Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v16i31.2780

Artículos Científicos

Evaluación comparativa de la alfabetización de ciberseguridad en estudiantes universitarios

Benchmarking cybersecurity literacy in college students

Avaliação comparativa da literacia em cibersegurança dos estudantes universitários

Rolando Salazar Hernández
Universidad Autónoma de Tamaulipas, México
rsalazar@docentes.uat.edu.mx
https://orcid.org/0000-0001-5879-4083

Ramón Ventura Roque Hernández
Universidad Autónoma de Tamaulipas, México
rvhernandez@uat.edu.mx
https://orcid.org/0000-0001-9727-2608

Adán López Mendoza
Universidad Autónoma de Tamaulipas, México
alopez@uat.edu.mx
https://orcid.org/0000-0003-4801-640X

Resumen

Los avances tecnológicos han incrementado el uso de los dispositivos móviles y las computadoras personales con acceso a internet entre los estudiantes universitarios, exponiéndolos con más frecuencia a riesgos como estafas, ciberacoso, noticias falsas, robo de datos personales, entre otros. Aunque los jóvenes universitarios están muy familiarizados con la tecnología, carecen de conocimientos sólidos en ciberseguridad. El presente artículo tuvo los objetivos de diferenciar las prácticas en ciberseguridad de los estudiantes universitarios en computadoras personales y teléfonos inteligentes, así como describir sus conocimientos en ciberseguridad y asociar este conocimiento con el programa académico cursado. Para el levantamiento de los datos se aplicó parte del cuestionario de aspectos

humanos de la seguridad de la información (HAIS-Q) a 288 alumnos inscritos en cinco programas educativos de pregrado en la Facultad de Comercio, Administración y Ciencias Sociales Nuevo Laredo de la Universidad Autónoma de Tamaulipas. Los análisis de datos incluyeron pruebas estadísticas no paramétricas, como chi-cuadrado de asociación, Wilcoxon para muestras relacionadas y Kruskal-Wallis para más de dos grupos independientes, que permitieron evaluar las diferencias significativas sin asumir distribuciones específicas de los datos. Los resultados revelaron que los estudiantes identifican conceptos básicos de ciberseguridad, como virus, spyware y phishing. No obstante, se evidencia una brecha entre este conocimiento teórico y su aplicación práctica, destacando la necesidad apremiante de fomentar una cultura preventiva y diseñar estrategias integrales para mitigar ataques cibernéticos. El estudio confirma que, si bien existen nociones elementales, persiste un riesgo diferenciado según el tipo de dispositivo (móvil vs. Computadora). Esto subraya la necesidad de integrar planes educativos adaptados a cada plataforma, reforzando las prácticas seguras y conscientes. Una investigación futura con enfoques metodológicos mixtos podría profundizar en estos hallazgos.

Palabras clave: ciberseguridad, ataques cibernéticos, educación superior, HAIS-Q, vulnerabilidades.

Abstract

Technological advances have increased the use of mobile devices and personal computers with internet access among university students, exposing them more frequently to risks such as scams, cyberbullying, fake news, and personal data theft, among others. Although young university students are very familiar with technology, they lack solid knowledge of cybersecurity. The objectives of this article were to differentiate the cybersecurity practices of university students on personal computers and smartphones, as well as to describe their knowledge of cybersecurity and associate this knowledge with the academic program they are enrolled in. To collect the data, part of the Human Aspects of Information Security Questionnaire (HAIS-Q) was administered to 288 students enrolled in five undergraduate programs at the Nuevo Laredo Faculty of Commerce, Administration, and Social Sciences of the Autonomous University of Tamaulipas. Data analysis included nonparametric statistical tests, such as chi-square for association, Wilcoxon for related samples, and Kruskal-Wallis for more than two independent groups, which allowed for the evaluation of

significant differences without assuming specific data distributions. The results revealed that students identify basic cybersecurity concepts, such as viruses, spyware, and phishing. However, there is a gap between this theoretical knowledge and its practical application, highlighting the urgent need to foster a culture of prevention and design comprehensive strategies to mitigate cyberattacks. The study confirms that, although basic notions exist, there is still a differentiated risk depending on the type of device (mobile vs. computer). This underscores the need to integrate educational plans adapted to each platform, reinforcing safe and conscious practices. Future research with mixed methodological approaches could further explore these findings.

Keywords: cybersecurity, cyberattacks, higher education, HAIS-Q, vulnerabilities.

Resumo

Os avanços tecnológicos aumentaram o uso de dispositivos móveis e computadores pessoais com acesso à internet entre estudantes universitários, expondo-os com maior frequência a riscos como golpes, cyberbullying, notícias falsas e roubo de dados pessoais, entre outros. Embora os estudantes universitários estejam bastante familiarizados com a tecnologia, eles carecem de um sólido conhecimento em cibersegurança. Este artigo teve como objetivo diferenciar as práticas de cibersegurança de estudantes universitários em computadores pessoais e smartphones, bem como descrever seu conhecimento em cibersegurança e associá-lo aos seus cursos acadêmicos. Os dados foram coletados por meio da aplicação de parte do Questionário de Aspectos Humanos da Segurança da Informação (HAIS-Q) a 288 estudantes matriculados em cinco cursos de graduação da Faculdade de Comércio, Administração e Ciências Sociais em Nuevo Laredo, na Universidade Autônoma de Tamaulipas. A análise dos dados incluiu testes estatísticos não paramétricos, como qui-quadrado para associação, Wilcoxon para amostras relacionadas e Kruskal-Wallis para mais de dois grupos independentes, o que permitiu a avaliação de diferenças significativas sem pressupor distribuições específicas dos dados. Os resultados revelaram que os alunos identificam conceitos básicos de cibersegurança, como vírus, spyware e phishing. No entanto, observa-se uma lacuna entre esse conhecimento teórico e sua aplicação prática, o que destaca a necessidade urgente de fomentar uma cultura preventiva e desenvolver estratégias abrangentes para mitigar ciberataques. O estudo confirma que, embora existam noções básicas, persiste um risco diferenciado dependendo do tipo de dispositivo (móvel vs.

computador). Isso reforça a necessidade de integrar planos educacionais adaptados a cada plataforma, consolidando práticas seguras e responsáveis. Pesquisas futuras com abordagens metodológicas mistas poderiam aprofundar esses achados.

Palavras-chave: cibersegurança, ciberataques, ensino superior, HAIS-Q, vulnerabilidades.

Fecha Recepción: Junio 2025 **Fecha Aceptación:** Diciembre 2025

Introducción

En la era digital, la ciberseguridad se ha convertido en una prioridad crítica para proteger los datos y la infraestructura de las amenazas cibernéticas. La creciente dependencia de la tecnología en todas las facetas de la vida diaria hace que sea esencial no solo contar con medidas técnicas, sino también con una sólida concienciación y educación en ciberseguridad. En este sentido, las Instituciones de Educación Superior (IES) se enfrentan a grandes desafíos para hacer frente a los ciberataques que se presentan en forma constante (Cheng & Wang, 2022).

Para minimizar los riesgos asociados a las violaciones de la seguridad de la información, Rohan y cols. mencionan que estos pueden ser ayudados a través de la concienciación sobre la seguridad de información Information Security Awareness (ISA). Este concepto ha recibido una considerable atención en los últimos años (Rohan et al., 2023).

Este artículo aborda los siguientes tres objetivos: 1. Caracterizar y comparar las prácticas de ciberseguridad entre estudiantes de diferentes programas educativos, distinguiendo entre el uso de computadoras personales (PC) y teléfonos inteligentes (smartphones); 2. Caracterizar y comparar el nivel de conocimiento sobre ciberseguridad de los estudiantes de diferentes programas educativos; 3. Determinar si existe una asociación entre el nivel de conocimiento sobre ciberseguridad de los estudiantes y el programa educativo que cursan.

Trabajos relacionados

La concienciación sobre ciberseguridad en instituciones educativas es un tema de creciente interés. Estudios como el de Khader, Karam, y Fares (2021) proponen un marco de concienciación para asegurar que los graduados estén bien equipados para enfrentar ciberamenazas. El cual sugiere la integración de la ciberseguridad en los currículos universitarios, no solo en cursos de informática, sino en una variedad de disciplinas para promover una cultura de seguridad integral en el ámbito académico (Khader et al., 2021).

Por otro lado, Çiftçi y Delialioğlu (2016) demostraron que el uso de herramientas digitales, como un portal de seguridad en línea, puede mejorar significativamente los conocimientos y habilidades de los estudiantes en materia de ciberseguridad. Esto destaca la eficacia de las soluciones tecnológicas en la educación sobre ciberseguridad, sugiriendo que los recursos digitales pueden ser una forma eficaz de complementar los métodos de enseñanza tradicionales (Çiftçi & Delialioğlu, 2016).

Venter et al. (2019) plantean que la educación en ciberseguridad debería comenzar en los niveles educativos más bajos y ser considerada "tan esencial como la lectura, la escritura y la aritmética". Este enfoque integral ayudaría a cerrar la brecha de género en la concienciación sobre ciberseguridad, especialmente en países en desarrollo, donde las mujeres tienden a estar más desprotegidas frente a las amenazas cibernéticas. La educación temprana y continua es fundamental para asegurar que todos los individuos, independientemente de su género o nivel socioeconómico, estén equipados para enfrentar los desafíos de un mundo digital (Venter et al., 2019).

Las instituciones académicas son especialmente vulnerables a los ataques cibernéticos debido a la gran cantidad de datos sensibles que manejan. Según Cheng y Wang (2022), la ciberseguridad en la educación superior requiere un enfoque sistémico para protegerse contra ciberataques. Proponen estrategias como fortalecer la gobernanza en ciberseguridad y revisar los indicadores clave de rendimiento para asegurar que las instituciones estén mejor preparadas para enfrentar estos desafíos (Cheng & Wang, 2022).

Hong et al. (2023) sugieren que el nivel de educación de una sociedad influye significativamente en la conciencia y comportamiento de ciberseguridad de los individuos. Aseguran que una educación sólida en ciberseguridad debe ser accesible para todos, no solo para los estudiantes universitarios, sino también para la población en general (Hong et al., 2023).

La evaluación del comportamiento relacionado con la ciberseguridad y la efectividad de las iniciativas de concienciación es crítica para mejorar la postura de seguridad. Kannelønning y Katsikas (2023) resaltan la necesidad de métodos de evaluación más objetivos para medir la concienciación y el comportamiento de los usuarios en materia de ciberseguridad. Este enfoque ayudará a identificar áreas de mejora y a desarrollar estrategias educativas más efectivas que respondan a las necesidades específicas de diferentes grupos de usuarios (Kannelønning & Katsikas, 2023).

La cultura organizacional es un factor determinante en la eficacia de las estrategias de ciberseguridad. Wiley, McCormac, y Calic (2020) encontraron que una fuerte cultura de seguridad dentro de una organización puede tener un impacto significativo en la concienciación de seguridad de la información (ISA) de sus empleados. Una cultura de seguridad bien establecida no solo incluye la implementación de políticas y procedimientos de seguridad, sino también la promoción de valores y comportamientos que prioricen la seguridad. Esto puede incluir desde la formación regular en ciberseguridad hasta la creación de un entorno en el que los empleados se sientan responsables y motivados para seguir prácticas seguras (Wiley, McCormac & Calic, 2020).

Hadlington y Parsons (2017) también subrayan que problemas como el ciberocio (*cyberloafing*) (uso de Internet para actividades no laborales durante el trabajo) y la adicción a Internet pueden socavar la seguridad de la información en las organizaciones. Los empleados con mayores niveles de ciberocio tienden a mostrar una menor conciencia de seguridad, lo que sugiere que las organizaciones deben considerar no solo la capacitación técnica, sino también la gestión de comportamientos que puedan poner en riesgo la seguridad (Hadlington & Parsons, 2017).

Zulfia et al. (2019) utilizaron el cuestionario HAIS-Q para evaluar la conciencia de seguridad de los empleados en una organización, identificando áreas vulnerables como la relación en la descarga de archivos y la gestión de correos electrónicos. Sus hallazgos sugieren que mejorar las políticas y procedimientos, junto con la formación continua, es crucial para fortalecer la postura de seguridad de una organización (Zulfia et al., 2019).

En la investigación de Ibrahim, McKee, Sikos y Johnson (2024), se realizó una revisión sistemática sobre educación en ciberseguridad en niveles básicos K-12 (educación básica K-12) en todo el mundo. Su investigación abarca los periodos 2013 a 2023, y presentan una clasificación sobre diferentes temáticas recurrentes que abarcan habilidades y competencias de ciberseguridad que permitan que los estudiantes de niveles básicos apliquen sus conocimientos. Dentro de las temáticas que clasificaron se encuentran artículos sobre la concienciación de la ciberseguridad. En esta temática señalan que se centran en los usuarios a nivel individual y organizativo donde son conscientes y se comprometen a ser conscientes sobre la ciberseguridad. En su investigación citan al estudio de Witsenboer et al. (2022) realizado con estudiantes de niveles básicos de Países Bajos, y se refieren a la concienciación de la ciberseguridad como el grado que un usuario entiende y se compromete con comportamientos seguros en línea (Ibrahim et al., 2024; Witsenboer et al., 2022).

Comparación entre el Uso de Smartphones y Computadoras

La expansión del uso de dispositivos móviles plantea nuevos desafíos de ciberseguridad. Taha y Dahabiyeh (2021) compararon la concienciación sobre la seguridad de la información entre estudiantes universitarios en el uso de smartphones y computadoras. Sus hallazgos indican que, aunque los estudiantes son conscientes de los riesgos, su comportamiento en la protección del smartphone es menos riguroso que en el uso de computadoras. Este estudio sugiere la necesidad de campañas educativas específicas que aborden las vulnerabilidades particulares de los dispositivos móviles, una tendencia que se vuelve cada vez más relevante con la creciente dependencia de estos dispositivos en entornos educativos y profesionales (Taha & Dahabiyeh, 2021).

Por otro lado, Breitinger et al. (2020) revelaron en su encuesta que, aunque muchos usuarios configuran adecuadamente la seguridad básica de sus smartphones, tienden a ignorar otras prácticas de seguridad importantes, como el uso de las redes privadas virtuales (VPN Virtual Private Network) y la desactivación de funciones innecesarias (NFC, Bluetooth, servicios de localización). Esto resalta una laguna en la concienciación de seguridad que debe ser abordada mediante la educación continua sobre prácticas de seguridad integral (Breitinger et al., 2020).

Ayyash et al. (2024) en su investigación comentan que, a pesar de la creciente conciencia en ciberseguridad, su implementación enfrenta tres desafíos críticos: docentes, recursos, comunidad. Uno de los obstáculos principales es la insuficiente capacitación de los docentes, lo que limita su capacidad para impartir conocimientos actualizados y efectivos en esta área. Asimismo, la carencia de recursos educativos adecuados dificulta la creación de programas estructurados y atractivos para los estudiantes. Además, comunicar conceptos complejos de ciberseguridad de manera comprensible y accesible para los niños representa otro desafío significativo. Sin embargo, tanto padres como maestros coinciden en que los métodos educativos basados en narrativas, resolución de problemas y el uso de videos son las estrategias pedagógicas más efectivas para abordar estos riesgos y fomentar una mayor comprensión entre los estudiantes (Ayyash et al., 2024).

Alotibi propone un marco para mitigar los riesgos asociados a los ataques de ingeniería social. En primer lugar, sugiere el desarrollo de programas de concienciación y capacitación que aborden directamente las vulnerabilidades humanas explotadas en estos ataques, como la tendencia a la confianza excesiva, la ignorancia en temas de ciberseguridad y la susceptibilidad a la influencia social. Además, el autor destaca la importancia de crear

simulaciones y escenarios de entrenamiento que reflejen los 16 métodos de ataque de ingeniería social, esto permitiría a las organizaciones y usuarios prepararse para estos riesgos en un entorno controlado (Alotibi, 2024).

Metodología

Participantes

En la investigación se analizaron las opciones de respuesta de 288 estudiantes de distintos semestres de las licenciaturas que se ofertan en la Facultad de Comercio, Administración y Ciencias Sociales de Nuevo Laredo, quedando la distribución siguiente: 34 alumnos de Licenciado en Derecho (LD), 42 alumnos de Licenciado en Administración(LA), 40 alumnos de Contador Público (CP), 112 de Licenciado en Comercio Exterior (LCE), 60 de Licenciado en Tecnologías de la Información (LTI), de los cuales 147 fueron alumnas y 141 alumnos, las edades de los encuestados oscilaron entre 18 y 26 años, el estudio se realizó durante el periodo lectivo de primavera de 2023.

Este estudio se apoyó en las coordinaciones de carrera que fueron los que a través de invitaciones por mensajes de texto a Profesores y ellos a su vez a sus alumnos se realizó el levantamiento de los datos. La muestra fue no probabilística por conveniencia, lo cual es una limitación del estudio al introducir posibles sesgos de selección y cobertura. Los datos se recabaron a través de una encuesta implementada en la plataforma Microsoft Forms (Office 365).

Instrumento

El instrumento se basa en un cuestionario se basa en el *Human Aspects of Information Security Questionnaire* (HAIS-Q) utilizado a nivel mundial, este ha sido adaptado seleccionando las preguntas que se consideraron adecuadas al nivel de estudio de pregrado de los participantes (Parsons et al., 2017). El instrumento consta de 26 preguntas, 16 en la escala de Likert de 5 puntos con las siguientes respuestas Totalmente de acuerdo; De acuerdo; Ni de acuerdo ni en desacuerdo; En desacuerdo; Totalmente en desacuerdo, estas preguntas se muestran en la tabla 1. Y 10 preguntas que permitan saber si los alumnos conocen los conceptos básicos de ciberseguridad se muestran en la tabla 2.

Tabla 1 Preguntas tipo Likert

Identificador	Pregunta
P1	Utilizo filtro de contenido en mi computadora para bloquear sitios web que puedan presentar amenazas para la seguridad.
P2	Utilizo filtro de contenido en mi smartphone para bloquear sitios web que puedan presentar amenazas para la seguridad.
P3	Utilizo un programa antivirus en mi computadora.
P4	Utilizo un programa antivirus en mi smartphone.
P5	Actualizo el antivirus que utilizo en mi smartphone cada 3 a 6 meses.
P6	Actualizo el antivirus en mi computadora cada 3 a 6 meses.
P7	Hago copias de seguridad de los datos de mi computadora al menos mensual.
P8	Hago copias de seguridad de los datos de mi smartphone al menos mensual.
P9	Leo los acuerdos de política de seguridad de los programas informáticos antes de descargarlos en mi computadora.
P10	Leo los acuerdos de política de seguridad de los programas informáticos antes de descargarlos en mi smartphone.
P11	Utilizo parches de software (actualizaciones/patches) en mi computadora.
P12	Utilizo parches de software en mi smartphone.
P13	Actualizo el antivirus en mi smartphone cada 3 a 6 meses.
P14	Actualizo el antivirus en mi computadora cada 3 a 6 meses.
P15	Utilizo un bloqueador de ventanas emergentes en mi computadora.
P16	Utilizo un bloqueador de ventanas emergentes en mi smartphone.

Fuente: Elaboración propia

Tabla 2 Preguntas de definición

Identificador	Pregunta	Respuestas
P17	¿Cuál es la definición de seguridad de la información?	1) Se refiere a la protección de datos digitales mediante el uso de candados y cerraduras físicas en los servidores y dispositivos electrónicos. 2) Es un concepto obsoleto en la era digital, ya que todos los datos en línea son inherentemente seguros y no pueden ser vulnerados. 3) Son procesos, buenas prácticas y metodologías que buscan proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada.
P18	¿Cuál es el concepto de malware?	1) Software inofensivo y solo se utiliza para mejorar la seguridad de un sistema informático. 2) Es software diseñado para causar daño o utilizar recursos de una computadora. 3) Es un tipo de virus que se propaga de una computadora a otra a través del aire, como un virus biológico.
P19	¿Cuál es el concepto de software antivirus?	1) Es un software de seguridad informática diseñado para detectar, prevenir, y eliminar programas maliciosos o malware de un sistema informático. 2) Software que protege tu computadora al interceptar y bloquear todos los correos electrónicos entrantes para evitar que los virus se propaguen a través de tu bandeja de entrada. 3) Es un dispositivo físico que se conecta a tu computadora para evitar que los virus y el malware ingresen a través de los puertos USB.
P20	Es un protocolo más seguro usado para la navegación de Internet	1) http. 2) https (HTTP sobre TLS). 3) Restringe el dominio a navegación Web.
P21	¿Qué es el fraude o pérdida financiera por Internet?	1) Se envían correos electrónicos o mensajes falsos que parecen provenir de fuentes legítimas, como bancos o empresas. 2) Se refiere a actividades delictivas en línea diseñadas para engañar a personas o entidades con el fin de obtener ganancias financieras ilegítimas.

		3) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre.
P22	Define el concepto de suplantación de identidad	1) Se refiere a actividades delictivas en línea diseñadas para engañar a personas o entidades con el fin de obtener ganancias financieras ilegítimas. 2) Se envían correos electrónicos o mensajes falsos que parecen provenir de fuentes legítimas, como bancos o empresas. 3) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre.
P23	Selecciona el concepto de robo de información	1) Se refiere a actividades delictivas en línea diseñadas para engañar a personas o entidades con el fin de obtener ganancias financieras ilegítimas. 2) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre. 3) Se refiere al acto de obtener, acceder, copiar, transferir o adquirir información confidencial o protegida sin la autorización del propietario legítimo de dicha información.
P24	Selecciona el concepto de phishing	1) Se refiere al acto de obtener, acceder, copiar, transferir o adquirir información confidencial o protegida sin la autorización del propietario legítimo de dicha información. 2) Es el envío de correos electrónicos o mensajes falsos que parecen provenir de fuentes legítimas, como bancos o empresas, con el objetivo de obtener información confidencial, como números de tarjetas de crédito, contraseñas u otra información financiera sensible. 3) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre.
P25	¿Qué es la fuga de información sensible?	1) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre. 2) Se refiere a actividades delictivas en línea diseñadas para engañar a personas o entidades con el fin de obtener ganancias financieras ilegítimas. 3) Se refiere al incidente en el cual información confidencial o sensible, que debería haber sido resguardada y protegida, es divulgada,

		filtrada o puesta en manos de personas no autorizadas.
P26	Selecciona el concepto de ransomware	1) Es el uso no autorizado y malintencionado de tus datos personales por parte de alguien con el fin de actuar en tu nombre. 2) Se cifran los archivos de las víctimas y exigen un rescate a cambio de la clave de descifrado, lo que puede resultar en pérdidas financieras significativas. 3) Se refiere al acto de obtener, acceder, copiar, transferir o adquirir información confidencial o protegida sin la autorización del propietario legítimo de dicha información.

Fuente: Elaboración propia

La aplicación del instrumento a los estudiantes encuestados donde no se impartieron capacitaciones previas especificas en ciberseguridad. La Universidad ofrece a través de la dirección de infraestructura tecnológica webinars de temas muy diversos de ciberseguridad, donde la comunidad universitaria es invitada a través de correos electrónicos personalizados, redes sociales y portales universitarios, pero estos eventos tienen una periodicidad bimensual.

Para la recolección de datos se utilizó la herramienta de Microsoft Forms de la suite de Office 365, y la aplicación se realizó durante una pausa dentro del salón de clases a través de los dispositivos móviles con que cada uno de los participantes cuenta, sin guardar datos personales.

Técnicas de Análisis de datos

Posterior a la recolección de datos, se ha seleccionado el software jamovi versión 2.3.28 para la codificación, para la estadística descriptiva y las pruebas de hipótesis. Después de realizar una codificación de los datos, se realizaron las primeras pruebas con la herramienta obteniendo los resultados de estadística descriptiva. Se realizaron pruebas de Wilcoxon para comparar las respuestas provenientes de los participantes sobre sus hábitos de ciberseguridad en computadoras personales y teléfonos inteligentes (P1↔P2, P3↔P4, P5↔P6, P7↔P8, P9↔P10, P11↔P12, P13↔P14, P15↔P16). Posteriormente se caracterizaron los aciertos de las preguntas de definición y se realizó una prueba Kruskal-Wallis para determinar diferencias en la cantidad de aciertos registrada en cada uno de los programas educativos. No se aplicaron pruebas posteriores ya que no se encontraron diferencias estadísticas significativas en la cantidad de aciertos. Asimismo, se realizaron pruebas de chi-cuadrado para determinar asociaciones entre cada una de las carreras

analizadas y el conocimiento de los alumnos, representado por lo correcto o incorrecto de sus respuestas (programa académico x (Correcto o incorrecto)).

En las pruebas de Wilcoxon se utilizó la correlación biserial de rangos como medida del tamaño del efecto. Mayores valores de la correlación biserial se interpretan como mayores tamaños del efecto. En las pruebas chi-cuadrado se calculó la V de Cramér como indicador de la fuerza de las asociaciones estadísticamente significativas. Valores más grandes de V de Cramér significan mayor fuerza en las asociaciones. En todos los casos se utilizó un nivel de confianza del 90% = $\alpha = 0.10$.

Participantes

En la tabla 3 se muestran los alumnos encuestados por cada uno de los programas académicos de la facultad, también se muestra los resultados obtenidos por sexo.

Tabla 3 Alumnos encuestados por carrera y sexo

Carrera	Alumnado participante	Participantes de género femenino	Participantes de género masculino
Contador Público	40	16	24
Licenciado en Administración	42	29	13
Licenciado en Comercio Exterior	112	65	47
Licenciado en Derecho	34	18	16
Licenciado en Tecnologías de la Información	60	19	41
Totales	288	147	141

Fuente: Elaboración propia

Los alumnos proporcionaron su consentimiento informado antes de ser parte de la investigación. Todos los participantes podían abandonar el presente estudio en cualquier momento. No se les proporcionó ningún incentivo o recompensa por contestar el cuestionario.

Resultados

Tabla 4 Estadísticos descriptivos por carrera (P1-P16)

CARRERA	CP (Media, DE)		LA (Media, DE)		LCE (Media, DE)		LD (Media, DE)		LTI (Media, DE)	
P1	3.8	1.07	3.83	1.12	3.84	1.2	4.06	1.1	4.03	0.88
P2	3.75	1.08	3.76	1.14	3.76	1.14	4.12	1.09	3.88	0.99
P3	4.15	1	4.52	0.70	3.95	1.1	4.15	1.26	3.92	1.14
P4	3.4	1.39	3.48	1.31	3.5	1.22	3.76	1.26	3.33	1.17
P5	3.77	1.25	3.55	1.37	3.64	1.18	3.85	1.28	3.73	1.25
P6	3.67	1.19	4.07	0.94	3.7	1.14	3.88	1.23	3.9	1.12
P7	3.83	1.17	4.02	1.22	3.8	1.09	4.35	1.01	3.63	1.12
P8	3.98	1.14	3.98	1.16	3.97	1.07	4.38	0.95	3.63	1.18
P9	3.17	1.34	3.48	1.42	3.41	1.21	4.21	1.09	3.43	1.25
P10	3.2	1.29	3.43	1.43	3.45	1.21	4.03	1.17	3.65	1.26
P11	3.15	1.27	3.17	1.41	3.29	1.27	3.68	1.17	4.03	0.86
P12	3.1	1.22	3.17	1.41	3.28	1.3	3.5	1.29	3.9	0.96
P13	3.33	1.27	3.43	1.31	3.44	1.21	3.76	1.35	3.4	1.24
P14	3.55	1.26	3.6	1.21	3.51	1.24	3.74	1.33	3.42	1.24
P15	3.35	1.37	3.45	1.33	3.38	1.3	3.68	1.17	3.78	1.17
P16	3.17	1.32	3.45	1.33	3.21	1.24	3.88	1.09	3.58	1.21

Nota: Escala Likert (1-5). Mayores valores indican mayor frecuencia o mayor hábito. Ver Tabla 1 para la redacción de cada pregunta

Fuente: Elaboración propia

En la tabla 4 presenta los descriptivos (Media y Desviación Estándar) de las acciones, costumbres y hábitos que tienen los estudiantes de las 5 carreras en los conceptos de ciberseguridad (P1-P16) se ha realizado.

Diferenciación entre hábitos de ciberseguridad en computadoras personales (PC Personal Computer) y teléfonos inteligentes en cada programa educativo.

Tabla 5 Resultados de Wilcoxon por carrera (pares PC vs Smartphone)

Carrera CP	p	Tamaño del efecto: Correlación biserial de rangos
Software Antivirus P3-P4	p = .001	0.826
Carrera LA		
Software Antivirus P3-P4	p < .001	0.964
Actualizo Antivirus P5-P6	p = .002	0.853
Carrera LCE		
Software Antivirus P3-P4	p < .001	0.7322
Bloqueador de ventanas emergentes P15-P16	p = .026	0.5217
Copias de seguridad P7-P8	p = .043	-0.3746
Carrera LD		
Software Antivirus P3-P4	p = .073	0.5897
Lectura de políticas de seguridad P9-P10	p = .095	1.0
Carrera LTI		
Software Antivirus P3-P4	p < .001	0.9015
Lectura de políticas de seguridad P9-P10	p = .011	-0.7802
Filtros sitios web P1-P2	p = .078	0.5048

Nota: Se reportan comparaciones significativas con $\alpha = 0.10$. Un signo negativo en el tamaño del efecto significa que la puntuación fue mayor en Smartphone que en computadora personal.

Fuente: Elaboración propia.

En la tabla 5 se muestran los resultados estadísticamente significativos de la prueba Wilcoxon ($\alpha = 0.10$). Esto ha permitido responder en qué medida los alumnos de las diferentes carreras presentan hábitos de los conceptos de ciberseguridad.

Se puede observar en la tabla 5 que la pregunta que fue estadísticamente significativa en todas las carreras analizadas se encuentra en la pregunta 3 ¿Utilizas antivirus en la computadora? contrastada con la 4 ¿Utilizas antivirus en los teléfonos inteligentes? Estos cuestionamientos en todas las carreras es la que presenta mayor puntuación en donde los participantes respondieron que usan el antivirus en las computadoras.

En la tabla 5, en la carrera de LA, los estudiantes actualizan el software de protección con mayor frecuencia en la PC que en el smartphone (P5 y P6).

Los estudiantes de la carrera de LCE utilizan un software bloqueador de ventanas emergentes (*pop-ups*) en las computadoras (P15) más que en los smartphones (P16). Estos

mismos alumnos encuestados realizan copias de seguridad en la computadora (P7) con mayor frecuencia más que en los teléfonos inteligentes (P8).

Los estudiantes de LD leen los acuerdos más en la PC (P9) que en el smartphone (P10). Los estudiantes de LTI leen los acuerdos más en el smartphone que en la PC.

Los estudiantes de la carrera de LTI, han obtenido un mayor puntaje al utilizar filtros para bloquear sitios web que pudieran representar una amenaza en la computadora (P1) que en los teléfonos inteligentes (P2).

Conocimientos

En la Tabla 6 se muestran los valores descriptivos del número de aciertos registrados en los cinco programas analizados. La Figura 1 presenta las medias y sus intervalos de confianza de α=.10.

No se encontraron diferencias estadísticas significativas en el número medio de aciertos entre cada programa educativo (H=1.81, gl=4, p=.77) de acuerdo con la prueba de Kruskal-Wallis.

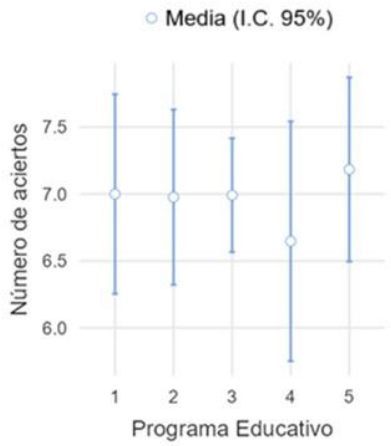
Tabla 6 Aciertos en ítems de definición por carrera

Programa Educativo	N	Media	DE	Error estándar (EE)
CP	40	7	2.33	0.37
LA	42	6.98	2.10	0.32
LCE	112	6.99	2.27	0.22
LD	34	6.65	2.57	0.44
LTI	60	7.18	2.67	0.34

Nota: Rango de posibles valores para la media: 0 a 10 aciertos. Representa el número medio de respuestas correctas P17-P26 de los participantes de cada programa educativo.

Fuente: Elaboración propia.

Figura 1 Medidas de aciertos e IC 95% por carrera



Fuente: Elaboración propia.

En la Tabla 7 se presenta el porcentaje de respuestas correctas para cada una de las preguntas en cada programa educativo.

Tabla 7. Porcentaje de correctas ítem/carrera

Carrera	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26
CP	43%	78%	85%	85%	58%	73%	85%	55%	73%	68%
LA	52%	71%	79%	71%	60%	74%	71%	83%	76%	60%
LCE	54%	70%	85%	83%	60%	70%	70%	69%	74%	66%
LD	56%	71%	85%	79%	68%	59%	56%	62%	71%	59%
LTI	53%	75%	85%	88%	68%	68%	70%	70%	72%	68%

Fuente: Elaboración propia

Asociación entre conocimientos sobre seguridad y programa académico

Los resultados de las pruebas chi-cuadrado para determinar asociaciones entre el conocimiento de los estudiantes y las carreras se muestran en la Tabla 8.

Tabla 8 Asociación entre acierto por ítem y carrera (chi-cuadrado)

Pregunta	Chi cuadrado	gl	Valor p
P17	1.81	4	0.77
P18	1.22	4	0.87
P19	1.10	4	0.89
P20	5.34	4	0.25
P21	2.16	4	0.70
P22	2.37	4	0.66
P23	7.60	4	0.10
P24	8.43	4	0.07
P25	0.439	4	0.97
P26	1.58	4	0.81

Fuente: Elaboración propia

En la tabla 8 se muestran los resultados de la relación de dos variables: la carrera cursada y la verificación de lo correcto o incorrecto de los conceptos relacionados a la ciberseguridad. En la pregunta sobre el concepto de robo de información (P23) se observó que los estudiantes de la carrera de CP proporcionaron más respuestas correctas de lo esperado, mientras que los participantes de la carrera de LD contestaron incorrectamente más veces de lo esperado (P=0.10, V=.16, | Residuos Estandarizados | > 1.96).

Por otra parte, en la pregunta de phishing (P24) se observó que los estudiantes de la carrera de CP obtuvieron más respuestas incorrectas de lo esperado, mientras que los alumnos de LA obtuvieron más respuestas correctas de lo esperado (P=.07, V=.17, | Residuos Estandarizados | > 1.96).

Discusión

Los resultados obtenidos en este estudio reflejan una diferencia notable en la percepción y aplicación de prácticas de ciberseguridad dependiendo del tipo de dispositivo utilizado. Se evidenció que, si bien los estudiantes universitarios poseen un conocimiento básico de los conceptos fundamentales de ciberseguridad, sus hábitos de protección y prevención varían considerablemente entre el uso de computadoras personales y teléfonos inteligentes.

El análisis de los hábitos realizado indica que el uso de antivirus en computadoras personales es significativamente mayor en comparación con los teléfonos inteligentes en todas las carreras evaluadas. Este hallazgo es consistente con investigaciones previas (Breitinger et al., 2020; Taha & Dahabiyeh, 2021) que señalan que los usuarios suelen

subestimar los riesgos de seguridad en dispositivos móviles, a pesar de que estos se han convertido en herramientas esenciales tanto en entornos académicos como personales. De manera similar, estudios como el de Alotibi (2024) destacan la necesidad de programas de concienciación enfocados en ataques de ingeniería social dirigidos a dispositivos móviles, donde los estudiantes tienden a ser más vulnerables debido a la confianza excesiva en la seguridad implícita de estos dispositivos.

Asimismo, en las pruebas a la realización de copias de seguridad solo se presentaron diferencias estadísticas significativas (α=0.10) en la carrera de LCE. En la lectura de acuerdos de políticas de seguridad se observaron diferencias significativas en las carreras de LD y LTI; (Çiftçi & Delialioğlu, 2016; Hong et al., 2023). Los de LTI leen más en el smartphone, lo que sugiere una percepción de mayor vulnerabilidad en estos dispositivos. Esta discrepancia puede atribuirse a la falta de educación específica sobre seguridad en dispositivos móviles y a la suposición errónea de que los teléfonos inteligentes están automáticamente protegidos por los sistemas operativos y aplicaciones (Çiftçi & Delialioğlu, 2016). De hecho, la educación en ciberseguridad en muchos programas académicos sigue enfocándose en amenazas tradicionales relacionadas con computadoras de escritorio, dejando de lado riesgos específicos de los dispositivos móviles (Hong et al., 2023).

Aunque no se encontraron diferencias estadísticas significativas al comparar el número medio de respuestas correctas por cada programa educativo, al evaluar con mayor granularidad la distribución de respuestas correctas e incorrectas observadas y esperadas (α=0.10) se encontró que los estudiantes de Contador Público mostraron mayor conocimiento sobre el robo de información, mientras que los estudiantes de Administración demostraron mayor familiaridad con el concepto de phishing. No obstante, los alumnos del área de Derecho presentaron el nivel más bajo de conocimiento sobre robo de información, mientras que los alumnos de Contador Público tuvieron menor conocimiento sobre phishing. Estas diferencias pueden estar relacionadas con el enfoque curricular de cada carrera, ya que investigaciones previas han identificado que los programas académicos con un componente legal o tecnológico tienden a incluir más formación en ciberseguridad (Khader et al., 2021; Venter et al., 2019).

Otro hallazgo relevante es que, aunque existen esfuerzos institucionales para ofrecer formación en ciberseguridad, estos no parecen ser suficientes para generar un cambio significativo en la conducta de los estudiantes. En este sentido, estudios como el de Cheng y Wang (2022) subrayan la necesidad de integrar estrategias de concienciación en los

programas educativos de manera continua y sistemática, en lugar de depender exclusivamente de seminarios o eventos aislados. Kannelønning y Katsikas (2023) también enfatizan que la medición del impacto de estas iniciativas educativas es clave para determinar su efectividad y ajustar los métodos de enseñanza en función de los resultados obtenidos.

Por otro lado, la cultura organizacional y el entorno social también desempeñan un papel crucial en la concienciación sobre ciberseguridad. Wiley, McCormac y Calic (2020) encontraron que una cultura de seguridad bien establecida dentro de una organización puede influir positivamente en la adopción de buenas prácticas de seguridad digital. Este factor podría explicar por qué algunos estudiantes, especialmente aquellos con mayor exposición a contextos laborales relacionados con la ciberseguridad, muestran mejores hábitos de protección. Asimismo, estudios recientes han evidenciado que el uso excesivo de Internet con fines recreativos (ciberocio) puede afectar la conciencia de seguridad de los individuos Hadlington y Parsons (2017), lo que sugiere que los hábitos digitales generales de los estudiantes pueden influir en su comportamiento en materia de ciberseguridad.

Estos hallazgos refuerzan la importancia de estrategias educativas diferenciadas que aborden tanto las brechas de conocimiento como las variaciones en el comportamiento de seguridad digital. La creciente dependencia de los dispositivos móviles en el ámbito universitario y profesional demanda un enfoque más integral que incluya formación específica en ciberseguridad para estos dispositivos, así como una evaluación continua del impacto de estas estrategias en la conducta de los estudiantes.

Dentro de las limitantes de este trabajo se encuentran que el estudio se realizó en una sola institución educativa y el muestreo fue por conveniencia. Por otra parte, dada la naturaleza exploratoria del estudio, las comparaciones estadísticas se consideraron individuales e independientes del resto, por lo que no se aplicó ninguna corrección a los valores p.

Conclusiones

El estudio confirma la necesidad de fortalecer la alfabetización en ciberseguridad en el ámbito universitario, con especial énfasis en la protección de dispositivos móviles. Aunque los estudiantes universitarios son conscientes de los riesgos de ciberseguridad, sus prácticas de seguridad no son homogéneas y dependen en gran medida del tipo de dispositivo utilizado. Dentro de los principales hallazgos, destaca una mayor preocupación por la seguridad en computadoras personales. Los estudiantes aplican más medidas de protección en sus computadoras que en sus teléfonos inteligentes, a pesar de que estos últimos son los dispositivos de uso más frecuente. Asimismo, a nivel ítem, se encontraron asociaciones estadísticas significativas (α=0.10) entre la disciplina académica y el nivel de conocimiento de los conceptos de ciberseguridad, concretamente en cuanto al robo de información y phishing lo que sugiere la necesidad de adaptar la enseñanza de estos temas a cada contexto educativo.

También se detectó una deficiencia en la cultura de seguridad digital en dispositivos móviles. A pesar del alto uso de smartphones, los estudiantes no aplican con la misma rigurosidad medidas de protección en estos dispositivos, lo que representa un riesgo significativo. El caso significativo más recurrente en todos los programas educativos fue el uso de antivirus en computadoras personales, pero no en dispositivos móviles. Estos resultados evidencian la necesidad de implementar programas educativos específicos, campañas de sensibilización, gestión de copias de seguridad, instalación y actualización de antivirus para fortalecer la conciencia en ciberseguridad y mejorar las prácticas de protección digital.

Futuras líneas de investigación

Como trabajo a futuro, se plantea ampliar la aplicación del instrumento a un mayor número de participantes de otras instituciones educativas de nivel superior de la región. Se propone alfabetizar en conceptos básicos sobre ciberseguridad y aplicar el instrumento periódicamente con el objetivo de analizar el cambio en los hábitos y el nivel de conocimientos. Se sugiere realizar mediciones cada seis meses, por lo menos, para contar con datos longitudinales y analizar la evolución y las tendencias encontradas a lo largo del tiempo. Los resultados permitirán tomar decisiones para mejorar el conocimiento sobre la ciberseguridad.

Referencias

Alotibi, G. (2024). A cybersecurity awareness model for the protection of Saudi students from social media attacks. Engineering, Technology and Applied Science Research, 14(2), 13787–13795. https://doi.org/10.48084/etasr.7123

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. IEEE Access, 12, 86596–86617. https://doi.org/10.1109/ACCESS.2024.3416045

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. Computers & Security, 88, 101647. https://doi.org/10.1016/j.cose.2019.101647

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4). https://doi.org/10.3390/info13040192

Çiftçi, N. P., & Delialioğlu, Ö. (2016). Supporting students' knowledge and skills in information technology security through a security portal. Information Development, 32(5), 1417–1427. https://doi.org/10.1177/0266666915601463

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? Cyberpsychology, Behavior, and Social Networking, 20(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Education and Information Technologies, 28(1), https://doi.org/10.1007/s10639-022-11121-5

Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of K-12 cybersecurity education around the world. IEEE Access, Vol. 12, 59726–59738. https://doi.org/10.1109/ACCESS.2024.3393425

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. Information and Computer Security, Vol. 31(4). https://doi.org/10.1108/ICS-08-2022-0139

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information (Switzerland), 12(10), 1–20. https://doi.org/10.3390/info12100417

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3). https://doi.org/10.1016/j.heliyon.2023.e14234

Taha, N., & Dahabiyeh, L. (2021). College students' information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". Heliyon, 5(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. Computers & Security, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186(October 2021), 104536. https://doi.org/10.1016/j.compedu.2022.104536

Zulfia, A., Adawiyah, R., Hidayanto, A. N., & Fitriah Ayuning Budi, N. (2019). En Proceedings of the 5th International Conference on Computing Engineering and Design (ICCED 2019). IEEE pp 1-5. https://doi.org/10.1109/ICCED46541.2019.9161120

Rol de Contribución	Autor (es)
Conceptualización	Rolando Salazar Hernández
Metodología	Rolando Salazar Hernández
Software	Rolando Salazar Hernández (igual), Ramón Ventura Roque Hernández (igual)
Validación	Rolando Salazar Hernández (igual), Ramón Ventura Roque Hernández (igual)
Análisis Formal	Ramón Ventura Roque Hernández
Investigación	Rolando Salazar Hernández
Recursos	Rolando Salazar Hernández
Curación de datos	Rolando Salazar Hernández (igual), Ramón Ventura Roque Hernández (igual)
Escritura - Preparación del borrador original	Rolando Salazar Hernández (igual), Ramón Ventura Roque Hernández (igual)
Escritura - Revisión y edición	Rolando Salazar Hernández (igual), Ramón Ventura Roque Hernández (igual)
Visualización	Ramón Ventura Roque Hernández (igual), Adán López Mendoza (igual)
Supervisión	Rolando Salazar Hernández
Administración de Proyectos	Rolando Salazar Hernández
Adquisición de fondos	Adán López Mendoza