TIES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Percepción de la ciberseguridad entre estudiantes universitarios en entornos digitales: Un estudio en la Facultad de Informática Mazatlán

Héctor Luis López López
Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán, Mazatlán, Sinaloa, México.
ORCID: 0000-0002-9401-9807

Lucio Guadalupe Quirino Rodríguez
Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán, Mazatlán, Sinaloa, México.
ORCID: 0009-0009-5128-1870

Asia Cecilia Carrasco Valenzuela
Universidad Autónoma de Sinaloa, Preparatoria Rubén Jaramillo, Mazatlán, Sinaloa, México.
ORCID: 0000-0002-3515-358X

Recepción: 05 de septiembre de 2024.
Aceptación: 11 de noviembre de 2024.

Diciembre 2024 • número de revista 11 • https://doi.org/10.22201/dgtic.26832968e.2024.11.30

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Percepción de la ciberseguridad entre estudiantes universitarios en entornos digitales: Un estudio en la Facultad de Informática Mazatlán

Resumen

El presente estudio, realizado en la Facultad de Informática Mazatlán, analiza cómo los estudiantes perciben la seguridad en línea y las prácticas que emplean para proteger sus datos personales en la modalidad virtual. A través de una encuesta a estudiantes, se investigaron aspectos como la percepción sobre ciberseguridad y las experiencias personales con dichos ataques. Los resultados muestran que una parte significativa de los estudiantes está preocupada por la seguridad de sus datos, careciendo muchos de ellos de los conocimientos necesarios para identificar y prevenir potenciales amenazas. Un hallazgo relevante es que sólo una minoría ha sido víctima de algún ciberataque, pero la mayoría de los encuestados tiene una percepción moderada de la seguridad en los entornos digitales, lo que sugiere que, si bien no se sienten completamente desprotegidos, existe una falta de confianza en las medidas de seguridad actuales. El estudio concluye que es esencial integrar asignaturas específicas sobre ciberseguridad en los programas académicos para capacitar a los estudiantes en la identificación de riesgos y en la adopción de prácticas de seguridad adecuadas.

Palabras Clave: Ciberseguridad, privacidad digital, protección de datos, vulnerabilidad informática, conciencia digital

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Perception of Cybersecurity Among University Students in Digital Environments: A Study at the Faculty of Informatics Mazatlan

Abstract

This study, conducted at the Facultad de Informática Mazatlán, analyzes how students perceive online security and the practices they use to protect their personal data in a virtual setting. Through a survey of students, aspects such as cybersecurity perception and personal experiences with such attacks were investigated. The results show that a significant portion of students are concerned about the security of their data, with many lacking the necessary knowledge to identify and prevent potential threats. A noteworthy finding is that only a minority have been victims of cyberattacks, yet most respondents have a moderate perception of security in digital environments. This suggests that, although they do not feel completely unprotected, there is a lack of confidence in current security measures. The study concludes that it is essential to integrate specific cybersecurity courses into academic programs to train students in identifying risks and adopting appropriate security practices.

Keywords: *Cybersecurity, digital privacy, data protection, computer vulnerability, digital awareness.*

1. Introducción

Actualmente, la ciberseguridad se ha convertido en una preocupación dentro del ámbito educativo de la educación superior y, especialmente, en la enseñanza virtual, donde el uso de entornos digitales es cada vez más frecuente. La digitalización de procesos académicos, la gestión de datos personales y el acceso a plataformas educativas en línea han convertido a las universidades en objetivos atractivos para ataques cibernéticos. La vulnerabilidad de los sistemas de información en las instituciones educativas plantea riesgos significativos, no sólo para la protección de la información personal de estudiantes y docentes, sino también para la integridad de los datos académicos y la continuidad de los procesos educativos.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

En este contexto, según Galinec [1], la ciberseguridad abarca prácticas de protección enfocadas en acciones defensivas que implican o dependen de sistemas y entornos de tecnología de la información y tecnología operativa. A juicio de Bishop [2], ciberseguridad consiste en proteger la infraestructura de redes, incluidos enrutadores, servidores de nombres de dominio y conmutadores, asegurando una comunicación informática precisa y confiable. Finalmente, según Veale [3], ciberseguridad incluye tanto aspectos técnicos como sociales para proteger los sistemas de información en red, cobrando así mayor relevancia a medida que más actividades gubernamentales, comerciales y diarias migran a Internet. La ciberseguridad no sólo se refiere a la protección de la infraestructura tecnológica, sino también a la creación de una cultura de seguridad dentro de las comunidades educativas. Es fundamental que las instituciones de educación superior adopten medidas proactivas para sensibilizar a los estudiantes y personal académico sobre las amenazas cibernéticas, promoviendo prácticas seguras en el manejo de la información digital [4]. La creciente dependencia de plataformas digitales para la enseñanza y la gestión académica ha aumentado la superficie de ataque, haciendo imprescindible el fortalecimiento de las políticas y sistemas de seguridad dentro de las universidades.

La seguridad de los datos en la educación superior adquiere una relevancia especial debido a la naturaleza sensible de la información manejada. Las universidades e instituciones de educación no sólo custodian datos personales de miles de estudiantes, sino que también manejan información relacionada con investigaciones científicas, patentes y propiedad intelectual, lo que las convierte en objetivos prioritarios para los ciberdelincuentes [5]. La pérdida o manipulación de estos datos puede tener consecuencias catastróficas, desde el daño a la reputación de la institución hasta la interrupción de actividades académicas.

Por otro lado, en un entorno donde la educación a distancia se ha consolidado como una modalidad clave, especialmente en tiempos de pandemia, la protección de los datos personales y académicos en plataformas digitales es crucial. La reciente transición hacia el aprendizaje en línea ha expuesto nuevas vulnerabilidades, como el incremento de intentos de phishing y accesos no autorizados, lo que exige a las universidades una actualización constante de sus protocolos de ciberseguridad [6]. Desde el punto de vista de Jain y Gupta [7], el phishing es una forma de robo de identidad que manipula a los usuarios de Internet para que revelen información confidencial, como credenciales de acceso y datos de tarjetas

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

de crédito o débito. El reto no sólo radica en proteger la infraestructura tecnológica, sino también en garantizar que los usuarios, es decir, estudiantes y profesores, comprendan los riesgos y adopten comportamientos que mitiguen dichos riesgos.

Investigar la percepción de ciberseguridad, entre los estudiantes de la Facultad de Informática Mazatlán (FIMAZ), es de vital importancia para comprender las actitudes, conocimientos y comportamientos que estos futuros profesionales desarrollan en relación con la seguridad digital. Dado que la facultad forma a especialistas que estarán al frente de la protección de datos en diversas industrias, es fundamental que su formación incluya no sólo competencias técnicas, sino también una conciencia profunda sobre los riesgos y mejores prácticas en ciberseguridad. Según un estudio, la percepción de ciberseguridad entre los estudiantes de informática influye directamente en su capacidad para identificar y mitigar riesgos en entornos digitales, lo cual es esencial para su futuro desempeño profesional [3].

Además, la percepción que tienen los estudiantes sobre la seguridad de los datos afecta directamente su desempeño digital, lo que tiene implicaciones significativas para la seguridad de la información dentro de la misma facultad. Un alto nivel de percepción de ciberseguridad se correlaciona con una mayor adherencia a las políticas de seguridad establecidas por las instituciones educativas, reduciendo así la vulnerabilidad a ciberataques [8]. En este sentido, entender cómo perciben los estudiantes los riesgos digitales permitirá a la FIMAZ diseñar estrategias de formación más efectivas que no sólo aumenten el conocimiento técnico, sino que también promuevan una cultura de seguridad que se extienda a todas las prácticas académicas y profesionales.

La relevancia de este conocimiento radica también en la capacidad de la facultad para adaptarse y responder a las nuevas amenazas cibernéticas que surgen constantemente. Investigaciones recientes han demostrado que los estudiantes que comprenden mejor las dinámicas de la ciberseguridad están más preparados para enfrentar desafíos complejos y para contribuir al desarrollo de soluciones innovadoras en el campo de la seguridad informática [9]. Por lo tanto, la facultad tiene la responsabilidad de evaluar y mejorar continuamente sus programas educativos, asegurándose de que los estudiantes no sólo dominen las herramientas y técnicas actuales, sino que también desarrollen una mentalidad crítica y preventiva frente a las nuevas amenazas cibernéticas. Una percepción deficiente de

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

los riesgos cibernéticos puede llevar a un cumplimiento superficial de las normas de seguridad, lo que, a su vez, incrementa la posibilidad de incidentes que comprometan la integridad de la información académica y administrativa [10].

2. Metodología

Para analizar la percepción de ciberseguridad entre los estudiantes de la FIMAZ, se ha adoptado un enfoque de investigación cuantitativa que se ha complementado con elementos cualitativos, constituyendo así un diseño de investigación mixto. Este tipo de investigación se justifica por la necesidad de obtener tanto datos numéricos, que permitan identificar tendencias y patrones en la percepción de ciberseguridad, como una comprensión más profunda de las actitudes y experiencias subyacentes que no pueden ser capturadas únicamente mediante cifras. Según los investigadores, la combinación de métodos cuantitativos y cualitativos en estudios de ciberseguridad permite obtener una visión más completa y matizada de los problemas y desafíos que enfrentan los estudiantes en entornos digitales [11].

El componente cuantitativo de la investigación se centra en la recolección de datos a través de un instrumento de evaluación tipo encuesta estructurada, diseñada para medir la percepción de ciberseguridad en una muestra representativa de estudiantes del programa educativo de la Licenciatura en Ingeniería en Sistemas de Información (LISI), modalidad virtual. Este enfoque permite la recolección de datos a gran escala, facilitando el análisis estadístico para identificar correlaciones, tendencias y diferencias significativas entre diversos grupos de estudiantes. El uso de técnicas cuantitativas en estudios de ciberseguridad es esencial para obtener un panorama general de las percepciones y comportamientos en poblaciones amplias, lo que, a su vez, puede informar el diseño de políticas educativas más efectivas [12] [13].

Las entrevistas con ítems abiertos brindan a los estudiantes la oportunidad de expresar sus preocupaciones, experiencias y sugerencias en sus propios términos, lo que enriquece el análisis con perspectivas personales y contextuales sobre tema a investigar. La elección de un diseño mixto responde también a la necesidad de triangulación, es decir, la validación de los resultados a través de múltiples métodos y fuentes de datos. La triangulación en la

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

investigación educativa no sólo aumenta la credibilidad y validez de los hallazgos, sino que también permite abordar las complejidades inherentes al estudio de fenómenos como la percepción de ciberseguridad, que están influenciados por factores tanto individuales como contextuales [14].

La investigación se centra en los estudiantes de la FIMAZ, específicamente aquellos matriculados en el programa educativo de la LISI, modalidad virtual. Esta población está compuesta por un total de 102 alumnos oficialmente inscritos en el programa. Dado el tamaño de la población y la naturaleza del estudio, se ha seleccionado una muestra representativa de 50 estudiantes distribuidos entre los primeros cuatro años de la carrera.

La elección de la muestra se fundamenta en la necesidad de obtener una visión más clara y representativa con respecto a la percepción que tienen los alumnos sobre la ciberseguridad en la FIMAZ a lo largo de los diferentes niveles del programa académico. Seleccionar una muestra equilibrada que incluya a estudiantes de varios años académicos permite capturar variaciones en la percepción y comprensión de la ciberseguridad, que pueden estar influenciadas por la experiencia acumulada y el avance en el currículo [15]. Esta estrategia asegura que las conclusiones del estudio reflejen adecuadamente la diversidad de experiencias y conocimientos dentro del programa.

Para la selección de la muestra, se han aplicado criterios de inclusión; los estudiantes deben estar actualmente matriculados en el programa de la LISI y participar activamente en la modalidad virtual, además, se considera esencial que los estudiantes tengan al menos un semestre completo cursado en el programa para garantizar que posean una comprensión suficiente del entorno virtual de aprendizaje. Los criterios de exclusión incluyen a aquellos estudiantes que no se encuentren activos en el programa, ya sea por haber suspendido temporalmente sus estudios o por haber cambiado de programa educativo. Se excluyen igualmente a los estudiantes que no han completado un semestre en la modalidad virtual, ya que su experiencia puede no ser representativa de la percepción general de los estudiantes con mayor tiempo en el programa. La aplicación rigurosa de estos criterios de exclusión es crucial para evitar sesgos que podrían afectar la validez de los resultados [16].

La selección final de los 50 estudiantes se realizó mediante un muestreo aleatorio estratificado, asegurando una representación equitativa de cada año académico (1ro, 2do, 3ro y 4to). Este método de muestreo ayuda a garantizar que todos los niveles del programa

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

estén adecuadamente representados en el estudio, permitiendo un análisis más detallado de las diferencias en la percepción de ciberseguridad entre los años de estudio.

Para evaluar la percepción de ciberseguridad entre los estudiantes, se ha diseñado un instrumento de recolección de datos que combina diferentes tipos de preguntas para captar tanto aspectos cuantitativos como cualitativos. El instrumento principal utilizado es una encuesta estructurada que integra 14 preguntas de opción múltiple, 2 preguntas tipo Likert y 4 preguntas abiertas. Esta combinación permite una evaluación integral de las actitudes, conocimientos y experiencias relacionadas con la ciberseguridad.

Las 14 preguntas de opción múltiple están diseñadas para captar datos cuantitativos sobre el conocimiento general y las prácticas de ciberseguridad de los estudiantes, abarcando temas como la familiaridad con conceptos básicos de seguridad digital, la frecuencia con la que aplican prácticas seguras y la percepción de las políticas de seguridad implementadas en la facultad. Las respuestas son codificadas numéricamente, facilitando el análisis estadístico para identificar patrones y correlaciones significativas. Este tipo de preguntas es eficaz para obtener datos precisos y fácilmente comparables sobre conocimientos y comportamientos específicos [17].

Las 2 preguntas tipo Likert se utilizan para medir actitudes y percepciones más subjetivas de los estudiantes. Estas consultas permiten a los encuestados expresar su grado de acuerdo o desacuerdo con afirmaciones relacionadas con la eficacia de las medidas de seguridad y la confianza en las prácticas de ciberseguridad en la modalidad virtual. La escala Likert proporciona un rango de respuestas que va desde "totalmente en desacuerdo" hasta "totalmente de acuerdo", lo que facilita una evaluación matizada de las opiniones de los estudiantes. Las escalas Likert son útiles para capturar la intensidad de las actitudes y percepciones, proporcionando una visión más detallada de las opiniones de los encuestados [18].

Finalmente, las 4 preguntas abiertas están diseñadas para explorar aspectos cualitativos de la percepción de ciberseguridad. Estas preguntas permiten a los estudiantes expresar sus experiencias personales, preocupaciones y sugerencias de manera detallada. Preguntas abiertas como "¿Cuáles son los principales desafíos que enfrentas en términos de ciberseguridad en tu modalidad virtual?" y "¿Qué medidas consideras necesarias para mejorar la seguridad en los entornos digitales de la facultad?" ofrecen una visión profunda

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

de las percepciones individuales y pueden revelar problemas no abordados por las preguntas cerradas. Las preguntas abiertas son esenciales para obtener insights ricos y contextuales que ayudan a interpretar los datos cuantitativos de manera más completa [19].

El proceso de recolección de datos para evaluar la percepción de ciberseguridad entre los estudiantes se llevó a cabo utilizando encuestas diseñadas en Google Forms, ya que es una herramienta accesible y eficiente para la gestión de datos en línea. Esta elección se basó en la facilidad de uso de la plataforma, su capacidad para automatizar la recopilación de respuestas y su compatibilidad con el entorno virtual en el que se encuentra la población objetivo, utilizando correos electrónicos institucionales y plataformas de comunicación académica empleadas por la facultad. Para maximizar la tasa de respuesta, se realizó un seguimiento mediante recordatorios periódicos y se ofreció un breve periodo de tiempo para completar la encuesta, asegurando que los estudiantes pudieran participar sin interferir con sus horarios de estudio.

Una vez que los estudiantes completaron las encuestas, los datos se recopilaron automáticamente en Google Forms y se exportaron a una hoja de cálculo de Excel para un análisis más detallado. A su vez, la herramienta de Google Forms facilitó la recopilación de datos en tiempo real y permitió la integración con otras herramientas analíticas, lo que optimizó el proceso de análisis de los datos. Para asegurar la validez y confiabilidad de los datos recopilados, se implementaron varias estrategias. Primero, se realizó una prueba piloto de la encuesta con un grupo pequeño de estudiantes para identificar posibles problemas en la formulación de las preguntas y en la interfaz de la encuesta. Esta prueba permitió ajustar el diseño y el contenido de la encuesta antes de su distribución masiva. Las pruebas piloto son fundamentales para mejorar la calidad del instrumento de recolección de datos y asegurar que las preguntas sean claras y pertinentes [20].

El análisis estadístico descriptivo de las preguntas de opción múltiple y las preguntas tipo Likert nos proporcionan una visión general de los datos cuantitativos recopilados. El análisis descriptivo es esencial para interpretar las características básicas de los datos y para obtener una visión clara de las tendencias generales en las respuestas [21]. Para las preguntas abiertas, se empleó el análisis de contenido, una técnica cualitativa que permite identificar temas, patrones y significados en las respuestas textuales. Este análisis de contenido se llevó a cabo mediante la codificación y categorización de las respuestas

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

cualitativas, que incluye la identificación de categorías temáticas, el análisis de la frecuencia de aparición de ciertos términos y la interpretación de las respuestas en contexto. El análisis de contenido es crucial para extraer insights profundos y contextuales a partir de datos cualitativos, proporcionando una comprensión más rica de las percepciones y experiencias individuales [22].

3. Resultados

A continuación, se presentan y analizan los datos obtenidos a partir de la investigación realizada en este análisis, enfocándonos en identificar las tendencias, patrones, y percepciones de los estudiantes de la LISI, en su modalidad virtual, en relación con la seguridad de sus datos personales en entornos digitales.

En la figura 1, observamos que la distribución de estudiantes por grado revela que el 4to grado tiene la mayor representación con un 28% (14 estudiantes), seguido del 3er grado con un 26% (13 estudiantes), el 1er grado representa el 24% (12 estudiantes) y, finalmente, el 2do grado el 22% (11 estudiantes). Esta distribución muestra una progresión ligeramente ascendente en la participación de estudiantes en la investigación a medida que avanzan en su grado académico.

TIES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

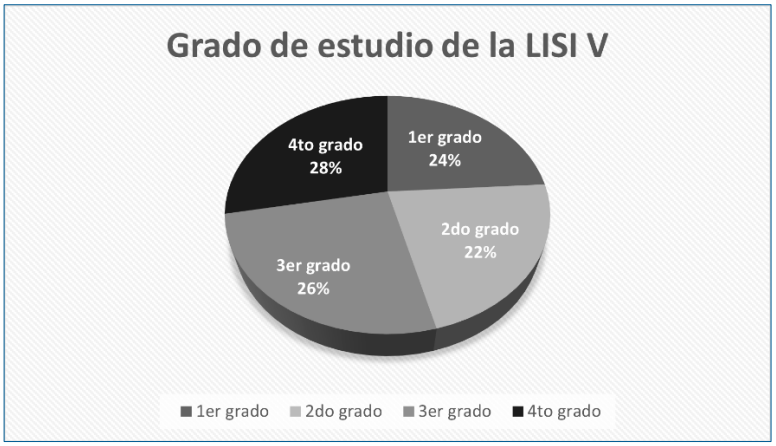

Fig.1. Grado y grupo de los alumnos participantes en el estudio.

Los resultados obtenidos en la figura 2, sobre la percepción que tienen los estudiantes acerca de la seguridad de los datos personales en la facultad, nos presenta una valoración significativamente alta entre los estudiantes encuestados, con un abrumador 86% (43 estudiantes). Esta población considera que la seguridad de sus datos personales es muy importante, lo que subraya la conciencia generalizada sobre la relevancia de proteger la información personal en el entorno académico y, especialmente, en el virtual; en concordancia con las investigaciones de Kumi-Yeboah, se argumenta que los estudiantes experimentan temor y ansiedad debido a la recolección de datos, las complicaciones de los procedimientos burocráticos y las preocupaciones de privacidad en los LMS y redes sociales utilizados en la educación en línea [23]. El 14% restante (7 estudiantes) cree que la seguridad de sus datos es importante, aunque no la sitúan en el nivel más alto de prioridad. No se registraron respuestas en las categorías de "no muy importante" o "nada importante", lo que indica que todos los encuestados reconocen al menos alguna medida de importancia en la protección de sus datos personales. Este consenso resalta la necesidad de mantener y posiblemente fortalecer las medidas de seguridad implementadas para asegurar la confianza continua de los estudiantes en el manejo de su información personal.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Fig.2. Importancia de la seguridad de los datos en la facultad.

En la figura 3, apreciamos los resultados de la encuesta sobre la percepción de protección de la información compartida en internet reflejan una marcada falta de confianza entre los estudiantes, solo el 18% (9 estudiantes) considera que la información que comparten en línea está protegida, lo que indica que una minoría confía en las medidas de seguridad actuales.

Por otro lado, el 46% (23 estudiantes) creen que su información no está protegida en internet, lo que representa casi la mitad de los encuestados, esta cifra revela una preocupación considerable sobre la vulnerabilidad de sus datos y una desconfianza hacia las plataformas o sistemas que manejan su información.

Además, un 36% (18 estudiantes) no está seguro sobre la protección de su información en internet, esto muestra una falta de claridad o conocimiento sobre la efectividad de las medidas de seguridad en línea, lo que subraya la necesidad de una mayor educación y concienciación en temas de ciberseguridad aplicados a la facultad, y tal como señala Doraisamy en su investigación, el 91.2% de los estudiantes optaron por usar una VPN durante su educación en línea, lo cual refleja un alto grado de conciencia respecto a la privacidad y seguridad [24].

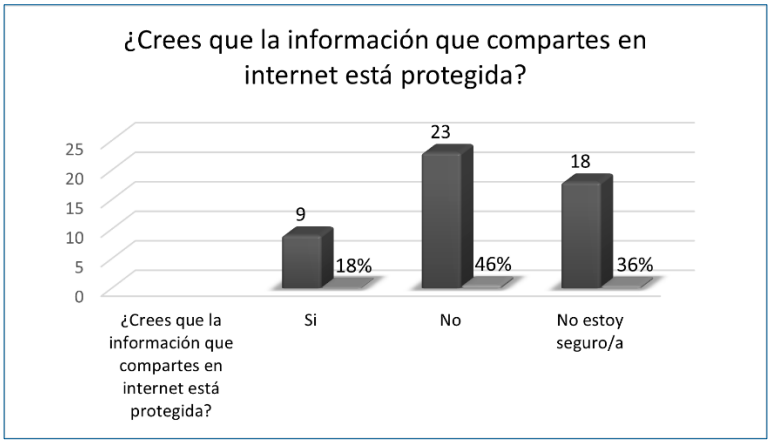

Fig. 3. Opinión de los Alumnos sobre la Seguridad de la Información en Internet.

En relación a la figura 4, los resultados indican que la mitad de los encuestados (50%) ha experimentado sentimientos de invasión a su privacidad en línea. Un porcentaje significativo, el 38%, no ha tenido tales experiencias, mientras que el 12% de los participantes no está seguro/a sobre si su privacidad en línea ha sido invadida.

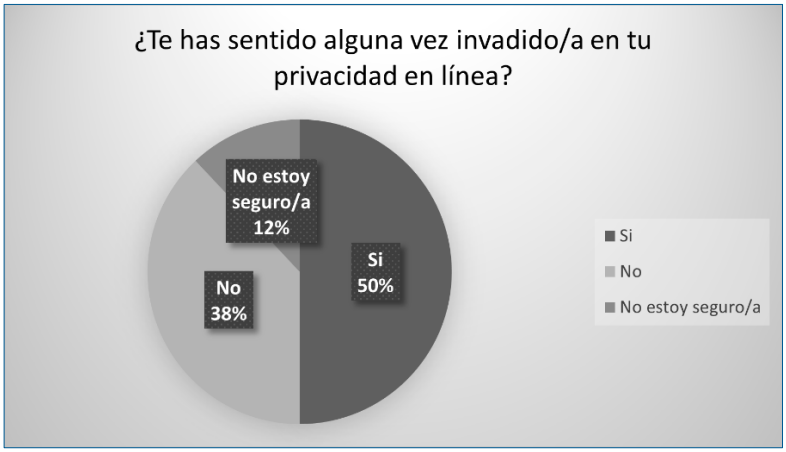

Fig. 4. Percepción de invasión de la privacidad en el entorno digital.

Como se observa en la figura 5, los resultados revelan que la mitad de los estudiantes 50% (25 alumnos) manifiestan una gran preocupación por la seguridad de sus datos

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

personales en entornos virtuales, el 38% (19 alumnos) indicaron estar "un poco preocupado/a", lo que muestra que una proporción significativa de los encuestados siente inquietud, aunque en menor medida, solamente el 12% de los estudiantes afirmaron que no están preocupados por este tema. Este hallazgo pone evidencia que la mayoría de los estudiantes encuestados tiene algún grado de preocupación respecto a la protección de sus datos personales en la modalidad virtual, lo que subraya la importancia de implementar medidas robustas de ciberseguridad y concientización en los entornos educativos digitales de la facultad.

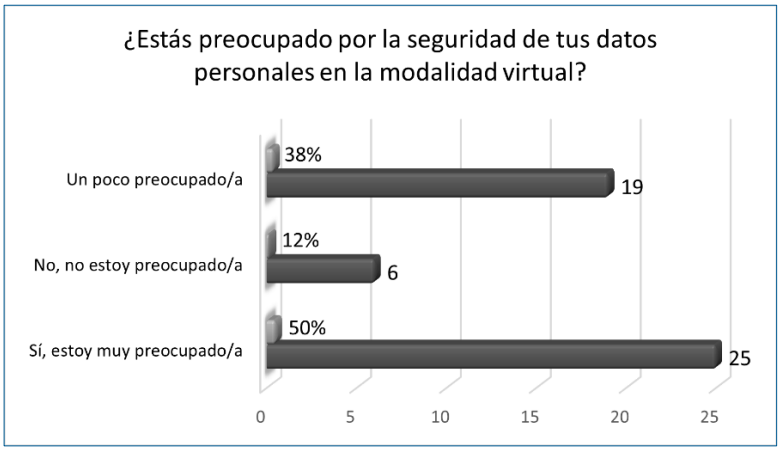

Fig. 5. Preocupación estudiantil por la protección de datos en ambientes virtuales.

En la figura 6, mostrada a continuación, se indica que la mayoría de los estudiantes, el 66%, percibe que el nivel de seguridad en la protección de datos en la modalidad virtual de la LISI es "medio", lo que sugiere que, aunque no consideran que la seguridad sea insuficiente, tampoco la califican como totalmente confiable, lo que podría reflejar ciertas dudas o inquietudes sobre la efectividad de las medidas de protección implementadas.

Por otro lado, un 28% de los encuestados valora el nivel de seguridad como "alto", lo que demuestra que una porción considerable de los estudiantes confía en los mecanismos de ciberseguridad aplicados en la modalidad virtual. Este grupo parece tener una mayor sensación de seguridad con respecto a la gestión de sus datos personales y académicos.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Sin embargo, es importante destacar que un 6% de los estudiantes percibe el nivel de seguridad como "bajo", lo que señala un área de preocupación para esta pequeña minoría, quienes podrían sentir que sus datos no están lo suficientemente protegidos.

En general, los resultados reflejan una percepción general positiva pero moderada, con una confianza mayoritaria en el sistema, pero también con un espacio claro para mejorar las medidas de seguridad y, posiblemente, la comunicación sobre las políticas y prácticas de ciberseguridad que protegen a los usuarios en esta modalidad educativa. Como indican estudios [25], las inquietudes sobre seguridad y privacidad afectan de manera negativa la percepción de facilidad para participar en clases en línea en tiempo real, lo cual influye en la participación de los estudiantes.

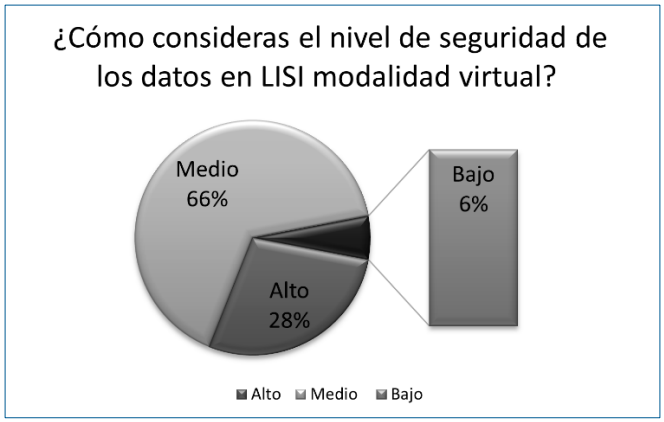

Fig. 6. Nivel de seguridad de los datos en LISI, modalidad virtual, según los estudiantes.

Como parte del estudio sobre las prácticas de seguridad en línea, se preguntó a los estudiantes "¿Con qué frecuencia cambias tu contraseña?". Como se observa en la figura 7, una proporción relativamente pequeña de los estudiantes, apenas el 4% (2 estudiantes), adopta una práctica de cambio de contraseña mensual, una recomendación común en el ámbito de la ciberseguridad para garantizar la protección de los datos personales. La mayor parte de los encuestados, el 34% (17 estudiantes), cambia sus contraseñas cada varios meses, lo que representa una frecuencia moderada y cierto nivel de conciencia sobre la importancia de mantener sus credenciales actualizadas, aunque no con la frecuencia ideal recomendada por los expertos en ciberseguridad.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Otro 32% (16 estudiantes) indicó que cambia su contraseña una vez al año, lo que refleja una actitud más relajada respecto al manejo de sus credenciales de acceso; si bien no es una práctica extremadamente descuidada, cambiar la contraseña solo una vez al año puede dejar las cuentas vulnerables durante largos periodos. Un 18% (9 alumnos) cambia su contraseña menos de una vez al año, lo que sugiere una falta de hábitos consistentes en cuanto a la protección de sus cuentas y puede ser un riesgo potencial para la seguridad de sus datos en entornos digitales, ya que las contraseñas no actualizadas pueden volverse más susceptibles a ataques o robos de información.

Por otro lado, un 12% de los encuestados afirmó que nunca cambia su contraseña, éste sería el grupo más vulnerable, ya que mantener la misma contraseña por largos periodos puede aumentar significativamente el riesgo de sufrir ataques cibernéticos, como el robo de identidad o el acceso no autorizado a información personal.

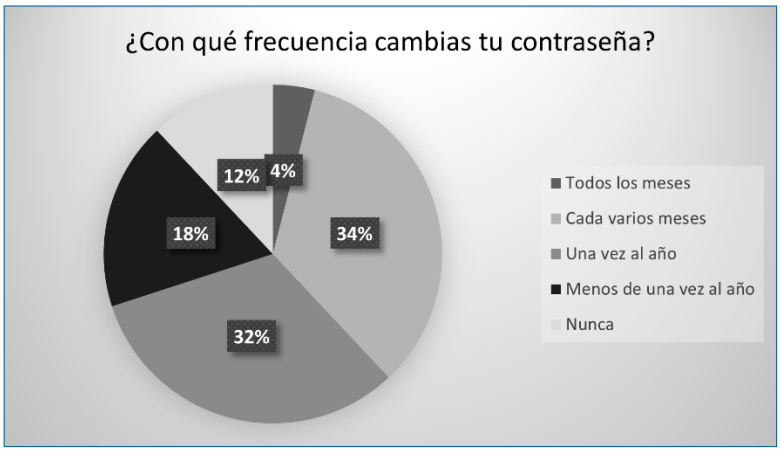

Fig. 7. Frecuencia en el cambio de contraseñas.

Finalmente, en el contexto cualitativo de la investigación, se preguntó a los estudiantes: "¿Confías en la seguridad de las páginas web y aplicaciones que utilizas para almacenar y compartir información personal? ¿Por qué sí o por qué no?". Las respuestas obtenidas revelan una percepción mixta respecto a la confianza en la seguridad de las páginas web y aplicaciones utilizadas para almacenar y compartir información personal.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Una proporción significativa de estudiantes muestra desconfianza en la seguridad de las páginas y aplicaciones; entre las razones más comunes se incluyen el temor a que terceros accedan a sus datos, la creencia de que la mayoría de las plataformas no son seguras y la percepción de que, en última instancia, los datos pueden ser vendidos o utilizados de manera inapropiada. Esta desconfianza refleja una preocupación por la privacidad y la seguridad digital, a menudo alimentada por la conciencia de que cualquier sistema puede ser hackeado.

Algunos estudiantes expresan que su confianza depende del contexto o de la fuente de la aplicación o página web. Por ejemplo, confían en sitios web o aplicaciones de instituciones conocidas. Otros estudiantes, aunque utilizan estas plataformas, reconocen la existencia de vulnerabilidades, pero lo hacen con una cierta resignación y expresan que, aunque son conscientes de los riesgos, confían en que las medidas de seguridad existentes son suficientes para mitigar los peligros más graves o simplemente no ven otra alternativa viable para el uso de estas herramientas.

Otros estudiantes presentan respuestas contradictorias o ambiguas, lo que puede indicar una falta de certeza o una comprensión incompleta del tema. Por ejemplo, hay respuestas que simultáneamente expresan confianza en las medidas de seguridad y desconfianza en la manipulación de datos por parte de terceros.

En general, la mayoría de los estudiantes parecen ser conscientes de los riesgos, aunque sus actitudes varían desde una confianza cautelosa hasta una desconfianza abierta, por lo tanto, este análisis sugiere la necesidad de una mayor educación sobre ciberseguridad para que los estudiantes puedan tomar decisiones más informadas y conscientes sobre el uso de sus datos personales en línea.

Otra pregunta cualitativa que se les aplico fue: "Si fuiste víctima de un ciberataque, ¿cuál fue el motivo y cómo sucedió?". De los 50 estudiantes encuestados, sólo 22 respondieron a esta pregunta, lo que representa un 44% del total de participantes. La mayoría de los encuestados (14 de los 22 que respondieron) afirmaron no haber sido víctimas de un ciberataque, con respuestas como "No" o "Ninguno", lo que sugiere que un gran número de estudiantes no ha experimentado vulnerabilidades digitales significativas o no es consciente de ellas. Algunos estudiantes mostraron incertidumbre con respuestas como "No sé", lo que indica una posible falta de conocimiento para identificar ciberataques. Un grupo menor

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

compartió experiencias directas, que van desde la pérdida de cuentas por "links maliciosos" hasta casos más graves como el robo de dinero mediante clonación de tarjetas. Estos estudiantes describieron reacciones proactivas, como recuperar cuentas o transferir fondos rápidamente tras detectar robos, pero las respuestas también revelan una falta de preparación previa hacia esos ilícitos.

Este análisis subraya la necesidad de educar a los estudiantes sobre la prevención, identificación y manejo de ciberataques, además, la falta de conciencia de algunos sobre haber sido atacados resalta la urgencia de incluir asignaturas sobre ciberseguridad para los futuros programas académicos ofertados en la facultad.

4. Conclusiones

La investigación realizada sobre la percepción y experiencia de los estudiantes en relación con la ciberseguridad en entornos digitales arroja una serie de hallazgos clave que permiten identificar áreas de oportunidad en la formación académica de ellos, así como desafíos para la comunidad educativa de la FIMAZ.

En primer lugar, los resultados muestran que, aunque la mayoría de los estudiantes encuestados no ha sido víctima directa de ciberataques o no tiene conciencia de haberlo sido, existe una preocupante falta de ésta misma y de conocimientos sobre cómo identificar y prevenir amenazas digitales.

Los estudiantes que expresaron no estar seguros de haber sido atacados reflejan una carencia significativa de alfabetización digital en temas de ciberseguridad, lo cual los coloca en una situación de vulnerabilidad frente a los crecientes riesgos en la modalidad virtual. Además, aquellos estudiantes que sí han sido víctimas de ciberataques describen experiencias que varían en gravedad, desde el robo de cuentas de redes sociales hasta problemas financieros como la clonación de tarjetas de débito. Estas experiencias muestran que, si bien algunos han reaccionado de manera proactiva para mitigar el daño (por ejemplo, usando métodos de recuperación de cuentas o transferencias bancarias rápidas), muchos no están adecuadamente preparados para prevenir este tipo de situaciones.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

Es importante reconocer algunas limitaciones en este estudio que podrían haber influido en los resultados obtenidos, como el hecho de que sólo 22 de los 50 estudiantes encuestados respondieron a una de las preguntas cualitativas sobre ciberataques, restringiendo así el alcance del análisis. Esto podría limitar la capacidad de generalizar las conclusiones a toda la población estudiantil, ya que los estudiantes que optaron por no responder podrían tener percepciones y experiencias distintas.

5. Recomendaciones

Con base en estos resultados, es altamente recomendable que la facultad integre asignaturas especializadas en ciberseguridad en sus planes de estudio. Estas asignaturas deben abordar temas como la gestión segura de contraseñas, el reconocimiento de ataques de *phishing*, el uso seguro de redes Wi-Fi y dispositivos móviles, así como la importancia del cifrado de datos. Al incluir estas materias, los estudiantes podrán adquirir las herramientas y habilidades necesarias para desempeñarse de manera segura y eficiente en el entorno digital, tanto en el ámbito académico como en su vida profesional.

Sería recomendable realizar estudios que midan de forma más precisa la relación entre el conocimiento de ciberseguridad y la prevención de ataques cibernéticos, así como también sería valioso diseñar investigaciones que incluyan evaluaciones de competencias en ciberseguridad antes y después de recibir formación especializada, pudiendo observar así los efectos de programas educativos enfocados en este ámbito.

Otra recomendación para futuras investigaciones sería ampliar el tamaño de la muestra y asegurar una mayor representatividad de los estudiantes, lo que permitiría obtener resultados más robustos y la realización de estudios longitudinales que permitan observar la evolución de las prácticas de seguridad digital entre los estudiantes de los programas virtuales a lo largo del tiempo. Esto sería relevante después de la implementación de asignaturas o programas de capacitación en ciberseguridad, para evaluar si estas medidas contribuyen efectivamente a la reducción de riesgos y al desarrollo de mejores hábitos digitales entre la comunidad estudiantil.

TiES Revista de Tecnología e Innovación en Educación Superior
www.ties.unam.mx

6. Propuestas y Aportaciones

La recién y creciente digitalización en todos los aspectos de la vida, incluida la educación, ha expuesto a los estudiantes y trabajadores de la Universidad Autónoma de Sinaloa (UAS) a diversos riesgos cibernéticos, por lo que se debe crear una cultura de ciberseguridad dentro de la institución. Sin embargo, la falta de conciencia sobre la seguridad informática sigue siendo un desafío, ya que muchos estudiantes y personal de la institución sólo toman acción cuando son víctimas directas de delitos como el *hackeo* de cuentas bancarias o el acceso no autorizado a sus redes sociales, por lo que, para transformar esta realidad y fomentar una mayor conciencia sobre la ciberseguridad, se proponen las siguientes propuestas:

Es crucial que los estudiantes reciban formación sobre ciberseguridad desde el inicio de sus programas educativos mediante la incorporación de módulos o asignaturas enfocadas en los ataques de seguridad cibernética, pudiendo ayudar a que todos los alumnos, independientemente de su área de estudio, desarrollen una comprensión básica de la protección en línea y de los riesgos a los que están expuestos.

La Unidad de Bienestar Social de la Universidad debe de organizar talleres y conferencias impartidas por expertos en los temas de ciberseguridad, proporcionándole a la comunidad educativa conocimientos prácticos sobre cómo protegerse contra ataques cibernéticos, como la creación de contraseñas seguras o el reconocimiento de correos fraudulentos (*phishing*), entre otros.

Dado que muchos estudiantes pasan gran parte de su tiempo en plataformas como Facebook, Instagram y Twitter, se pueden lanzar campañas de concientización sobre ataques seguridad digital. Estas campañas pueden incluir consejos semanales sobre cómo mantener la seguridad en línea, testimonios de personas afectadas por *hackeos* y guías sencillas sobre cómo proteger las cuentas bancarias y personales. Además, se podrían ofrecer simulaciones de ciberataques para que los estudiantes experimenten de primera mano cómo reaccionar ante una amenaza.

La Universidad debe implementar protocolos institucionales que detallen los pasos a seguir en caso de algún ilícito en ciberataques, tanto para estudiantes como para personal administrativo, ya que nadie pasa desapercibido en estos casos. La existencia de un proceso

claro, accesible y transparente ante incidentes de *hackeo* ayudaría a crear un entorno universitario más seguro y responsable.

Referencias

[1] D. Galinec, D. Možnik, y B. Guberina, "Ciberseguridad y ciberdefensa: enfoque estratégico a nivel nacional", *Automatika*, vol. 58, pp. 273–286, 2017, doi: 10.1080/00051144.2017.1407022.

[2] M. Bishop, "¿Qué es la seguridad informática?", *IEEE Secur. Priv.*, vol. 1, pp. 67-69, 2003, doi: 10.1109/MSECP.2003.1176998.

[3] M. Veale y I. Brown, "Cybersecurity", *Internet Policy Rev.*, vol. 9, no. 4, 2020, doi: 10.14763/2020.4.1533.

[4] N. J. Pinda Román y L. A. Moya Martínez, "Ciberseguridad enfocada en el futuro digital de los estudiantes: Cybersecurity focused on the digital future of students", *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, vol. 5, núm. 2, 2024, doi: 10.56712/latam.v5i2.1910.

[5] D. Díaz Lima, "Transparencia y protección de datos personales en el ámbito universitario: ¿avance o retroceso?", *RET*, núm. 17 Extra, pp. 201-224, jul. 2023, doi: 10.51915/ret.311.

[6] A. González Torres, M. L. Pereira Hernández, y C. C. Lacruhy Enríquez, "Hombres y mujeres en el aprendizaje virtual: ¿Opinión diferenciada de la calidad en la formación en línea?", *Eduweb*, vol. 18, núm. 1, pp. 66–80, 2024, doi: 10.46502/issn.1856-7576/2024.18.01.5.

[7] A. Jain y B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges", *Enterprise Information Systems*, vol. 16, 2021, doi: 10.1080/17517575.2021.1896786.

[8] A. Antonio y J. Manuel, "Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y

política exterior", *Estudios internacionales* (*Santiago*), vol. 53, núm. 198, pp. 169–197, abr. 2021, doi: 10.5354/0719-3769.2021.57067.

[9] L. Rodríguez Matías, H. B. Palacios Pérez, J. I. Zambrano Dávila, y M. Torres Gatica, "Análisis de la Seguridad Informática en el Uso de Redes Sociales de Alumnos de la Escuela Preparatoria No. 48", *Ciencia Latina*, vol. 8, núm. 2, pp. 1498-1505, abr. 2024, doi: 10.37811/cl_rcm.v8i2.10583.

[10] W. E. Martínez Chérrez y D. F. Ávila Pesantez, "Ciberseguridad en las redes sociales: una revisión teórica", *Uniandes Episteme*, vol. 8, núm. 2, pp. 211–234, 2021. Disponible en: https://revista.uniandes.edu.ec/ojs/index.php/EPISTEME/article/view/2089/1659

[11] P. Ramírez y L. Gómez, "Investigación mixta en ciberseguridad: Integrando enfoques cuantitativos y cualitativos", *Revista Mexicana de Ciencias Sociales y Humanidades*, vol. 12, núm. 2, pp. 144-158, 2021.

[12] J.-J. Igartua, "Tendencias actuales en los estudios cuantitativos en comunicación", *Comun. Soc. (Guadalaj.)*, núm. 17, pp. 15–40, 2012.

[13] A. Hernández y M. López, "Explorando la percepción de ciberseguridad a través de métodos cualitativos," *Revista Latinoamericana de Estudios en Tecnología Educativa*, vol. 8, núm. 3, pp. 45-60, 2022.

[14] E. Torres Campos, "Propuesta metodológica en la realización de la investigación educativa en el CAMCM", *PD*, vol. 5, núm. 9, pp. 105-117, ene. 2023, doi: 10.56865/dgenam.pd.2023.5.9.249.

[15] D. Valverde-Crespo, A. de Pro Bueno, y J. González-Sánchez, "La fiabilidad de la información sobre ciencia de Internet y criterios utilizados para justificarla por parte de estudiantes de educación secundaria", *Rev_Eureka_enseñ_divulg_cienc*, vol. 19, núm. 3, 2022, doi: 10.25267/Rev_Eureka_ensen_divulg_cienc.2022.v19.i3.3103.

[16] M. Astudillo-Torres y Y. Oviedo-Vargas, "La exclusión social y las Tecnologías de la Información y la Comunicación: una visión estadística de su relación en la educación

superior", *LiminaR*, vol. 18, núm. 1, pp. 177–193, 2020, doi: 10.29043/liminar.v18i1.721.

[17] L. A. Camacho-Saavedra, J. J. Huamán-Saavedra, y J. O. Plasencia-Alvarez, "Eficiencia de preguntas de opción múltiple con 3 alternativas", *Rev Med Trujillo*, vol. 15, núm. 4, dic. 2020, doi: 10.17268/rmt.2020.v15i04.06.

[18] M. I. Landaluce Calvo, "Recodificación de escalas tipo Likert a través de la clasificación no supervisada. Las implicaciones de las relaciones por Internet respecto a las relaciones presenciales como estudio de caso", *Rev. int. sociol.*, vol. 82, núm. 2, p. e251, jun. 2024, doi: 10.3989/ris.2024.82.2.M23-06.

[19] A. Matas, "Diseño del formato de escalas tipo Likert: un estado de la cuestión", *Revista Electrónica de Investigación Educativa*, vol. 20, núm. 1, pp. 38-47, ago. 2018, doi: 10.24320/redie.2018.20.1.1347.

[20] M.Á. Hernández Alvarado, M. de las M. de Agüero Servín, y M. A. Benavides Lara, "Piloteando ando: ajustes a un cuestionario de investigación a partir del estudio piloto", *Rev. Digit. Univ.*, vol. 25, núm. 1, 2024, doi: 10.22201/cuaieed.16076079e.2024.25.1.16.

[21] P. I. Vizcaíno Zúñiga, R. J. Cedeño Cedeño, y I. A. Maldonado Palacios, "Metodología de la investigación científica: guía práctica", *Ciencia Latina*, vol. 7, núm. 4, pp. 9723-9762, sep. 2023, doi: 10.37811/cl_rcm.v7i4.7658.

[22] H. Avila y S. M. Magarita Matilla González, "La entrevista y la encuesta: ¿métodos o técnicas de indagación empírica?", *Didasc@lia: didáctica y educación*, vol. 11, pp. 62–79, 2020.

[23] A. Kumi-Yeboah, Y. Kim, B. Yankson, S. Aikins, y Y. A. Dadson, "Diverse students' perspectives on privacy and technology integration in higher education", Br. J. Educ. Technol., vol. 54, núm. 6, pp. 1671–1692, 2023, doi: 10.1111/bjet.13386.

[24] T. Doraisamy, D. Murad, R. Hassan, y F. Qamar, "Student's Awareness of Privacy and Security During Online Classes. 2023 8ª Conferencia Internacional sobre

Investigación Empresarial e Industrial (ICBIR)", pp. 161–164, 2023, doi: 10.1109/ICBIR57571.2023.10147603.

[25] S. Kim, "Motivators and concerns for real-time online classes: focused on the security and privacy issues", *Interactive Learning Environments*, vol. 31, pp. 1875–1888, 2021, doi: 10.1080/10494820.2020.1863232.