Phishing y Spam: Un correo malintencionado. Seguridad digital de tu información ante el robo de datos

Ricardo M. Candanedo Yau
Universidad de Panamá, Centro Regional Universitario de Panamá Este (CRUPE). Facultad de Informática Electrónica y Comunicación.
Panamá
ricardo.candanedo@up.c.pa
https://orcid.org/0009-0002-5017-9830

Fecha de entrega: 1 de julio de 2025
Fecha de aprobación: 29 de septiembre de2025

DOI: https://doi.org/10.48204/j.are.n51.a8862

Resumen

En la Era de la digitalización, amenazas como el phishing y el spam malicioso representan un riesgo considerable para la seguridad de los datos personales y organizacionales. Esta investigación, llevada a cabo en el Centro Regional Universitario de Panamá Este y la Extensión Universitaria de Tortí de la Universidad de Panamá, evaluó la concienciación y las prácticas de seguridad digital frente a estas amenazas. El objetivo fue identificar el conocimiento y las deficiencias de la comunidad educativa para reconocer y responder a un correo electrónico fraudulento. Se empleó una metodología empírica cuantitativa a través de encuestas, que midieron la percepción de riesgo, el conocimiento para identificar correos fraudulentos y las acciones tomadas frente ataques de ingeniería social y prevención del crimen. Los resultados revelaron brechas significativas en el conocimiento sobre cómo identificar y manejar correos fraudulentos, lo que aumenta la vulnerabilidad al robo de datos, a pesar de la conciencia del riesgo. Se resalta la necesidad de diseñar programas de alfabetización digital y ciberseguridad en entornos educativos de aprendizajes. Se proponen estrategias para fortalecer la resiliencia y prevenir el cibercrimen, destacando la importancia de la educación digital y políticas de seguridad para mitigar los riesgos del correo malicioso.

Palabras clave: alfabetización digital, correos electrónicos, digitalización, educación, prevención, seguridad de los datos.

Phishing and Spam: A malicious email. Digital security for your information against data theft

Abstract

In the age of digitalization, threats such as phishing and malicious spam pose a considerable risk to the security of personal and organizational data. This research, carried out at the East Panama Regional University Center and the Tortí University Extension of the University of Panama, evaluated awareness and digital security practices in the face of these threats.The objective was to identify the knowledge and deficiencies of the educational community in recognizing and responding to fraudulent emails. A quantitative empirical methodology was used through surveys, which measured risk perception, knowledge to identify fraudulent emails, and actions taken against social engineering attacks and crime prevention.The results revealed significant gaps in knowledge about how to identify and handle fraudulent emails, which increases vulnerability to data theft, despite awareness of the risk. The need to design digital literacy and cybersecurity programs in educational learning environments is highlighted. Strategies to strengthen resilience and prevent cybercrime are proposed, emphasizing the importance of digital education and security policies to mitigate the risks of malicious email.

Keywords: digital literacy, emails, digitization, education, prevention, data security.

Introducción

En la era digital, el correo electrónico se ha consolidado como una herramienta esencial para la comunicación en entornos educativos. Sin embargo, su uso generalizado ha sido aprovechado por ciberdelincuentes para llevar a cabo ataques como el *phishing* y el *spam*, que buscan obtener información confidencial de los usuarios mediante engaños y suplantación de identidad (Butavicius et al., 2016; Salahdine et al., 2022). Estos ataques representan una amenaza significativa para la seguridad de la información, ya que pueden conducir al robo de datos personales y académicos. La creciente sofisticación de estas técnicas, impulsada por el uso de inteligencia artificial y la ingeniería social, exige una comprensión profunda de sus mecanismos y la implementación de estrategias efectivas para su prevención (Wang et al., 2019; Ifinedo, 2017).

La digitalización ha transformado radicalmente la forma en que las instituciones educativas operan enseña y aprenden. La vasta cantidad de información personal (datos de estudiantes, registros académicos, información financiera) y la dependencia de plataformas en línea hacen que el sector educativo sea un objetivo atractivo para los ciberdelincuentes (European Union Agency for Cybersecurity [ENISA], 2023). Dentro del amplio espectro de amenazas cibernéticas, el *phishing* y el *spam* malicioso se destacan como vectores primarios de ataque, explotando la ingeniería social para engañar a los usuarios y obtener acceso no autorizado a información sensible o sistemas (Microsoft, 2024; Lain et al., 2021).

El *phishing* es una forma de fraude en línea donde los atacantes se hacen pasar por entidades legítimas (bancos, financieras, servicios en línea, instituciones educativas e incluso proveedores de correo electrónico) para engañar a las víctimas y que revelen información confidencial, como contraseñas o números de tarjetas de crédito. A menudo se manifiesta a través de correos electrónicos falsos, mensajes de texto o sitios web clonados. El *spam*, si bien en su forma más simple es correo no deseado, frecuentemente sirve como vehículo para ataques de *phishing*, distribuyendo *malware* o enlaces fraudulentos. La combinación de estos ataques representa una amenaza persistente y sofisticada, capaz de comprometer cuentas, robar identidades y causar pérdidas financieras o de datos significativas (Cybersecurity and Infrastructure Security Agency [CISA], 2023); Schneier, 2000).

La vulnerabilidad ante ataques de *phishing* y *spam* no reside únicamente en fallas tecnológicas, sino en la "capa humana" de la ciberseguridad (Schneier, 2000). Los ciberdelincuentes

explotan principios psicológicos como la urgencia, la autoridad y la curiosidad para manipular a las víctimas. Las campañas de *phishing* a menudo se disfrazan de comunicaciones importantes, como actualizaciones de sistemas, notificaciones bancarias o incluso mensajes de la propia institución educativa, buscando generar una respuesta impulsiva (Wang et al., 2019; Lain et al., 2021).

La concienciación sobre ciberseguridad se ha convertido en una disciplina crucial. Se entiende como el grado en que los usuarios comprenden la importancia de la seguridad de la información y sus responsabilidades individuales en la protección de los datos (Ifinedo, 2017). Sin embargo, una mera concienciación no es suficiente; debe complementarse con la alfabetización digital, que capacita a los individuos con las habilidades prácticas para navegar de forma segura en el entorno digital, incluyendo la identificación de correos sospechosos, la gestión de contraseñas y el uso de la autenticación (Organisation for Economic Co-operation and Development [OECD], 2018; CISA, 2023).

En el ámbito educativo, la amenaza del robo de datos trasciende la vulnerabilidad de las credenciales individuales, ya que un ciberataque exitoso puede comprometer información altamente sensible, como bases de datos de investigación, registros académicos, información personal de estudiantes y docentes, publicaciones científicas, entre otros activos digitales. Esta situación no solo pone en riesgo la privacidad de las personas, sino que también afecta directamente la reputación institucional y socava la confianza de la comunidad educativa (ENISA, 2023), el sector educativo se ha convertido en un objetivo creciente de ciberamenazas, dada la cantidad de datos valiosos que gestiona y el uso intensivo de entornos digitales con medidas de seguridad frecuentemente inadecuadas.

Por su parte, la (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO], 2011) destaca la importancia de establecer políticas de tecnología educativa que incorporen consideraciones de seguridad digital desde su diseño, asegurando así la protección de los sistemas de información y fomentando un entorno de aprendizaje seguro. En este contexto, comprender las brechas existentes en la concienciación y en las prácticas de seguridad digital dentro de las instituciones educativas se vuelve un paso imprescindible para fortalecer su postura ante las amenazas cibernéticas. Fomentar una cultura de ciberseguridad basada en la formación, la prevención y la responsabilidad compartida es esencial para preservar la integridad de los procesos educativos en la era digital.

Tal y como se advierte la vulnerabilidad es multifacética, por lo que la comunidad educativa del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí, podría verse afectada con el robo de información debido a la falta de conocimiento para identificar estas amenazas (Tecno Futuro, 2025). En este sentido, la presente investigación busca profundizar en cómo la seguridad de la información —pilar fundamental en la sociedad digital— se ve comprometida en los entornos educativos de aprendizaje por las deficiencias en la capacidad de reconocer y responder adecuadamente a correos electrónicos fraudulentos. De este modo, se pretende arrojar luces sobre el nivel de concienciación y las prácticas de seguridad digital que se requieren para garantizar la ciberseguridad.

Materiales y métodos

Se empleó un enfoque empírico cuantitativo, con un diseño no experimental, de tipo correlacional y explicativo, con el objetivo de evaluar el nivel de conocimiento y las prácticas de ciberseguridad —específicamente en relación con phishing y spam— dentro de una muestra de la comunidad educativa (estudiantes, docentes y personal administrativo) del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí de la Universidad de Panamá.

La unidad de análisis estuvo compuesta por los miembros de dicha comunidad, y para su selección se aplicó un muestreo estratificado proporcional, con el fin de asegurar que cada uno de los subgrupos (estudiantes, docentes y administrativos) estuviera adecuadamente representado en la muestra. Esta técnica permitió obtener una muestra más precisa y representativa, minimizando el sesgo que podría haberse generado mediante un muestreo aleatorio simple aplicado sobre la población total.

La población del estudio estuvo conformada por un total de 301 personas, distribuidas en tres estratos: 178 estudiantes de la Facultad de Informática, Electrónica y Comunicación; 81 docentes; y 42 administrativos. Todos pertenecían al Centro Regional Universitario de Panamá Este (CRUPE) y a la Extensión Universitaria de Tortí.

A partir de esta población, se seleccionó una muestra de 100 personas, utilizando un muestreo estratificado proporcional que respetó la representatividad de cada grupo. La distribución de la muestra fue la siguiente: 58 estudiantes de la Facultad de Informática, Electrónica y Comunicación, 25 docentes y 17 administrativos.

En términos porcentuales, la representación muestral por estrato y al azar se calculó de la siguiente manera:

- Estudiantes de la Facultad de Informática, Electrónica y Comunicación: (58 / 178) × 100 = 32.58 %
- Docentes: (25 / 81) × 100 = 30.86 %
- Administrativos: (17 / 42) × 100 = 40.48 %

Asimismo, el promedio general de representación muestral estratificada se obtuvo a partir del siguiente cálculo: (100 / 301) × 100 = 33.22 %, lo que indica una adecuada distribución proporcional entre los distintos grupos. Esta estrategia permitió que cada estrato aportara información de forma equilibrada, fortaleciendo así la validez de los resultados y favoreciendo su generalización al contexto institucional.

En cuanto a la composición detallada de la muestra, participaron 58 estudiantes de la Facultad de Informática, Electrónica y Comunicación. De estos, 25 eran estudiantes de tercer año del programa de Licenciatura en Informática para la Gestión Educativa y Empresarial, y 16 correspondían al nivel de la Maestría en Tecnología de la Información y la Comunicación, ambos grupos pertenecían al Centro Regional Universitario de Panamá Este (CRUPE). Por su parte, 17 estudiantes cursaban el cuarto año del mismo programa de Licenciatura en Informática para la Gestión Educativa y Empresarial, en la Extensión Universitaria de Tortí. Además, se incluyeron 25 docentes de distintas facultades y 17 miembros del personal administrativo, tanto del Centro Regional Universitario de Panamá Este (CRUPE), como de la Extensión Universitaria de Tortí.

Todos los participantes estaban activos durante el primer semestre de 2025, y asistían al turno nocturno de los días de semana en la sede del del Centro Regional Universitario de Panamá Este (CRUPE), y los fines de semana en la Extensión de Tortí. La distribución completa de la muestra por estrato, según el muestreo estratificado proporcional utilizado, se presenta en la Tabla 1.

Tabla 1

Distribución de la muestra por estrato (muestreo estratificado proporcional).

	Población (total)	Muestra	% de representación muestral por estrato
Estudiantes de la Facultad de Informática, Electrónica y Comunicación (a)	178	58	32.58 %
Docentes (b)	81	25	30.86 %
Administrativos (b)	42	17	40.48 %

Nota. (a) La muestra fue seleccionada mediante muestreo estratificado proporcional, considerando la matrícula del primer semestre de 2025 (turno nocturno-CRUPE, Fin de Semana-Ext. Tortí – Universidad de Panamá).
(b) Del CRUPE y la Extensión Universitaria de Tortí

La participación de todos los individuos fue de carácter voluntario y anónimo, con consentimiento informado previo. Todos los participantes son mayores de 18 años y cuentan con correo electrónico, ya sea institucional o personal, activo.

Se diseñó un cuestionario en línea de tipo autoadministrado, compuesto por un total de 30 ítems distribuidos en cuatro secciones temáticas.

La primera sección, Datos Sociodemográficos (3 ítems): Esta sección buscó caracterizar a la población encuestada, en cuanto a edad, género y tipo de actor dentro de la institución.

La segunda sección, Conocimiento sobre Phishing y Spam (12 ítems): Esta sección buscó evaluar la comprensión teórica y práctica de los participantes sobre las amenazas más comunes como el phishing y el spam, así como conceptos fundamentales de ciberseguridad. Las preguntas de opción múltiple y verdadero/falso diseñadas para evaluar la capacidad de identificar características de correos fraudulentos, técnicas de ingeniería social y conceptos básicos de ciberseguridad.

La tercera sección, Prácticas de Seguridad Digital (10 ítems): Se indagó sobre el comportamiento real de los individuos en relación con la ciberseguridad. Se utilizó Escala tipo Likert (1=Nunca a 5=Siempre) sobre la frecuencia con la que los participantes realizan acciones de seguridad, permiten cuantificar la frecuencia con la que los participantes realizan acciones específicas para proteger su información y sus dispositivos. Esto ayuda a identificar fortalezas y debilidades en los hábitos de seguridad.

La cuarta sección, Percepción de Riesgo (5 ítems): consideró el componente psicológico y subjetivo de la seguridad digital esto es, cómo los individuos y la institución perciben la vulnerabilidad. Si alguien no se siente vulnerable, es menos probable que tome precauciones. Se utilizó escala tipo Likert (1=Totalmente en desacuerdo a 5=Totalmente de acuerdo) sobre la percepción de vulnerabilidad personal e institucional frente a ciberataques.

El cuestionario fue distribuido a toda la muestra (docentes, administrativos y estudiantes) mediante un enlace a un formulario de Google por vía correo electrónico institucional, correo personal y otra vía de comunicación proporcionada durante un período de tres semanas en el mes de Junio del año 2025. Se envió un recordatorio semanal a los participantes que no habían respondido. Los datos se recopilaron a través de una plataforma segura, garantizando la confidencialidad de las respuestas.

Los datos recopilados fueron analizados de forma manual, sin software estadístico avanzado, con apoyo de la misma herramienta del Google Forms, ya que es una excelente manera de comprender a fondo los datos. Requiere más paciencia y organización, pero te permite una conexión directa con las respuestas. Se realizaron estadísticas descriptivas (frecuencias, porcentajes, medias y desviaciones estándar) para caracterizar la muestra y el nivel de conocimiento y prácticas.

Para interpretar de manera objetiva los resultados de los datos obtenidos en esta investigación, se establecieron criterios de análisis que permiten clasificar los porcentajes o puntuaciones en tres niveles que reflejan el grado de conocimiento, práctica o percepción en relación con la ciberseguridad: *bajo (0–49 %), medio (50–74 %) y alto (75–100 %).*

Resultados

A continuación, se presentan los resultados de las encuestas aplicada, con datos que corresponden a la distribución por género de los 100 participantes encuestados del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí.

Perfil de los participantes

El análisis de la participación de los encuestados seleccionados reveló la distribución por género de la muestra, observándose que en su mayoría son mujeres (53%) mientras que el 47% son hombres. Esta distribución relativamente equilibrada entre géneros sugiere que las perspectivas de ambos grupos están representadas en los resultados, aunque con un ligero predominio de la visión

femenina. En cuanto a la distribución por edad, los datos reflejan una clara predominancia de personas jóvenes en la muestra, con un 61 % de los participantes entre 18 y 35 años. En comparación, a el grupo de 36 a 60 años que representa un 35 % y el grupo de más de 60 años que representa un 4% del total. Esta distribución etaria sugiere que los resultados del estudio reflejan en gran medida las percepciones y experiencias de una población joven, lo cual puede influir en las prácticas y nivel de conocimiento en ciberseguridad, particularmente en temas relacionados con el uso cotidiano de tecnologías digitales.

En la siguiente tabla 2, se muestra los porcentajes del promedio de respuestas positivas de cada grupo (estudiantes, docentes y administrativos) del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí, en las dimensiones evaluadas.

Tabla 2

Resultados por grupo sobre el nivel de conocimiento, práctica y percepción de los encuestados en relación con la gestión de riesgos cibernéticos.

Grupo	% Nivel de Conocimiento	% Capacidad de identificación	% Práctica y Respuesta	% Percepción de la gestión.
Estudiantes	81.3 %	79 %	55.9 %	79.25 %
Docentes	97.5 %	88 %	75 %	80.00 %
Adminstrativos	89.4 %	82 %	90 %	80.00 %
Promedio	*89.4 %*	*83 %*	*73.63 %*	*79.75 %*

Nota: Porcentajes correspondientes al nivel de conocimiento, práctica y percepción de los encuestados en relación con la gestión de riesgos cibernéticos.

Los porcentajes presentados en esta tabla reflejan los niveles de conocimiento, capacidad de identificación, práctica y respuesta, así como la percepción de la gestión frente a amenazas cibernéticas (como *phishing* y *spam*) por parte de los distintos grupos de interés: estudiantes, docentes y personal administrativo. Los resultados se expresan en función del nivel de preparación, la capacidad de reacción y la percepción que cada grupo tiene respecto a la gestión de la ciberseguridad. En términos globales, se observa un alto nivel de conocimiento conceptual (89.4%), así como una percepción uniforme de la gestión (79.75%) entre todos los grupos.

No obstante, los hallazgos revelan una paradoja preocupante: si bien la mayoría de los participantes manifiesta sentirse vulnerable ante las amenazas cibernéticas y reconoce la importancia de estos riesgos, el conocimiento específico para identificar ataques sofisticados, así como la

aplicación sistemática de prácticas de seguridad digital, continúa siendo insuficiente. Esta situación se refleja en la capacidad general para identificar amenazas, que si bien alcanza un promedio del 83%, presenta limitaciones críticas. Solo una proporción reducida de los encuestados logró identificar correctamente direcciones URL sutilmente disfrazadas, lo que evidencia una baja efectividad frente a técnicas más avanzadas de ingeniería social. Esta brecha entre percepción y acción resulta especialmente preocupante, ya que los ciberatacantes suelen aprovechar precisamente la falta de discernimiento y la confianza implícita de los usuarios para ejecutar sus ataques con éxito.

Nivel de Conocimiento de Ciberseguridad, Phishing y Spam

Los resultados indicaron un nivel de conocimiento general elevado en la población estudiada, con una media aritmética de 8.94 sobre 10 en la sección de conocimientos. Esto significa que, en promedio, los participantes respondieron correctamente al 89.4 % de las preguntas formuladas. La desviación estándar (DE) fue de 1.96, lo que indica una dispersión moderada de las puntuaciones individuales con respecto a la media. En otras palabras, las respuestas de los participantes se distribuyeron alrededor de ese valor central, con diferencias de aproximadamente ±1.96 puntos. Esto evidencia que, aunque la mayoría obtuvo resultados cercanos a la media, existió variabilidad en el nivel de conocimiento entre los encuestados (véase Tabla 3).

Tabla 3

Nivel de conocimiento sobre conceptos clave de ciberseguridad e identificación de amenazas.

Concepto evaluado	% de Respuestas Correctas	% de Respuestas Incorrectas
¿Qué es el 'phishing'?	88 %	12 %
¿Qué es el 'spam'?	90 %	10 %
¿Qué es la 'ingeniería social'?	86 %	14 %
¿Cuáles son las buenas prácticas de ciberseguridad?	94 %	6 %
¿Qué es la autenticación de dos factores (2FA)?	89 %	11 %

Nota: Estadística porcentual basada en las respuestas obtenidas en la sección de conocimientos sobre conceptos clave de ciberseguridad (phishing, spam, ingeniería social, buenas prácticas y 2FA).

Según los datos presentados en la Tabla 3, se observa que los participantes demostraron un alto nivel de conocimiento sobre diversos conceptos clave de ciberseguridad. Los porcentajes más altos de respuestas correctas se registraron en los conceptos de *buenas prácticas de ciberseguridad* (94%) y *¿qué es el spam?* (90%), lo cual sugiere una sólida comprensión sobre la importancia de adoptar medidas preventivas y reconocer correos electrónicos no deseados.

Asimismo, se evidencia un conocimiento igualmente elevado en torno a los conceptos de *phishing* (88%) y *autenticación de dos factores (2FA)* (89%), aspectos fundamentales para prevenir accesos no autorizados y reforzar la seguridad en cuentas personales e institucionales.

Por otro lado, con relación a la pregunta sobre *ingeniería social* (86%), la diferencia respecto a los demás resultados es mínima, este dato podría señalar una posible área de mejora en la formación de los participantes. Sin embargo, es importante aclarar que una puntuación ligeramente inferior no implica, por sí sola, que este concepto deba considerarse una prioridad de intervención, especialmente porque la ingeniería social representa una forma sutil y efectiva de manipulación utilizada por ciberdelincuentes para engañar a los usuarios y obtener acceso a información confidencial.

Identificación de Correos Maliciosos y Fraudulentos

En la tabla 4, se presentan las respuestas con relación a la identificación de correos fraudulentos.

Tabla 4

Capacidad de detección de señales comunes de correos fraudulentos

Afirmación evaluada	% de Respuestas Correctas	% de Respuestas Incorrectas
Los correos de phishing contienen errores ortográficos o gramaticales.	84 %	16 %
Un correo que presiona a actuar de inmediato es señal de phishing.	95 %	5 %
El spam solo es molesto y nunca peligroso.	44 %	56 %
Cuando un ciberdelincuente falsifica el remitente de correo electrónicos parece que proviene de una fuente legítima	96 %	4 %
Cuando hay que reconocer que no es una buena práctica de ciberseguridad	83 %	17 %
Aunque un correo de 'spam' no te engañe, puede ser peligroso si contiene un archivo adjunto.	96 %	4 %

Nota: Porcentaje de participantes que identificaron correcta o incorrectamente características típicas asociadas a mensajes electrónicos maliciosos y sospechosos.

De lo anterior se observa una dicotomía interesante: si bien demuestran una sólida comprensión de las señales más obvias asociadas al phishing, como la presencia de errores ortográficos o gramaticales (84 %) y la presión para actuar de inmediato (95 %). También identifican adecuadamente que un correo puede parecer legítimo, aunque haya sido falsificado (96 %), y que un archivo adjunto en un mensaje de spam puede ser peligroso (96 %).

Los resultados de la Tabla 4, evidencian que la gran mayoría de los participantes muestra una buena conciencia sobre las tácticas de phishing comunes. Un impresionante 84% reconoce que los correos de phishing suelen contener errores ortográficos o gramaticales, y un notable 95% identifica la presión por actuar de inmediato como una clara señal de alerta. Además, un 96% es consciente de que los ciberdelincuentes pueden falsificar remitentes (spoofing) para simular una fuente legítima, y el mismo porcentaje entiende que, aunque un correo de spam no sea directamente engañoso, puede ser peligroso si contiene archivos adjuntos maliciosos. Esta alta tasa de reconocimiento en características evidentes sugiere que los programas de concienciación básica están teniendo un impacto positivo.

Sin embargo, los resultados también exponen una vulnerabilidad crítica ya que un poco más de la mitad de los encuestados (56%) respondió que el spam "solo es molesto y nunca peligroso", lo cual revela una percepción errónea que podría derivar en actitudes complacientes frente a amenazas reales. Esta desconexión entre el conocimiento teórico y la interpretación práctica de riesgos sugiere que aún hay necesidad de fortalecer la formación en escenarios realistas de ciberseguridad.

Aunque la identificación de estas señales es alta, los resultados muestran que más de la mitad de los participantes aún subestima el peligro verdadero del spam. Esta idea equivocada es clave, porque el spam, lejos de ser solo una molestia, a menudo es la puerta de entrada para ataques más serios, trayendo enlaces o archivos dañinos que pueden abrir otras vulnerabilidades.

Estos hallazgos sugieren que, aunque debemos es necesario brindar información sobre el *phishing*, es urgente intensificar las campañas de concienciación sobre la naturaleza variada y los peligros que el spam trae consigo, más allá de ser solo algo molesto. La educación debe ir más allá, explicando cómo el spam encaja en la cadena de ataques cibernéticos y los riesgos ocultos que puede presentar, incluso sin que el usuario haga clic o interactúe directamente con él, solo con recibirlo. Al

cerrar esta brecha de conocimiento, la comunidad del CRUPE estará mucho mejor preparada para protegerse de una gama más amplia de amenazas cibernéticas.

En cuanto a las diferencias entre los grupos, se observó que los docentes y el personal administrativo mostraron puntuaciones de conocimiento ligeramente superiores (medias de 7.3 y 7.1 respectivamente) en comparación con los estudiantes (media de 6.4). Sin embargo, al aplicar un análisis estadístico (por ejemplo, ANOVA de un factor), no se encontraron diferencias significativas entre los grupos ($p > 0.05$), lo cual indica que las variaciones observadas pueden deberse al azar y no a diferencias reales en el nivel de conocimiento

Implementación de Prácticas de Seguridad Digital

Los resultados evidencian un cumplimiento moderado de las prácticas recomendadas en materia de seguridad digital. Entre el 66 % y el 95 % de los encuestados afirmaron aplicar acciones clave como evitar enlaces sospechosos (79 %), verificar la identidad del remitente (66 %), revisar visualmente los enlaces antes de hacer clic (81 %) y activar la autenticación de dos factores (69 %), lo que sugiere un nivel funcional de concienciación y capacidad de respuesta ante amenazas digitales. No obstante, algunas prácticas presentan una menor frecuencia de adopción, como el cambio regular de contraseñas (74 %) y la confianza en las medidas de seguridad institucional (55 %), lo que revela una incorporación desigual de ciertas acciones preventivas. Estos hallazgos señalan áreas específicas que requieren atención para fortalecer la participación activa de la comunidad educativa en la promoción de una cultura de ciberseguridad institucional.

Aunque no todos los participantes siguen estas prácticas de manera uniforme, el patrón general sugiere que existe una base de conocimiento funcional, con claras oportunidades de refuerzo educativo y mejora continua en áreas específicas. La Tabla 5 resume hallazgos clave en relación con las prácticas de seguridad digital y evidencia áreas de mejora y posibles desconexiones entre la percepción y la realidad operativa de los participantes.

Tabla 5

Aplicación de prácticas ante correos sospechosos

Preguntas	% de Frecuencia Correcta
Verificar la dirección de correo electrónico del remitente antes de abrir un archivo adjunto.	66 %
Evitar hacer clic en enlaces sospechosos o acortados sin verificar su destino.	79 %
Estar atento a las alertas de seguridad o notificaciones sobre mis cuentas en línea.	70 %
Creer que la institución está bien protegida contra posibles ciberataques.	55 %
Conocer a quién contactar si sospecho un ataque de seguridad, en mi correo electrónico institucional.	95 %
Revisar visualmente los enlaces sospechosos para confirmar si el acceso a ese contenido sea real, ya que le preocupa que su información sea comprometida.	81 %
Cambiar regularmente mis contraseñas de cuentas importantes como el correo electrónico y banca en línea.	74 %
Habilitar la autenticación de dos factores (2FA) en la cuenta de correo electrónico siempre que está disponible.	69 %

En primer lugar, un 95 % de los encuestados afirma saber a quién contactar en caso de sospecha de un ataque de seguridad en su correo institucional, lo que representa un activo importante para una respuesta rápida y coordinada ante incidentes. Asimismo, un 81 % revisa visualmente los enlaces sospechosos antes de hacer clic, y un 79 % evita abrir enlaces acortados o sospechosos sin verificación previa, lo que indica una preocupación activa por proteger su información personal y evitar ataques como el phishing.

Sin embargo, a pesar de estos resultados positivos, se evidencia cierta inconsistencia en la adopción de medidas clave, como la habilitación de la autenticación de dos factores (2FA), utilizada por solo el 69 % de los encuestados. Dado que esta práctica es considerada una de las más efectivas para prevenir accesos no autorizados, su menor adopción en comparación con otras prácticas sugiere una brecha entre el conocimiento de las amenazas y la implementación proactiva de soluciones más técnicas o menos visibles.

Además, solo el 55 % de los participantes considera que su institución está bien protegida contra ciberataques, lo cual podría reflejar una falta de confianza en la infraestructura de seguridad

institucional o una percepción de vulnerabilidad que podría ser abordada mediante mayor comunicación, formación o medidas de transparencia en torno a las políticas de ciberseguridad.

Estos hallazgos sugieren que, aunque hay aspectos positivos en las prácticas de seguridad digital, como el conocimiento de contactos de emergencia y la precaución general con enlaces sospechosos, persisten desafíos importantes relacionados con la consistencia en la verificación del remitente, la adopción de 2FA y una posible sobre confianza en la facilidad de identificación de phishing. Las diferencias significativas entre los grupos sugieren que las estrategias de capacitación y sensibilización en ciberseguridad deberían ser adaptadas a las necesidades específicas de cada segmento de la comunidad del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí

Percepción General de Riesgo

La percepción general de riesgo cibernético en la comunidad del Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí se considera moderadamente alta. A partir del análisis de los datos recolectados mediante una escala tipo Likert, se obtuvo una media aritmética de 3.9 (M = 3.9), lo que indica que los participantes están significativamente sensibilizados respecto a los riesgos que implican los ciberataques. Además, la desviación estándar de 0.7 (DE = 0.7) sugiere que las respuestas individuales no presentan una gran dispersión, reflejando una percepción relativamente homogénea entre los encuestados.

Tabla 6

Percepción de vulnerabilidad y preparación individual frente a ciberataques

Preguntas	% de respuestas "De acuerdo"
Me considero vulnerable ante ataques de phishing.	84 %
Estoy consciente de los tipos de amenazas de ciberseguridad que podría enfrentar.	88 %
Siento que tengo el conocimiento suficiente para identificar un intento de ciberataque.	72 %
Me preocupa que la información personal que tengo en línea pueda ser comprometida.	75 %

Nota: Considera las respuestas a "Totalmente de acuerdo (5) y "De acuerdo (4)" .

La tabla 6, presenta resultados interesantes sobre la relación entre percepción de riesgo, conocimiento y prácticas de seguridad digital. Los hallazgos indican una alta percepción de vulnerabilidad frente a amenazas específicas: un 84 % de los participantes se considera vulnerable ante ataques de phishing, y un 88 % está consciente de los diversos tipos de amenazas de ciberseguridad que podrían enfrentar. Asimismo, el 75 % expresa preocupación por el posible compromiso de su información personal en línea.

Sin embargo, a pesar de este elevado nivel de percepción de riesgo, también se observa una notable confianza en las capacidades personales para identificar ciberataques, ya que un 72 % considera tener el conocimiento suficiente para reconocer un intento de ataque. Esta confianza podría interpretarse como un signo positivo de preparación individual, pero también puede enmascarar una contradicción: mientras que un 84 % se siente vulnerable al phishing, un 40 % no se considera vulnerable en términos más generales. Esta discrepancia podría deberse a una diferenciación entre tipos de amenazas o, alternativamente, revelar un exceso de confianza o un desconocimiento parcial de los riesgos reales. En cualquiera de los casos, esta falta de correlación evidencia una posible debilidad en la comprensión integral de la ciberseguridad, lo que plantea un reto importante para las estrategias de formación y sensibilización institucional.

Un hallazgo crucial revela que percibir un alto riesgo no se traduce automáticamente en un mayor conocimiento o en la implementación de mejores prácticas de seguridad. En otras palabras, aunque las personas sean conscientes de los peligros y perciban un riesgo significativo, esta conciencia por sí sola no es suficiente para impulsarlas a aprender más o a cambiar su comportamiento y aplicar medidas de seguridad.

Esto sugiere que existen factores adicionales que obstaculizan la traducción de la percepción de riesgo en acciones concretas de seguridad digital. Entre las posibles barreras se incluyen la falta de tiempo, el desconocimiento sobre las medidas a tomar, la baja motivación o la percepción de complejidad en las acciones requeridas. En este sentido, una elevada conciencia del riesgo no garantiza, por sí sola, la adopción de prácticas preventivas efectivas.

Discusión

La persistencia y evolución de amenazas como el *phishing* y el *spam* evidencian la necesidad de estrategias multifacéticas para su mitigación en entornos educativos. En este contexto, la educación digital emerge como una herramienta crucial para empoderar a los usuarios en la identificación y

prevención de correos electrónicos maliciosos. Los programas de concienciación y formación en ciberseguridad pueden reducir significativamente la susceptibilidad a estos ataques.

Complementariamente, la adopción de tecnologías como filtros avanzados de correo electrónicos, autenticación de dos factores y sistemas de detección de anomalías pueden contribuir a reforzar la infraestructura defensiva institucional contra estas amenazas. Es fundamental que las instituciones educativas implementen políticas de seguridad robustas y promuevan una cultura de vigilancia activa y reporte de incidentes, con el fin de responder de forma eficaz a las amenazas emergentes, como son los intentos de phishing y spam.

La dificultad para detectar técnicas como el spoofing de correos electrónicos y otras formas de suplantación subraya la creciente sofisticación de los ataques actuales, que ya no dependen únicamente de errores ortográficos o diseños burdos. En este sentido, los programas de concienciación tradicionales, centrados en advertencias generales, resultan insuficientes. Se requiere un enfoque más práctico, basado en simulaciones, ejercicios reales y herramientas interactivas que fortalezcan la capacidad de detección del usuario frente a amenazas avanzadas.

En cuanto a las prácticas de seguridad digital, los datos reflejan diferencias esperadas entre los grupos: el personal administrativo muestra los mejores resultados (90%), seguido por los docentes (75%) y los estudiantes (55.9 %). Esta tendencia puede estar relacionada con la mayor exposición de docentes y administrativos a capacitaciones institucionales o a la responsabilidad asociada a sus roles. No obstante, un hallazgo relevante es la baja adopción, generalizada en todos los grupos, de herramientas fundamentales como los gestores de contraseñas y la autenticación en dos factores (2FA). Esta omisión representa una oportunidad crítica desaprovechada para fortalecer la seguridad digital básica en el entorno educativo.

Adicionalmente, la percepción sobre la gestión institucional en ciberseguridad se mantiene estable en todos los grupos (79.75 %), lo que sugiere una valoración positiva de las políticas y acciones implementadas. Sin embargo, la ausencia de una correlación significativa entre esta percepción y las prácticas individuales de seguridad refuerza la idea de que sentir preocupación o riesgo no garantiza una respuesta activa. La sensación de vulnerabilidad, por sí sola, no constituye un impulsor eficaz del cambio conductual.

Estos hallazgos apuntan a la necesidad de adoptar un enfoque más integral para la formación en ciberseguridad, que no se limite a crear conciencia sobre los riesgos, sino que también fomente habilidades prácticas, provea herramientas accesibles y refuerce conductas seguras mediante

incentivos o recordatorios sistemáticos. En síntesis, aunque la comunidad del CRUPE muestra una percepción moderadamente alta del riesgo cibernético, esta conciencia aún no se traduce de forma consistente en un conocimiento operativo ni en una cultura activa de seguridad digital. Las futuras intervenciones deberían orientarse a cerrar esta brecha entre la percepción del riesgo y el comportamiento preventivo efectivo, especialmente entre la población estudiantil.

Conclusiones

En el Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí, la batalla contra amenazas como el *phishing*, el *spam* y el robo de datos es un desafío constante. Aunque la comunidad educativa muestra una alta percepción del riesgo, este estudio revela una brecha crítica entre esa conciencia y la aplicación efectiva de prácticas de seguridad robustas.

Si bien los encuestados reconocen el peligro del *phishing* y el *spam* en sus formas más evidentes, su capacidad para identificar ataques sutiles (como URL maliciosas disfrazadas o el *spoofing*) es limitada. Esto subraya cómo la sofisticación de los ciberataques ha superado los mensajes con fallas obvias. Además, la ausencia de diferencias estadísticamente significativas en el nivel de conocimiento sobre ciberseguridad entre docentes, administrativos y estudiantes indica que las vulnerabilidades son transversales a todos los roles en la institución.

Preocupa el hecho de que a pesar de una alta percepción generalizada del riesgo, esta conciencia no se traduce en un conocimiento específico suficiente sobre ataques más avanzados ni en una adopción consistente de prácticas de seguridad. Esta brecha es fundamental porque la ingeniería social, una táctica común de los ciberdelincuentes, explota precisamente la falta de discernimiento del usuario. Por tanto, es evidente la necesidad de mejorar la formación en la detección de amenazas más sofisticadas y de profundizar en la comprensión de los peligros asociados al *spam*, que a menudo sirve como puerta de entrada para ataques complejos.

Aunque se detectaron algunas diferencias en las prácticas de seguridad entre roles (el personal administrativo demuestra mejores hábitos que los estudiantes), la baja adopción de herramientas críticas como gestores de contraseñas y la autenticación de dos factores (2FA) en todos los grupos es una señal de alerta. A pesar de que la política de 2FA para el correo institucional ya está establecida, su uso generalizado sigue siendo una oportunidad perdida para fortalecer la ciberhigiene. Es crucial destacar que una elevada percepción de riesgo no se correlaciona significativamente con un mayor

conocimiento o la adopción de prácticas de seguridad, lo que sugiere que sentirse vulnerable por sí solo no es un motor suficiente para el cambio de comportamiento.

Es fundamental que se desarrollen programas de educación digital holísticos que ofrezcan capacitación práctica con ejemplos reales para mejorar la capacidad de detección de ataques sofisticados. De esta manera los programas de capacitación deberían considerar el uso de herramientas críticas como gestores de contraseñas y la activación de 2FA.

Se debe promover una cultura de seguridad activa mediante políticas robustas y el impulso de una cultura de vigilancia y reporte de incidentes. La implementación de tecnologías de seguridad avanzadas, como filtros de correo y sistemas de detección de anomalías, reforzará la protección. La realización de simulacros de *phishing* regulares, la promoción obligatoria de 2FA para cuentas críticas, el desarrollo de guías de ciberhigiene y la creación de un canal de reporte de incidentes accesible son técnicas esenciales para educar y proteger a la comunidad.

Superar la brecha entre la percepción del riesgo y la acción requiere estrategias integrales que combinen la concienciación con el desarrollo de habilidades, la disponibilidad de herramientas fáciles de usar y el refuerzo positivo de conductas seguras. La seguridad de la información en entornos educativos no es solo una cuestión técnica, supone el logro de competencias digitales. Abordar estas vulnerabilidades humanas mediante la educación y la formación continua permitirá al Centro Regional Universitario de Panamá Este (CRUPE) y la Extensión Universitaria de Tortí, protegerse eficazmente de las crecientes amenazas cibernéticas.

Referencias

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015, noviembre 30–diciembre 4). *Breaching the human firewall: Social engineering in phishing and spear-phishing emails* [Conference session]. Australasian Conference on Information Systems, Adelaide, Australia. https://arxiv.org/pdf/1606.00887v1

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Phishing guidance: Stopping the attack cycle at phase one*. CISA. https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf

European Union Agency for Cybersecurity (ENISA). (2023). *Cybersecurity in the education sector*. https://www.enisa.europa.eu/news/european-cybersecurity-skills-conference-intensifying-our-efforts-to-close-the-cybersecurity-skills-gap-in-the-eu

Ifinedo, P. (2017). Effects of culture and national information infrastructure on users' information security awareness: Empirical evidence from two countries. *Information & Management, 54*(3), 365–378.

Lain, D., Kostiainen, K., & Capkun, S. (diciembre 6–10, 2021). *Phishing in organizations: Findings from a large-scale and long-term study* [Conference session]. 37th Annual Computer Security Applications Conference (ACSAC 2021), Austin, TX, Estados Unidos. https://arxiv.org/pdf/2112.07498

Microsoft. (marzo 3, 2024). *What is phishing?* Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing

Salahdine, F., El Mrabet, Z., & Kaabouch, N. (2021, noviembre 7–10). *Phishing attacks detection — A machine learning-based approach* [Conference session]. 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2021), New York, NY, Estados Unidos. https://arxiv.org/pdf/2201.10752

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley.

Tecno Futuro. (2025). *Conciencia en ciberseguridad: Importancia educativa*. https://tecnofuturo.net/ciberseguridad/rol-factor-humano-ciberseguridad-educacion-conciencia/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2011). *Transforming Education: The Power of ICT Policies*. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000211842

Wang, Y., Chen, W., Li, Y., & Wei, R. (2019). Understanding users' susceptibility to phishing attacks: An integrated model of protection motivation theory and trust. *Computers in Human Behavior, 92*, 19–32.