Concientización en ciberseguridad para futuros administradores: Fortaleciendo la ciberresiliencia estudiantil

Rolando Salazar Hernández[1], Ramón Ventura Roque Hernández[2], Adán López Mendoza[3]

https://doi.org/10.6084/m9.figshare.30783839

Resumen

La creciente dependencia de tecnologías digitales en la educación superior ha aumentado los riesgos de ciberseguridad y, aunque se han conseguido mejoras técnicas para preservar los sistemas, el ser humano sigue siendo el eslabón más débil en esta cadena de protección. Este artículo investiga la factibilidad de implementar actividades de concientización en seguridad informática entre estudiantes universitarios. Se condujo una revisión bibliográfica en la base de datos de Web of Science (2010-2023). También se utilizaron datos secundarios, de donde se extrajeron respuestas de los estudiantes de los primeros cuatro semestres de la Licenciatura en Administración de una universidad mexicana para evaluar sus prácticas de seguridad y su disposición hacia programas de concientización. Los artículos encontrados recomendaron constantemente implementar programas para concientizar sobre la ciberseguridad. Esto fue consistente a través de diferentes períodos tecnológicos y sociales. Por otra parte, se identificaron vulnerabilidades en las prácticas de ciberseguridad de los estudiantes. Se evidenciaron escenarios en donde ellos se encuentran en altos niveles de riesgo. Notablemente, el 81% de los participantes expresó acuerdo con la implementación de actividades para fortalecer la seguridad informática, superando el interés en mejorar habilidades tecnológicas generales (74.7%). Se concluye que la implementación de programas de concientización en ciberseguridad es tanto factible como necesaria, dada la convergencia entre las recomendaciones de la literatura, las vulnerabilidades detectadas y la alta receptividad de los estudiantes. Este estudio proporciona una base para el diseño de programas efectivos de concientización en ciberseguridad adaptados al contexto universitario.

Palabras clave: ciberseguridad, concientización, ciberresiliencia.

Abstract

The increasing reliance on digital technologies in higher education has increased cybersecurity risks, and although technical improvements have been made to preserve systems, humans remain the weakest link in this protection chain. This article investigates the feasibility of implementing cybersecurity awareness activities among university students. A literature review was conducted in the Web of Science database (2010-2023). Secondary data was also used, from which responses from students in the first four semesters of the Bachelor of Administration program at a Mexican university were extracted to assess their security practices and their willingness to engage in awareness programs. The articles found consistently recommended implementing programs to raise awareness about cybersecurity. This was consistent across different technological and social periods. On the other hand, vulnerabilities in students' cybersecurity practices were identified. Scenarios where they are at high risk levels were evidenced. Notably, 81% of participants expressed agreement with the implementation of activities to strengthen cybersecurity, surpassing the interest in improving general technological skills (74.7%). It is concluded that the implementation of cybersecurity awareness programs is both feasible and necessary, given the convergence between the recommendations of the literature, the vulnerabilities detected, and the

[1] Universidad Autónoma de Tamaulipas 831 176 7135, rsalazar@docentes.uat.edu.mx
[2] Universidad Autónoma de Tamaulipas 867 129 0303, rvhernandez@uat.edu.mx
[3] Universidad Autónoma de Tamaulipas 831 212 3982, alopez@uact.edu.mx

high receptivity of students. This study provides a basis for the design of effective cybersecurity awareness programs adapted to the university context.
Keywords: cybersecurity, awareness, cyber resilience.

Introducción

A medida que dependemos más de la tecnología para las actividades cotidianas, la cantidad de riesgos cibernéticos a los que estamos expuestos se incrementa también. Y es que cada vez incorporamos más la tecnología en todos los aspectos desde la educación hasta el trabajo, sin olvidar la vida personal. Sin embargo, más allá de las soluciones técnicas, la concientización y la educación en ciberseguridad siguen teniendo roles fundamentales para mitigar los riesgos asociados con las amenazas cibernéticas. La literatura existente destaca la importancia de abordar la ciberseguridad desde múltiples perspectivas y niveles, asegurando que tanto individuos como organizaciones estén preparados para enfrentar las amenazas cibernéticas en constante evolución.

El presente trabajo surgió en el contexto de una Universidad pública estatal mexicana (Universidad X) con la siguiente pregunta de investigación: ¿Cuál es la viabilidad de implementar actividades de concientización en ciberseguridad para estudiantes universitarios de pregrado, considerando las recomendaciones de la literatura reciente y el contexto específico de los estudiantes de Licenciatura en Administración (LA) de la Universidad X? Al abordar esta pregunta, como trabajo inicial se establecieron tres objetivos: 1. Analizar las recomendaciones de la literatura publicada e indexada en Web of Science entre 2010 y 2023 sobre la implementación de programas y actividades de concientización en seguridad informática para estudiantes universitarios. 2. Evaluar el nivel de riesgo en las prácticas de seguridad informática de los estudiantes de LA de la Universidad X. 3. Determinar la receptividad de los estudiantes de LA de la Universidad X hacia el desarrollo de habilidades en tecnología y seguridad informática.

La creciente dependencia de las tecnologías digitales en todos los aspectos de la vida moderna, incluyendo la educación superior, ha aumentado la relevancia de la ciberseguridad. No obstante, existe una brecha significativa entre la rapidez con la que avanzan las amenazas cibernéticas y el nivel de preparación de los usuarios, especialmente entre los estudiantes universitarios. Esta investigación se justifica por la urgente necesidad de comprender y abordar esta disparidad, concretamente en el contexto de los estudiantes de LA, quienes en su futura vida profesional manejarán información sensible y tomarán decisiones críticas basadas en sistemas informáticos. Al analizar los artículos publicados, evaluar las conductas de riesgo de los

estudiantes y caracterizar su receptividad hacia la formación en seguridad informática, esta investigación no solo contribuye al cuerpo de conocimiento existente, sino que también proporciona una base para el diseño de programas de concientización efectivos y adaptados al contexto local. Los resultados tienen el potencial de mejorar significativamente la resiliencia cibernética de los futuros profesionales, contribuyendo así a la seguridad de las organizaciones y la sociedad en general.

A continuación, se presenta la fundamentación teórica, la descripción del método, los resultados y su discusión y finalmente, las conclusiones.

Fundamentación teórica

En 2010, Aliyu y otros, en Universidad de Malasia llevaron a cabo un estudio para examinar la comprensión de la seguridad informática y la ética entre los estudiantes que se especializan en ciencias de la computación y educación. Los resultados indicaron que los estudiantes encuestados mostraron niveles satisfactorios de conciencia, en particular entre los que estudiaban informática. Se comprobó que carecían de conocimientos sustanciales en esta área y que se dedicaban con más frecuencia a prácticas en línea poco éticas y a actividades ilegales en comparación de sus compañeros de educación (Aliyu et al., 2010).

En 2012, Aloul aplicó una encuesta para determinar el nivel de conciencia con respecto a los ciberataques, asi como para explorar las medidas para mitigarlos y evaluar la inclusión de iniciativas de sensibilización sobre la ciberseguridad. Los resultados iniciales revelaron que los estudiantes afirmaban poseer conocimientos fundamentales sobre ciberseguridad, pero mostraban una falta de comprensión a la hora de proteger sus datos. El investigador encontró que las instituciones de educación superior carecían de un plan activo de sensibilización sobre la ciberseguridad destinado a mejorar la comprensión por parte de los estudiantes de las medidas de protección contra las posibles amenazas. El autor escribió un informe donde expuso los resultados sobre la concienciación en materia de seguridad informática realizados entre estudiantes y profesionales de los Emiratos Árabes Unidos, haciendo hincapié en la necesidad de evaluar la concienciación sobre la seguridad mediante evaluaciones estructuradas y proponiendo varios factores fundamentales para reforzar los conocimientos de los usuarios en este ámbito (Aloul, 2012).

Durante el 2012, los investigadores Slusky y Partow-Navid, llevaron a cabo la aplicación de un instrumento sobre la seguridad de la información a estudiantes de una Universidad de California. Los resultados revelaron que el principal problema relacionado con la concienciación en materia de seguridad no proviene de una deficiencia de conocimientos relacionados con la seguridad, sino más bien de la aplicación de estos conocimientos en situaciones prácticas. Se formularon sugerencias para ayudar a las instituciones académicas a desarrollar planes de estudio que integren la formación en materia de concienciación sobre la ciberseguridad basada en contextos del mundo real (Slusky & Partow-Navid, 2012).

El estudio de Ahlan y otros en 2015, identificó varios factores clave que determinan los niveles de conciencia y su interacción con otras variables, como el impacto de los marcadores religiosos y las influencias sociales en el desempeño de los compañeros (Ahlan et al., 2015).

En 2016, Çiftçi y Delialioğlu realizaron un estudio a alumnos de secundaria en materia de seguridad de las tecnologías de la información, donde se midió el grado de conocimientos y habilidades percibidos por los estudiantes en la infección por virus, la concientización de los delitos informáticos, en los productos informáticos software sin licencia, configuración de los sistemas operativos Windows y Android, y cuestiones de seguridad relacionadas con el correo electrónico y la navegación por la Web. El estudio consistió en la aplicación de un pretest y un postest después de que los estudiantes utilizaron un portal web de seguridad. Los resultados de su investigación mostraron que el uso del portal web tuvo un efecto significativo en la percepción del nivel de conocimientos y habilidades en seguridad informática de los alumnos (Çiftçi & Delialioğlu, 2016).

Ese mismo 2016, Sarathchandra y otros realizaron un estudio en donde coinciden con otros autores en que los estudiantes universitarios en materia de ciberseguridad no son concientes de los riesgos en Internet, y que no reciben educación ni información sobre los riesgos potenciales. En su investigación, proponen formas creativas para difundir información sobre esos peligros de ciberseguridad en Internet. Por ejemplo, el incluir historias convincentes, evocadoras con personajes que creen empatía puede tener un impacto positivo. Comentan los autores que los relatos convincentes presentados por diversos personajes como influencers, políticos, reporteros, etc. durante un periodo de tiempo tendrán mayores efectos. Se concluye que comprender el lado humano de la ciberseguridad es escencial para abordar las implicaciones a medida que se acerca

cada vez el involucramiento con la realidad virtual y la inteligencia artificial (Sarathchandra et al., 2016).

En 2017 Hadlington y Parsons realizaron una investigación sobre si el ciberocio (ciberloafing) y la adicción al Internet pueden afectar a la seguridad de la información organizacional. Encontraron que el uso de las computadoras personales para fines ajenos al trabajo implica un mayor riesgo de amenaza por fallos de ciberseguridad, esto debido a que se tiene una menor conciencia de la seguridad de la información, la ciberafición a los sitios web de adultos y juegos de azar en línea. El resultado del estudio sugiere que las organizaciones deben considerar proporcionar la formación y talleres para ayudar a los empleados para el tratamiento de adicciones o comportamientos adictivos al Internet, tambien sugieren la formación sobre la seguridad de la información y las politicas claras sobre el uso de las tecnologías en el trabajo (Hadlington & Parsons, 2017).

Senthilkumar y Easwaramoorthy, en 2017, en los centros urbanos de Tamil Nadu llevaron a cabo una encuesta para evaluar el nivel de conciencia de los estudiantes universitarios sobre la ciberseguridad. El cuestionario incluyó preguntas sobre diversas amenazas de seguridad, como la seguridad del correo electrónico, los virus, los ataques de suplantación de identidad, la publicidad engañosa, los anuncios emergentes y otras formas de ciberamenazas. Los hallazgos indicaron que estos estudiantes mostraron un nivel de conciencia superior a la media en relación con los problemas de ciberseguridad (Senthilkumar & Easwaramoorthy, 2017).

Ese mismo 2017, otro estudio evaluó la comprensión de los estudiantes sobre la ciberseguridad, su autopercepción de las habilidades de ciberseguridad, sus competencias y comportamientos reales relacionados con la ciberseguridad, así como sus actitudes hacia la ciberseguridad. Los resultados subrayaron la necesidad de implementar campañas de sensibilización sobre la ciberseguridad para mejorar la comprensión en este campo (Chandarman & Niekerk, 2017).

Zulfia y otros en 2019 expresaron que “El error humano es una de las violaciones de la seguridad de la información que desempeña un papel significativo”. Los investigadores realizaron un caso de estudio para medir en los empleados los niveles de concienciación de la seguridad de la información. Utilizaron el cuestionario HAIS-Q, que aplicaron a 51 empleados. Los autores despues de analizar los resultados de la aplicación del instrumento, recomendaron mejorar las políticas, programas de concienciación de la seguridad, así como implementar mejoras

tecnológicas. Particularmente, recomendaron mejorar los procedimientos para la descarga de archivos y el acceso a sitos Web permitidos. En cuanto a mejoras tecnologícas, aconsejaron la adquisición de programas de cifrado de correo electrónico, filtros antispam para correo basura, hardware cortafuegos para limitar el uso de internet, red privada virtual para que los empleados accedan de manera segura desde el exterior (Zulfia et al., 2019).

Ese mismo año, Moallem, realizó un análisis con estudiantes universitarios. En el estudio se observó que, a pesar de que están bajo vigilancia mientras usan internet y sistemas universitarios, los alumnos carecen de plena conciencia sobre la protección de sus datos (Moallem, 2019).

Ese mismo 2019, Venter y otros en su investigación en Sudáfrica sobre la protección de sus teléfonos inteligentes sugieren que se requiere un alto nivel de concientización y conocimientos en materia de seguridad. Ellos critican la inexistencia de un plan oficial sobre la ciberseguridad en las escuelas. Esa falta de estrategia educativa deja a los jóvenes de ese país desproporcionadamente vulnerables a los ciberataques. Estos autores centraron su estudio en la concientización de la ciberseguridad en los teléfonos inteligentes por tres razones: la primera es que los ciberataques aumentan año con año, la segunda es que la posesión de teléfonos inteligentes está en aumento constantemente y la tercera es que cada vez con menor edad, los alumnos poseen y utilizan los teléfonos inteligentes. Ellos concluyen que la falta de educación y concientización hace que los usuarios sean blancos de ciberataques (Venter et al., 2019).

En el año 2020, Breitinger y otros realizaron un estudio sobre la educación y la concientización de la ciberseguridad en los telefónos inteligentes. Esta investigación se centró en las generaciones X y Z de jóvenes. Encontraron que la mayoría tienen una adecuada configuración en el bloqueo de pantalla para proteger el acceso físico, pero hacen caso omiso a las buenas prácticas de seguridad. La encuesta reveló que tendían a ignorar buenas prácticas como el uso de una red privada virtual (VPN por sus siglas en inglés) al utilizar una red wifi pública. También quedó en evidencia el desconocimiento de productos de seguridad instalados en sus dispositivos y la confianza en la configuración por defecto. Asimismo, descubrieron que los telefónos inteligentes estaban menos protegidos que las computadoras personales. Los resultados encontrados ponen de manifiesto que se tiene la necesidad de mejorar la educación y la concienciación de los usuarios de teléfonos inteligentes sobre las prácticas de seguridad. Los autores sugieren programas educativos específicos, hacer énfasis en las prácticas de seguridad integral, capacitación en el

conocimiento de configuración de los teléfonos inteligentes y por último formación continúa y actualizaciones. Esto permitiría que los usarios estén informados y equipados para proteger sus dispositivos y su información de forma eficaz (Breitinger et al., 2020).

Según Rahman y otros en 2020 se tenía la percepción de que las investigaciones sobre la importancia de la educación en ciberseguridad en las instituciones educativas era baja o bastante moderada. Según los autores es necesario educar a los niños, adolecentes para que actuén de forma segura en el ciberespacio. Ellos realizaron una revisión sistemática sobre la promoción de la actividad en el ciberespacio y promover la educación sobre la ciberseguridad. Los autores sugieren las siguientes estrategías: que los profesores organicen actividades escolares sobre la ciberseguridad, que se celebren semanas de la concienciación en ciberseguridad. El tema de educar en ciberseguridad radica en que cada vez más los estudiantes interactuan con Internet, creando dependencia en muchas de las actividades que realizan y pueden ser vulnerables a delitos como el ciberacoso, el fraude en línea, los abusos raciales, la pornografía y el juego. Además, Internet puede ser un canal poco saludable para los delitos y el mal comportamiento, y puede hacer que los adolescentes se vuelvan adictos e ignoren las actividades productivas (Rahman et al., 2020).

Khader y otros, en el año 2021 realizaron un trabajo de investigación y propusieron un marco conceptual de concientización sobre la ciberseguridad. Este servirá de referencia para guiar a cualquier institución académica para mejorar la conciencización sobre la ciberseguridad. Los investigadores comentan que los foros, los correos electrónicos, el fraude, el robo de identidad, el phishing, el ciberacoso, el ransomware y la ingeniería social son algunas formas en que los atacantes se dirigen a sus víctimas. La forma dinámica de los métodos, herramientas de ataque, y las vulnerabiliades crecen continuamente, consideran que la importancia del factor humano en la gestión y concienciación de la ciberseguridad ha adquirido una gran importancia. Los autores concluyen que los estudiantes universitarios suelen facilitar las violaciones de datos y la mala conducta digital. Así, la falta de conocimiento y concienciación de la ciberseguridad los hace blancos fáciles de ataques (Khader et al., 2021).

Ese mismo 2021 se llevó a cabo un estudio empírico para evaluar el nivel de conciencia, conocimientos y comportamiento sobre la ciberseguridad de los estudiantes universitarios que utilizan teléfonos inteligentes en comparación con los que utilizan computadoras. Los resultados revelaron que, si bien todos los estudiantes demostraron estar familiarizados con ciertos principios de seguridad de la información, su enfoque para proteger los teléfonos inteligentes difería del de

los ordenadores. Se recomendó que se intensificaran las iniciativas de formación para informar a los estudiantes sobre las posibles amenazas a la seguridad de la información asociadas con el uso de teléfonos inteligentes en entornos académicos (Taha & Dahabiyeh, 2021).

En 2022 Cheng y Wang comentan que las instituciones de educación superior son especialmente vulnerables y que los problemas derivados de la ciberseguridad están recibiendo mayor atención. Mencionan que los responsables de las instituciones se suelen centrar en la tecnología para la prevención de ataques y no en la concientización y prevención sobre el tema de ciberseguridad. Sintetizan sus hallazgos con un conjunto de estrategias que las instituciones de educación superior deben implementar para hacer frente a las amenazas de ciberseguridad. Los autores citan a Arina y Anatolie donde el aprendizaje a distancia debido a la pandemia COVID-19 los dispositivos que se conectan a la red y los sistemas informáticos de la Universidad han alcanzado altos riesgos de ciberseguridad (Cheng & Wang, 2022)(Arina & Anatolie, 2021).

Un estudio realizado por Rashed y otros en 2022, exploró el nivel de concienciación sobre la ciberseguridad entre instituciones educativas de Yemen. Los investigadores se centraron en cuatro variables: conocimientos sobre ciberseguridad, autopercepción de las aptitudes de ciberseguridad, aptitudes y comportamientos reales en materia de ciberseguridad y en las actitudes en ciberseguridad. El estudio reveló que los estudiantes son potencialmente vulnerables a los ciberataques. Los resultados indicaron dirigir campañas específicas de las debilidades de concienciación de ciberseguridad (Rashed et al., 2022).

En el año 2023, Hong y otros detectaron que en algunos estudios sobre los factores que influyen en la concienciación sobre la seguridad en internet, conducidos en distintos niveles educativos se han obtenido resultados inconsistentes. Ellos proponen un estudio basado en un modelo ampliado de conocimiento-actitud y comportamiento (KAB por sus siglas en inglés). En este estudio se encontró que la actitud a la ciberseguridad se verá influenciada por el entorno externo y sugieren que la educación en ciberseguridad no debe limitarse a los estudiantes universitarios, sino extenderse al público en general. Se concluye que para la mejora de la formación en ciberseguridad se tienen que adaptar los programas de formación a las necesidades específicas de los distintos niveles educativos (Hong et al., 2023).

En 2023, Kannelønning y Katsikas realizaron una revisión sistemática de cómo se ha evaluado el comportamiento relacionado con la ciberseguridad. En este trabajo, los investigadores identificaron 2,153 artículos, de los cuales 26 fueron analizados después de pasar por los filtros de

exclusion. Encontraron que la mayoría utilizó el cuestionario HAIS-Q de Parsons y otros del 2014. Descubrieron que es una vía clara para evaluar el comportamiento, pero que puede producir datos sesgados. También encontraron que no se obtuvieron resultados concluyentes entre los directivos y empleados. En este sentido, comentan que podría hacerse un esfuerzo para anonimizar los datos personales cuando se procede de una misma organización y que para futuras investigaciones se pueda utilizar un método híbrido que consista en la recopilación de datos objetivos y subjetivos (Kannelønning & Katsikas, 2023).

Rohan y otros en 2023 realizaron una revisión sistemática de las escalas de ciberseguridad que evalúan la concienciación sobre la seguridad de la información. Encontraron que algunas escalas durante el desarrollo y validación presentan algunos aspectos desconocidos. Los autores realizaron una revision exhaustiva de escalas específicas utilizando el método de PRISMA con criterios de inclusión y exclusión. Analizaron 24 artículos y encontraron que la mayoría de los estudios tratan a la concientización sobre la seguridad de la información (ISA por sus siglas en inglés) como un constructo multidimensional y rara vez llevan a cabo pruebas piloto para las evaluaciones previas a la validación y el perfeccionamiento de las escalas. Los autores mencionan que la definición del ISA incluye dos aspectos significativos: el primero se refiere al grado en que los usuarios comprenden los riesgos y amenazas asociados a la seguridad de la información y el segundo se refiere al grado en que los usuarios cumplen las políticas y procedimientos de seguridad. Por último, sugieren que las instituciones deberían invertir en programas de formación y concientización adaptados a sus necesidades específicas y que puedan ayudar a mejorar la seguridad de la información (Rohan et al., 2023).

Guo y otros en 2023 proponen estrategias de prevención, como, por ejemplo, mejorar las politicas de ciberseguridad, en la infraestructura y la tecnologia, la optimización de la gestión y supervisión, así como mejorar las capacidades y concienciación. Esas propuestas de mejoras estratégicas surgen después de analizar la situación actual y los desafíos de la ciberseguridad en los campus inteligentes de las instituciones de educación superior. Al igual que otros autores, Gou y otros coinciden en que los estudiantes y profesores utilizan los dispositivos móviles y computadoras personales donde varia la seguridad de estos dispositivos, debido a que utilizan contraseñas debiles y no instalan los últimos parches de los sistemas operativos y aplicaciones de software que se encuentran instalados. En su artículo mencionan que se deben desarrollar y aplicar normas y politicas de ciberseguridad. Los autores resumen que las Universidades e instituciones

de educación superior deben dar prioridad a la educación de ciberseguridad y aumentar la concientización de estudiantes y del personal para garantizar la seguridad en la infraestrutura de las redes y sistemas de información (Guo et al., 2023).

Descripción del método

Tipo de estudio.- El estudio tuvo un alcance exploratorio-descriptivo. Se realizó una revisión de la literatura y se utilizaron dos conjuntos de datos cuantitativos previamente recolectados y publicados. Aunque estos datos fueron originalmente recabados por los autores de la presente investigación en dos ocasiones distintas y con objetivos diferentes a los del presente estudio, su uso en este nuevo contexto los clasifica como datos secundarios. Esta situación ofrece la ventaja de contar con un conocimiento profundo de la metodología de recolección y del contexto original de los participantes.

Descripción de los sujetos.- Los participantes que originalmente participaron en los estudios de donde ahora se obtuvieron los datos, fueron alumnos inscritos en los semestres de primero a cuarto de la carrera de LA en la universidad X, en dos momentos distintos: mayo de 2021 (n=104) y septiembre de 2021(n=79).

Instrumentos.- Los instrumentos utilizados se describen en: (Maldonado Ortiz et al., 2022) y en: (Pérez et al., 2022). Las fuentes de datos secundarias corresponden a estos mismos trabajos.

Procedimiento.- Se condujo una revisión de la literatura en la base de datos de Web of Science sobre la concientización sobre la ciberseguridad. En la búsqueda y análisis se incluyeron trabajos de 2010 a 2023. Los trabajos se eligieron por criterio de los investigadores, y no se aplicó ninguna metodología de revisión sistemática. Posteriormente se retomaron los dos conjuntos de datos secundarios previamente referenciados y se filtraron para conservar solamente las respuestas de los estudiantes del programa de LA y de los semestres de 1 a 4. Se aplicó un nuevo enfoque de análisis que consistió en la obtención de frecuencias y porcentajes presentados en categorías de riesgo bajo, medio y alto, para las preguntas con respuestas entre 1 y 10; de riesgo bajo y alto, para las preguntas dicotómicas; y de acuerdo, neutral y en desacuerdo, para las preguntas en escala de Likert.

Resultados y discusión

La exploración bibliográfica en WoS de 2010 a 2023 acerca de la concientización en el área de seguridad informática se presenta en la Tabla 1.

Tabla 1. Resultados de la revisión de la literatura.

Autores y Año	Resumen del Trabajo
Aliyu et al. (2010)	Examinaron la comprensión de seguridad informática y ética entre estudiantes de ciencias de la computación y educación, encontrando niveles satisfactorios de conciencia, pero carencias en conocimientos sustanciales.
Aloul (2012)	Aplicó una encuesta para determinar el nivel de conciencia sobre ciberataques, revelando falta de comprensión en la protección de datos y ausencia de planes de sensibilización en instituciones de educación superior.
Slusky & Partow-Navid (2012)	Revelaron que el principal problema en la concienciación de seguridad es la aplicación de conocimientos en situaciones prácticas, no la falta de conocimientos.
Ahlan et al. (2015)	Identificaron factores clave que determinan los niveles de conciencia, incluyendo el impacto de marcadores religiosos e influencias sociales.
Çiftçi & Delialioğlu (2016)	Realizaron un estudio con alumnos de secundaria sobre seguridad de TI, mostrando que el uso de un portal web mejoró significativamente la percepción de conocimientos y habilidades en seguridad informática.
Sarathchandra et al. (2016)	Propusieron formas creativas para difundir información sobre peligros de ciberseguridad, como incluir historias convincentes con personajes que creen empatía.
Hadlington & Parsons (2017)	Investigaron cómo el ciberocio y la adicción a Internet pueden afectar la seguridad de la información organizacional, sugiriendo formación para tratar adicciones y comportamientos adictivos.
Senthilkumar & Easwaramoorthy (2017)	Evaluaron el nivel de conciencia sobre ciberseguridad en estudiantes universitarios, encontrando un nivel superior a la media.
Chandarman & Niekerk (2017)	Evaluaron la comprensión, autopercepción, competencias y actitudes de los estudiantes hacia la ciberseguridad, subrayando la necesidad de campañas de sensibilización.
Zulfia et al. (2019)	Midieron los niveles de concienciación de seguridad de la información en empleados, recomendando mejoras en políticas, programas de concienciación y tecnología.
Moallem (2019)	Observó que los estudiantes universitarios carecen de plena conciencia sobre la protección de sus datos, a pesar de estar bajo vigilancia.
Venter et al. (2019)	Investigaron la protección de teléfonos inteligentes en Sudáfrica, criticando la falta de un plan oficial sobre ciberseguridad en las escuelas.
Breitinger et al. (2020)	Estudiaron la educación y concienciación de ciberseguridad en teléfonos inteligentes de las generaciones X y Z, revelando descuido de buenas prácticas de seguridad.
Rahman et al. (2020)	Realizaron una revisión sistemática sobre la promoción de la actividad en el ciberespacio y la educación sobre ciberseguridad, sugiriendo estrategias para educar a niños y adolescentes.
Khader et al. (2021)	Propusieron un marco conceptual de concienciación sobre ciberseguridad para instituciones académicas, destacando la importancia del factor humano.
Taha & Dahabiyeh (2021)	Evaluaron la conciencia e interés de los estudiantes en aprender sobre ciberseguridad en universidades nigerianas.
Cheng & Wang (2022)	Sintetizaron estrategias para que las instituciones de educación superior hagan frente a las amenazas de ciberseguridad, enfatizando la concientización y prevención.
Rashed et al. (2022)	Exploraron el nivel de concienciación sobre ciberseguridad en instituciones educativas de Yemen, revelando vulnerabilidades potenciales de los estudiantes a ciberataques.

Hong et al. (2023)	Propusieron un estudio basado en un modelo ampliado de conocimiento-actitud y comportamiento, sugiriendo adaptar los programas de formación a distintos niveles educativos.
Kannelønning & Katsikas (2023)	Realizaron una revisión sistemática de cómo se ha evaluado el comportamiento relacionado con la ciberseguridad, identificando el cuestionario HAIS-Q como el más utilizado.
Rohan et al. (2023)	Revisaron sistemáticamente las escalas de ciberseguridad que evalúan la concienciación sobre la seguridad de la información, sugiriendo inversión en programas de formación adaptados.
Guo et al. (2023)	Propusieron estrategias de prevención para mejorar la ciberseguridad en campus inteligentes de instituciones de educación superior, enfatizando la prioridad de la educación en ciberseguridad.

Fuente: Elaboración propia.

El análisis de las conductas riesgosas en ciberseguridad por parte de los estudiantes (mayo, 2021, n=104) se presenta en las Tablas 2 y 3.

Tabla 2. Análisis de conductas de riesgo en el área de ciberseguridad por parte de los estudiantes (Parte 1).

Pregunta	Riesgo Bajo (1 a 3 puntos)	Riesgo medio (4 a 6 puntos)	Riesgo alto (7 a 10 puntos)
¿Qué tan probable es que compartas tu contraseña de Teams con otra persona?	84.6%	8.7%	6.7%
¿Qué tan probable es que compartas alguna contraseña a través de redes sociales?	93.2%	4.8%	2%
¿Qué tan probable es que uses la misma contraseña en más de un sitio?	42.3%	24%	33.7%
¿Qué tan probable es que abras un enlace de una fuente desconocida estando en Facebook?	65.5%	24%	10.5%
¿Qué tan probable es que abras un archivo adjunto de un correo de origen desconocido?	72.1%	20.2%	7.7%

Fuente: Elaboración propia.

Tabla 3. Análisis de conductas de riesgo en el área de ciberseguridad por parte de los estudiantes (Parte 2).

Pregunta	Riesgo bajo (Respuesta No)	Riesgo alto (Respuesta Sí)
¿Mantuviste sin cambio tu contraseña de Facebook durante la contingencia por COVID?	59.6%	40.4%
¿Has compartido información personal por internet?	61.5%	38.5%
¿Has agregado contactos desconocidos a tus redes sociales?	53.8%	46.2%
¿Has instalado software ilegal en tu computadora?	90.4%	9.6%
¿Has realizado transacciones de compras en línea?	41.3%	58.7%

Fuente: Elaboración propia.

El análisis de la aceptación estudiantil de un futuro programa de concientización sobre ciberseguridad (septiembre, 2021, n=79) se presenta en la Tabla 4.

Tabla 4. Análisis de aceptación estudiantil de un programa de concientización sobre ciberseguridad.

Pregunta	En desacuerdo	Neutral	De acuerdo

	(Totalmente de acuerdo, en desacuerdo)		(Totalmente de acuerdo, de acuerdo)
Se deben impulsar actividades para fortalecer las habilidades tecnológicas entre la comunidad estudiantil	7.6%	17.7%	74.7%
Se deben impulsar actividades para fortalecer la seguridad informática entre la comunidad estudiantil.	2.5%	16.5%	81%

Fuente: Elaboración propia.

La revisión de la literatura publicada en revistas indizadas en WoS entre 2010 y 2023 mostró que la investigación sobre la concientización en ciberseguridad se ha realizado de manera consistente en todos estos años. Además, las recomendaciones de promover la sensibilización en estos temas entre la población estudiantil también aparecieron consistentemente entre los artículos analizados. Esta tendencia se ha mantenido durante el periodo de la popularización de los teléfonos inteligentes (2013-2016), así como en el inicio de un periodo de incremento significativo de ataques de ransomware (2017-2019), en el periodo de pandemia por COVID-19 (2020-2022) y en el periodo post-pandemia (2022 – 2023), que coincide con el auge de la inteligencia artificial.

Por otra parte, la exploración de conductas riesgosas en los participantes dejó en evidencia que existen múltiples oportunidades para fortalecer los niveles de ciberseguridad en el estudiantado. Llama la atención, de manera especial, que existen escenarios en donde hasta la tercera parte (o más) de los estudiantes se encuentren en estado de cibervulnerabilidad.

Finalmente, es destacable que el 81% de los participantes haya estado de acuerdo en que se deben impulsar actividades para fortalecer los niveles de seguridad informática entre la comunidad estudiantil. Este porcentaje, incluso fue superior al 74.7% de los estudiantes que estuvo de acuerdo en impulsar actividades para mejorar las habilidades tecnológicas. Esto indica una clara disposición para participar en los programas de concientización sobre ciberseguridad que se llegaran a implementar.

Conclusiones

La literatura científica analizada respalda consistentemente la necesidad de programas de concientización en ciberseguridad para estudiantes universitarios. La importancia de la concientización se ha destacado en los artículos a pesar de los cambios tecnológicos y sociales que han ocurrido desde 2010. Por otra parte, se identificaron vulnerabilidades significativas en las prácticas de ciberseguridad de los estudiantes de Licenciatura en Administración, con escenarios

en donde un alto porcentaje de ellos se encontraría en situaciones de alto riesgo. Asimismo, se detectó una disposición favorable y una necesidad percibida entre los estudiantes para participar en programas de fortalecimiento de habilidades en seguridad informática, superando incluso el interés en mejorar habilidades tecnológicas generales. Así, la implementación de programas de concientización en ciberseguridad en la universidad es no solo factible sino también necesaria, dada la convergencia entre las recomendaciones de la literatura, las vulnerabilidades detectadas y la receptividad de los estudiantes. Como trabajo futuro queda la realización de un estudio de mayor alcance en donde se utilicen datos primarios y se exploren las características específicas del programa de concientización que se implementará.

Referencias

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, *72*, 361–373. https://doi.org/10.1016/j.procs.2015.12.151

Aliyu, M., Abdallah, N. A. O., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World: ICT Connecting Cultures, ICT4M 2010*. https://doi.org/10.1109/ICT4M.2010.5971884

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3), 176–183. https://doi.org/10.4304/jait.3.3.176-183

Arina, A. (Lachi), & Anatolie, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *International Journal of Scientific and Technology Research*, *3*, 128–133. www.ijstr.org

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

Chandarman, R., & Niekerk, B. Van. (2017). Students ' Cybersecurity Awareness at a Private Tertiary Educational. *The African Journal of Information and Communication (AJIC)*, *20*, 133–155.

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *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

Guo, Y., Sun, J., Xu, S., & Yang, Y. (2023). Cybersecurity Challenges and Prevention Strategies in the Construction of Smart Campuses in Higher Education Institutions. *The Frontiers of*

Society, Science and Technology, *5*(7), 20–25. https://doi.org/10.25236/fsst.2023.050704

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. In *Education and Information Technologies* (Vol. 28, Issue 1). Springer US. https://doi.org/10.1007/s10639-022-11121-5

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security*, *310105*. 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

Maldonado Ortiz, F. B., Roque Hernández, R. V., Salazar Hernández, R., & Llamas Mangin, Y. (2022). La paradoja de la seguridad informática durante la pandemia. ¿Son más vulnerables los alumnos de tecnologías de la información? *Dilemas Contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v9i3.3180

Moallem, A. (2019). Cyber Security Awareness Among College Students. In *Advances in Intelligent Systems and Computing* (Vol. 782). Springer International Publishing. https://doi.org/10.1007/978-3-319-94782-2_8

Pérez, G. R. F., Hernández, R. V. R., Mendoza, A. L., & Martínez, S. M. (2022). Higher education in the post-pandemic: student perceptions at a Mexican university. *Nova Scientia*, *14*(28), 1–13. https://doi.org/10.21640/NS.V14I28.2972

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Rashed, A., Abdulrazzek, F., & Kurkshy, S. (2022). Students' Cybersecurity Awareness at Yemenis Educational Institutions. *Applied Research Frontiers*, *1*(3), 22–25. https://doi.org/10.36686/ariviyal.arf.2022.01.03.016

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

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. *Proceedings - 2016 Cybersecurity Symposium, CYBERSEC 2016*, 68–73. https://doi.org/10.1109/CYBERSEC.2016.018

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, *263*(4). https://doi.org/10.1088/1757-899X/263/4/042043

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

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), 0–7. https://doi.org/10.1016/j.heliyon.2019.e02855

Zulfia, A., Adawiyah, R., Hidayanto, A. N., & Fitriah Ayuning Budi, N. (2019). Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS. *5th International Conference on Computing Engineering and Design, ICCED 2019*. https://doi.org/10.1109/ICCED46541.2019.9161120