49 años	6	4	10
Total		92	157	249

Figura 3: edad*vulnerabilidad

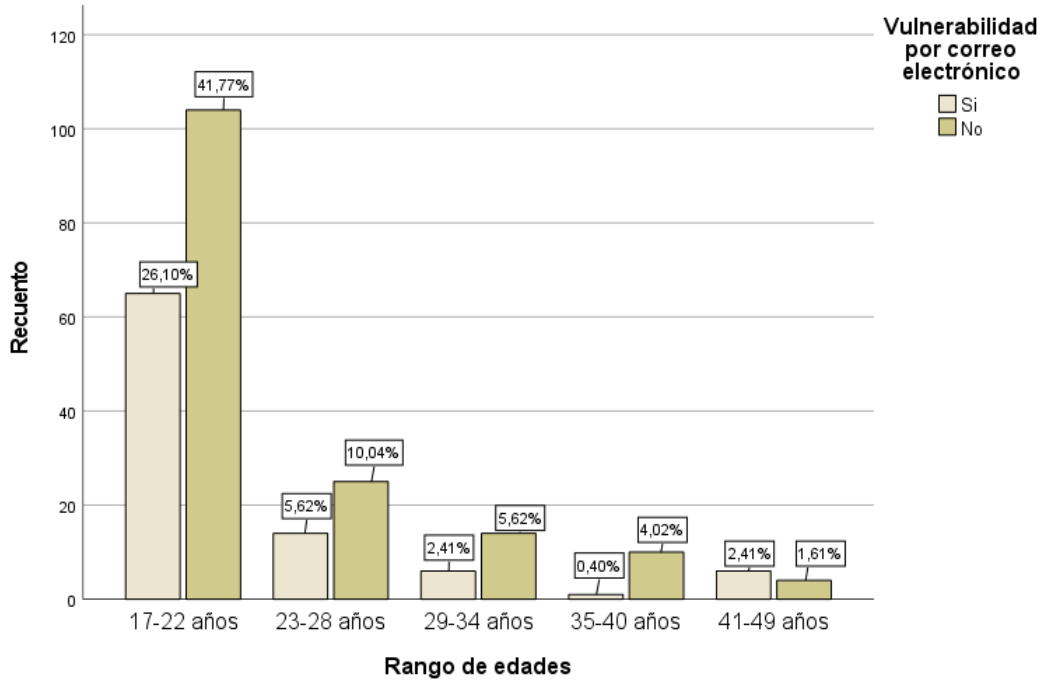


Tabla 9: año que cursa*vulnerabilidad

		Vulnerabilidad por correo electrónico		Total
		Si	No	
Año que cursa	Primer Año	32	63	95
	Segundo Año	19	31	50
	Tercer Año	16	15	31
	Cuarto Año	11	22	33
	Quinto Año	14	24	38
	Sexto Año	0	2	2
Total		92	157	249

Figura 4: año que cursa*vulnerabilidad

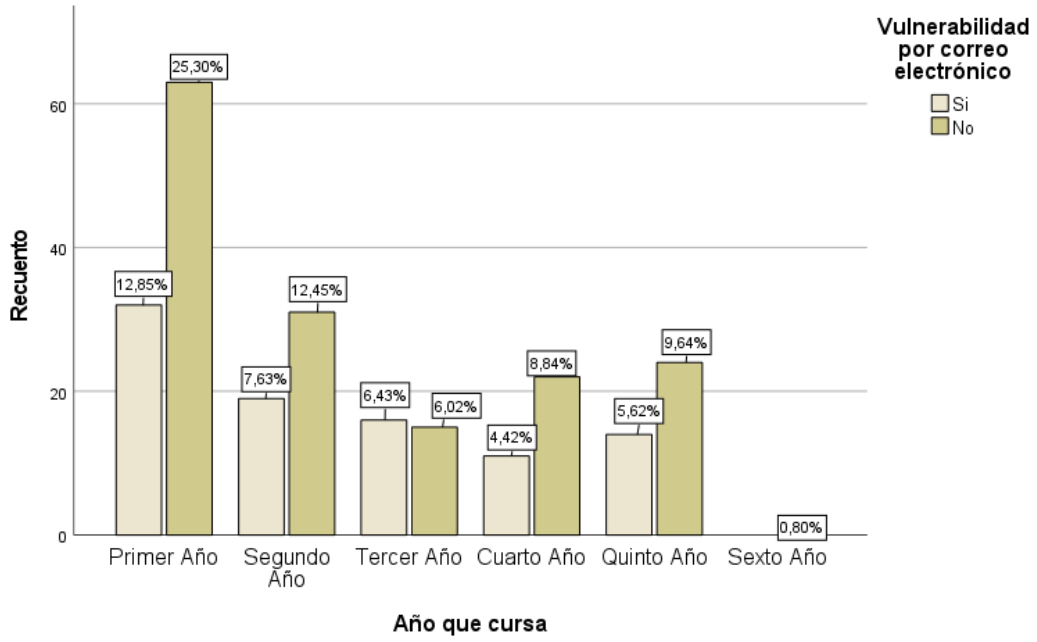
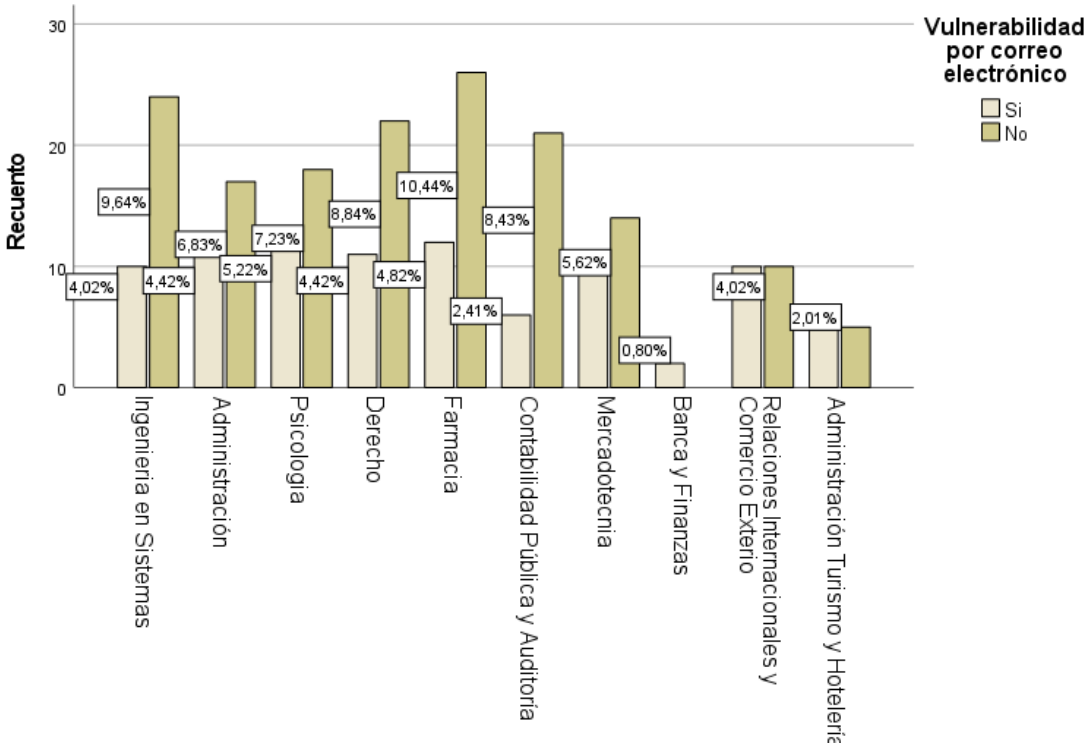


Tabla 10: carrera *vulnerabilidad

		Vulnerabilidad por correo electrónico		Total
		Si	No	
Carrera que cursa	Ingenieria en Sistemas	10	24	34
	Administración	11	17	28
	Psicología	13	18	31
	Derecho	11	22	33
	Farmacia	12	26	38
	Contabilidad Pública y Auditoría	6	21	27
	Mercadotecnia	11	14	25
	Banca y Finanzas	2	0	2
	Relaciones Internacionales y Comercio Exterior	10	10	20
	Administración Turismo y Hotelería	6	5	11
Total		92	157	249

Figura 5: carrera *vulnerabilidad



Anexo 3: Pruebas de Chi-cuadrado

Tabla 11: chi-cuadrado sexo x vulnerabilidad

	Valor	gl	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	,384[a]	1	,535		
Corrección de continuidad[b]	,236	1	,627		
Razón de verosimilitud	,385	1	,535		
Prueba exacta de Fisher				,593	,314
Asociación lineal por lineal	,382	1	,536		
N de casos válidos	249				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 37,32.

b. Sólo se ha calculado para una tabla 2x2

Tabla 12:chi-cuadrado edad x vulnerabilidad

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	25,599[a]	28	,595
Razón de verosimilitud	33,322	28	,224
Asociación lineal por lineal	,419	1	,518
N de casos válidos	249		

a. 43 casillas (74,1%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,37.

Tabla 13: chi-cuadrado carrera x vulnerabilidad

	Valor	gl	Significación asintótica (bilateral)	Sig. Monte Carlo (bilateral)			Sig. Monte Carlo (unilateral)		
				Significación	Intervalo de confianza al 99%		Significación	Intervalo de confianza al 99%	
					Límite inferior	Límite superior		Límite inferior	Límite superior
Chi-cuadrado de Pearson	11,265[a]	9	,258	,262[b]	,250	,273			
Razón de verosimilitud	11,949	9	,216	,257[b]	,246	,268			
Prueba exacta de Fisher-Freeman-Halton	10,802			,278[b]	,267	,290			
Asociación lineal por lineal	2,986[c]	1	,084	,084[b]	,077	,091	,039[b]	,034	,044
N de casos válidos	249								

a. 3 casillas (15,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,74.

b. Se basa en 10000 tablas de muestras con una semilla de inicio 957002199.

c. El estadístico estandarizado es -1,728.

Anexo 4: Simulación de Ataques

Ejemplo 1: Spear Phishing

Asunto: "Invitación exclusiva a la conferencia online de Innovación Tecnológica"
Remitente: soporte@eventos-tec.com (falso)

Cuerpo:
Estimado(a),

Ha sido seleccionado para participar en la Conferencia Internacional de Innovación Tecnológica 2025. Para confirmar su asistencia, ingrese sus datos en el siguiente enlace:

www.eventos-tec-inscripcion.com

Agradecemos su pronta respuesta.

Indicadores de ataque:

- El correo está dirigido específicamente al destinatario (personalización).
- El enlace dirige a un sitio no oficial.
- Solicita información personal sensible (credenciales, datos de registro).

Objetivo: Robo de credenciales y datos personales mediante personalización del mensaje.

Ejemplo 2: Correo con enlace falso

Asunto: "Problema con su suscripción en un servicio digital"
Remitente: soporte@serviciosonline.com (falso)

Cuerpo:
Estimado(a) usuario:

Se ha detectado un error en su suscripción. Para corregirlo, por favor haga clic en el siguiente enlace y actualice sus datos:

[www.serviciosonline-verificacion.com]

Si no actualiza sus datos, su cuenta podría ser suspendida.

Indicadores de ataque:

- El enlace parece legítimo, pero dirige a un dominio falso.

- Mensaje urgente que busca que el usuario actúe sin reflexionar.

Objetivo: Obtener credenciales y datos financieros del usuario.

Ejemplo 3: Correo de urgencia o recompensa

Asunto: "¡Felicidades! Ha ganado un bono de $50 por participar en nuestra encuesta"
Remitente: promociones@encuestas-premios.com (falso)

Cuerpo:
Estimado(a) participante:

¡Felicidades! Ha sido seleccionado para recibir un bono de $50 por completar nuestra encuesta. Para reclamar su premio, haga clic en el enlace a continuación e ingrese su usuario y contraseña:

[www.encuestas-premios-claim.com]

Indicadores de ataque:

- Promete una recompensa para atraer al usuario.
- Solicita credenciales de acceso a cambio de un beneficio.

Objetivo: Robar credenciales aprovechando incentivos y motivación.

Anexo 5: Consentimiento Informado

UNIVERSIDAD CENTRAL DE NICARAGUA

Formato de Evaluación de Expertos – Simulaciones de Phishing

Nombre del evaluador: Jorge A Tercy Hernández
Cargo / Área de especialización: Informática
Fecha: 30/08/2025

Objetivo de la evaluación: Evaluar la efectividad, seguridad y calidad educativa de las simulaciones de phishing aplicadas a estudiantes universitarios.

1. Aspectos Generales de la Simulación (20 puntos)

Criterio	Puntos máximos	Puntos obtenidos	Comentarios
Claridad en los objetivos de la simulación	5	5	
Relevancia educativa del ejercicio	5	5	
Adecuación al nivel académico de los estudiantes	5	5	

2. Aspectos Técnicos (30 puntos)

Criterio	Puntos máximos	Puntos obtenidos	Comentarios
Seguridad del entorno de simulación (sin impacto en sistemas externos)	10	8	
Realismo de los correos y enlaces de phishing	10	9	
Claridad en la redacción de la simulación del phising.	10	10	

3. Aspectos de Seguridad y Ética (30 puntos)

Criterio	Puntos máximos	Puntos obtenidos	Comentarios
Cumplimiento de la Ley de Ciberseguridad y Ciberdelitos de Nicaragua	10	10	
Protección de la información personal de los participantes	10	8	
Evaluación sin riesgos físicos ni psicológicos	5	5	
Registro de resultados de forma anónima y segura	5	5	

UNIVERSIDAD CENTRAL DE NICARAGUA

4. Evaluación Global y Observaciones (20 puntos)

Criterio	Puntos máximos	Puntos obtenidos	Comentarios
Impacto general de la simulación en el aprendizaje y concienciación	10	10	
Recomendaciones de mejora implementables	10	8	

Puntuación Total: 93 / 100

Comentarios generales del experto:

La forma en que se planteó el ataque fué muy atractiva a la vista de los estudiantes los correos tienen una forma practica de inducir a caer en el ataque y solo una observación en cuestión de phishing las acciones pueden representarse en momentos que los usuarios sabían que x empresa estaban en proceso de realizar alguna actividad y de allí iniciar a pensar en el tipo o forma de ataque.