UNIVERSIDAD CATÓLICA DE CUENCA

Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Análisis de Amenazas Cibernéticas en el Sector Educativo.

Autor: Ing. Eulalia Lissette Ortíz Figueroa

Asesores: Ing. Marco Vinicio Yamba Yugsi. Mgs.
Ing. Juan Carlos Ortega Castro. Mgs.

Cuenca, 2025

Certificación de Asesores

Se certifica que:

El informe de investigación “Análisis de Amenazas Cibernéticas en el Sector Educativo”, de autoría de la Señora Ingeniera de Sistemas Eulalia Lissette Ortíz Figueroa, CC: 0704867167 ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Cuenca, Marzo 2025.

MARCO VINICIO YAMBA YUGSI

Firmado digitalmente por MARCO VINICIO YAMBA YUGSI
Fecha: 2025.04.02 11:20:07 -05'00'

Ing. Marco Vinicio Yamba Yugsi. Mgs.
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mgs
Asesor Metodológico

Certificación de Asesores

Se certifica que:

El informe de investigación “Análisis de Amenazas Cibernéticas en el Sector Educativo”, de autoría de la Señora Ingeniera de Sistemas Eulalia Lissette Ortíz Figueroa, CC: 0704867167 ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

MARCO VINICIO YAMBA YUGSI

Firmado digitalmente por MARCO VINICIO YAMBA YUGSI
Fecha: 2025.04.02 11:25:33 -05'00'

Cuenca, Marzo 2025.

Ing. Marco Vinicio Yamba Yugsi. Mgs.
Asesor Científico

Certificación de Autoría

Certifico que:

“Análisis de Amenazas Cibernéticas en el Sector Educativo”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Cuenca, Marzo 2025.

Firmado electrónicamente por:
EULALIA LISSETTE
ORTIZ FIGUEROA

Ing. Eulalia Lissette Ortiz Figueroa

CC: 0704867167

Agradecimiento

En primer lugar, quiero expresar mi más sincero agradecimiento a Dios, por haberme otorgado la salud, la sabiduría y la fortaleza necesarias para llevar a cabo este trabajo investigativo. Sin su guía constante, no habría sido posible cumplir con este sueño de obtener esta Maestría. Gracias por iluminar mi camino y darme las fuerzas para enfrentar cada desafío con determinación y esperanza.

A mi tutor, quien fue una pieza clave en el desarrollo de esta investigación. Su orientación, paciencia y apoyo fueron esenciales para el adecuado desempeño de este trabajo. Gracias por ser un faro de conocimiento y por guiarme con sabiduría durante todo el proceso. Sus valiosos consejos y su constante disposición a ayudarme fueron fundamentales para alcanzar esta meta.

Y, por supuesto, a mi familia, quienes son mi pilar fundamental que siempre me impulsan a seguir adelante. A mis hijos, mi esposo, mi madre y mis seres queridos, gracias por su amor incondicional. Son mi fuente constante de motivación, y sin ustedes, este logro no habría sido posible. Gracias por estar siempre a mi lado y por ser mi mayor fuente de fuerza.

Dedicatoria

Mi amado hijo Sebastian, mi guerrero de luz. Este logro, esta meta alcanzada, sin duda es para ti. Cada línea de este informe, cada hora de estudio, cada sacrificio, fue impulsado por tu sonrisa, por tu fuerza, por tu manera única de ver el mundo. Eres mi inspiración, mi motor, y mi razón de ser.

A mis hermosos bebés, Alfonsito y Laita, quienes, a través de su inocencia y travesuras han sido parte de este viaje, cada sonrisa y gesto de amor me han llenado de energía para continuar, y a mi querido esposo, mi compañero de batallas, gracias por sostenerme, por creer en mí y por ser el mejor padre para nuestros hijos.

A mi madre, a quien, aunque la distancia física nos separe, su amor y apoyo nunca han tenido fronteras. Siempre he podido contar con ella, y sus palabras de aliento, su sabiduría y su cariño me han dado fuerza en los momentos más difíciles.

A mi papito Humberto, quien, en el transcurso de este año tan significativo, partió de este mundo, pero su presencia y amor continúa siendo parte fundamental de mi vida. Aunque el dolor de su pérdida ha sido inmenso, sé que esta meta alcanzada es también un homenaje a todo lo que me dieron junto a mi mamita, a todo lo que me enseñaron y a la forma en que siempre me apoyaron. Ellos fueron mis bases, me vieron crecer, me dieron su amor incondicional y me enseñaron lecciones de vida que me han acompañado en todo momento. A pesar de su partida, me ha dejado un legado de fortaleza y sabiduría, y quiero hacerlos sentir orgullosos con este logro, que es también de ellos.

Este título de Magíster en Ciberseguridad es cumplido por Ustedes y para ustedes por ser mi refugio, mi fuerza y mi mayor tesoro.

Resumen

El presente estudio analizó el impacto de las amenazas cibernéticas en la seguridad, privacidad y acceso a la información académica en entornos educativos. El objetivo principal fue evaluar los riesgos cibernéticos que enfrentan los estudiantes y proponer estrategias para mitigar sus efectos. Mediante un enfoque mixto, que combina enfoques cuantitativos y cualitativos, se aplicaron encuestas a 150 estudiantes y entrevistas a 5 docentes para obtener una visión integral de la percepción sobre la ciberseguridad y sus implicaciones. Los resultados revelaron una alta vulnerabilidad en las instituciones educativas debido a la falta de capacitación en ciberseguridad y deficiencias en las medidas de protección digital. Las correlaciones obtenidas reflejaron que una percepción positiva sobre seguridad digital está relacionada con la formación adecuada, mientras que los riesgos cibernéticos afectan negativamente la continuidad académica. Las entrevistas destacaron la necesidad de mejorar las políticas de protección y fortalecer los programas de capacitación para docentes y estudiantes. Finalmente, las conclusiones subrayan la urgencia de implementar estrategias de mitigación y aumentar la sensibilización sobre ciberseguridad en las instituciones educativas.

Palabras claves: Ciberseguridad, Amenazas digitales, Continuidad académica, Protección de datos.

Abstract

This study analyzes the impact of cyberthreats on security, privacy, and access to academic information in educational settings. The main objective was to assess the cyber risks faced by students and propose strategies to mitigate their effects. Using quantitative and qualitative methodology, surveys were conducted with 150 students and interviews with five faculty members to obtain a comprehensive view of perceptions about cybersecurity and its implications. The results revealed high vulnerability in educational institutions due to a lack of cybersecurity training and deficiencies in digital protection measures. The correlations obtained showed that a positive perception of digital security is related to adequate training, while cyber risks negatively affect academic continuity. The interviews highlighted the need to improve protection policies and strengthen training programs for faculty and students. Finally, the conclusions underscore the urgency of implementing mitigation strategies and increasing cybersecurity awareness in educational institutions.

Keywords: Cybersecurity, Digital Threats, Academic Continuity, Data Protection.

Índice de Contenidos

Certificación de Asesores 2
Certificación de Asesores i
Certificación de Autoría ii
Agradecimiento iii
Dedicatoria iv
Resumen v
Abstract vi
Capítulo I. Introducción 1
Metodología 5
Resultados 9
Resultados de la Encuesta sobre Ciberseguridad en el Entorno Educativo 9
Correlación de variables 11
Correlación de las dimensiones 13
Análisis de Componentes Principales 16
Análisis de las Cargas Factoriales 17
Unicidad (Uniqueness) 18
Comprobación de Supuestos 18
Análisis Factorial Confirmatorio: Evaluación de la Ciberseguridad y el Impacto de las Amenazas Cibernéticas en el Entorno Educativo 19
Resultados de las entrevistas 21
Tipos de Ataques Cibernéticos en la Institución Educativa 21
Evaluación de la Seguridad de los Sistemas Informáticos 22
Capacitación en Ciberseguridad Recibida por los Docentes 22
Interrupciones en el Acceso a Plataformas Educativas 23
Impacto de los Ataques en la Continuidad del Aprendizaje 23
Percepción sobre el Nivel de Ciberseguridad para Proteger la Información 24
Conclusiones y discusión 25
Implicaciones para Investigaciones Futuras 29
Consideraciones Éticas 29
Referencias 30

Capítulo I. Introducción

El avance acelerado de la digitalización en el ámbito educativo ha transformado la manera en que los estudiantes acceden a la información, interactúan con los contenidos académicos y desarrollan sus competencias en un entorno cada vez más interconectado (Barletta et al., 2024; Dapitan et al., 2024; Ibrahim et al., 2024). Sin embargo, esta evolución también ha generado una creciente exposición a riesgos cibernéticos que comprometen la seguridad de los datos, la privacidad de los usuarios y la integridad de los sistemas educativos.

La educación, como pilar fundamental en la formación de las nuevas generaciones, enfrenta el desafío de garantizar un entorno digital seguro para los estudiantes, quienes se han convertido en el grupo más vulnerable ante ataques cibernéticos que afectan tanto su acceso a la información como la continuidad de sus procesos de aprendizaje (Prior & Renaud, 2024; Srivastava et al., 2024; Williams & Daugherty, 2024). Investigaciones recientes han abordado la importancia de la concienciación en ciberseguridad dentro del ámbito educativo, resaltando la necesidad de fortalecer las estrategias de protección y la formación en seguridad digital para los estudiantes.

En este sentido, estudios como el de Awang et al. (2024) han analizado el papel del control parental en la concienciación sobre ciberseguridad en estudiantes con necesidades especiales, concluyendo que la supervisión activa de los padres y docentes es un factor determinante en la prevención de amenazas cibernéticas. Por otro lado, Ayyash et al. (2024) exploraron la educación en ciberseguridad desde la perspectiva de padres y docentes, destacando que la falta de formación específica sobre seguridad digital en estos actores contribuye a la vulnerabilidad de los estudiantes. Asimismo, la investigación de Dapitan et al. (2024) midió el nivel de concienciación en ciberseguridad entre estudiantes de educación secundaria, evidenciando una brecha significativa en el conocimiento sobre riesgos digitales y las medidas de protección necesarias para mitigar estas

amenazas. Estas investigaciones reflejan la urgencia de fortalecer la educación en ciberseguridad y de implementar estrategias eficaces para reducir los riesgos asociados al uso de plataformas digitales en el ámbito educativo (Thomas et al., 2024).

El problema central de esta investigación radica en la creciente exposición de los estudiantes a amenazas cibernéticas en el sector educativo, las cuales impactan su seguridad, privacidad y acceso a la información académica como se ha visto en (Pramod, 2024; Radday et al., 2024; Santa Barletta et al., 2024). El diseño no experimental de este estudio permite analizar cómo la falta de formación en ciberseguridad, la deficiencia en políticas de protección digital, el uso inadecuado de plataformas educativas y la insuficiencia de mecanismos de supervisión afectan la experiencia de los estudiantes en entornos digitales (Prior & Renaud, 2024).

En primer lugar, la falta de formación en ciberseguridad genera un desconocimiento sobre los riesgos digitales (Radday et al., 2024), lo que incrementa la posibilidad de que los estudiantes sean víctimas de ataques como el phishing, el robo de identidad y la explotación de datos personales. En segundo lugar, la deficiencia en políticas de protección digital dentro de las instituciones educativas, propician brechas de seguridad que facilitan el acceso no autorizado a información académica y administrativa, comprometiendo la integridad de los sistemas educativos (Prior & Renaud, 2024). En tercer lugar, el uso inadecuado de plataformas educativas, en muchos casos por desconocimiento o por falta de regulaciones claras, expone a los estudiantes a software no seguro y a prácticas que pueden derivar en la vulneración de sus datos personales (Santa Barletta et al., 2024), la insuficiencia de mecanismos de supervisión por parte de docentes y familias agrava la situación, ya que los estudiantes no cuentan con el acompañamiento necesario para identificar y prevenir amenazas cibernéticas, lo que los deja en una situación de mayor vulnerabilidad ante ataques digitales (Mohanty et al., 2024).

A partir de esta problemática, se plantea la siguiente pregunta de investigación: ¿De qué manera las amenazas cibernéticas en el sector educativo afectan la seguridad, privacidad y acceso a la información académica de los estudiantes, y qué estrategias pueden implementarse para mitigar estos riesgos? El objeto de estudio de esta investigación es la ciberseguridad en el sector educativo, enfocándose en la experiencia de los estudiantes y en los factores que influyen en su vulnerabilidad ante amenazas digitales (Manganello et al., 2024; Mohanty et al., 2024). La necesidad de abordar este problema se justifica desde tres perspectivas fundamentales: teórica, metodológica y práctica.

Desde la teoría, la investigación se fundamenta en el concepto de alfabetización digital y seguridad informática, destacando la importancia de dotar a los estudiantes de competencias que les permitan navegar de manera segura en entornos digitales. Metodológicamente, el estudio se basa en un diseño no experimental que permite analizar el impacto de las amenazas cibernéticas en los estudiantes y evaluar la efectividad de estrategias de protección en el ámbito educativo. En la práctica, los resultados de esta investigación contribuirán a la implementación de políticas de ciberseguridad más efectivas en las instituciones educativas, proporcionando recomendaciones concretas para la capacitación de docentes y estudiantes en seguridad digital (Mohanty et al., 2024).

El objetivo general de esta investigación es analizar el impacto de las amenazas cibernéticas en la seguridad, privacidad y acceso a la información académica de los estudiantes en el sector educativo. Para alcanzar este propósito, se establecen los siguientes objetivos específicos. I. Identificar los principales riesgos y vulnerabilidades a los que están expuestos los estudiantes en entornos digitales educativos, mediante una revisión de la literatura y estudios previos sobre ciberseguridad en el ámbito educativo. II. Evaluar el nivel de concienciación en ciberseguridad entre los estudiantes, así como la efectividad de las medidas de protección implementadas en sus

instituciones educativas, a través de un análisis de datos obtenidos mediante encuestas y entrevistas. III. Interpretar los hallazgos del estudio para diseñar recomendaciones prácticas que contribuyan al fortalecimiento de la ciberseguridad en el sector educativo, orientadas a mejorar la formación en seguridad digital.

Este estudio se inscribe en un contexto de creciente preocupación por la seguridad digital en la educación, donde la rápida digitalización ha expuesto a los estudiantes a nuevos desafíos y riesgos que requieren una respuesta integral y fundamentada (Barletta et al., 2024; Ismail et al., 2024). La ciberseguridad en el sector educativo no solo es un tema de interés académico, sino también una cuestión de urgencia social que demanda la implementación de estrategias efectivas para garantizar un entorno digital seguro y confiable para los estudiantes (Costa et al., 2025; Manganello et al., 2024). A partir del análisis de las amenazas cibernéticas y la identificación de las vulnerabilidades presentes en los entornos educativos, esta investigación busca aportar soluciones concretas para mitigar los riesgos asociados a la digitalización de la educación, fortaleciendo así la seguridad digital en el ámbito académico (Mohanty et al., 2024).

Metodología

Este estudio adoptó un diseño no experimental, en el cual se observaron las variables en su entorno natural sin manipulación alguna. A través del enfoque mixto, se identifican patrones y relaciones tanto cualitativos como cuantitativos entre las variables sin intervenir en los procesos educativos. El tipo de investigación fue descriptivo-correlacional, ya que se analizaron y caracterizaron las amenazas cibernéticas en el sector educativo, contrastando la relación entre las variables estudiadas.

La variable independiente del estudio fue la ciberseguridad en el sector educativo, evaluada a partir de la percepción de estudiantes y docentes sobre las medidas de protección y vulnerabilidades existentes en las instituciones educativas. La variable dependiente fue el impacto de las amenazas cibernéticas en el acceso a la información y la continuidad del aprendizaje, reflejado en incidentes de seguridad y sus consecuencias en la operatividad académica.

El estudio se realizó bajo un enfoque mixto (Observable en tabla 1), combinando métodos cuantitativos y cualitativos para obtener una visión integral del fenómeno. Se aplicaron como técnicas las encuestas a estudiantes con el objetivo de recopilar datos medibles sobre sus experiencias con ciberseguridad en sus instituciones, mientras que las entrevistas a docentes permitieron profundizar en la interpretación y análisis de los resultados obtenidos en las encuestas.

Las dimensiones evaluadas del estudio dentro de la variable independiente incluyen el tipo de incidentes cibernéticos, la percepción sobre la seguridad de los sistemas educativos y el nivel de capacitación en ciberseguridad. Por otro lado, en la variable dependiente se analizaron los efectos

de los ataques en el acceso a plataformas digitales, la integridad de los datos académicos y la percepción de riesgo dentro del entorno educativo.

La población estuvo conformada por estudiantes y docentes de instituciones educativas de nivel secundario y superior con acceso a plataformas digitales. Se utilizó un muestreo no probabilístico intencionado, seleccionando participantes con experiencia en el uso de herramientas tecnológicas en el aula y con conocimiento de incidentes cibernéticos en una institución de educación media. En total, se encuestaron 150 dicentes del nivel de bachillerato y se entrevistaron 5 docentes. Los estudiantes fueron seleccionados para evaluar su percepción sobre la seguridad digital y los incidentes de ciberseguridad en su entorno académico, mientras que los docentes proporcionan información sobre las políticas de protección y los desafíos en la implementación de estrategias de ciberseguridad.

Los datos cuantitativos obtenidos a través de las encuestas fueron analizados mediante estadística *descriptiva y correlacional*. Se aplicó el coeficiente de evaluación de Rho de Spearman para evaluar la relación entre la percepción de ciberseguridad y el impacto de los ataques en el acceso a la información y de entre sus dimensiones. Los datos cualitativos de las entrevistas fueron procesados mediante análisis temático, identificando categorías y patrones recurrentes en las respuestas de los docentes. Se determinaron códigos para clasificar las respuestas según las principales preocupaciones y experiencias en la gestión de la ciberseguridad en el entorno educativo. Para garantizar la precisión en los resultados, se utilizó software estadístico como SPSS para el análisis de las encuestas y Taguette para la sistematización de los datos cualitativos obtenidos en las entrevistas.

El cuestionario (Tabla 1) utilizado fue sometido a un proceso de validación mediante juicio de expertos, quienes evalúan la pertinencia de las preguntas en relación con los objetivos del estudio.

Para medir la confiabilidad del instrumento, se aplicó luego de una encuesta previa a 10 estudiantes, el coeficiente alfa de Cronbach, obteniendo un valor superior a 0,932, lo que indicó una alta consistencia interna en las respuestas.

Tabla 1. ***Operacionalización de las variables***

Variable	Dimensión	Preguntas en la Entrevista	Preguntas en la Encuesta (Escala Likert 1-5)
Ciberseguridad en el sector educativo	Tipos de amenazas	¿Qué tipos de ataques cibernéticos han ocurrido en su institución educativa?	¿Ha experimentado problemas de seguridad en plataformas educativas?
	Percepción sobre seguridad digital	¿Cómo evalúa la seguridad de los sistemas informáticos en su institución?	¿Cree que las medidas de seguridad implementadas en su institución son suficientes?
	Capacitación en ciberseguridad	¿Qué tipo de capacitaciones han recibido en ciberseguridad?	¿Recibe capacitación sobre ciberseguridad?
Impacto de amenazas	Acceso a la información	¿Ha habido interrupciones en el acceso a plataformas educativas por ataques cibernéticos?	¿Ha experimentado problemas de acceso a información académica debido a ciberataques?

cibernéticas	Impacto en la continuidad académica	¿Cómo han afectado los ataques cibernéticos la continuidad del aprendizaje en su institución?	¿Cree que los ataques cibernéticos han afectado la calidad de la educación en su institución?
	Percepción de riesgo en el entorno educativo	¿Considera que el nivel de ciberseguridad en su institución es adecuado para proteger la información de estudiantes y docentes?	¿Percibe que su institución está en riesgo de sufrir ataques cibernéticos?

Fuente: Elaboración propia con base en múltiples referencias bibliográficas.

Resultados

Resultados de la Encuesta sobre Ciberseguridad en el Entorno Educativo

Los resultados de la encuesta (Tabla 2) reflejan percepciones mixtas entre los encuestados en cuanto a la seguridad digital y la preparación para enfrentar riesgos cibernéticos en el entorno educativo. En cuanto a los Tipos de amenazas, un 43.3% de los encuestados está de acuerdo en que existen amenazas frecuentes en las plataformas educativas, mientras que un 12.7% está muy de acuerdo. Sin embargo, un 32.0% está en desacuerdo, lo que indica que una parte importante de los estudiantes no percibe estas amenazas o no las considera un problema relevante. Esto sugiere que, aunque una mayoría reconoce la presencia de amenazas cibernéticas, hay un porcentaje considerable que podría estar subestimando la magnitud del riesgo o no es consciente de las amenazas existentes.

En relación con la percepción sobre la seguridad digital, un 34.7% de los encuestados considera que las medidas implementadas son adecuadas, mientras que un 24.0% está muy de acuerdo con esta afirmación, lo que indica que casi el 59% de los participantes confía en la seguridad de sus plataformas educativas. Sin embargo, un 30.0% de los encuestados está en desacuerdo, lo que refleja que una parte significativa de los estudiantes cree que las medidas de seguridad implementadas son insuficientes. Esta división de opiniones resalta la necesidad de reforzar y mejorar las estrategias de protección digital para aumentar la confianza en las medidas de seguridad aplicadas.

En cuanto a la capacitación en ciberseguridad, un 32.0% de los encuestados está de acuerdo en que recibe suficiente capacitación para enfrentar riesgos digitales, y un 30.0% está muy de acuerdo, lo que sugiere que una mayoría moderada considera que la formación en ciberseguridad es adecuada. Sin embargo, un 28.0% está en desacuerdo, lo que indica que una proporción importante considera que la capacitación recibida es insuficiente. Esta percepción refuerza la necesidad de fortalecer los programas de formación para dotar a los estudiantes y al personal de herramientas efectivas para protegerse contra amenazas cibernéticas.

En cuanto al acceso a la información académica, un 37.3% está de acuerdo y un 17.3% está muy de acuerdo en que no han enfrentado problemas de acceso debido a ciberataques. No obstante, un 41.3% está en desacuerdo, lo que indica que una parte significativa de los encuestados ha experimentado dificultades para acceder a la información académica debido a problemas de ciberseguridad. Esta situación destaca la importancia de mejorar la infraestructura tecnológica para garantizar el acceso seguro a los recursos educativos en línea.

Respecto al impacto de los ciberataques en la continuidad académica, un 45.3% está de acuerdo y un 8.0% está muy de acuerdo en que estos ataques han afectado la continuidad de su proceso educativo, lo que indica que más de la mitad de los encuestados reconoce que los ciberataques han tenido un impacto negativo. Sin embargo, un 38.7% está en desacuerdo, lo que refleja que una parte significativa no ha experimentado interrupciones graves debido a ciberataques. Esta discrepancia sugiere que, aunque los ataques cibernéticos afectan a muchos estudiantes, sus efectos pueden no ser uniformes en todas las plataformas o contextos educativos.

En cuanto a la percepción de riesgo en el entorno educativo, un 29.3% de los encuestados está de acuerdo y un 24.0% está muy de acuerdo en que su institución está en riesgo de sufrir ataques cibernéticos, lo que implica que más del 53% de los participantes perciben una vulnerabilidad

potencial. Sin embargo, un 40.7% está en desacuerdo, lo que indica que una parte importante no percibe este riesgo como una amenaza inminente. Esta disparidad en la percepción del riesgo sugiere que es necesario fortalecer la cultura de ciberseguridad dentro de la comunidad educativa y fomentar una mayor conciencia sobre los posibles peligros cibernéticos.

Tabla 2. ***Operacionalización de las variables***

Dimensiones estudiadas	1	2	3	4	5
Tipos de amenazas	6,0%	32,0%	6,0%	43,3%	12,7%
Percepción sobre seguridad digital	9,3%	30,0%	2,0%	34,7%	24,0%
Capacitación en ciberseguridad	10,0%	28,0%	0,0%	32,0%	30,0%
Acceso a la información	3,3%	41,3%	0,7%	37,3%	17,3%
Impacto en la continuidad académica	6,0%	38,7%	2,0%	45,3%	8,0%
Percepción de riesgo en el entorno educativo	4,0%	40,7%	2,0%	29,3%	24,0%

Nota: 1 equivale a muy en desacuerdo y 5 equivale a muy de acuerdo

Correlación de variables

El análisis de correlación (Tabla 3) realizado mediante el Rho de Spearman entre las variables "Ciberseguridad en el sector educativo" y "Impacto de amenazas cibernéticas" revela una relación altamente significativa y positiva. El coeficiente de correlación obtenido es 0.819, lo que indica una correlación positiva muy fuerte entre ambas variables. Esto implica que, a medida que aumenta la percepción de ciberseguridad en el sector educativo, también crece la percepción del impacto que las amenazas cibernéticas pueden tener sobre las plataformas y procesos educativos.

El valor de significancia bilateral (p = 0.000) es menor que 0.01, lo que significa que la relación es estadísticamente significativa al 99% de confianza. Este resultado indica que la probabilidad de que esta correlación haya ocurrido por azar es prácticamente nula, lo que refuerza la solidez de la relación encontrada entre ambas variables.

Además, el análisis se llevó a cabo con una muestra de 150 casos (N = 150), lo que proporciona una base sólida para la interpretación y aumenta la fiabilidad de los resultados obtenidos. La fuerte correlación observada sugiere que una mayor percepción de ciberseguridad en las instituciones educativas está asociada con una mayor conciencia del impacto que pueden tener las amenazas cibernéticas.

Tabla 3. ***Correlación de variables***

Rho de Spearman		Ciberseguridad en el sector educativo	Impacto de amenazas cibernéticas
Ciberseguridad en el sector educativo	Coeficiente de correlación	1,000	,819**
	Sig. (bilateral)		0,000
	N	150	150
Impacto de amenazas cibernéticas	Coeficiente de correlación	,819**	1,000
	Sig. (bilateral)	0,000	
	N	150	150

Nota: La correlación es significativa en el nivel 0,01 (bilateral).

Correlación de las dimensiones

El análisis de correlación (Tabla 4) realizado mediante el Rho de Spearman entre las dimensiones evaluadas en la encuesta sobre ciberseguridad en el ámbito educativo revela una serie de relaciones significativas y moderadamente fuertes entre las variables analizadas. Los resultados reflejan que existe una fuerte relación positiva entre la percepción de amenazas cibernéticas y el impacto en la continuidad académica, con un coeficiente de correlación de 0.781 (p = 0.000). Esto indica que, a medida que los estudiantes perciben un mayor tipo de amenazas, también tienden a reconocer un mayor impacto negativo en la continuidad de su proceso académico. Este hallazgo sugiere que los ataques cibernéticos no solo amenazan la seguridad digital, sino que también afectan directamente la fluidez del aprendizaje y la estabilidad del proceso educativo.

La percepción sobre seguridad digital también muestra una correlación positiva fuerte con la capacitación en ciberseguridad, con un coeficiente de 0.782 (p = 0.000). Esta relación sugiere que los estudiantes que reciben una formación adecuada en ciberseguridad tienden a valorar positivamente las medidas de protección digital implementadas en sus instituciones.

Además, esta percepción positiva de la seguridad digital está relacionada con una menor percepción de riesgo en el entorno educativo, lo que implica que, a medida que los estudiantes adquieren mayores conocimientos en ciberseguridad, son más conscientes de las amenazas, pero también desarrollan una mayor confianza en las medidas adoptadas por su institución para proteger sus sistemas. En cuanto a la capacitación en ciberseguridad, los resultados muestran que también está fuertemente correlacionada con el acceso a la información académica (ρ=0.667, p=0.000).

La percepción de riesgo en el entorno educativo también presenta una correlación significativa con la mayoría de las dimensiones evaluadas, especialmente con la percepción sobre seguridad digital

(ρ=0.714, p=0.000) y la capacitación en ciberseguridad (ρ=0.705, p=0.000). Esto indica que los estudiantes que valoran positivamente la seguridad digital y reciben formación en ciberseguridad tienden a ser más conscientes de los riesgos cibernéticos que enfrenta su institución. Esta percepción de riesgo sugiere que una mayor formación no solo mejora la capacidad de los estudiantes para enfrentar amenazas digitales, sino que también los sensibiliza sobre la necesidad de fortalecer las medidas de protección para evitar vulnerabilidades.

Tabla 4. ***Correlación de las dimensiones de las variables***

Rho de Spearman		Tipos de amenazas	Percepción sobre seguridad digital	Capacitación en ciberseguridad	Acceso a la información	Impacto en la continuidad académica	Percepción de riesgo en el entorno educativo
Tipos de amenazas	Coeficiente de correlación	1,000					
	Sig. (bilateral)						
Percepción sobre seguridad digital	Coeficiente de correlación.	,730**	1,000				

	Sig. (bilateral)	0,000		0,000		
Capacitación en ciberseguridad	Coeficiente de correlación	,623**	,782**	1,000		
	Sig. (bilateral)	0,000	0,000			
Acceso a la información	Coeficiente de correlación.	,701**	,617**	,667**	1,000	
	Sig. (bilateral)	0,000	0,000	0,000		
Impacto en la continuidad académica	Coeficiente de correlación.	,781**	,665**	,621**	,695**	1,000
	Sig. (bilateral)	0,000	0,000	0,000	0,000	
Percepción de riesgo en	Coeficiente de	,672**	,714**	,705**	,577**	,710**	1,000

el entorno educativo	correlación.					
	Sig. (bilateral)	0,000	0,000	0,000	0,000	0,000

Nota: **. La correlación es significativa en el nivel 0,01 (bilateral).

Análisis de Componentes Principales

Conforme al análisis de las dimensiones y al notar que hay más de dos de ellas con una correlación alta, se procedió a hacer el análisis de las cargas factoriales (Tabla 5), que indican cómo cada una de ellas originalmente contribuye a cada uno de los componentes principales (CP), se escogieron 3 componentes que tenían la mayor carga. En este caso:

Tabla 5. ***Cargas de los Componentes***

	Componente			
	1	2	3	Unicidad
Tipos de amenazas	0.352	0.654	0.545	0.1518
Percepción sobre seguridad digital	0.795	0.418	0.313	0.0951
Capacitación en ciberseguridad	*0.842*		0.380	0.0584
Acceso a la información	0.370		*0.850*	0.0589
Impacto en la continuidad académica		*0.766*	0.492	0.1037

	Componente			
	1	2	3	Unicidad
Percepción de riesgo en el entorno educativo	0.529	*0.766*		0.1152

Nota. Se utilizó la rotación ‘varimax’

Análisis de las Cargas Factoriales

Componente 1 (CP1): Está fuertemente relacionado con capacitación en ciberseguridad (0.842) y percepción sobre seguridad digital (0.795). Este componente refleja el nivel de preparación y percepción de seguridad digital, lo que sugiere que la percepción positiva sobre la ciberseguridad está altamente influenciada por la capacitación. CP1 (Capacitación y percepción de seguridad): Explica la mayor parte de la varianza y está relacionado con la capacitación en ciberseguridad y la percepción positiva sobre la seguridad digital.

Componente 2 (CP2): Está asociado principalmente con impacto en la continuidad académica (0.766) y percepción de riesgo en el entorno educativo (0.766). Este componente representa la percepción del impacto que tienen los riesgos cibernéticos en la continuidad del proceso educativo. CP2 (Impacto del riesgo en la continuidad académica): Refleja cómo las amenazas afectan la continuidad del proceso educativo y el nivel de riesgo percibido.

Componente 3 (CP3): Relacionado fuertemente con acceso a la información (0.850) y tipos de amenazas (0.545). Este componente está asociado con problemas en el acceso a la información y la percepción de amenazas cibernéticas. CP3 (Acceso a la información y amenazas): Está vinculado a problemas en el acceso a la información y la percepción de amenazas frecuentes.

Unicidad (Uniqueness)

- Los valores de unicidad reflejan la proporción de varianza de cada variable que no es explicada por los componentes.
- Valores bajos de unicidad indican que la variable está bien explicada por los componentes extraídos.
- En este caso, la mayoría de las variables tienen unicidad baja (por debajo de 0.2), lo que indica que los componentes explican muy bien la varianza de estas variables.

Comprobación de Supuestos

La prueba de Esfericidad de Bartlett arrojó los siguientes resultados:

- Chi-cuadrado (χ^2): 778
- Grados de libertad (gl): 15
- *p*-valor: < 0.001

Interpretación: La prueba de Bartlett indica que la matriz de correlación no es una matriz de identidad, lo que significa que las variables están correlacionadas y son adecuadas para un análisis factorial o PCA.

Un valor de KMO (Tabla 6) superior a 0.80 indica que el modelo es altamente adecuado para el análisis factorial/PCA. Todos los valores individuales también son altos, lo que significa que cada variable tiene una correlación fuerte con el resto de las variables.

Tabla 6. Medida de Idoneidad del Muestreo KMO

	MSA
Global	0.865
Tipos de amenazas	0.868
Percepción sobre seguridad digital	0.827
Capacitación en ciberseguridad	0.811
Acceso a la información	0.887
Impacto en la continuidad académica	0.891
Percepción de riesgo en el entorno educativo	0.929

Nota: Obtenido de la matriz ACP

Análisis Factorial Confirmatorio: Evaluación de la Ciberseguridad y el Impacto de las Amenazas Cibernéticas en el Entorno Educativo

El Análisis Factorial Confirmatorio (AFC) realizado tiene como objetivo validar si las dimensiones evaluadas, relacionadas con la percepción de seguridad digital, capacitación en ciberseguridad, impacto de amenazas y continuidad académica, se ajustan a un modelo teórico previamente planteado. Los resultados obtenidos reflejan que las variables analizadas presentan cargas factoriales elevadas y estadísticamente significativas, lo que sugiere una sólida relación entre los indicadores observados y el factor latente identificado, el cual puede interpretarse como una "Percepción General de la Ciberseguridad y el Impacto de las Amenazas Cibernéticas".

Las cargas factoriales obtenidas muestran que todas las variables tienen una fuerte asociación con el factor identificado, destacándose las siguientes: percepción sobre seguridad digital (1.213) y capacitación en ciberseguridad (1.230), que presentaron los valores más altos. Esto indica que estos dos indicadores son los más influyentes en la percepción global de ciberseguridad en el entorno educativo. Los estudiantes que reciben una formación adecuada en ciberseguridad tienden a desarrollar una percepción más positiva de la seguridad digital y, a su vez, aquellos que valoran positivamente las medidas de seguridad implementadas tienen una menor percepción de riesgo. Por otro lado, frecuencia y tipos de amenazas (1.036), acceso a la información (0.985) y impacto en la continuidad académica (0.988) también presentaron cargas significativas, lo que sugiere que los problemas derivados de ciberataques afectan tanto la percepción de la seguridad como la continuidad del proceso académico. Finalmente, la percepción de riesgo en el entorno educativo (1.081) también mostró una fuerte asociación con el factor identificado, lo que implica que los estudiantes que perciben mayores riesgos tienden a evaluar de manera negativa la seguridad del entorno digital.

La significancia estadística de estas relaciones fue confirmada por los Z-scores elevados (superiores a 11.41) y los valores p menores a 0.001, lo que indica que todas las cargas factoriales son altamente significativas. Además, la prueba de esfericidad de Bartlett arrojó un valor de $\chi^2 = 778$, gl = 15, $p < 0.001$, lo que confirma que la matriz de correlación es significativamente diferente de una matriz identidad, justificando la aplicación del análisis factorial.

La Medida de Adecuación del Muestreo (KMO) presentó un valor global de 0.865, indicando una excelente adecuación del modelo. Los valores individuales de KMO para cada variable también fueron altos, oscilando entre 0.811 y 0.929, lo que sugiere que cada variable tiene una correlación adecuada con el resto de las variables del modelo. Estos valores confirman que el muestreo es

apropiado para el análisis factorial y que los datos analizados son adecuados para extraer factores significativos.

Los resultados del AFC indican que el modelo propuesto es altamente adecuado para explicar la relación entre las dimensiones analizadas, lo que confirma que todas las variables observadas convergen en un único factor latente que representa la percepción general de la ciberseguridad y el impacto de las amenazas cibernéticas. Este modelo sugiere que la percepción de seguridad digital y la capacitación en ciberseguridad son los indicadores más influyentes para determinar cómo los estudiantes evalúan el entorno de seguridad digital en sus instituciones educativas. Además, el impacto de las amenazas cibernéticas sobre la continuidad académica y los problemas de acceso a la información también contribuyen significativamente a esta percepción global.

Resultados de las entrevistas

Las entrevistas realizadas a cinco docentes de la institución educativa permitieron obtener información valiosa acerca de la percepción, experiencia y evaluación de la ciberseguridad en su entorno académico. Los resultados de la entrevista reflejan diversas opiniones y experiencias en relación con los tipos de ataques cibernéticos, la evaluación de la seguridad informática, la capacitación recibida, las interrupciones del acceso a plataformas educativas, el impacto en la continuidad del aprendizaje y la percepción de la efectividad de las medidas de protección de información.

Tipos de Ataques Cibernéticos en la Institución Educativa

Al preguntar sobre los tipos de ataques cibernéticos ocurridos en la institución, los docentes coincidieron en señalar que los incidentes más frecuentes incluyen ataques de phishing, intentos de acceso no autorizado y malware en correos electrónicos dirigidos al personal académico y

administrativo. También mencionaron que, en algunas ocasiones, ataques de denegación de servicio (DDoS) han afectado temporalmente el acceso a las plataformas institucionales, generando interrupciones en las actividades académicas. Estos hallazgos sugieren que la institución ha sido blanco de amenazas cibernéticas comunes en entornos educativos, donde los atacantes buscan vulnerar la seguridad de los sistemas para obtener información confidencial o interrumpir la operatividad de las plataformas.

Evaluación de la Seguridad de los Sistemas Informáticos

En cuanto a la evaluación de la seguridad de los sistemas informáticos, la mayoría de los docentes consideró que, aunque existen medidas de seguridad básicas implementadas, estas no son del todo suficientes para hacer frente a ataques más sofisticados. Algunos docentes expresaron que las plataformas cuentan con firewalls y sistemas de autenticación, pero señalaron que la falta de actualizaciones periódicas y auditorías de seguridad representa una debilidad significativa. Otros mencionaron que la respuesta a incidentes es lenta, lo que incrementa el riesgo de que los ataques tengan un impacto más profundo antes de ser mitigados. Estos resultados sugieren que, aunque la institución ha implementado algunas medidas de protección, existe una percepción generalizada de que la infraestructura de seguridad podría ser más robusta y proactiva.

Capacitación en Ciberseguridad Recibida por los Docentes

Respecto a la capacitación en ciberseguridad, los resultados reflejan una brecha significativa en la formación del personal docente. Solo dos de los cinco docentes entrevistados afirmaron haber recibido capacitaciones formales en temas de ciberseguridad, centradas principalmente en buenas prácticas para la gestión de contraseñas y prevención de phishing. Sin embargo, estos docentes destacaron que la formación fue superficial y poco frecuente, lo que limita su capacidad para

detectar y responder eficazmente a incidentes cibernéticos. Los otros tres docentes afirmaron no haber recibido capacitación alguna o que la formación recibida fue autodidacta, lo que evidencia una falta de programas sistemáticos de formación en ciberseguridad en la institución. Esta situación refuerza la necesidad de implementar programas continuos de capacitación para dotar al personal docente de herramientas efectivas para prevenir y gestionar posibles amenazas digitales.

Interrupciones en el Acceso a Plataformas Educativas

Al abordar la cuestión de interrupciones en el acceso a plataformas educativas debido a ataques cibernéticos, todos los docentes coincidieron en que han ocurrido episodios de interrupción temporal que han afectado el normal desarrollo de las actividades académicas. En la mayoría de los casos, las interrupciones fueron provocadas por ataques de denegación de servicio (DDoS) o errores en la infraestructura tecnológica tras intentos de intrusión. Estas interrupciones, aunque temporales, generaron dificultades para acceder a los materiales educativos y para la entrega de tareas y evaluaciones, afectando el flujo normal del proceso de enseñanza-aprendizaje. Estos hallazgos destacan la necesidad de fortalecer los protocolos de seguridad y mejorar la infraestructura tecnológica para evitar futuras interrupciones.

Impacto de los Ataques en la Continuidad del Aprendizaje

En relación con el impacto de los ataques cibernéticos en la continuidad del aprendizaje, los docentes manifestaron que estos incidentes han tenido un efecto negativo significativo en el proceso educativo. Las interrupciones provocadas por ataques cibernéticos no solo afectaron el acceso a plataformas educativas, sino que también generaron retrasos en la entrega de contenidos, desorganización en la planificación académica y pérdida de información valiosa. Algunos docentes señalaron que la falta de planes de contingencia efectivos hizo que la recuperación de la

continuidad académica fuera más lenta, afectando el rendimiento y la motivación de los estudiantes. Esto evidencia la importancia de establecer planes de contingencia y protocolos de respuesta rápida para mitigar el impacto de los ciberataques en la continuidad académica.

Percepción sobre el Nivel de Ciberseguridad para Proteger la Información

Al consultar sobre si el nivel de ciberseguridad en la institución es adecuado para proteger la información de estudiantes y docentes, las opiniones de los entrevistados fueron mixtas. Si bien algunos docentes consideran que las medidas implementadas son suficientes para mitigar riesgos básicos, la mayoría expresó que la protección de la información sensible sigue siendo vulnerable debido a la falta de actualizaciones frecuentes, monitoreo proactivo y capacitación adecuada. Esta percepción refleja que existen deficiencias en la protección de datos confidenciales, lo que podría exponer la información personal de estudiantes y docentes a riesgos significativos en caso de ataques cibernéticos. Esta situación pone de manifiesto la necesidad de reforzar la protección de datos mediante auditorías de seguridad periódicas, implementación de protocolos avanzados de protección y concienciación del personal sobre las mejores prácticas en ciberseguridad.

Conclusiones y discusión

La identificación de riesgos y vulnerabilidades en entornos digitales educativos permitió establecer que las principales amenazas cibernéticas que enfrentan las instituciones educativas incluyen ataques de phishing, intentos de acceso no autorizado, malware y ataques de denegación de servicio (DDoS). Los resultados de las encuestas a estudiantes revelaron que un 43.3% de los encuestados percibió que las amenazas cibernéticas son frecuentes, mientras que el 32% de los participantes manifestó preocupación por la seguridad de los sistemas informáticos de su institución.

Este hallazgo es consistente con los resultados de las entrevistas a docentes, quienes confirmaron haber experimentado interrupciones en las plataformas educativas debido a ataques DDoS que afectaron la continuidad académica. Estos resultados concuerdan con los hallazgos de Awang et al. (2024), quienes señalaron que las amenazas cibernéticas son una preocupación creciente en el ámbito educativo, especialmente debido al aumento del uso de plataformas digitales para el aprendizaje.

Los resultados del Análisis Factorial Confirmatorio (AFC) corroboraron que la frecuencia de amenazas y la percepción de riesgo cibernético están fuertemente asociadas con el impacto de estas amenazas en la continuidad académica y el acceso a la información (0.7810.7810.781 y 0.6950.6950.695 respectivamente). Este resultado refuerza las conclusiones de Ibrahim et al. (2024), quienes destacaron que la falta de medidas preventivas y de respuesta rápida ante ataques cibernéticos puede generar interrupciones significativas en los procesos de enseñanza-aprendizaje, afectando el rendimiento y la motivación de los estudiantes. La presencia de estos riesgos y

vulnerabilidades indica la necesidad urgente de fortalecer las medidas de protección digital y la capacitación en ciberseguridad para prevenir y mitigar el impacto de las amenazas.

En relación con el nivel de concienciación en ciberseguridad y la efectividad de las medidas de protección implementadas, los resultados reflejan deficiencias significativas en la formación de estudiantes y docentes para enfrentar amenazas cibernéticas. Las encuestas mostraron que solo un 32% de los estudiantes indicó haber recibido formación adecuada en ciberseguridad, mientras que un 28% expresó no haber recibido capacitación alguna o considerarla insuficiente. Este hallazgo fue confirmado por las entrevistas a docentes, donde tres de los cinco entrevistados afirmaron que no han recibido capacitación formal en temas de ciberseguridad, mientras que los otros dos docentes señalaron que la capacitación recibida fue esporádica y poco profunda. Estos resultados coinciden con los hallazgos de Dapitan et al. (2024), quienes encontraron que la falta de capacitación adecuada en ciberseguridad genera brechas significativas en la prevención y respuesta ante incidentes cibernéticos en entornos educativos.

El AFC también corroboró que la capacitación en ciberseguridad tiene una fuerte relación con la percepción de seguridad digital y la mitigación del impacto de amenazas cibernéticas. La carga factorial de esta dimensión (0.8420.8420.842) indica que la capacitación es uno de los factores más influyentes para mejorar la percepción de seguridad digital y reducir la percepción de vulnerabilidad en entornos educativos. Este hallazgo está respaldado por Barletta et al. (2024), quienes argumentan que la formación en ciberseguridad debe ser continua y adaptada a las necesidades del entorno académico para garantizar una respuesta efectiva a las amenazas digitales.

En cuanto al impacto de las amenazas cibernéticas en la continuidad académica, tanto las encuestas como las entrevistas reflejaron que los ataques cibernéticos han tenido efectos significativos en la estabilidad del proceso educativo. Los docentes entrevistados señalaron que las interrupciones en

el acceso a plataformas educativas debido a ataques DDoS generaron retrasos en la entrega de contenidos, evaluaciones y actividades académicas, lo que afectó negativamente la planificación del proceso de

enseñanza-aprendizaje. Este impacto también fue corroborado en el análisis factorial, donde la percepción del impacto en la continuidad académica presentó una carga factorial alta (0.988), lo que confirma que las interrupciones cibernéticas afectan gravemente la continuidad educativa. Estos resultados son consistentes con el estudio de Mohanty et al. (2024), quienes señalaron que las interrupciones tecnológicas causadas por ataques cibernéticos generan desorganización académica y pérdida de información crítica en entornos educativos.

La percepción de riesgo cibernético también emergió como una dimensión clave en la investigación. Las encuestas revelaron que un 29.3% de los estudiantes consideraba que su institución estaba en riesgo de sufrir ataques cibernéticos, mientras que un 40.7% expresó desacuerdo, lo que indica una percepción dividida entre los estudiantes. Los docentes entrevistados también manifestaron que, si bien existen medidas básicas de protección, estas no son suficientes para enfrentar amenazas más sofisticadas, lo que genera una sensación de vulnerabilidad en el entorno educativo. Esta percepción coincide con lo señalado por Prior y Renaud (2024), quienes concluyen que una percepción elevada de riesgo está asociada con la falta de medidas preventivas y la falta de concienciación sobre ciberseguridad en el ámbito educativo.

La interpretación de estos hallazgos permitió diseñar una serie de recomendaciones prácticas orientadas a fortalecer la ciberseguridad en el sector educativo y mejorar la formación en seguridad digital. Los resultados sugieren que es necesario implementar programas de formación continua y

actualizada en ciberseguridad para docentes y estudiantes, con énfasis en la prevención de amenazas cibernéticas y la respuesta eficaz ante incidentes. Estas recomendaciones están alineadas con las propuestas de Ismail et al. (2024), quienes destacan que la integración de contenidos de ciberseguridad en los currículos académicos puede mejorar la preparación de estudiantes y docentes para enfrentar riesgos digitales.

Además, la actualización y monitoreo de los sistemas informáticos debe ser una prioridad para prevenir ataques cibernéticos y mitigar su impacto. La realización de auditorías de seguridad periódicas y el establecimiento de protocolos de contingencia pueden garantizar la continuidad académica en caso de incidentes. Estas acciones coinciden con las recomendaciones de Manganello et al. (2024), quienes sugieren que el monitoreo constante de los sistemas digitales y la implementación de estrategias de mitigación proactivas son esenciales para mejorar la ciberseguridad en entornos educativos.

Los resultados de este estudio reflejan que las instituciones educativas enfrentan riesgos significativos en términos de ciberseguridad, con un impacto directo en la continuidad académica, la percepción de seguridad digital y el acceso a la información. La falta de capacitación continua en ciberseguridad y la insuficiencia de medidas de protección robustas aumentan la vulnerabilidad del entorno educativo frente a amenazas cibernéticas. Por tanto, fortalecer la formación en ciberseguridad, actualizar los sistemas informáticos y establecer protocolos de respuesta y contingencia son acciones esenciales para garantizar un entorno educativo más seguro y resiliente. Estas acciones no solo reducirán la percepción de riesgo, sino que también permitirán mejorar la protección de la información académica y garantizar la continuidad del proceso de enseñanza-aprendizaje.

Implicaciones para Investigaciones Futuras

Los resultados del presente análisis abren la puerta para futuros estudios que puedan validar este modelo en diferentes contextos educativos o evaluar cómo cambian estas percepciones a lo largo del tiempo con la implementación de programas de formación y sensibilización en ciberseguridad. Además, sería valioso realizar un Análisis Factorial Confirmatorio Longitudinal para evaluar el impacto de las intervenciones de ciberseguridad y su efecto en la percepción general de seguridad digital y el manejo del impacto de las amenazas cibernéticas en las instituciones educativas. Con estos resultados, las instituciones pueden tomar decisiones informadas para mejorar la seguridad digital y garantizar la continuidad académica, contribuyendo así a la creación de entornos educativos más seguros y resilientes frente a las amenazas cibernéticas.

Consideraciones Éticas

Para garantizar la ética en la investigación, se implementaron medidas clave. Se obtuvo el consentimiento informado de estudiantes y docentes, explicando el propósito del estudio y asegurando su derecho a retirarse en cualquier momento sin consecuencias. La confidencialidad se garantizó mediante la anonimización de los datos, asignando códigos en lugar de nombres para proteger la identidad de los participantes. Además, la protección de datos se aseguró almacenando la información en servidores seguros, con acceso restringido al equipo de investigación, garantizando así la integridad y privacidad de la información recopilada durante el proceso.

Referencias

Awang, H., Mansor, N. S., Zolkipli, M. F., Malami, S. T. S., Zaini, K. M., & Yau, T. D. (2024). Cybersecurity awareness among special needs students: The role of parental control. *Mesopotamian Journal of CyberSecurity*, *4*(2), 63-73. https://journals.mesopotamian.press/index.php/CyberSecurity/article/view/259

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dute, I., Khan, S., & Parkinson, S. (2024). Cybersecurity Education and Awareness among Parents and Teachers: A Survey of Bahrain. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10559810/

Barletta, V. S., Caruso, F., Di Mascio, T., Greco, F., Islam, T., Rossano, V., & Xiao, H. (2024). CyberSecurity Education for Industry and Academia (CSE4IA 2024). *Proceedings of the 2024 International Conference on Advanced Visual Interfaces*, 1-4. https://doi.org/10.1145/3656650.3660536

Costa, G., De Francisci, S., Renieri, M., & Valiani, S. (2025). Tackling the Gender Gap in Cybersecurity Education. *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, 234-240. https://doi.org/10.1145/3641554.3701807

Dapitan, J. U., Butchayo, J. M. M., Palma, J. L. R., Arevalo, M. A., Alvarico, A. B., & Cuevas Jr, J. F. (2024). Measuring the Level of Cybersecurity Awareness among Senior High School Students. *Mediterranean Journal of Basic and Applied Sciences (MJBAS)*, *8*(2), 208-217. https://mjbas.com/data/uploads/6366.pdf

Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of k-12 cybersecurity education around the world. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10508377/

Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports*, *16*, 100501. https://www.sciencedirect.com/science/article/pii/S2451958824001349

Manganello, F., Earp, J., Fante, C., Bassi, G., Fabbri, S., Matteucci, I., Vaccarelli, A., Olesen, N., De Vibraye, A., & Callaghan, P. (2024). Shaping the foundation of the SuperCyberKids Learning Framework: A comprehensive analysis of cybersecurity education initiatives. *Frontiers in Education*, *9*, 1375853. https://www.frontiersin.org/articles/10.3389/feduc.2024.1375853/full

Mohanty, S. N., Singh, T., Goel, R., Baral, S. K., & Kumar, R. (2024). A study on building awareness in cyber security for educational system in India using interpretive structural modellings. *International Journal of System Assurance Engineering and Management*, *15*(6), 2518-2528. https://doi.org/10.1007/s13198-024-02273-3

Pramod, D. (2024). Gamification in cybersecurity education; a state of the art review and research agenda. *Journal of Applied Research in Higher Education*. https://www.emerald.com/insight/content/doi/10.1108/JARHE-02-2024-0072/full/html

Prior, S., & Renaud, K. (2024). Are UK Parents Empowered to Act on Their Cybersecurity Education Responsibilities? En A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (Vol. 14728, pp. 77-96). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61379-1_6

Radday, E., Mekni, M., Page, L., Sula, A., & Brown, L. (2024). Evolving Cybersecurity Education: An Analysis of the GenCyber Teacher Academy's Progression from 2022 to 2023 and Beyond. *Journal of computing sciences in colleges*, *39*(8). https://par.nsf.gov/biblio/10519497

Santa Barletta, V., Caruso, F., Di Mascio, T., Greco, F., Islam, T., Rossano, V., & Xiao, H. (2024). CyberSecurity Education for Industry and Academia. *17th International Conference on Advanced*

Visual Interfaces AVI2024, 1-4. https://kclpure.kcl.ac.uk/portal/en/publications/cybersecurity-education-for-industry-and-academia

Srivastava, A. K., Singh, A. V., & Som, S. (2024). Critical Analysis of Cybersecurity Awareness Programs in School Education. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=09701052&AN=180918867&h=w%2F%2B9K4zNv8wofEYr5at%2F0tK7pdvWGCNlhbyMsdXgk2YYoRLiNHnRLgsmqfdavFzyZFbbsB%2BsS9ZsV24v3gJ3CA%3D%3D&crl=c

Thomas, M., Elmore, E., Chavez, B., Ruth, R., Avery, C., Cukier, M., & Cateté, V. (2024). Equitable Access to Cybersecurity Education: A Case Study of Underserved Middle School Students. *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, 625-632. https://doi.org/10.1145/3649217.3653581

Williams, T., & Daugherty, J. (2024). *The State of Cybersecurity Programs in High Schools: A Case Study Analysis of Their Development, Sustainment, and Inclusiveness*. https://aisel.aisnet.org/hicss-57/sj/stem/3/