Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 8.1
Edición Especial VIII 2026

EVALUACIÓN DEL NIVEL DE CONCIENCIA Y PRÁCTICAS DE CIBERSEGURIDAD EN ESTUDIANTES DE LA FACULTAD DE CIENCIAS INFORMÁTICAS DE LA UNIVERSIDAD TÉCNICA DE MANABÍ Y PROPUESTA DE MEJORA FORMATIVA

EVALUATION OF THE LEVEL OF AWARENESS AND PRACTICES OF CYBERSECURITY IN STUDENTS OF THE FACULTY OF COMPUTER SCIENCE OF THE TECHNICAL UNIVERSITY OF MANABÍ AND PROPOSAL FOR FORMATIVE IMPROVEMENT

Autores: [1]Bryan Javier Robles García y [2]María Genoveva Moreira Santos.
[1]ORCID ID: https://orcid.org/0009-0000-2033-5578
[2]ORCID ID: https://orcid.org/0000-0003-3216-9831
[1]E-mail de contacto: brobles0480@utm.edu.ec
[2]E-mail de contacto: genoveva.moreira@utm.edu.ec
Afiliación: [1*2*]Universidad Técnica de Manabí, (Ecuador).
Artículo recibido: 04 de Agosto del 2026.
Artículo revisado: 06 de Agosto del 2026.
Artículo aprobado: 06 de Agosto del 2026.
[1]Estudiante de la Universidad Técnica de Manabí, (Ecuador).
[2]Ingeniera en Sistemas Informáticos, egresada de la Universidad Técnica de Manabí, (Ecuador). Magister Informática Empresarial, egresada de la Universidad Regional Autónoma de los Andes, (Ecuador). Actualmente, Docente de la Universidad Técnica de Manabí, (Ecuador).

Resumen

La transformación digital que están viviendo las instituciones de educación superior ha llevado a un aumento en la dependencia de las tecnologías de la información. Esto, a su vez, ha incrementado la exposición a amenazas cibernéticas que pueden poner en riesgo la seguridad de los datos y sistemas de estas instituciones. En este escenario, el factor humano se convierte en uno de los puntos más vulnerables, por lo que es crucial entender el nivel de conciencia, conocimientos y prácticas de ciberseguridad entre los estudiantes universitarios. Esta investigación tuvo como objetivo evaluar esos aspectos en los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí, buscando identificar tanto fortalezas como debilidades y proponer mejoras en la formación. Se llevó a cabo un estudio con un enfoque cuantitativo, de alcance descriptivo, con un diseño no experimental y un corte transversal. La información se recolectó a través de una encuesta estructurada dirigida a los estudiantes de la facultad, que incluía preguntas sobre conocimientos básicos de ciberseguridad, hábitos digitales, percepción del riesgo y experiencias con incidentes de seguridad informática. Los datos fueron procesados y analizados utilizando estadísticas descriptivas, enfocándose en frecuencias y porcentajes. Los resultados mostraron diferencias entre el nivel de conocimiento que los estudiantes afirmaban tener y sus prácticas reales de seguridad digital. Se identificaron fortalezas en aspectos conceptuales, pero también debilidades en la adopción de medidas preventivas y en la percepción del riesgo ante las amenazas cibernéticas. En conclusión, aunque los estudiantes tienen un nivel aceptable de conocimiento sobre ciberseguridad, es fundamental reforzar su formación con estrategias educativas que fomenten hábitos seguros, reduzcan las vulnerabilidades relacionadas con el factor humano y ayuden a construir una cultura de ciberseguridad en el ámbito universitario.

Palabras clave: Ciberseguridad, Conciencia en ciberseguridad, Estudiantes universitarios, Educación superior, Seguridad de la información, Cultura de ciberseguridad.

Abstract

The digital transformation underway in higher education institutions has led to an increased reliance on information technologies. This, in turn, has increased exposure to cyber threats

that can jeopardize the security of these institutions' data and systems. In this context, the human factor becomes one of the most vulnerable points, making it crucial to understand the level of cybersecurity awareness, knowledge, and practices among university students. This research aimed to evaluate these aspects among students in the Faculty of Computer Science at the Technical University of Manabí, seeking to identify both strengths and weaknesses and propose improvements in training. A quantitative, descriptive, non-experimental, cross-sectional study was conducted. Data was collected through a structured survey administered to students in the faculty, which included questions about basic cybersecurity knowledge, digital habits, risk perception, and experiences with cybersecurity incidents. The data were processed and analyzed using descriptive statistics, focusing on frequencies and percentages. The results showed discrepancies between the level of knowledge students reported having and their actual digital security practices. Strengths were identified in conceptual aspects, but weaknesses were also found in the adoption of preventative measures and in risk perception regarding cyber threats. In conclusion, although students have an acceptable level of cybersecurity knowledge, it is essential to reinforce their training with educational strategies that promote safe habits, reduce vulnerabilities related to the human factor, and help build a cybersecurity culture within the university setting.

Keywords: Cybersecurity, Cybersecurity awareness, University students, Higher education, Information security, Cybersecurity culture.

Sumário

A transformação digital em curso nas instituições de ensino superior levou a uma maior dependência das tecnologias de informação. Isso, por sua vez, aumentou a exposição a ciberameaças que podem comprometer a segurança dos dados e sistemas dessas instituições. Nesse contexto, o fator humano torna-se um dos pontos mais vulneráveis, tornando crucial a compreensão do nível de conscientização, conhecimento e práticas de cibersegurança entre os estudantes universitários. Esta pesquisa teve como objetivo avaliar esses aspectos entre os estudantes da Faculdade de Ciência da Computação da Universidade Técnica de Manabí, buscando identificar pontos fortes e fracos e propor melhorias na formação. Foi realizado um estudo quantitativo, descritivo, não experimental e transversal. Os dados foram coletados por meio de um questionário estruturado aplicado aos estudantes da faculdade, que incluía perguntas sobre conhecimento básico de cibersegurança, hábitos digitais, percepção de risco e experiências com incidentes de cibersegurança. Os dados foram processados e analisados utilizando estatística descritiva, com foco em frequências e percentagens. Os resultados mostraram discrepâncias entre o nível de conhecimento relatado pelos estudantes e suas práticas reais de segurança digital. Foram identificados pontos fortes em aspectos conceituais, mas também foram encontradas fragilidades na adoção de medidas preventivas e na percepção de risco em relação às ciberameaças. Em conclusão, embora os estudantes possuam um nível aceitável de conhecimento em cibersegurança, é essencial reforçar sua formação com estratégias educacionais que promovam hábitos seguros, reduzam as vulnerabilidades relacionadas ao fator humano e contribuam para a construção de uma cultura de cibersegurança no ambiente universitário.

Palavras-chave: Cibersegurança, Conscientização sobre cibersegurança, Estudantes universitários, Ensino superior, Segurança da informação, Cultura de cibersegurança.

Introducción

La rápida transformación digital ha llevado a una adopción masiva de tecnologías de la información en casi todos los sectores de nuestra sociedad, y las instituciones de educación superior no son la excepción. Gracias al uso de plataformas de aprendizaje virtual,

servicios en la nube, aplicaciones colaborativas, dispositivos móviles y sistemas de gestión académica, se han optimizado los procesos de enseñanza, investigación y administración en las universidades (Haque et al., 2023). Sin embargo, esta creciente dependencia de la tecnología también ha aumentado la exposición a amenazas cibernéticas cada vez más complejas, lo que convierte la ciberseguridad en un aspecto crucial para asegurar la confidencialidad, integridad y disponibilidad de la información. En este escenario, las universidades no solo necesitan reforzar su infraestructura tecnológica, sino que también deben cultivar habilidades humanas que les permitan prevenir, identificar y responder de manera efectiva a los riesgos que surgen en el entorno digital (Chen y Hu, 2024).

Las instituciones de educación superior manejan a diario enormes cantidades de información académica, administrativa y personal, lo que las convierte en un blanco atractivo para los ciberdelincuentes. La rápida digitalización de procesos en los últimos años ha ampliado la superficie de ataque y ha puesto de manifiesto la urgente necesidad de implementar estrategias de ciberseguridad más completas (Ganesen et al., 2022). Estas estrategias deben combinar controles tecnológicos, políticas institucionales y programas de formación continua para toda la comunidad universitaria. Varios estudios coinciden en que la protección efectiva de los activos digitales no solo depende de las herramientas tecnológicas, sino también del nivel de preparación de las personas que interactúan con estos sistemas a diario (De Ramos y Esponilla, 2022). A pesar de que las universidades han ido mejorando sus sistemas de seguridad informática, todavía hay muchos incidentes que surgen por errores humanos. Cosas que parecen inofensivas, como reutilizar contraseñas, hacer clic en enlaces sospechosos, usar redes Wi-Fi públicas sin protección o compartir información sensible sin asegurarse de su veracidad, son algunas de las principales fuentes de vulnerabilidad. Por ende, muchos expertos coinciden en que el comportamiento de los usuarios es uno de los factores más críticos en la gestión de la ciberseguridad, y que aumentar la conciencia digital debería ser una prioridad para las instituciones (Alzahrani, 2021; Erendor y Yildirim, 2022). Así que, cultivar hábitos seguros es tan esencial como implementar soluciones tecnológicas de vanguardia.

En los últimos años, varias investigaciones realizadas en universidades de diferentes países han estado evaluando el nivel de conciencia y conocimiento en ciberseguridad entre los estudiantes, utilizando encuestas como herramienta principal (Aljohni et al., 2021). Los hallazgos indican que, aunque la mayoría de los estudiantes entiende la importancia de proteger su información digital, todavía hay notables deficiencias en áreas como la identificación de ataques de phishing, el uso de autenticación multifactor, la creación de contraseñas seguras y la adopción de buenas prácticas para salvaguardar dispositivos y cuentas personales. Además, se ha notado que los estudiantes de carreras de informática tienden a obtener mejores resultados en estas evaluaciones que sus compañeros de otras disciplinas.

Sin embargo, estas diferencias no aseguran que adopten comportamientos seguros frente a las amenazas digitales, lo que pone de manifiesto una brecha entre el conocimiento teórico y la aplicación práctica de las medidas de protección (Huraj et al., 2023). Frente a este desafío, la literatura científica sugiere que la educación en ciberseguridad debe ir más allá de simplemente enseñar conceptos teóricos. Es fundamental

incorporar metodologías activas que fomenten un aprendizaje práctico y el desarrollo de competencias. Entre las estrategias más efectivas se encuentran el aprendizaje basado en problemas, las simulaciones, la gamificación, los laboratorios virtuales y los ejercicios tipo Capture the Flag (CTF) (Ramezanian y Niemi, 2024; Schafeitel y Lazarov, 2025). Estas técnicas han demostrado ser eficaces para mejorar el conocimiento, la capacidad de respuesta ante incidentes y la adopción de buenas prácticas en seguridad digital. Además, se subraya la importancia de actualizar los planes de estudio universitarios de acuerdo con marcos internacionales de competencias, lo que permitirá a los futuros profesionales adquirir habilidades que se alineen con las exigencias del entorno tecnológico actual (Hajny et al., 2021).

En América Latina, y especialmente en Ecuador, todavía hay una falta de estudios empíricos que examinen el nivel de conciencia y las prácticas de ciberseguridad entre los estudiantes universitarios utilizando herramientas estandarizadas. Esta falta de información hace que sea complicado para las instituciones de educación superior obtener diagnósticos claros sobre las fortalezas y debilidades de sus estudiantes frente a las amenazas digitales. Por lo tanto, es fundamental llevar a cabo investigaciones que ayuden a entender la realidad de cada contexto institucional y que sirvan como base para diseñar programas de formación y sensibilización que se ajusten a las necesidades locales. Esto, a su vez, contribuirá a fortalecer la cultura de ciberseguridad en el entorno universitario (Vera, 2024; Zamora et al., 2025). La Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí se dedica a formar profesionales que, debido a la naturaleza de su campo, estarán estrechamente relacionados con el diseño, desarrollo, gestión y protección de sistemas de información. En este sentido, es crucial entender el nivel de conocimientos, conciencia y prácticas de ciberseguridad de sus estudiantes, ya que ellos serán parte del talento humano encargado de enfrentar los retos que conlleva la protección de la información en organizaciones tanto públicas como privadas. Además, identificar las principales debilidades permitirá dirigir acciones de mejora que ayuden a fortalecer no solo la formación académica, sino también la cultura institucional de seguridad digital.

Con este panorama en mente, el presente estudio tiene como meta evaluar el nivel de conciencia, conocimientos y prácticas de ciberseguridad de los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí a través de una encuesta estructurada. A partir de los resultados obtenidos, se pretende identificar fortalezas, debilidades y oportunidades de mejora que faciliten la propuesta de estrategias formativas enfocadas en el fortalecimiento de competencias, la promoción de comportamientos seguros y la consolidación de una cultura de ciberseguridad que ayude a disminuir las vulnerabilidades relacionadas con el factor humano en el entorno universitario.

Materiales y Métodos

La investigación se desarrolló bajo un enfoque cuantitativo, lo que nos permitió recolectar, medir y analizar datos numéricos sobre el nivel de conciencia, conocimientos y prácticas de ciberseguridad entre los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí. El estudio tuvo un alcance descriptivo, ya que su objetivo fue caracterizar el estado actual de las variables en cuestión sin intervenir en ellas ni establecer relaciones de causa y efecto. Además, se utilizó

un diseño no experimental de corte transversal, dado que los datos se recopilaron en un solo momento a través de una encuesta. Esto nos permitió obtener un diagnóstico claro sobre la situación actual de la población estudiada en relación con la conciencia y las prácticas de ciberseguridad.

La población que se estudió estaba compuesta por los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí. Para recolectar la información, se utilizó un muestreo no probabilístico por conveniencia, donde se tuvo en cuenta la participación voluntaria de aquellos estudiantes que decidieron responder el cuestionario de investigación. Al final, la muestra quedó conformada por 200 estudiantes, quienes completaron la encuesta a través de un formulario digital. Solo se tomaron en cuenta las respuestas completas, descartando aquellos registros que estaban incompletos asegurando así que la información utilizada en la investigación fuera consistente.

La técnica que se utilizó para recolectar información fue la encuesta, elegida por su habilidad para obtener datos de manera sistemática sobre lo que saben, piensan y hacen los estudiantes en cuanto a la ciberseguridad. Se diseñó un cuestionario estructurado que se implementó a través de Google Forms. La encuesta se dividió en seis secciones principales:

Tabla 1. *Secciones de la encuesta.*

Pregunta	Numero de Sección	Sección
1 - 5	1	Datos generales de los participantes.
6 - 8	2	Conocimiento objetivo sobre conceptos básicos de ciberseguridad.
9 - 11	3	Autopercepción y nivel de conciencia en ciberseguridad.
12 - 17	4	Prácticas habituales relacionadas con la seguridad digital.
18 - 19	5	Experiencia y percepción del riesgo frente a incidentes de ciberseguridad.
20	6	Pregunta abierta para recoger recomendaciones sobre los temas de ciberseguridad que los estudiantes consideran prioritarios fortalecer dentro de la facultad.

Fuente: Elaboración propia.

El cuestionario abarcó una variedad de preguntas, incluyendo opciones de selección única, escalas tipo Likert de cinco niveles, preguntas dicotómicas y una pregunta abierta. Esto permitió obtener información tanto objetiva como subjetiva sobre las variables en estudio. Antes de que los participantes comenzaran a responder, se les explicó el propósito de la investigación, que su participación era completamente voluntaria y que la información que compartieran sería tratada con total confidencialidad. Al principio de la investigación, se llevó a cabo una revisión bibliográfica sobre la conciencia, los conocimientos y las prácticas de ciberseguridad en las instituciones de educación superior. Esto se hizo con el objetivo de fundamentar el estudio y guiar el diseño del instrumento de investigación. Una vez que se completó el proceso de recolección de datos, las respuestas se exportaron a Microsoft Excel para organizarlas, depurarlas y verificarlas, eliminando cualquier inconsistencia antes de proceder con el análisis estadístico. La información que recopilamos fue procesada con Microsoft Excel y Microsoft Power BI. Primero, nos enfocamos en depurar y organizar la base de datos. Luego, calculamos las frecuencias absolutas, las frecuencias relativas y los porcentajes para cada una de las variables que analizamos. Después, utilizamos Power BI para crear tablas y gráficos que hicieron mucho más fácil visualizar e interpretar los resultados. Finalmente, analizamos los hallazgos en

función de los objetivos específicos de la investigación, lo que nos permitió identificar el nivel de conocimientos, las prácticas habituales y la percepción del riesgo en ciberseguridad de los estudiantes que participaron.

Resultados y Discusión

Para una mejor comprensión de los hallazgos, los resultados se organizaron en diferentes secciones según las dimensiones que evaluó el instrumento de investigación. Primero, se presenta la caracterización de los participantes, teniendo en cuenta variables como el semestre académico, la edad, el género y la formación previa en ciberseguridad. Luego, se analizan los resultados relacionados con el conocimiento de conceptos fundamentales, el nivel de conciencia y autopercepción, las prácticas habituales de seguridad digital, la experiencia con incidentes de ciberseguridad y, por último, las necesidades de formación que los estudiantes han identificado.

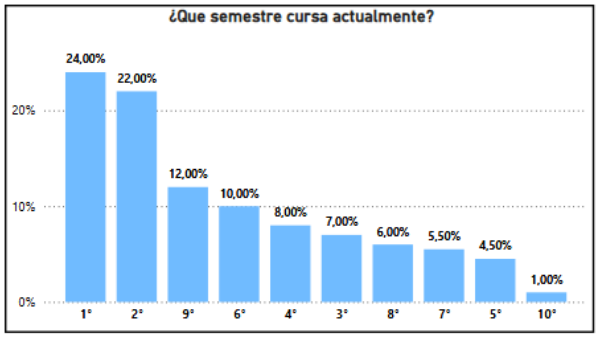


Figura 1. *Distribución de los estudiantes según el semestre que cursan actualmente.*

Fuente: Elaboración propia.

Como se puede ver en la Figura 1, la mayor parte de la muestra estuvo compuesta por estudiantes de primer semestre, quienes representaron un 24,0%. Les siguieron los estudiantes de segundo semestre con un 22,0%. Juntos, estos dos grupos abarcaron casi la mitad de los participantes, lo que muestra que hay una mayor representación de aquellos que están en las primeras etapas de su formación académica. Por otro lado, los semestres superiores mostraron una distribución más equilibrada, con el noveno semestre destacándose con un 12,0% y el octavo con un 10,0%. En contraste, el décimo semestre tuvo la menor participación, con solo un 1,0%. Esta distribución asegura que haya representación de estudiantes de todos los niveles académicos, lo que permite analizar la conciencia y las prácticas de ciberseguridad desde diferentes etapas del proceso educativo.

La inclusión de estudiantes de todos los niveles académicos nos brinda una perspectiva amplia sobre el estado de la conciencia y las prácticas de ciberseguridad en la Facultad de Ciencias Informáticas. Además, la mayor presencia de estudiantes de los primeros semestres ofrece información valiosa para entender sus conocimientos y hábitos de seguridad digital desde el inicio de su formación profesional.

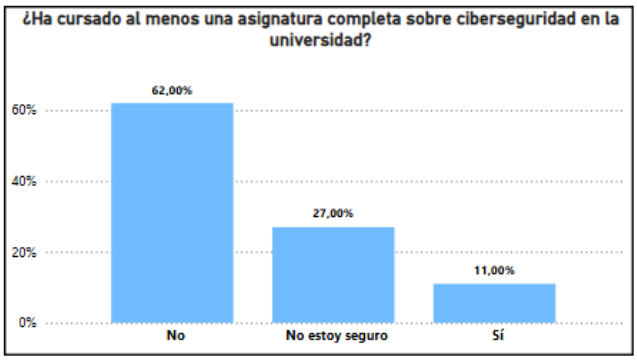


Figura 2. *Estudiantes que han cursado al menos una asignatura completa sobre ciberseguridad.*

Fuente: Elaboración propia

Los resultados revelan que la mayoría de los estudiantes no ha tenido la oportunidad de cursar una asignatura completa sobre ciberseguridad durante su paso por la universidad. De hecho, un 62,0% admitió no

haber recibido este tipo de formación, mientras que solo un 11,0% afirmó haber tomado al menos una asignatura específica relacionada con el tema. Además, un 27,0% expresó no estar seguro de si había recibido formación formal en ciberseguridad. Estos hallazgos ponen de manifiesto la escasa inclusión de contenidos específicos de ciberseguridad en la trayectoria académica de una parte significativa de los estudiantes. Asimismo, el porcentaje de participantes que mostró incertidumbre sobre este tema podría sugerir que algunos aspectos de la seguridad digital se han tratado de manera transversal en otras asignaturas, sin que se identifiquen claramente como formación en ciberseguridad.

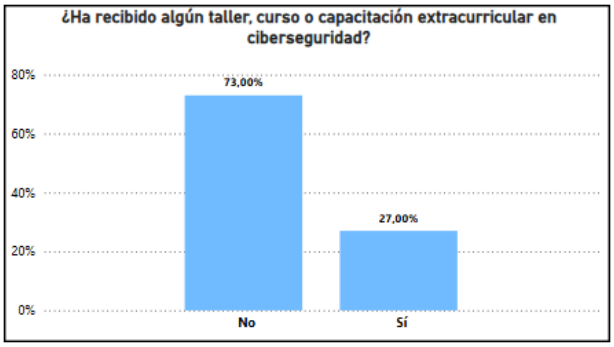


Figura 3. Participación en talleres, cursos o capacitaciones extracurriculares sobre ciberseguridad

Fuente: Elaboración propia.

Cuando se trata de la formación extracurricular, un sorprendente 73,0% de los estudiantes admitió que no ha participado en talleres, cursos o capacitaciones sobre ciberseguridad fuera de sus clases universitarias. En contraste, solo el 27,0% dijo haber recibido algún tipo de formación adicional en este campo. Este dato revela que la mayoría de los encuestados ha tenido pocas oportunidades para enriquecer sus conocimientos a través de actividades complementarias. Dado el constante aumento de las amenazas digitales y la rápida evolución de las tecnologías de protección, la escasa participación en estas iniciativas resalta la urgente necesidad de impulsar programas de capacitación que complementen la educación formal y ayuden a fortalecer las habilidades en ciberseguridad.

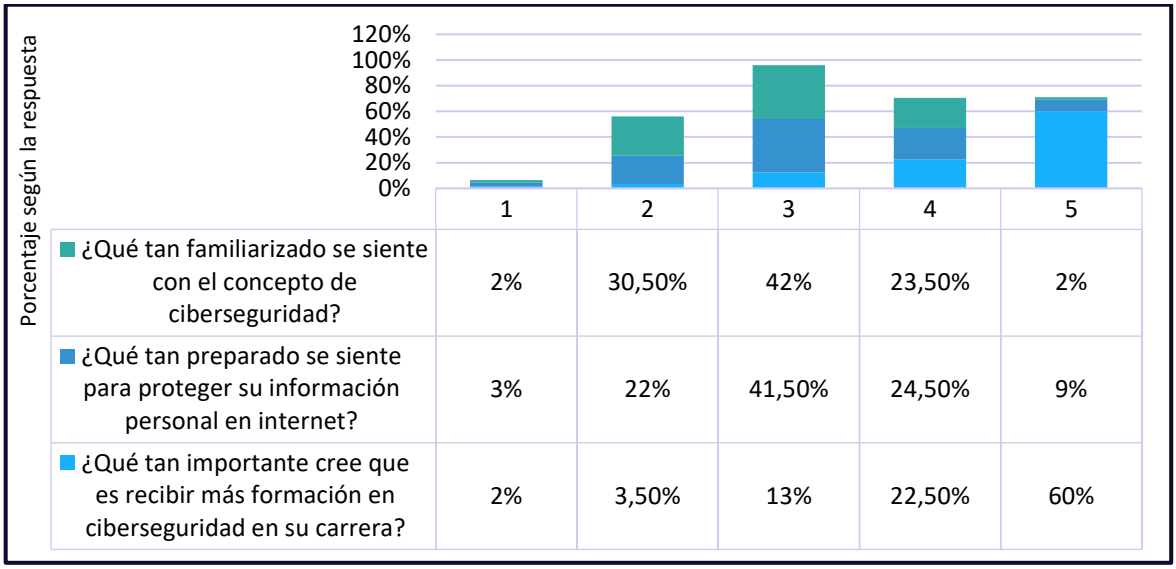
Tabla 2. *Respuestas correctas e incorrectas en las preguntas de conocimiento objetivo.*

Pregunta	Opción correcta	Respuestas correctas (%)	Respuestas incorrectas (%)
¿Cuál de las siguientes opciones es la mejor definición de ciberseguridad?	Protección de redes, dispositivos y datos contra ataques digitales	84,5%	15,5%
Marque si la siguiente afirmación es VERDADERA o FALSA: Usar una red Wi-Fi pública sin contraseña es seguro si solo entro a redes sociales	Falso	77,0%	23,0%
En un correo sospechoso, ¿cuál es la acción más segura antes de hacer clic en un enlace?	Pasar el mouse sobre el enlace para ver la URL real	77,0%	23,0%

Fuente: Elaboración propia.

Los resultados que se evidencian en la Tabla 2 demuestran que los estudiantes tienen un buen nivel de conocimiento sobre los conceptos básicos de ciberseguridad que se evaluaron. La pregunta sobre la definición de ciberseguridad fue la que obtuvo el mayor porcentaje de respuestas correctas, alcanzando un 84,5 %. Por otro lado, las preguntas sobre el uso seguro de redes Wi-Fi públicas y cómo identificar la acción más segura ante un correo electrónico sospechoso lograron un 77,0 % de aciertos. Aunque estos resultados indican que la mayoría de los participantes comprenden bien los principios fundamentales de la ciberseguridad, alrededor de uno de cada cuatro estudiantes cometió errores en las dos últimas preguntas. Esto resalta la necesidad de reforzar el

contenido relacionado con la identificación de riesgos y la adopción de prácticas seguras en situaciones cotidianas. Para entender mejor cómo perciben los estudiantes la ciberseguridad, se analizaron tres aspectos: su familiaridad con el concepto, su percepción sobre su preparación para proteger su información personal en Internet y la importancia que le dan a fortalecer la formación en ciberseguridad dentro de su carrera. Para facilitar la interpretación de los resultados, las respuestas se agruparon en una escala de cinco niveles, que va desde "Nada (1)" hasta "Totalmente (5)", lo que permite identificar las tendencias más comunes en la percepción de los participantes.



	1	2	3	4	5
¿Qué tan familiarizado se siente con el concepto de ciberseguridad?	2%	30,50%	42%	23,50%	2%
¿Qué tan preparado se siente para proteger su información personal en internet?	3%	22%	41,50%	24,50%	9%
¿Qué tan importante cree que es recibir más formación en ciberseguridad en su carrera?	2%	3,50%	13%	22,50%	60%

Figura 4. *Nivel de conciencia y autopercepción de los estudiantes sobre la ciberseguridad*

Fuente: Elaboración propia

Los resultados revelan que los estudiantes tienen una buena conciencia sobre lo crucial que es la ciberseguridad, aunque sus percepciones sobre cuán preparados están personalmente es un poco más moderada. En cuanto a su familiaridad con el concepto de ciberseguridad, la opción más elegida fue "Moderadamente", con un 42,0 %, seguida de "Bastante" con un 23,5 %. Además, un 30,5 % se sintió "Poco" familiarizado con el tema, mientras que solo un 2,0 % se consideró "Totalmente" familiarizado. Esto indica que, aunque la mayoría tiene nociones generales sobre ciberseguridad, hay un grupo significativo de estudiantes que siente que su conocimiento en este ámbito es insuficiente. Respecto a cómo perciben su capacidad para proteger su información personal en Internet, la respuesta más común fue nuevamente "Moderadamente" (41,5 %), seguida por "Bastante" (24,5 %) y "Poco" (22,0 %). Solo el 9,0 % se sintió "Totalmente" preparado, mientras que un 3,0 % admitió no sentirse preparado en absoluto. Estos resultados sugieren que, aunque una parte considerable de los estudiantes tiene una confianza parcial en sus habilidades para enfrentar riesgos digitales, todavía hay cierta incertidumbre sobre cómo aplicar medidas de protección en su vida diaria. La percepción cambia notablemente cuando se les pregunta sobre la necesidad de reforzar la formación en ciberseguridad dentro de su carrera. En esta ocasión, la opción "Totalmente" fue la más elegida, con un 60,0 % de los participantes, seguida de "Bastante" con un 22,5

%. En total, más de cuatro quintas partes de los estudiantes creen que es necesario aumentar la formación académica en este tema, mientras que solo un pequeño porcentaje tiene una opinión contraria. Este resultado muestra un amplio acuerdo sobre la importancia de incorporar o fortalecer estrategias educativas que desarrollen competencias en ciberseguridad. En términos generales, los hallazgos muestran que los estudiantes son conscientes de la importancia de la ciberseguridad en su formación profesional y expresan un gran interés en recibir una capacitación más completa. Sin embargo, su percepción moderada sobre su nivel de familiaridad y preparación personal sugiere que todavía hay espacio para mejorar sus conocimientos y habilidades prácticas en el ámbito de la seguridad digital, lo cual se alinea con los resultados obtenidos en la dimensión de conocimiento objetivo.

Tabla 3. Frecuencia de aplicación de prácticas de ciberseguridad por parte de los estudiantes.

Práctica de ciberseguridad	Nunca (1)	Casi nunca (2)	A veces (3)	Casi siempre (4)	Siempre (5)
Uso la misma contraseña para varias cuentas importantes (correo, redes, banco).	11,5%	23%	37,5%	21%	7%
Cuando una plataforma ofrece autenticación en dos pasos (2FA), la activo.	3,5%	14%	34%	22%	26,5%
Antes de hacer clic en un enlace de un correo o mensaje sospechoso, verifico la dirección real.	4%	14,5%	28%	23%	30,5%
Instalo las actualizaciones de seguridad del sistema operativo cuando están disponibles.	3,5%	8,5%	30,5%	25,5%	32%
Mi dispositivo principal tiene protección antivirus activa (incluye Windows Defender).	8%	11,5%	30%	19%	31,5%
Me conecto a redes Wi-Fi públicas (cafeterías, aeropuertos, parques) sin usar VPN ni protección adicional.	21,5%	17%	26%	22,5%	13%

Fuente: Elaboración propia.

En las prácticas relacionadas con el uso de una misma contraseña en varias cuentas y la conexión a redes Wi-Fi públicas sin protección adicional, las frecuencias más altas representan una mayor exposición a riesgos de ciberseguridad. Los resultados presentados en la Tabla 3 revelan que las prácticas de ciberseguridad entre los estudiantes son bastante variadas. En cuanto al uso de la misma contraseña para varias cuentas importantes, un 37,5 % admitió hacerlo “A veces”, mientras que un 28,0 % confesó que lo hace “Casi siempre” o “Siempre”. Esta tendencia aumenta el riesgo de que múltiples cuentas se vean comprometidas en caso de una filtración de credenciales, lo que sugiere que una parte significativa de los participantes necesita mejorar sus hábitos de gestión de contraseñas. Por otro lado, un 34,5 % afirmó que “Nunca” o “Casi nunca” reutiliza contraseñas, lo que indica que algunos sí están adoptando prácticas más seguras. En lo que respecta a la autenticación en dos pasos, el 48,5 % de los estudiantes dijo activarla “Casi siempre” o “Siempre”, mientras que un 34,0 % solo lo hace “A veces”. Aunque hay una tendencia positiva hacia el uso de este mecanismo de seguridad, los datos muestran que aún no es algo generalizado. De manera similar, la verificación de la dirección real antes de hacer clic en enlaces sospechosos tuvo una buena respuesta, ya que el 53,5 % afirmó realizar esta acción “Casi siempre” o “Siempre”. Este resultado se alinea con el desempeño observado en la

dimensión de conocimientos, donde la mayoría identificó correctamente esta medida como la más segura frente a correos sospechosos. Las prácticas relacionadas con la actualización de sistemas y el uso de protección antivirus mostraron los porcentajes más altos en cuanto a comportamientos favorables. Un 57,5 % indicó que instala actualizaciones de seguridad "Casi siempre" o "Siempre", mientras que un 50,5 % mantiene activa la protección antivirus con la misma frecuencia. Sin embargo, en ambos casos, alrededor de un tercio de los participantes optó por la opción "A veces", lo que sugiere que hay margen para mejorar.

Cuando se trata de conectarse a redes Wi-Fi públicas sin usar una VPN o alguna protección extra, un 35,5 % de las personas admitió que lo hace "Casi siempre" o "Siempre", mientras que un 26,0 % lo hace "A veces". Dado que esta práctica puede ser bastante arriesgada, estos números muestran que hay una exposición significativa a amenazas relacionadas con el uso de redes públicas. Por otro lado, un 38,5 % afirmó que "Nunca" o "Casi nunca" se conecta a estas redes sin tomar medidas de protección adicionales. Con el objetivo de entender cómo los estudiantes se enfrentan a posibles amenazas digitales y qué piensan sobre la probabilidad de ser víctimas de un ciberataque, se examinaron las experiencias que han reportado en el último año, así como su percepción del riesgo a futuro. Estos elementos nos ayudan a captar no solo el contacto previo de los participantes con incidentes de ciberseguridad, sino también el grado de vulnerabilidad que sienten ante posibles amenazas. Los resultados de la figura 5 revelan que un 71,5 % de los estudiantes afirmó no haber sido víctima de ningún intento de ciberataque en el último año. Sin embargo, el 28,5 % restante sí reportó haber vivido al menos una situación relacionada con estas amenazas. Entre los incidentes mencionados, el phishing se destacó como el más común, con un 13,0 %, seguido de cerca por los casos de malware o virus, que representaron un 9,5 %. Además, un 5,0 % indicó haber sufrido suplantación de identidad, mientras que un 1,0 % mencionó haber enfrentado otro tipo de incidente.

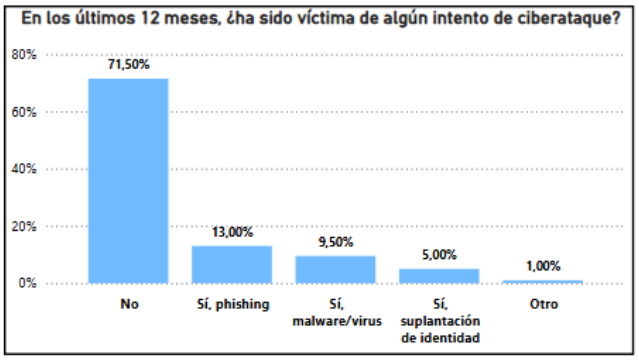


Figura 5. *Experiencias de los estudiantes frente a intentos de ciberataque durante los últimos 12 meses*

Fuente: Elaboración propia

A pesar de que la mayoría de los participantes no reportó experiencias directas con ciberataques, la proporción de estudiantes que sí enfrentó alguna amenaza pone de manifiesto que estos riesgos son parte de la realidad digital que afecta a una parte significativa de la población estudiada. La prevalencia del phishing como el incidente más común es especialmente relevante, ya que este tipo de ataque suele aprovechar la falta de conocimiento, la confianza o la falta de verificación de mensajes y enlaces para robar información personal o acceder a cuentas digitales. Los resultados que se muestran en la Figura 6 indican que los estudiantes tienden a ver la probabilidad de sufrir un ciberataque en los próximos 12 meses como baja o moderada. La respuesta más común fue el 40 %, con un 27 % de los participantes eligiendo esta opción, seguida de cerca por el 20 %, que obtuvo un 23 %. Además, un 22 % de los encuestados opinó que la probabilidad era nula. Por otro lado, las

percepciones más altas fueron disminuyendo gradualmente, llegando al 17 % en el nivel del 60 % y al 11 % en la probabilidad el 80 %. En resumen, estos resultados sugieren que los estudiantes ven una posibilidad moderada de enfrentar un ciberataque, aunque hay un grupo significativo que considera que es poco probable o incluso improbable que se encuentren con esta amenaza.

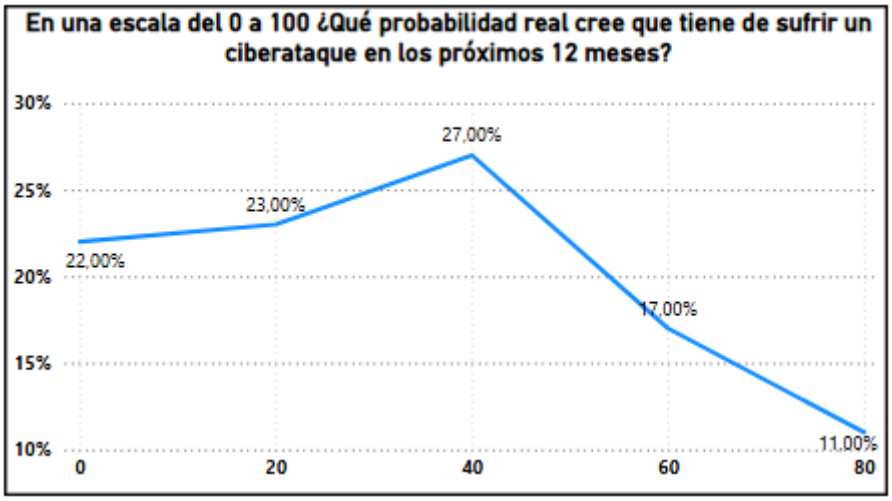


Figura 6. *Percepción de los estudiantes sobre la probabilidad de sufrir un ciberataque en los próximos 12 meses.*

Fuente: Elaboración propia

Tabla 4. *Principales necesidades de formación en ciberseguridad identificadas mediante las respuestas abiertas.*

Tema prioritario	Aspectos mencionados por los estudiantes
Protección de datos y privacidad	Protección de información personal, privacidad, identidad digital y seguridad de datos
Prevención de ataques y fraudes digitales	Phishing, correos y enlaces maliciosos, estafas, suplantación de identidad y malware
Seguridad de cuentas y dispositivos	Contraseñas seguras, autenticación en dos pasos, protección de cuentas y uso de antivirus
Seguridad en redes y conexiones	Riesgos de las redes Wi-Fi públicas, uso de VPN y protección de conexiones
Ciberseguridad aplicada al ámbito profesional	Programación segura, análisis de vulnerabilidades, seguridad en aplicaciones, sistemas y bases de datos

Fuente: Elaboración propia.

Las respuestas abiertas mostraron que los estudiantes sienten que es fundamental fortalecer sus conocimientos sobre la protección de datos y la privacidad, así como sobre cómo prevenir ataques y fraudes digitales. Esto incluye temas como el phishing, los enlaces maliciosos, las estafas y la suplantación de identidad. Además, se notó un interés por mejorar las prácticas de seguridad en cuentas y dispositivos, utilizando contraseñas seguras, autenticación en dos pasos y métodos de protección contra malware. Asimismo, varios participantes subrayaron la importancia de entender los riesgos que conlleva el uso de redes Wi-Fi públicas y la necesidad de implementar medidas de protección adicionales, como las VPN. Además, se mencionaron necesidades relacionadas con la ciberseguridad en el ámbito

profesional, que abarcan la programación segura, el análisis de vulnerabilidades y la protección de aplicaciones, sistemas y bases de datos. La propuesta de mejora formativa surge como una respuesta a las necesidades que se han identificado en el estudio. Los resultados mostraron que una parte significativa de los estudiantes no ha recibido formación académica o extracurricular específica en ciberseguridad. Aunque se notó un nivel básico de conocimientos que es bastante favorable, la familiaridad y la percepción de estar preparados se situaron principalmente en niveles moderados. También se detectaron prácticas que podrían aumentar la exposición a riesgos digitales, como reutilizar contraseñas y conectarse a redes Wi-Fi públicas sin medidas de protección adicionales.

Además, la mayoría de los participantes expresó una fuerte necesidad de recibir más formación en ciberseguridad, destacando como temas prioritarios la protección de datos y la privacidad, la prevención de ataques y fraudes digitales, la seguridad de cuentas y dispositivos, la protección de redes y la aplicación de la ciberseguridad en el ámbito profesional. Con base en estos hallazgos, se propone implementar un programa formativo que fortalezca los conocimientos, habilidades y prácticas de seguridad digital entre los estudiantes de la Facultad de Ciencias Informáticas. El objetivo de la propuesta es potenciar los conocimientos, la conciencia y las prácticas de ciberseguridad entre los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí. Esto se logrará a través de un programa formativo que combine contenidos teóricos con actividades prácticas, todo enfocado en la prevención de riesgos digitales y en el desarrollo de habilidades que sean útiles tanto en el ámbito académico como en el profesional. La propuesta se organiza en cinco componentes formativos, definidos a partir de las principales necesidades identificadas en la encuesta.

Tabla 5. *Componentes de la propuesta de mejora formativa en ciberseguridad.*

Componente	Contenidos principales	Estrategias formativas
Fundamentos de ciberseguridad y protección de datos	Conceptos básicos, amenazas digitales, privacidad, protección de datos personales e identidad digital	Talleres introductorios, recursos digitales y análisis de situaciones cotidianas
Prevención de ataques y fraudes digitales	Phishing, ingeniería social, correos y enlaces maliciosos, estafas y suplantación de identidad	Estudio de casos, análisis de ejemplos y simulaciones de ataques
Seguridad de cuentas y dispositivos	Gestión de contraseñas, autenticación en dos pasos, actualizaciones de seguridad, antivirus y protección de dispositivos	Actividades prácticas, demostraciones y listas de verificación
Seguridad en redes y conexiones	Riesgos asociados a redes Wi-Fi públicas, uso de VPN, protección de conexiones y buenas prácticas de navegación	Ejercicios aplicados, demostraciones y resolución de escenarios de riesgo
Ciberseguridad aplicada al ámbito profesional	Programación segura, análisis básico de vulnerabilidades, seguridad en aplicaciones, sistemas y bases de datos	Laboratorios prácticos, proyectos colaborativos y análisis de casos técnicos

Fuente: Elaboración propia

Los componentes que se proponen combinan aspectos generales de seguridad digital con conocimientos técnicos específicos del perfil profesional de los estudiantes de Ciencias Informáticas. Esta fusión permitiría no solo tratar las prácticas diarias de protección, sino también desarrollar las habilidades necesarias para identificar y mitigar vulnerabilidades en entornos tecnológicos.

La propuesta se llevará a cabo a través de talleres regulares, actividades prácticas y recursos digitales diseñados para reforzar tanto los conocimientos como las prácticas en

ciberseguridad. Se tratarán temas como la protección de datos, cómo identificar ataques de phishing, la seguridad de cuentas, el uso seguro de redes y la protección de dispositivos.

Además, se sugiere incorporar contenidos de ciberseguridad en asignaturas que estén relacionadas con el desarrollo de software, redes, bases de datos y sistemas de información. La implementación podría comenzar con un programa piloto, cuyos resultados ayudarán a hacer ajustes antes de ampliarlo al resto de los estudiantes. La propuesta se evaluará comparando lo que los estudiantes saben, sus prácticas y cómo perciben su preparación antes y después de participar en las actividades formativas. La idea es fortalecer su capacidad para identificar amenazas, fomentar la adopción de medidas de protección y reducir comportamientos de riesgo, como reutilizar contraseñas o conectarse a redes Wi-Fi públicas sin la debida protección.

En resumen, esta propuesta tiene como objetivo promover una cultura de ciberseguridad que se enfoque en la prevención y el uso responsable de la tecnología, desarrollando conocimientos y habilidades que sean útiles tanto en el ámbito académico como en el profesional. Los resultados obtenidos muestran que los estudiantes de la Facultad de Ciencias Informáticas tienen una base de conocimientos sobre ciberseguridad que es bastante positiva. Sin embargo, también se observan algunas limitaciones en su formación previa, así como una percepción moderada de su familiaridad y preparación en el tema. Además, sus prácticas actuales podrían aumentar su exposición a riesgos digitales. Esta situación indica que, aunque tienen un buen entendimiento teórico, esto no siempre se traduce en comportamientos seguros y consistentes. Por lo tanto, es crucial que la formación universitaria combine teoría con actividades prácticas que se enfoquen en la prevención y en la implementación de medidas de protección. La escasa participación en asignaturas y capacitaciones específicas subraya la urgencia de integrar la ciberseguridad de una manera más estructurada en la educación universitaria. En este contexto, el estudio de (Towhidi & Pridmore, 2023) sugiere que los programas de educación superior deben alinearse con las competencias que demanda el mundo laboral y propone un modelo de diseño de cursos que responda a las necesidades de la industria. La implementación de este modelo ha mostrado resultados positivos en cuanto a la satisfacción de los estudiantes, la valoración por parte del sector profesional y el rendimiento académico. Estos hallazgos refuerzan la idea de que la formación no debe limitarse a contenidos generales, sino que debe incluir competencias específicas que se alineen con el perfil profesional de los estudiantes de Ciencias Informáticas.

Además, los resultados revelan una discrepancia entre el conocimiento demostrado y la percepción de preparación. Aunque la mayoría de los participantes pudo identificar correctamente conceptos y situaciones básicas relacionadas con la ciberseguridad, una parte significativa expresó que se sentía solo moderadamente familiarizada y preparada para proteger su información. Esta situación podría indicar que el aprendizaje recibido no ha sido suficiente para generar confianza en la aplicación de medidas preventivas. Por lo tanto, es crucial que la formación se enfoque en el desarrollo de habilidades prácticas, en lugar de limitarse a la transmisión de conocimientos teóricos. En cuanto a las prácticas observadas, se notaron comportamientos positivos, como la verificación de enlaces, la instalación de actualizaciones y el uso de medidas de protección en los dispositivos. Sin embargo,

también se mantuvieron conductas de riesgo, como la reutilización de contraseñas y la conexión a redes Wi-Fi públicas sin una protección adicional. Estos hallazgos son consistentes con los desafíos que se mencionan en el estudio de (De Ramos & Esponilla, 2022), donde se destacó la educación de los usuarios y el uso de dispositivos personales sin protección como factores clave para la seguridad en las instituciones de educación superior. Además, el estudio subrayó la seguridad en la nube y la estrategia institucional como áreas que necesitan más atención.

La presencia de estudiantes que han reportado experiencias con phishing, malware y suplantación de identidad pone de manifiesto que las amenazas digitales son una realidad en el entorno universitario. Aunque la mayoría afirmó no haber sido víctima de intentos de ciberataque en el último año, los incidentes reportados subrayan la importancia de mantener medidas preventivas y mejorar la capacidad de respuesta. Desde una perspectiva institucional, el estudio realizado por (Ganesen et al., 2022) indica que la gestión de riesgos en las universidades debe integrar tanto soluciones tecnológicas como educativas. También resalta la necesidad de contar con mecanismos que permitan identificar, medir y evaluar la gravedad de los riesgos para facilitar la toma de decisiones.

Es importante tener en cuenta la percepción moderada del riesgo que tienen los estudiantes al momento de crear estrategias de formación. Si bien una valoración intermedia sobre la probabilidad de enfrentar un ciberataque puede ayudar a que se preste más atención a las amenazas, no siempre asegura que se adopten medidas de protección de manera constante. El estudio elaborado por (Conrad et al., 2022) resalta que las notificaciones de seguridad pueden afectar cómo navegamos y que las reacciones emocionales de los usuarios están ligadas a su cumplimiento con estas advertencias. Aunque este estudio aborda el tema desde un ángulo diferente al de nuestra investigación, sus hallazgos sugieren que los mensajes y recursos de sensibilización deben ser claros y capaces de motivar una respuesta activa de los usuarios.

En cuanto a las necesidades de formación que los estudiantes expresaron en sus respuestas abiertas, se observa que priorizan temas como la protección de datos, la prevención de ataques y fraudes digitales, la seguridad de cuentas, la protección de dispositivos y la seguridad en redes. Estos resultados subrayan la importancia de implementar estrategias formativas que integren contenidos teóricos con recursos interactivos y actividades prácticas. El estudio de (Blažič & Blažič, 2022) identificó temas clave que deberían incluirse en los programas educativos y destacó la efectividad de métodos innovadores e interactivos, como videos y juegos serios, para fomentar habilidades en ciberseguridad. Aunque la población estudiada pertenece a un nivel educativo diferente, su enfoque puede ofrecer ideas valiosas para diseñar actividades dinámicas que promuevan el desarrollo de competencias.

Es fundamental que el fortalecimiento de la formación estudiantil vaya de la mano con acciones institucionales que se enfoquen en la gestión y protección de la información. El estudio realizado por (Amine et al., 2023) examina cómo se aplican los estándares ISO/IEC 27001 y el NIST Cybersecurity Framework en las instituciones de educación superior, subrayando su importancia para establecer políticas, directrices y estrategias de gestión de riesgos. Aunque esta investigación se centra en la conciencia y las prácticas de los

estudiantes, estos marcos de referencia demuestran que la formación debe estar alineada con políticas institucionales y mecanismos organizacionales que ayuden a reforzar la seguridad de la información.

Por último, la propuesta de mejora que se presenta busca atender tanto las necesidades formativas detectadas como las competencias que se requieren en el ámbito profesional. En este contexto, el estudio de (Ramezan, 2025) ofrece una visión sobre las responsabilidades y habilidades necesarias para liderar en el campo de la ciberseguridad. Aunque se centra en un perfil profesional específico, resalta que la educación universitaria debe facilitar el desarrollo continuo de conocimientos técnicos, habilidades de gestión y capacidades para la toma de decisiones. Estos aspectos son especialmente relevantes para los estudiantes de Ciencias Informáticas, quienes podrían asumir roles relacionados con la protección de sistemas y la gestión de riesgos.

Conclusiones

El estudio permitió analizar cómo están los estudiantes de la Facultad de Ciencias Informáticas de la Universidad Técnica de Manabí en cuanto a su conciencia y prácticas de ciberseguridad. Los resultados mostraron que tienen un buen nivel de conocimientos básicos, especialmente cuando se trata de identificar conceptos clave, entender los riesgos de usar redes Wi-Fi públicas y saber cómo prevenirse ante enlaces sospechosos. Sin embargo, una parte significativa de los estudiantes admitió tener una familiaridad y preparación moderadas, lo que indica que hay espacio para mejorar en la aplicación práctica de lo que han aprendido. Además, se encontraron prácticas positivas, como la verificación de enlaces, la instalación de actualizaciones y el uso de medidas de protección en sus dispositivos. Aun así, algunas conductas que podrían aumentar su exposición a riesgos digitales siguen presentes, como la reutilización de contraseñas y la conexión a redes Wi-Fi públicas sin una protección adicional. También se reportaron experiencias con phishing, malware y suplantación de identidad, lo que pone de manifiesto las amenazas que enfrenta la comunidad estudiantil. Con base en los resultados, se propuso una mejora formativa que busca fortalecer los conocimientos, habilidades y prácticas de ciberseguridad. Esta propuesta incluye temas sobre la protección de datos, la prevención de ataques y fraudes digitales, la seguridad de cuentas y dispositivos, la protección de redes y la ciberseguridad en el ámbito profesional. Implementar esta propuesta ayudaría a crear una cultura de prevención y a desarrollar competencias valiosas para el desempeño académico y profesional de los estudiantes.

Referencias Bibliográficas

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, 12(3), 276-281. https://doi.org/10.14569/IJACSA.2021.0120334

Alzahrani, L. (2021). Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. International Journal of Advanced Computer Science and Applications, 12(11), 630-637. https://doi.org/10.14569/IJACSA.2021.0121172

Amine, A., Chakir, E, Issam, T., & Khamlichi, Y. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. International Journal of Safety and Security Engineering, 13(6), 1109-1116. https://doi.org/10.18280/ijsse.130614

Blažič, B. J., & Blažič, A. J. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. Sustainability (Switzerland), 14(8). https://doi.org/10.3390/su14084763

Chen, H., & Hu, Z. (2024). Exploring Data Traceability Methods in Information Management Within Universities: An Action Research and Case Study Approach. IEEE Access, 12, 175196-175217. https://doi.org/10.1109/ACCESS.2024.3493860

Conrad, C., Aziz, J. R., Henneberry, J. M., & Newman, A. J. (2022). Do emotions influence safe browsing? Toward an electroencephalography marker of affective responses to cybersecurity notifications. Frontiers in Neuroscience, 16. https://doi.org/10.3389/fnins.2022.922960

De Ramos, N, & Esponilla, F. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education, 11(3), 1198-1209. https://doi.org/10.11591/ijere.v11i3.22863

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access, 10, 52319-52335. https://doi.org/10.1109/ACCESS.2022.3171829

Ganesen, R., Bakar, A. A., Ramli, R., Rahim, F. A., & Zawawi, M. N. A. (2022). Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions. International Journal of Advanced Computer Science and Applications, 13(8), 355-362. https://doi.org/10.14569/IJACSA.2022.0130843

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, Tools and Good Practices for Cybersecurity Curricula. IEEE Access, 9, 94723-94747. https://www.researchgate.net/publication/352912571_Framework_Tools_and_Good_Practices_for_Cybersecurity_Curricula https://doi.org/10.1109/ACCESS.2021.3093952

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. SN Computer Science, 4(5). https://doi.org/10.1007/s42979-023-01984-x

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. TEM Journal, 12(2), 623-633. https://doi.org/10.18421/TEM122-05

Ramezan, C. A. (2025). Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. Computers and Security, 152. https://doi.org/10.1016/j.cose.2025.104363

Ramezanian, S., & Niemi, V. (2024). Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. IEEE Access, 12, 61741-61766. https://doi.org/10.1109/ACCESS.2024.3392970

Schafeitel-Tähtinen, T., & Lazarov, W. (2025). Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia. Computer Applications in Engineering Education, 33(5). https://doi.org/10.1002/cae.70082

Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. Journal of Information Systems Education, 34(1), 70-83. https://jise.org/volume34/n1/JISE2023v34n1pp70-83.pdf

Vera, F (2024). Revisión Sistemática de Modelos Educativos para la Capacitación en Buenas Prácticas de Ciberseguridad en Estudiantes y Empleados. Revista Cientifica Disciplinares, 3(4), 1-1. https://doi.org/10.71727/disciplinares.v3i4.291

Zamora, J. A. P., Vásquez, D. L. A., Canchari, J. M. V., Benites, M. F. A., & Ruiz, R. J. T. (2025). Educación segura en la era digital, aprendizajes desde la ISO 27002:2022: Una revisión sistemática. Revista Simón Rodríguez, 5(10), 132-142. https://doi.org/10.62319/simonrodriguez.v.5i10.55

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT) Bryan Javier Robles García: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio. María Genoveva Moreira Santos: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.
Declaración de conflicto de intereses Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.
Declaración del editor El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.
Declaración de los revisores Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.
Declaración sobre el uso de inteligencia artificial Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.
Disponibilidad de datos Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.