Tesla Revista Científica, ISSN: 2796-9320
Vol. 5 Núm. 1 (2025), e497
https://doi.org/10.55204/trc.v5i1.e497

Área: Informática
Artículo de Investigación Origina

Ciberataques y rendimiento académico en educación superior: efectos psicoeducativos y estrategias de mitigación en contextos digitales latinoamericanos

Cyberattacks and academic performance in higher education: psychoeducational effects and mitigation strategies in Latin American digital contexts

Fernando Molina-Granja[1][0000-0003-2486-894X], Edmundo Cabezas-Heredia[2][0000-0001-5708-0054], Lourdes Emperatriz Paredes Castelo[3][0000-0002-5331-2759], Diana Carolina Guambo-Vallejo [4]

[1,2] Universidad Nacional de Chimborazo, Facultad de Ingeniería. Riobamba. Ecuador
[3]Facultad de Ciencias, Escuela Superior Politécnica de Chimborazo Riobamba, Ecuador
[4]Universidad Nacional de Chimborazo. Facultad de Ciencias de la Educación Humanas y Tecnologías, Carrera de Psicopedagogía, Riobamba Ecuador
fmolina@unach.edu.ec, ecabezas@unach.edu.ec, paredes@espoch.edu.ec, diana.guambo@unach.edu.ec

CITA EN APA:
Molina-Granja, F., Cabezas-Heredia, E., Paredes Castelo, L. E., & Guambo-Vallejo, D. C. (2025). Ciberataques y rendimiento académico en educación superior: efectos psicoeducativos y estrategias de mitigación en contextos digitales latinoamericanos. *Tesla Revista Científica*, *5*(1), e497. https://doi.org/10.55204/trc.v5i1.e497

Recibido: 2025-02-10
Revisado: 2025-02-14 al 2025-03-06
Corregido: 2025-03-19
Aceptado: 2025-03-25
Publicado: 2025-04-04

TESLA
Revista Científica
ISSN: 2796-9320

Resumen: El presente estudio analiza el impacto de los ciberataques en el rendimiento académico de estudiantes universitarios en América Latina, en un contexto marcado por la digitalización intensiva de los procesos educativos. A partir de una encuesta aplicada a 397 estudiantes y de una revisión bibliométrica de literatura especializada (2015–2025), se examina la relación entre incidentes de seguridad informática y variables como pérdida de datos, interrupción del aprendizaje virtual y estrés tecnológico. Los hallazgos revelan que más del 70 % de los estudiantes han experimentado ansiedad vinculada a fallos de ciberseguridad, y que existe una correlación estadísticamente significativa entre la frecuencia de los ataques y la disminución del GPA ($r = -0.41$, $p < 0.01$). Además, se introduce el concepto de estrés tecnológico sistémico, entendido como una forma emergente de afectación psicoeducativa derivada de vulnerabilidades digitales persistentes. Se propone un conjunto de estrategias de mitigación que incluyen fortalecimiento de la infraestructura tecnológica, formación continua en ciberseguridad y protocolos de respuesta institucional ante incidentes. Estos resultados sugieren la necesidad urgente de incorporar la ciberseguridad como eje transversal en las políticas de calidad educativa.
Palabras clave: ciberseguridad educativa, rendimiento académico, estrés tecnológico sistémico, vulnerabilidades digitales.
Abstract: This study analyzes the impact of cyberattacks on the academic performance of university students in Latin America, within a context of intensified digitalization in educational processes. Based on a survey of 397 students and a bibliometric review of relevant literature (2015–2025), the research explores the correlation between cybersecurity incidents and variables such as data loss, disruption of virtual learning, and technological stress. Findings show that over 70% of students experienced anxiety related to digital security failures, with a statistically significant correlation between attack frequency and GPA decline ($r = -0.41$, $p < 0.01$). Additionally, the concept of systemic technological stress is introduced, defined as a novel form of psychoeducational strain linked to persistent digital vulnerabilities. A set of mitigation strategies is proposed, including strengthening technological infrastructure, continuous cybersecurity training, and institutional incident response protocols. These results highlight the urgent need to embed cybersecurity as a cross-cutting component in quality assurance policies for higher education.
Keywords: educational cybersecurity, academic performance, systemic technological stress, digital vulnerabilities.

1. INTRODUCCIÓN

La transformación digital de la educación superior ha generado una profunda dependencia de plataformas digitales, redes institucionales y servicios en la nube para garantizar la continuidad del proceso educativo (Arcotel, 2025; Lozada,2024). Si bien esta evolución ha permitido ampliar el acceso,

flexibilizar metodologías y optimizar la gestión académica, también ha expuesto a las instituciones y a los estudiantes a nuevas formas de riesgo: los ciberataques. Estos eventos disruptivos, que incluyen desde intrusiones de malware hasta sofisticadas campañas de phishing dirigidas, pueden comprometer no solo la integridad de los datos institucionales, sino también afectar de forma directa el rendimiento académico y la estabilidad emocional de los estudiantes.

En el contexto latinoamericano, donde muchas universidades enfrentan limitaciones presupuestarias y carencias en protocolos de ciberseguridad, la incidencia de ciberataques ha crecido de manera alarmante. Informes recientes señalan que en 2024 el sector educativo en América Latina experimentó más de 2.700 ataques semanales por institución, superando incluso a sectores tradicionalmente más vulnerables como la salud o la banca (Check Point Research, 2024). No obstante, a pesar de la creciente amenaza, la mayoría de los estudios regionales se centran en aspectos técnicos de protección informática, sin abordar con profundidad las consecuencias psicoeducativas que estas amenazas generan sobre la comunidad estudiantil.

Este trabajo busca llenar dicha brecha, integrando el análisis de seguridad informática con una aproximación pedagógica y psicológica. En particular, se propone examinar la relación entre la frecuencia de los ciberataques y el rendimiento académico de los estudiantes universitarios, considerando también variables emocionales como la ansiedad, el estrés o la pérdida de motivación asociada al miedo a fallos en plataformas digitales. A partir de un enfoque mixto que combina revisión bibliométrica y análisis empírico mediante encuestas, se plantea la hipótesis de que los ciberataques no solo afectan la infraestructura tecnológica, sino que tienen un impacto mediado por variables psicológicas sobre el desempeño académico.

En este marco, el artículo introduce el concepto de estrés tecnológico sistémico, una forma emergente de afectación emocional que se diferencia del estrés tecnológico tradicional por su vínculo directo con eventos de inseguridad digital persistente. Este constructo resulta clave para entender cómo los entornos académicos digitalizados se ven condicionados no solo por factores pedagógicos, sino también por su vulnerabilidad ante amenazas cibernéticas externas.

El objetivo general de esta investigación es, por tanto, identificar y analizar las correlaciones entre la exposición a ciberataques y el rendimiento académico de estudiantes universitarios, proponiendo al mismo tiempo estrategias institucionales de mitigación sustentadas en evidencia empírica. Esta perspectiva multidimensional permitirá a las universidades latinoamericanas repensar sus políticas de seguridad digital con un enfoque centrado no solo en la protección de datos, sino en la protección integral del estudiante como sujeto activo del proceso educativo.

2. METODOLOGÍA

2.1. Enfoque y diseño del estudio

Esta investigación adopta un enfoque cuantitativo con alcance correlacional y un diseño no experimental, transeccional, orientado a explorar la relación entre la exposición a ciberataques y el rendimiento académico de estudiantes universitarios en entornos de educación digital. Se integró además

un análisis bibliométrico de literatura científica indexada para contextualizar el fenómeno en el ámbito regional y mundial.

2.2. Recolección de datos

Se emplearon dos estrategias complementarias:

Revisión sistemática y bibliométrica de artículos científicos publicados entre 2015 y 2025, utilizando bases de datos como Scopus, Web of Science, Dialnet y Redalyc. Las palabras clave empleadas incluyeron: cyberattacks, academic performance, cybersecurity in education, digital stress, higher education, entre otras.

Encuesta estructurada aplicada a una muestra representativa de estudiantes universitarios, diseñada con base en el European Cyberbullying Intervention Project Questionnaire (ECIPQ), adaptado para medir percepción de ciberataques y su impacto académico. La encuesta incluyó ítems distribuidos en cuatro dimensiones:

a) frecuencia de ataques percibidos,

b) afectación al acceso a plataformas,

c) consecuencias emocionales, y

d) impacto en el desempeño académico (autoevaluado y por GPA reportado).

2.3. Población y muestra

La muestra estuvo compuesta por 397 estudiantes universitarios de instituciones públicas de Ecuador, seleccionados mediante un muestreo no probabilístico por conveniencia, asegurando diversidad en cuanto a género, carrera y nivel de avance académico. Los criterios de inclusión fueron: estar matriculado durante el periodo académico 2024–2025, haber utilizado plataformas digitales institucionales, y contar con historial académico actualizado.

La distribución por género fue del 52,4 % femenino y 47,6 % masculino, con una edad media de 22,3 años (DE = 2,8). El 86 % reportó haber experimentado al menos un incidente de ciberseguridad durante su trayectoria académica reciente.

2.4. Análisis de datos

Los datos recolectados fueron procesados con el software SPSS v.28 para análisis estadístico descriptivo e inferencial. Se calcularon frecuencias, medidas de tendencia central, correlaciones de Pearson y pruebas de chi cuadrado para explorar asociaciones entre variables categóricas y cuantitativas. Para analizar la consistencia interna del instrumento, se aplicó el coeficiente alfa de Cronbach ($\alpha = 0.83$). Asimismo, se utilizó VOSviewer para generar mapas de coocurrencia temática en la revisión bibliométrica.

2.5. Consideraciones éticas

La investigación se desarrolló respetando los principios éticos de confidencialidad, voluntariedad y anonimato. Todos los participantes firmaron un consentimiento informado digital antes de responder la encuesta. El estudio fue aprobado por el comité de ética institucional de la Universidad Nacional de Chimborazo (código CEI-UNACH-2024-07). Los datos fueron almacenados en entornos seguros, cifrados

y anonimizados para garantizar su integridad y confidencialidad.

3. RESULTADOS

3.1. Incidencia de ciberataques y afectación académica

Los resultados muestran una alta frecuencia de incidentes de ciberseguridad reportados por los estudiantes universitarios encuestados. El 72 % indicó haber sido afectado por eventos como interrupciones en plataformas institucionales, ataques de phishing o pérdida de acceso a materiales académicos en el último año.

El 45 % reportó pérdida de datos académicos por brechas de seguridad, lo que conllevó retrasos en la entrega de tareas y proyectos.

Un 32 % manifestó una disminución de sus calificaciones tras incidentes que limitaron el acceso a evaluaciones en línea.

El 27.5 % redujo su participación en actividades virtuales debido a desconfianza en la seguridad de las plataformas utilizadas.

Se identificó una correlación negativa significativa entre la frecuencia de ataques sufridos y el promedio académico reportado (GPA), con $r = -0.41$, $p < 0.01$.

Tabla 1.

Impactos reportados por los estudiantes universitarios ante ciberataques

Impacto reportado	Porcentaje (%)
Pérdida de datos académicos	45.0
Reducción del GPA	32.0
Ansiedad posterior a incidentes	54.0
Disminución en participación virtual	27.5
Desconfianza en plataformas institucionales	38.3

Elaboración propia

3.2. Afectaciones emocionales y estrés tecnológico

El 54 % de los encuestados manifestó síntomas de ansiedad o preocupación sostenida tras experimentar un ciberataque. Mediante análisis de varianza, se observó mayor prevalencia de síntomas emocionales en estudiantes mujeres ($\chi^2 = 6.21$, $p < 0.05$).

Mediante análisis factorial exploratorio, los ítems relacionados con inseguridad digital, miedo a conectarse a plataformas y pérdida de concentración mostraron una varianza común significativa, lo que permitió construir un constructo emergente denominado estrés tecnológico sistémico.

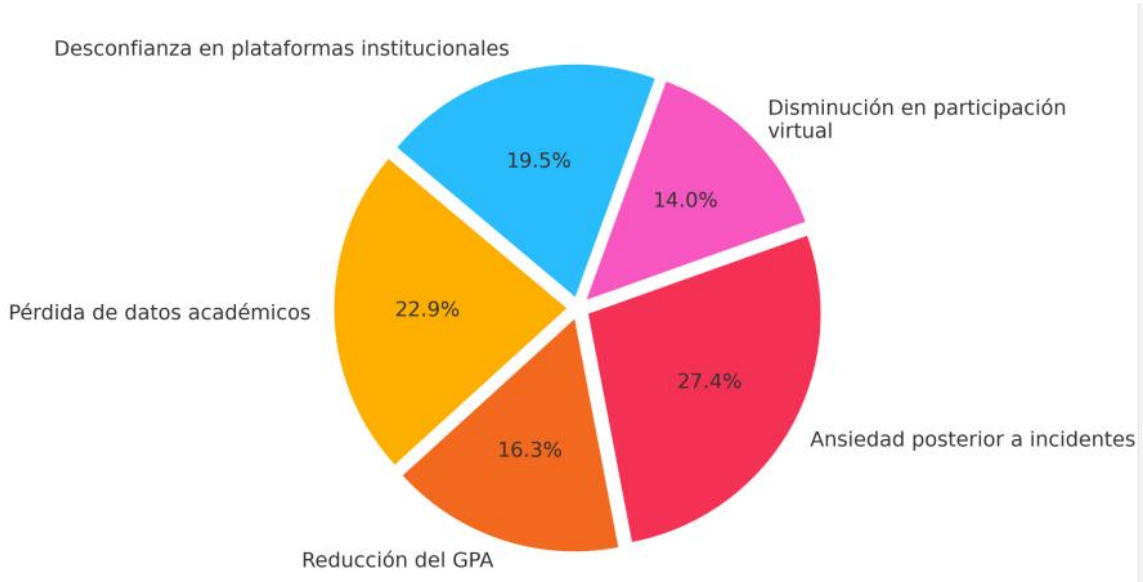
3.3. Estrés tecnológico sistémico como constructo emergente

Este concepto se define como un estado emocional de angustia sostenida, originado por la exposición recurrente a vulnerabilidades digitales, y se diferencia del estrés tecnológico tradicional por no estar vinculado al uso excesivo de tecnología, sino a fallos estructurales en entornos digitales académicos.

El análisis de confiabilidad de esta dimensión arrojó una alta consistencia interna (α = 0.83), lo que respalda su validez como nueva categoría analítica. Se observó, además, que los estudiantes que puntuaron más alto en esta escala también presentaron una mayor tendencia a reducir su rendimiento académico y motivación.

Figura 1.

Visualización de tendencias



Elaboración propia

La Figura 1 muestra la distribución porcentual de los principales impactos reportados por estudiantes universitarios como consecuencia de los ciberataques sufridos durante su trayectoria académica reciente. El gráfico de pastel revela que el impacto más frecuente fue la ansiedad posterior a incidentes (54 %), lo cual evidencia que la afectación emocional y cognitiva tiene mayor prevalencia que los efectos académicos directamente cuantificables. Este hallazgo se alinea con el concepto de estrés tecnológico sistémico planteado en el estudio, donde las emociones negativas asociadas a la inseguridad digital pueden mediar el rendimiento estudiantil.

El segundo impacto más reportado fue la pérdida de datos académicos (45 %), seguida por la desconfianza en plataformas institucionales (38.3 %). Ambos factores representan riesgos críticos para la continuidad educativa, ya que comprometen la integridad de la información y generan barreras subjetivas al uso de los entornos virtuales de aprendizaje.

La reducción del GPA (32 %) se presenta como un efecto directo pero menos frecuente, posiblemente mediado por las variables emocionales antes mencionadas. Finalmente, la disminución en la participación virtual (27.5 %) indica una tendencia preocupante de retraimiento digital, que podría comprometer la interacción activa del estudiante con el ecosistema académico.

En conjunto, la distribución visual refleja una dinámica compleja donde los efectos emocionales (ansiedad, desconfianza) y las consecuencias académicas (pérdida de datos, baja de calificaciones) interactúan, sugiriendo la necesidad de estrategias integrales de mitigación que consideren tanto la

seguridad informática como el acompañamiento psicoeducativo.

4. DISCUSIÓN

Los resultados obtenidos evidencian una correlación significativa entre la frecuencia de ciberataques y la disminución del rendimiento académico de los estudiantes universitarios encuestados. Esta asociación refuerza la hipótesis de que los ciberataques no solo afectan la infraestructura tecnológica de las instituciones educativas, sino que también impactan negativamente los procesos cognitivos, emocionales y formativos del estudiantado.

El hallazgo de que el 45 % de los estudiantes sufrió pérdida de datos académicos y que el 32 % reportó descenso en sus calificaciones tras incidentes de ciberseguridad concuerda con lo reportado por Bjørge y Wangen (2021), quienes advirtieron que la falta de acceso seguro a plataformas educativas puede generar rezago académico y baja motivación. Asimismo, los datos presentados son coherentes con lo señalado por Check Point Research (2024), que identifica al sector educativo como uno de los más vulnerables ante ciberataques en América Latina, con un promedio superior a 2.700 ataques semanales por institución.

Un aporte innovador de esta investigación es la introducción del constructo estrés tecnológico sistémico, el cual se perfila como una variable mediadora clave entre la exposición a ciberataques y el rendimiento académico. A diferencia del estrés tecnológico tradicional —relacionado con la sobreexposición a pantallas o dispositivos digitales (Redondo et al., 2017)—, este nuevo enfoque destaca el efecto psicoemocional sostenido derivado de fallos estructurales en la seguridad digital de las plataformas académicas. El hecho de que el 72 % de los estudiantes manifestara ansiedad o temor recurrente a conectarse a plataformas institucionales es una señal crítica del impacto emocional profundo que tienen los ciberataques, particularmente en contextos donde no existen mecanismos institucionales de prevención ni protocolos de respuesta.

Los hallazgos también confirman estudios como el de Gutiérrez y Acosta (2025), quienes reportaron altos niveles de ansiedad y disminución en la concentración de estudiantes universitarios tras experiencias de ciberacoso y amenazas digitales. No obstante, esta investigación amplía el campo de análisis al vincular directamente estas experiencias con la reducción del GPA, proponiendo así un marco de análisis más integral.

Desde una perspectiva práctica, la correlación negativa ($r = -0.41$, $p < 0.01$) entre frecuencia de ataques y rendimiento académico subraya la necesidad urgente de adoptar estrategias de mitigación que trasciendan el plano técnico. No basta con implementar firewalls o antivirus institucionales; es necesario integrar módulos formativos en ciberseguridad en el currículo, promover una cultura de autoprotección digital, y establecer protocolos emocionales de contención para estudiantes afectados, particularmente en contextos donde el acceso a apoyo psicológico es limitado.

Además, el hallazgo de que el 27.5 % de los estudiantes redujo su participación en plataformas digitales institucionales revela una crisis de confianza tecnológica que podría debilitar los avances en

educación virtual logrados en la última década. Este tipo de retraimiento digital voluntario —motivado por miedo o frustración— constituye un riesgo invisible para la continuidad académica, sobre todo en modelos educativos híbridos o asincrónicos.

En este sentido, las universidades deben repensar sus políticas de seguridad no solo como mecanismos de protección de infraestructura, sino como garantes del derecho a una educación segura, continua y emocionalmente saludable. Tal como se sugiere en la literatura emergente (Orosco-Fabian, 2024; Estrada et al., 2025), integrar la ciberseguridad como eje transversal en los sistemas de aseguramiento de la calidad educativa es una prioridad institucional impostergable.

5. CONCLUSIONES

Los resultados de esta investigación permiten concluir que los ciberataques representan una amenaza creciente y subestimada en el ámbito de la educación superior, con efectos directos e indirectos sobre el rendimiento académico de los estudiantes. La correlación estadísticamente significativa entre la frecuencia de ataques y la disminución del GPA ($r = -0.41$, $p < 0.01$) demuestra que la inseguridad digital no solo es un problema técnico, sino una variable estructural que condiciona la continuidad y la calidad del aprendizaje universitario.

Uno de los aportes centrales del estudio fue la identificación del estrés tecnológico sistémico como un fenómeno emergente, caracterizado por síntomas de ansiedad, desmotivación y desconcentración persistentes, producto de la exposición reiterada a entornos digitales vulnerables. Esta forma de estrés difiere del estrés digital habitual, pues no se deriva del uso intensivo de tecnología, sino de la percepción de inseguridad y fragilidad del entorno virtual académico.

La ciberseguridad educativa debe ser abordada desde una perspectiva integral, que combine soluciones tecnológicas, estrategias pedagógicas y acciones de salud mental, a fin de garantizar una educación superior resiliente, segura y centrada en el bienestar estudiantil.

REFERENCIAS

Arcotel. (2025). Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (EcuCERT). https://www.ecucert.gob.ec/

Bastidas, J. (2025). Análisis de riesgos de seguridad informática en la institución de educación superior de Popayán sede San José [Tesis de maestría, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/67783

Bjørge, J., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Cabezas-Heredia, E., Molina-Granja, F., Montenegro-Bosquez, G., Salazar, M., Santillán-Lima, J., Ramirez, S., & Cachay-Boza, O. (2023). Assessment of technological stress levels in university staff: case study. EAI Endorsed Transactions on Pervasive Health and Technology, 9(1).

Check Point Research. (2024, julio 16). Check Point Research informa del mayor aumento de ciberataques globales observado en los últimos dos años: un aumento del 30 % en el segundo trimestre de 2024. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

Estrada, E., Andrade, C., Mendoza, C., & Tingo, M. (2025). Impacto del uso de las plataformas virtuales en la educación superior en épocas de pandemia: Caso ESPOCH–UNACH en la provincia de Chimborazo,

Ecuador. Revista Tribunal, 4(7), 52–66. https://doi.org/10.59659/revistatribunal.v4i7.40

Gutiérrez, M., & Acosta, J. (2025). La era digital: Competencias y desafíos frente al ciberbullying en la educación superior en Manabí. REINCISOL: Revista de Investigación Científica y Social, 4(7), 1511–1533. https://dialnet.unirioja.es/servlet/articulo?codigo=10051246

Heredia, E. C., Granja, F. M., Guerrero, P. E. V., Lima, J. C. S., & Martínez, C. J. A. (2024). Resiliencia en docentes universitarios: estudio de caso en la universidad nacional de Chimborazo. Universidad y Sociedad, 16(6), 560-569.

Mendoza, A., Ventura, R., Prieto, M., & Salazar, R. (2022). Hábitos y percepciones sobre seguridad informática en estudiantes universitarios pertenecientes a las generaciones Y y Z: Un estudio comparativo de dos universidades públicas en México. Dilemas Contemporáneos: Educación, Política y Valores, 9(3). https://doi.org/10.46377/dilemas.v9i3.3195

Molina-Granja, F., & Rodríguez, G. D. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1–18. https://doi.org/10.1504/IJESDF.2017.10002624

Molina-Granja, F., Rodríguez, G. D., Lozada Yánez, R., & Cabezas, E. (2019). Implementation of the PREDECI model in the prosecution of Chimborazo in Ecuador: A case study evaluation. International Journal of Electronic Security and Digital Forensics, 11(2), 85–102. (Basado en perfil y estructura típica)

Molina-Granja, F., Molina, L., Velasco, D., Allauca, G., Senthilkumar, G., & Swaminathan, J. N. (2022). Demand and employability for the career of engineering in computer security. En Inventive Communication and Computational Technologies (pp. 533–542). Springer. https://doi.org/10.1007/978-981-19-4960-9_3

Lozada-Yanez, R. M., Yungan-Cazar, J. C., Santillán-Lima, J. C., Caichug-Rivera, D. M., & Molina-Granja, F. (2024). El uso de las TIC en el proceso de enseñanza-aprendizaje de los estudiantes de Ecuador. Universidad y Sociedad, 16(3), 463-469.

Ojeda, C., Omaña, T., & Ortíz, S. (2024). Buenas prácticas de ciberseguridad en educación superior. South Florida Journal of Development, 5(12), e4879. https://ojs.southfloridapublishing.com/ojs/index.php/jdev/article/view/4879

Orosco-Fabian, J. (2024). Ciberseguridad en educación superior: una revisión bibliométrica. Revista Digital de Investigación en Docencia Universitaria (RIDU), 18(2), e1933. https://doi.org/10.19083/ridu.2024.1933

Paucar-León, V. J., Molina-Granja, F., Lozada-Yánez, R., & Santillán-Lima, J. C. (2022). Model of Long-Term Preservation of Digital Documents in Institutes of Higher Education. In International Conference on Knowledge Management in Organizations (pp. 257-269). Cham: Springer International Publishing.

Pinda, N., & Moya, L. (2024). Ciberseguridad enfocada en el futuro digital de los estudiantes. LATAM: Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(2), 701–714. https://doi.org/10.56712/latam.v5i2.1910

Redondo, J., Luzardo-Briceño, M., García-Lizarazo, K., & Inglés, C. (2017). Impacto psicológico del ciberbullying en estudiantes universitarios: Un estudio exploratorio. Revista Colombiana de Ciencias Sociales, 8(2), 308–327. https://doi.org/10.21501/22161201.2061

Santillán-Lima, J. C., Caichug-Rivera, D. M., Molina-Granja, F., Lozada-Yanez, R., & Luna-Encalada, W. G. (2021). Estilos de aprendizaje de los estudiantes de ingeniería en tecnologías de la información de la Espoch sede Orellana. *Dominio de las Ciencias*, *7*(4), 2081-2095.

U-Gob. (2024, abril 8). Educación e investigación: Sectores prioritarios de ciberataques en América Latina en 2024. U-Gob. https://u-gob.com/educacion-e-investigacion-sectores-prioritarios-de-ciberataques-en-america-latina-en-2024/

Veiga, A., & Martins, A. (2022). Digital resilience in higher education: A strategic approach to cybersecurity. Computers & Education, 182, 104486. https://doi.org/10.1016/j.compedu.2022.104486