Artículo de Investigación Original

Ciberseguridad en la educación superior: evaluación y estrategias de formación

Cybersecurity in Higher Education: Assessment and Training Strategies

Víctor Guido Jiménez Sánchez [1] [0009-0003-7263-3392], Robinson Israel Tipanluisa Masabanda [2] [0009-0008-0971-660X] , Carlos Javier León Espinoza [3] [0009-0004-4828-8055]

[1] Investigador Independiente, Quito, Ecuador. vicojims@hotmail.com
[2] Investigador Independiente, Latacunga, Ecuador. itipanluisa95@gmail.com
[3] Investigador Independiente, Machala, Ecuador. carlosjleone@gmail.com

CITA EN APA:

Jiménez Sánchez, V. G., Tipanluisa Masabanda, R. I., & León Espinoza, C. J. (2025). Ciberseguridad en la educación superior: evaluación y estrategias de formación. *Technology Rain Journal*, *4*(2) https://doi.org/10.55204/trj.v4i1.e94

Recibido: 27 de abril del 2025
Aceptado: 12 de junio del 2025
Publicado: 01 de septiembre del 2025

Technology Rain Journal
ISSN: 2953-464X

Resumen. La ciberseguridad se ha convertido en un componente esencial para garantizar la integridad, disponibilidad y confidencialidad de la información en la educación superior. Las universidades, al gestionar grandes volúmenes de datos sensibles y plataformas digitales de enseñanza e investigación, se han transformado en objetivos prioritarios para los ciberdelincuentes. Este artículo presenta una revisión bibliográfica estructurada sobre la situación de la ciberseguridad en instituciones de educación superior en América Latina, identificando brechas, estrategias nacionales y buenas prácticas institucionales. Los resultados revelan que persisten vulnerabilidades críticas vinculadas a la falta de recursos, la escasez de personal especializado y la baja conciencia digital entre estudiantes y docentes. Asimismo, se observa una notable heterogeneidad en las políticas de ciberseguridad regionales: mientras Chile y Colombia avanzan con marcos normativos inclusivos y robustos, otros países muestran rezagos significativos. En cuanto a las universidades, la adopción de manuales de seguridad, la autenticación multifactor, la creación de centros de respuesta a incidentes (CSIRT) y programas de sensibilización se consolidan como prácticas efectivas, aunque aún limitadas en sostenibilidad. Se concluye que la ciberseguridad universitaria requiere un enfoque integral que articule políticas nacionales, estándares internacionales, formación transversal y cooperación interinstitucional.
Palabras Clave: Ciberseguridad, educación superior, formación digital, buenas prácticas, políticas institucionales..

Abstract: Cybersecurity has become an essential component to ensure the integrity, availability, and confidentiality of information in higher education. Universities, as managers of large volumes of sensitive data and digital teaching and research platforms, have increasingly become prime targets for cybercriminals. This article presents a structured literature review on the state of cybersecurity in higher education institutions in Latin America, identifying gaps, national strategies, and institutional best practices. The results show persistent critical vulnerabilities related to limited financial resources, lack of specialized personnel, and low digital awareness among students and faculty. Likewise, there is notable heterogeneity in regional cybersecurity policies: while Chile and Colombia have advanced with inclusive and robust regulatory frameworks, other countries show significant delays. At the institutional level, the of university incident response teams (CSIRT), and awareness programs are consolidated as effective practices, although still limited in sustainability. It is concluded that university cybersecurity requires a comprehensive approach that integrates national policies, international standards, transversal training, and inter-institutional cooperation.
Keywords: Cybersecurity, higher education, digital training, best practices, institutional policies.

1. INTRODUCCIÓN

En el contexto de la sociedad digital contemporánea, la ciberseguridad se ha convertido en un eje estratégico para el funcionamiento de las instituciones de educación superior. Las universidades, al ser espacios de generación y gestión de conocimiento, manejan grandes volúmenes de información sensible de estudiantes, docentes, investigaciones y procesos administrativos, lo que las convierte en objetivos altamente atractivos para los ciberdelincuentes (Aguilar et al., 2024). Entre las amenazas más frecuentes destacan el phishing, el ransomware, los ataques de denegación de servicio y la ingeniería social, los cuales pueden comprometer tanto la continuidad académica como la reputación institucional (Singh et al., 2021).

La literatura reciente evidencia que, en América Latina, las instituciones educativas enfrentan limitaciones significativas para implementar políticas robustas de ciberseguridad. Factores como la escasez de recursos, la falta de personal especializado y la baja conciencia digital de los usuarios son elementos críticos que debilitan la protección de la infraestructura tecnológica (González et al., 2023; Tiglla Tumbaico, 2024). Países como Chile y Colombia han mostrado avances normativos y estratégicos, mientras que otros permanecen rezagados, lo que profundiza la brecha regional en materia de resiliencia cibernética (Urbanovics & Guajardo, 2022).

En el ámbito formativo, diversos estudios han identificado una carencia notable de programas sistemáticos de capacitación en ciberseguridad para estudiantes universitarios. Esto genera vulnerabilidades que trascienden el plano académico y repercuten en el desempeño profesional futuro de los egresados (Suárez et al., 2021). Frente a este desafío, iniciativas como el uso de plataformas educativas basadas en metodologías lúdicas —por ejemplo, los “Capture The Flag” (CTF)— han demostrado ser herramientas innovadoras para desarrollar competencias prácticas en seguridad digital (Suárez et al., 2021; Newhouse et al., 2021).

Asimismo, se ha subrayado la necesidad de promover una cultura institucional de seguridad digital que trascienda lo meramente técnico e incorpore principios éticos, de privacidad y de inclusión (Herrera, 2020; Fonfría & Duch-Brown, 2020). En este sentido, la formación en ciberseguridad no solo debe centrarse en aspectos técnicos, sino también en la construcción de competencias críticas que permitan a los futuros profesionales reconocer y mitigar riesgos, garantizar la protección de datos y contribuir a entornos académicos más seguros y resilientes (Edwards, 2024).

Por tanto, el presente artículo tiene como objetivo evaluar el estado actual de la ciberseguridad en la educación superior e identificar estrategias formativas eficaces que fortalezcan las capacidades institucionales y el aprendizaje de los estudiantes. A través de una revisión bibliográfica se busca

establecer un marco que integre tanto las buenas prácticas como las políticas emergentes, con el fin de orientar la consolidación de una cultura de ciberseguridad en las universidades latinoamericanas.

2. MARCO TEÓRICO

2 1. Conceptos fundamentales de ciberseguridad

La ciberseguridad puede entenderse como el conjunto de políticas, prácticas y tecnologías destinadas a garantizar la confidencialidad, integridad y disponibilidad de la información, principios que constituyen el conocido triángulo CIA (Confidentiality, Integrity, Availability) (Stallings, 2018). Estos tres ejes representan la base sobre la cual se construyen las estrategias de seguridad en cualquier entorno digital.

Figura 1.- Ciberseguridad en la Educación Superior

En el contexto de la educación superior, la ciberseguridad adquiere una relevancia particular, ya que las universidades almacenan y gestionan no solo datos personales de estudiantes y docentes, sino también investigaciones científicas, convenios internacionales y recursos financieros (Aguilar et al., 2024). La protección de esta información es fundamental para mantener la confianza institucional y salvaguardar la continuidad de los procesos académicos y administrativos.

Diversos autores señalan que la ciberseguridad trasciende la dimensión técnica, pues implica también un enfoque organizacional, ético y legal. Por ejemplo, Fonfría y Duch-Brown (2020) sostienen que una política de ciberseguridad efectiva debe integrar factores socioeconómicos y culturales, además de los tecnológicos, ya que los ataques no solo buscan vulnerar sistemas, sino también explotar debilidades humanas y normativas.

En este sentido, el factor humano constituye tanto la primera línea de defensa como la mayor vulnerabilidad. Estudios recientes destacan que la mayoría de los incidentes de seguridad están relacionados con errores humanos, como el uso de contraseñas débiles, la falta de actualización de software o la apertura de correos fraudulentos (Yadav & Gupta, 2021). Por ello, la formación y concienciación de los usuarios finales se considera tan relevante como la implementación de soluciones técnicas avanzadas.

Asimismo, el desarrollo de la ciberresiliencia emerge como concepto complementario a la ciberseguridad. Mientras que la ciberseguridad busca prevenir y mitigar incidentes, la ciberresiliencia se orienta a garantizar la capacidad de una organización para resistir, recuperarse y adaptarse ante un ataque exitoso (Maan, 2021). En el ámbito universitario, esto implica no solo disponer de sistemas de respaldo y planes de continuidad académica, sino también fomentar una cultura institucional que responda de manera coordinada ante las crisis digitales.

Finalmente, el campo de la ciberseguridad se encuentra en constante evolución debido a la aparición de tecnologías emergentes como la inteligencia artificial, el internet de las cosas (IoT) y el blockchain. Estas tecnologías ofrecen nuevas oportunidades para reforzar la seguridad digital, pero también introducen vulnerabilidades inéditas que requieren ser comprendidas y gestionadas (Fernandes et al., 2021). Por tanto, el estudio de la ciberseguridad en la educación superior debe concebirse como un proceso dinámico que articula tecnología, formación y ética en la protección de la información y los entornos digitales.

2 2. Amenazas y vulnerabilidades en la educación superior

Las instituciones de educación superior constituyen un blanco prioritario para los ciberdelincuentes debido al valor de la información que administran y a la amplitud de sus ecosistemas tecnológicos. Los sistemas de gestión académica, los repositorios de investigación, las plataformas de educación en línea y las redes administrativas se convierten en puntos críticos de vulnerabilidad (Aguilar et al., 2024).

Entre las principales amenazas destacan:

1. **Phishing y suplantación de identidad.**

Se trata de uno de los ataques más comunes en universidades, en el que los estudiantes y docentes reciben correos electrónicos falsificados para obtener credenciales o información financiera. Aldaz (2019) documentó casos en instituciones públicas de Ecuador, evidenciando la necesidad de fortalecer la capacitación en detección de fraudes digitales.

2. Ransomware

Diversas universidades a nivel mundial han sido víctimas de ataques de secuestro de datos. Por ejemplo, en 2020, la Universidad de California en San Francisco pagó un rescate de 1,14 millones de dólares para recuperar información cifrada por un grupo de ciberdelincuentes (BBC, 2020). Estos ataques suelen dirigirse a laboratorios de investigación que manejan información sensible o valiosa para la industria.

3. Intrusiones en redes y vulnerabilidades de software

Los campus universitarios suelen ofrecer acceso libre a sus redes inalámbricas, lo que incrementa el riesgo de intrusiones. Según González et al. (2023), muchas universidades latinoamericanas carecen de sistemas de detección de intrusos (IDS) actualizados, lo que las hace más vulnerables frente a ataques dirigidos.

4. Explotación de plataformas de educación en línea

Con la masificación de la educación virtual tras la pandemia, aumentaron los ataques dirigidos a plataformas como Moodle, Blackboard y Zoom. Chérrez y Pesantez (2021) subrayan que estas plataformas se han convertido en objetivos de ciberataques debido a la gran cantidad de usuarios y al intercambio de información privada que gestionan.

5. Ingeniería social y bajo nivel de conciencia digital

La falta de formación en ciberseguridad entre estudiantes y personal administrativo constituye una de las mayores vulnerabilidades. Yadav y Gupta (2021) destacan que los atacantes suelen explotar la ingenuidad de los usuarios para obtener accesos indebidos, incluso cuando los sistemas cuentan con medidas técnicas robustas.

En el caso de América Latina, la situación se agrava por la escasez de recursos financieros y personal especializado, lo que limita la implementación de estrategias preventivas y correctivas (Tiglla Tumbaico, 2024). Además, la complejidad normativa y la falta de coordinación interinstitucional dificultan la respuesta efectiva ante incidentes (Urbanovics & Guajardo, 2022).

En conclusión, las amenazas y vulnerabilidades en la educación superior no solo son de carácter técnico, sino también organizacional y humano. La evidencia empírica muestra que la gestión de riesgos debe contemplar tanto la actualización tecnológica como la concienciación de los usuarios y la adaptación de marcos normativos.

Tabla 1. Principales amenazas de ciberseguridad en la educación superior

Amenaza	Descripción	Ejemplo / Evidencia	Fuente
Phishing	Correos falsificados para obtener credenciales	Casos documentados en instituciones públicas de Ecuador	Aldaz, 2019
Ransomware	Cifrado de datos con exigencia de pago	Ataque a la Univ. de California, rescate de $1,14 millones	BBC, 2020
Intrusiones en redes	Acceso indebido por fallos en redes abiertas	Universidades latinoamericanas sin IDS actualizado	González et al., 2023
Plataformas educativas	Ataques a Moodle, Blackboard, Zoom	Brechas en educación virtual durante pandemia	Chérrez & Pesantez, 2021
Ingeniería social	Manipulación psicológica de usuarios	Estudiantes con baja conciencia digital	Yadav & Gupta, 2021

2.3. Ciberseguridad en el contexto latinoamericano

En América Latina, el desarrollo de políticas y estrategias de ciberseguridad presenta una marcada heterogeneidad. Mientras algunos países han implementado planes nacionales consolidados, otros mantienen vacíos normativos y operativos que limitan su capacidad de respuesta frente a amenazas emergentes (Urbanovics & Guajardo, 2022). Esta disparidad refleja no solo diferencias en inversión tecnológica, sino también en la priorización política de la seguridad digital como componente del desarrollo sostenible.

Tabla 2. Comparación de estrategias de ciberseguridad en América Latina

País	**Enfoque principal**	**Avances destacados**	**Limitaciones**	**Fuente**
Chile	Política nacional con enfoque de género	Inclusión de diversidad e igualdad en ciberseguridad	Limitada inversión en capacitación masiva	Herrera, 2020
Colombia	Regulación integral y formación	Marco normativo robusto y programas educativos	Brechas de implementación regional	Jiménez-Almeira & López, 2023
Brasil	Defensa cibernética	Inversión en cooperación público–privada	Fragmentación a nivel federal	Tiglla Tumbaico, 2024
Argentina	Cooperación internacional y plataformas educativas	Impulso de campañas de sensibilización	Escasez de recursos financieros	Urbanovics & Guajardo, 2022

La comparación presentada en la Tabla 2 pone de manifiesto la diversidad de enfoques adoptados por los países latinoamericanos en materia de ciberseguridad. Mientras Chile y Colombia se consolidan como referentes regionales por su avance en marcos normativos y políticas inclusivas, Brasil y Argentina muestran progresos más focalizados en áreas específicas como la defensa cibernética o la cooperación internacional. Sin embargo, la mayoría de los países aún enfrentan limitaciones relacionadas con la falta de inversión, la fragmentación institucional y la carencia de programas de capacitación masiva. Estas diferencias reflejan la necesidad de una agenda regional coordinada que permita reducir las brechas de resiliencia cibernética y, al mismo tiempo, promueva la estandarización de buenas prácticas en el ámbito de la educación superior (Herrera, 2020; Jiménez-Almeira & López, 2023; Urbanovics & Guajardo, 2022; Tiglla Tumbaico, 2024).

La brecha regional se observa con claridad en el desarrollo de capacidades técnicas y en la formación de especialistas. Suárez et al. (2021) subrayan que aún existe una dependencia excesiva de soluciones importadas y una escasa inversión en investigación aplicada en ciberseguridad. Esto limita la autonomía tecnológica y refuerza la necesidad de programas de cooperación académica y tecnológica a nivel regional.

En conclusión, la ciberseguridad en América Latina se enfrenta a un escenario dual: por un lado, países que han avanzado con marcos normativos robustos y programas de formación inclusivos; por otro, naciones que continúan rezagadas en capacidades y políticas. Esta disparidad plantea la urgencia de promover una agenda regional coordinada, que fortalezca las competencias digitales, fomente la cooperación internacional y asegure la protección de los ecosistemas académicos y sociales en su conjunto.

2 4. Formación y estrategias educativas en ciberseguridad

La formación en ciberseguridad en la educación superior se ha consolidado como un elemento clave para garantizar que los futuros profesionales cuenten con competencias que les permitan enfrentar las amenazas digitales del siglo XXI. Sin embargo, existe un consenso en la literatura en torno a la brecha de conocimientos en esta área, tanto entre estudiantes como en el personal docente y administrativo de las universidades (Aguilar et al., 2024).

En muchos casos, los programas académicos incluyen únicamente nociones básicas de seguridad informática, sin un abordaje sistemático de la ciberseguridad aplicada a la protección de datos, la gestión de incidentes o la ciberética (Suárez et al., 2021). Esta situación genera una exposición considerable frente a ciberataques, pues la ausencia de formación se traduce en prácticas inadecuadas como el uso de contraseñas débiles, la falta de actualización de software y la desatención a políticas institucionales de seguridad (Yadav & Gupta, 2021).

Diversas iniciativas han buscado suplir esta brecha. Por ejemplo, las competencias NICE (National Initiative for Cybersecurity Education) desarrolladas por el NIST han propuesto un marco global para estandarizar la formación en ciberseguridad, definiendo perfiles de especialización y competencias laborales aplicables a distintos niveles académicos y profesionales (Newhouse et al., 2021). En América Latina, algunos países han comenzado a incorporar estos marcos de referencia en programas universitarios, aunque su implementación todavía es incipiente.

Asimismo, la educación en ciberseguridad requiere adoptar metodologías activas e innovadoras que permitan a los estudiantes experimentar escenarios reales de ataque y defensa. Un ejemplo de ello son las plataformas *Capture The Flag (CTF)*, que mediante dinámicas de gamificación y resolución de retos prácticos han demostrado eficacia en la adquisición de habilidades técnicas (Suárez et al., 2021).

Estos entornos no solo promueven el aprendizaje significativo, sino que también despiertan el interés de los estudiantes hacia una disciplina que tradicionalmente ha sido percibida como altamente técnica y compleja.

La colaboración universidad–empresa se presenta como otra estrategia fundamental. Susilo et al. (2022) destacan que los programas de capacitación desarrollados en conjunto con el sector privado permiten cubrir la brecha entre teoría y práctica, facilitando que los estudiantes se familiaricen con herramientas, normativas y estándares utilizados en el ámbito laboral. Esta cooperación es especialmente relevante en contextos como el latinoamericano, donde los recursos institucionales suelen ser limitados.

De igual manera, la formación docente se considera un componente crítico en la consolidación de una cultura de ciberseguridad universitaria. Según Edwards (2024), no basta con que los estudiantes adquieran competencias técnicas; es imprescindible que los educadores integren criterios de seguridad digital en sus prácticas pedagógicas, promoviendo la reflexión ética, la protección de datos y el uso responsable de tecnologías emergentes como la inteligencia artificial o el internet de las cosas .

Finalmente, la construcción de una cultura de ciberseguridad institucional implica integrar estas estrategias en todos los niveles de la comunidad universitaria. Programas de sensibilización periódicos, simulacros de respuesta a incidentes, talleres prácticos y asignaturas transversales son mecanismos que permiten reforzar el aprendizaje y reducir las vulnerabilidades humanas, que continúan siendo uno de los principales vectores de ataque (Maan, 2021).

En conclusión, la formación en ciberseguridad en educación superior requiere un enfoque multidimensional que combine contenidos curriculares, metodologías prácticas, colaboración intersectorial y cultura institucional. Solo de esta manera las universidades podrán garantizar que sus egresados estén preparados para enfrentar los desafíos de un entorno digital cada vez más hostil y dinámico.

2 .5. Buenas prácticas institucionales

La implementación de buenas prácticas de ciberseguridad en instituciones de educación superior constituye un elemento indispensable para garantizar un entorno académico seguro, resiliente y éticamente responsable. Estas prácticas no se limitan a la instalación de tecnologías de protección, sino que requieren la adopción de un enfoque integral que combine políticas, formación, gestión de riesgos y cultura institucional (Yadav & Gupta, 2021).

En primer lugar, se destacan las políticas institucionales claras y accesibles, que regulen el uso de recursos tecnológicos, la gestión de datos personales y la respuesta ante incidentes. Edwards (2024) sostiene que las universidades deben establecer normas explícitas sobre contraseñas, almacenamiento de información, acceso a redes y uso de dispositivos personales (BYOD), lo que contribuye a reducir la exposición a amenazas internas y externas.

En segundo lugar, la gestión de contraseñas y autenticación multifactor (MFA) es una de las medidas más efectivas para prevenir accesos no autorizados. Aguilar et al. (2024) identifican que muchos estudiantes desconocen la importancia de estas medidas, por lo que proponen manuales de buenas prácticas que incluyan estrategias sencillas, como el uso de gestores de contraseñas y la obligatoriedad de doble verificación en los sistemas académicos.

Otra práctica fundamental es la actualización periódica de software y sistemas. Según Stallings (2018), muchas brechas de seguridad se explotan a partir de vulnerabilidades conocidas, pero no corregidas, lo que convierte el mantenimiento tecnológico en una acción prioritaria para cualquier institución.

En el ámbito de la formación continua, se recomiendan talleres, campañas de sensibilización y simulacros de ciberataques. Estas iniciativas no solo preparan a la comunidad universitaria para identificar amenazas como el phishing o el malware, sino que también promueven una cultura de corresponsabilidad en la protección de datos (Maan, 2021).

Asimismo, resulta clave el establecimiento de centros de respuesta a incidentes (CSIRT universitarios), que permitan detectar, analizar y mitigar ciberataques en tiempo real. En América Latina, universidades como la Universidad de Chile y la Universidad Nacional de Colombia han

avanzado en la implementación de unidades especializadas de seguridad digital, lo que ha fortalecido su capacidad de respuesta frente a incidentes complejos (Jiménez-Almeira & López, 2023).

En cuanto a la cooperación interinstitucional, Tiglla Tumbaico (2024) enfatiza que las universidades deben integrarse a redes nacionales e internacionales de ciberseguridad para compartir información sobre amenazas y mejores prácticas. Ejemplos de ello son las alianzas promovidas por la Organización de Estados Americanos (OEA) y la RedCLARA, que han impulsado proyectos de cooperación en ciberseguridad en educación superior.

Por último, la inclusión de la ciberseguridad en los currículos no solo como asignatura técnica, sino como un eje transversal en todas las carreras, es una buena práctica emergente que fortalece la cultura digital de la comunidad académica. Esta estrategia responde a la necesidad de que todos los profesionales —independientemente de su disciplina— comprendan los riesgos y las responsabilidades asociados al uso de la información en entornos digitales (Susilo et al., 2022).

En síntesis, las buenas prácticas institucionales en ciberseguridad en universidades deben integrar medidas técnicas, normativas y formativas, alineadas con estándares internacionales, pero adaptadas a los contextos regionales. Su éxito depende de la articulación entre liderazgo institucional, participación comunitaria y cooperación externa.

Tabla 3. Buenas prácticas institucionales en universidades

Práctica	Aplicación	Ejemplo	Fuente
Políticas claras de seguridad digital	Normas sobre contraseñas, BYOD, gestión de datos	Manuales internos en universidades latinoamericanas	Edwards, 2024
Autenticación multifactor (MFA)	Acceso seguro a sistemas académicos	Guías de contraseñas y MFA en estudiantes	Aguilar et al., 2024
Actualización periódica de software	Aplicación de parches y gestión de vulnerabilidades	Protocolos en universidades chilenas y colombianas	Stallings, 2018
Formación continua	Talleres, simulacros, campañas de phishing simulado	Programas de sensibilización estudiantil	Maan, 2021
Centros de respuesta a incidentes (CSIRT)	Monitoreo en tiempo real de ataques	Univ. de Chile y Univ. Nacional de Colombia	Jiménez-Almeira & López, 2023

La síntesis presentada en la Tabla 3 evidencia que las buenas prácticas de ciberseguridad en las universidades deben ir más allá de la adopción de soluciones técnicas aisladas. La combinación de políticas claras, mecanismos de autenticación robustos, mantenimiento tecnológico constante, programas de formación continua y la creación de centros especializados de respuesta a incidentes conforma un modelo integral de protección.

Estos elementos, alineados con marcos internacionales como ISO/IEC 27001 y las competencias NICE, permiten fortalecer la cultura de seguridad digital en el ámbito universitario y responder de manera más efectiva a las amenazas emergentes. En consecuencia, la implementación de estas prácticas no solo contribuye a reducir vulnerabilidades, sino que también fomenta un entorno académico resiliente, ético e inclusivo (Aguilar et al., 2024; Edwards, 2024; Tiglla Tumbaico, 2024).

3. METODOLOGÍA O MATERIALES Y METODOS

La investigación se desarrolló bajo un enfoque bibliográfico y documental, con un diseño de revisión narrativa estructurada. Este tipo de metodología resulta idónea para analizar fenómenos complejos como la ciberseguridad en la educación superior, ya que integra dimensiones técnicas, pedagógicas y organizacionales, permitiendo identificar vacíos en la literatura y proponer estrategias de mejora (Hernández Sampieri et al., 2014; Ruiz, 2012).

3.1. Tipo de estudio

Corresponde a una revisión bibliográfica narrativa con elementos sistemáticos, orientada a:

- recopilar fuentes científicas relevantes,
- sintetizar los hallazgos en categorías temáticas,
- y establecer un marco comparativo de buenas prácticas y políticas aplicables a universidades latinoamericanas.

Este tipo de revisión se distingue por su carácter interpretativo y su capacidad para integrar múltiples perspectivas, más allá de la mera descripción (Taylor & Bogdan, 1998).

3.2. Fuentes de información y estrategia de búsqueda

La búsqueda se realizó en bases de datos internacionales de alto impacto como *Scopus, Web of Science, IEEE Xplore, SpringerLink, Redalyc y Google Scholar*, complementadas con repositorios institucionales de universidades latinoamericanas.

Se emplearon combinaciones de palabras clave en español e inglés, tales como:

- *"ciberseguridad en educación superior"*
- *"formación en seguridad digital"*
- *"buenas prácticas de ciberseguridad"*
- *"cybersecurity in higher education"*
- *"digital security policies"*

La búsqueda cubrió el período 2018–2024, priorizando estudios recientes y relevantes para el contexto latinoamericano. Además, se aplicó la técnica de bola de nieve para localizar artículos a partir de las referencias de los textos más citados.

3.3. Criterios de inclusión y exclusión

- **Criterios de inclusión:**
    - Artículos académicos arbitrados y libros publicados entre 2018–2024.
    - Estudios enfocados en ciberseguridad en universidades o instituciones de educación superior.
    - Documentos que analicen amenazas, políticas institucionales, formación y buenas prácticas.
- **Criterios de exclusión:**
    - Artículos de opinión o noticias sin respaldo académico.
    - Trabajos exclusivamente técnicos (infraestructura, software) sin conexión con el ámbito educativo.
    - Publicaciones duplicadas o que no aporten evidencia directa al tema.

3.4. Procedimiento de análisis

El corpus documental fue sometido a un proceso de cribado en tres fases:

1. Revisión preliminar de títulos y resúmenes, para descartar documentos sin relación directa.
2. Lectura integral de los textos seleccionados, evaluando su calidad metodológica, pertinencia y validez.

3. Codificación temática mediante análisis de contenido Ojeda et al., 2024, clasificando la información en cuatro ejes:

    - Amenazas y vulnerabilidades en la educación superior.
    - Estrategias y políticas institucionales en América Latina.
    - Formación y capacitación en ciberseguridad.
    - Buenas prácticas aplicables a universidades.

3.5. Rigor y validez

Para garantizar la validez de los hallazgos:

- Se trianguló la información entre múltiples fuentes y contextos.
- Se compararon enfoques normativos, pedagógicos y tecnológicos.
- Se implementó un proceso de revisión por pares entre investigadores colaboradores, con el fin de minimizar sesgos interpretativos (Hernández Sampieri et al., 2014).

De este modo, la metodología adoptada asegura una comprensión profunda, crítica y contextualizada del fenómeno de la ciberseguridad en la educación superior, permitiendo extraer implicaciones prácticas para la gestión institucional y la formación académica.

4. RESULTADOS

La revisión de la literatura permitió identificar hallazgos clave sobre la situación de la ciberseguridad en la educación superior, organizados en tres ejes principales: brechas y vulnerabilidades, estrategias en América Latina, y buenas prácticas institucionales. Estos resultados ofrecen un panorama comparativo de las principales amenazas que enfrentan las universidades, las respuestas adoptadas por diferentes países de la región y las prácticas recomendadas para fortalecer la resiliencia digital.

4.1. Brechas y vulnerabilidades en la educación superior

El análisis de la literatura revela que las instituciones de educación superior se encuentran entre los sectores más vulnerables frente a los ciberataques, debido a la amplia superficie de exposición digital que gestionan: redes abiertas de acceso público, repositorios de investigación, plataformas de educación virtual y bases de datos con información personal sensible (Aguilar et al., 2024; González et al., 2023). Esta complejidad convierte a las universidades en entornos atractivos para

los ciberdelincuentes, que encuentran en ellas un terreno fértil para explotar vulnerabilidades técnicas y humanas.

Las principales brechas identificadas en los estudios revisados son:

1. **Limitada asignación de recursos financieros y tecnológicos.**

Muchas universidades latinoamericanas carecen de presupuesto suficiente para implementar sistemas de protección avanzados, lo que dificulta la actualización de software, la adquisición de firewalls de nueva generación o la contratación de servicios especializados en ciberseguridad (Tiglla Tumbaico, 2024).

2. **Escasez de personal especializado.**

La carencia de equipos técnicos capacitados en seguridad informática provoca que la detección y respuesta a incidentes sea lenta e ineficiente. González et al. (2023) destacan que en varias instituciones un mismo profesional atiende tanto la administración de redes como la gestión de seguridad, lo que incrementa los riesgos operativos.

3. **Déficit en formación y conciencia digital.**

El factor humano se mantiene como una de las principales vulnerabilidades. Estudiantes y docentes suelen caer en ataques de phishing, emplean contraseñas débiles y no aplican actualizaciones periódicas a sus dispositivos (Yadav & Gupta, 2021). El estudio de Aldaz (2019) sobre phishing en universidades ecuatorianas confirmó que más del 60 % de los usuarios encuestados no reconocía señales de fraude digital.

4. **Falta de normativas internas unificadas.**

En muchos casos, las universidades carecen de protocolos claros de seguridad digital, lo que genera un uso desregulado de dispositivos, almacenamiento en nubes no seguras y ausencia de planes de continuidad académica frente a incidentes (Edwards, 2024).

5. **Incremento de amenazas en plataformas educativas virtuales.**

Tras la pandemia de COVID-19, las plataformas de educación en línea se convirtieron en objetivos recurrentes de ciberataques. Chérrez y Pesantez (2021) documentan que el uso masivo de Moodle y Zoom sin configuraciones adecuadas expuso a miles de estudiantes a accesos no autorizados y robo de datos.

Ejemplos empíricos refuerzan la gravedad de estas brechas.

En 2020, la Universidad de California en San Francisco pagó 1,14 millones de dólares tras un ataque de ransomware que afectó a su facultad de Medicina, evidenciando el alto costo económico y reputacional de estas vulnerabilidades (BBC, 2020). En América Latina, universidades de Brasil, México y Colombia han reportado intrusiones en sus sistemas de matrícula y gestión académica, lo que ha afectado directamente la continuidad de los procesos educativos (Urbanovics & Guajardo, 2022).

En conclusión, las brechas en la educación superior no se limitan a la falta de infraestructura tecnológica, sino que abarcan factores organizacionales y humanos. Estas vulnerabilidades deben abordarse mediante un enfoque integral que combine inversión en infraestructura, fortalecimiento de capacidades técnicas y programas de sensibilización en seguridad digital para toda la comunidad universitaria.

4.2. Estrategias de ciberseguridad en América Latina

El desarrollo de estrategias de ciberseguridad en América Latina refleja una evolución desigual entre países. Algunas naciones han avanzado en la construcción de planes nacionales de ciberseguridad, mientras que otras aún carecen de políticas consolidadas, lo que genera brechas regionales significativas. Estas disparidades impactan directamente en el ámbito educativo, ya que la ausencia de marcos regulatorios robustos limita la capacidad de las universidades para implementar medidas de protección efectivas (Urbanovics & Guajardo, 2022; González et al., 2023).

Tabla 4. Estrategias de ciberseguridad en países de América Latina

País	Marco normativo / estratégico	Enfoque principal	Avances destacados	Limitaciones	Fuente
Chile	Política Nacional de Ciberseguridad (2017–2022, 2022–2027)	Inclusión y diversidad en seguridad digital	Integración de género y cooperación internacional	Recursos limitados para educación masiva	Herrera (2020)
Colombia	CONPES 3854 (2016), Política de Seguridad Digital (2019–2023)	Protección de infraestructuras críticas y talento humano	Programas de formación y marcos regulatorios sólidos	Brechas de implementación en zonas rurales	Jiménez-Almeira & López (2023)
Brasil	Estrategia Nacional de Ciberseguridad, ComDCiber	Defensa cibernética y seguridad nacional	Fuerte cooperación público–privada	Fragmentación institucional federal	Tiglla Tumbaico (2024)

Argentina	Estrategia Nacional de Ciberseguridad (2019–2023)	Concienciación y cooperación internacional	Campañas educativas y participación ciudadana	Escasez de recursos financieros	Urbanovics & Guajardo (2022)
México	Estrategia Nacional de Ciberseguridad (2017)	Cooperación multisectorial	Marco inicial de referencia para universidades	Falta de actualización y mecanismos de control	González et al. (2023)
Ecuador	Plan Nacional de Gobierno Digital (2020–2025)	Seguridad de la información en gobierno digital	Avances parciales en ejes de ciberseguridad	Ausencia de estrategia nacional integral	Tiglla Tumbaico (2024)
Perú	Política Nacional de Ciberseguridad (2019)	Infraestructura crítica y cooperación internacional	Lineamientos claros en investigación y seguridad pública	Déficit de implementación en universidades	Urbanovics & Guajardo (2022)

La Tabla 4 refleja que, aunque existen esfuerzos en casi todos los países analizados, la brecha entre políticas y prácticas institucionales sigue siendo amplia. Chile y Colombia lideran la región con estrategias más completas, mientras que países como Ecuador y México presentan planes con bajo nivel de implementación. En general, las universidades latinoamericanas permanecen en un estado de vulnerabilidad, debido a que las políticas nacionales no siempre se traducen en lineamientos claros y recursos específicos para el sector educativo.

4.3. Buenas prácticas institucionales en universidades

La implementación de buenas prácticas institucionales en ciberseguridad constituye un pilar fundamental para mitigar riesgos en la educación superior. Estas prácticas no deben entenderse únicamente como soluciones tecnológicas, sino como un ecosistema integral de políticas, formación y cultura organizacional (Yadav & Gupta, 2021). La literatura destaca que aquellas universidades que han desarrollado protocolos claros y sostenibles han logrado reducir la incidencia de ciberataques y fortalecer la resiliencia de sus comunidades (Aguilar et al., 2024).

Entre las prácticas más recurrentes se encuentran:

- Elaboración de manuales internos de ciberseguridad con directrices claras sobre contraseñas, almacenamiento de datos y uso de redes.
- Implementación de autenticación multifactor (MFA) para acceso a plataformas académicas y administrativas.

- Creación de Centros de Respuesta a Incidentes (CSIRT) universitarios que permitan detectar y responder rápidamente a ataques.
- Campañas de formación continua y simulacros de ciberataques dirigidos a estudiantes, docentes y personal administrativo.
- Alianzas universidad–empresa para la capacitación y actualización de protocolos.

Estos elementos se observan en diferentes experiencias de universidades de la región, como se muestra en la Tabla 3.

Tabla 5. Buenas prácticas institucionales de ciberseguridad en universidades latinoamericanas

Universidad / Institución	**Prácticas adoptadas**	**Avances alcanzados**	**Limitaciones**	**Fuente**
ITSOEH (México)	Manual de buenas prácticas; capacitación en gestión de contraseñas y protección de dispositivos	Mayor concienciación estudiantil en ingeniería; reducción de incidentes reportados	Falta de continuidad y recursos para extender programas	Aguilar et al. (2024)
Universidad de Chile	CSIRT universitario; políticas de seguridad digital y simulacros de phishing	Detección temprana de incidentes y respuesta coordinada	Recursos limitados para ampliación a toda la comunidad	Herrera (2020)
Universidad Nacional de Colombia	Políticas institucionales integradas; colaboración con sector privado en formación	Inclusión de la ciberseguridad en planes curriculares; fortalecimiento de cooperación internacional	Dificultades de implementación en sedes regionales	Jiménez-Almeira & López (2023)
Universidad de São Paulo (Brasil)	Programas de defensa cibernética; cooperación público–privada	Fortalecimiento de la seguridad en redes de investigación	Fragmentación en la gestión a nivel federal	Tiglla Tumbaico (2024)
Universidad de Buenos Aires (Argentina)	Campañas de sensibilización y protocolos básicos en plataformas digitales	Creación de conciencia en estudiantes y docentes sobre riesgos digitales	Escasa inversión en infraestructura tecnológica	Urbanovics & Guajardo (2022)

La evidencia muestra que, aunque las universidades latinoamericanas han comenzado a implementar buenas prácticas, estas suelen estar limitadas por la escasez de recursos financieros y la ausencia de políticas nacionales sólidas que acompañen los esfuerzos institucionales. Experiencias como la del ITSOEH en México reflejan el impacto positivo de manuales adaptados al contexto académico, mientras que iniciativas más avanzadas como los CSIRT universitarios en Chile y Colombia demuestran la efectividad de estructuras especializadas de respuesta.

No obstante, las brechas persisten en universidades con recursos limitados, donde la sensibilización no siempre se traduce en cambios sostenibles en el comportamiento de los usuarios. Por ello, se destaca la importancia de institucionalizar estas prácticas mediante normativas internas vinculadas a estándares internacionales (ISO/IEC 27001, NIST NICE Framework) y reforzar la cooperación interuniversitaria para compartir protocolos exitosos y experiencias formativas.

5. DISCUSIÓN

Los resultados de esta revisión bibliográfica confirman que la ciberseguridad en la educación superior enfrenta un doble desafío: por un lado, la creciente sofisticación de las amenazas digitales y, por otro, las brechas estructurales que limitan la capacidad de respuesta de las universidades latinoamericanas. Esta situación coincide con lo señalado por Singh et al. (2021), quienes advierten que los entornos educativos constituyen objetivos estratégicos para el cibercrimen debido al volumen de datos y a la baja inversión en medidas de seguridad.

En primer lugar, la persistencia de vulnerabilidades críticas evidencia que los ciberataques no son únicamente un problema técnico, sino también organizacional y humano. La literatura internacional subraya que más del 80 % de los incidentes están relacionados con errores humanos o falta de formación (Yadav & Gupta, 2021). Esto coincide con los hallazgos de Aguilar et al. (2024), quienes documentan la necesidad de manuales y guías de buenas prácticas adaptados a estudiantes y docentes. La integración de programas de capacitación periódica y simulacros de phishing se presenta como una estrategia efectiva para fortalecer la resiliencia institucional.

En segundo lugar, se observa una heterogeneidad regional en las políticas nacionales de ciberseguridad. Mientras Chile y Colombia destacan por sus avances regulatorios y formativos, otros países como Ecuador y México muestran una débil articulación de políticas con el ámbito universitario (Urbanovics & Guajardo, 2022; Tiglla Tumbaico, 2024). Este contraste refleja lo planteado por Herrera (2020), quien sostiene que la efectividad de las estrategias depende no solo de la formulación de políticas, sino también de su implementación efectiva y contextualizada. En

este sentido, la educación superior requiere ser considerada un sector prioritario dentro de las políticas nacionales de seguridad digital.

Otro aspecto relevante es la necesidad de alinear las universidades con estándares internacionales como ISO/IEC 27001 y el marco NICE (Newhouse et al., 2021). La comparación con experiencias globales muestra que aquellas instituciones que han adoptado estándares reconocidos no solo reducen incidentes, sino que también generan confianza en su comunidad académica y en sus redes de cooperación internacional (Stallings, 2018). Esta alineación permitiría a las universidades latinoamericanas superar la fragmentación de sus protocolos internos y establecer un lenguaje común con actores internacionales.

Asimismo, la discusión revela que la formación en ciberseguridad debe ser transversal. No basta con incluir asignaturas optativas en carreras de ingeniería, sino que es necesario integrar competencias digitales en todas las áreas de formación universitaria. Edwards (2024) enfatiza que una cultura organizacional de seguridad requiere que tanto estudiantes de ciencias sociales como de salud o humanidades reconozcan riesgos y desarrollen prácticas responsables en el uso de tecnologías. Este enfoque transversal puede contribuir a reducir el sesgo tecnocrático y a fomentar una cultura inclusiva de seguridad digital.

Finalmente, el análisis evidencia que las buenas prácticas institucionales (autenticación multifactor, centros de respuesta a incidentes, campañas de sensibilización) constituyen herramientas efectivas, pero su impacto depende de la sostenibilidad y de la capacidad de las universidades para mantenerlas en el tiempo. Sin un compromiso institucional y una asignación adecuada de recursos, estas prácticas corren el riesgo de convertirse en acciones aisladas sin impacto real (González et al., 2023).

En conclusión, la discusión sugiere que la ciberseguridad universitaria debe entenderse como un ecosistema integrado que combina políticas nacionales, estándares internacionales, prácticas institucionales y formación transversal. La cooperación interuniversitaria y las alianzas con el sector privado se consolidan como estrategias clave para superar las brechas actuales y preparar a las universidades de la región frente a los desafíos de un entorno digital cada vez más hostil y complejo.

6. CONCLUSIONES

El análisis realizado permite afirmar que la ciberseguridad en la educación superior constituye un desafío complejo que combina factores técnicos, organizacionales y humanos. La revisión de la literatura muestra que las universidades son objetivos altamente vulnerables a los ciberataques

debido al valor de los datos que gestionan y a la limitada preparación de sus comunidades académicas (Aguilar et al., 2024; González et al., 2023).

En primer lugar, se evidencian brechas estructurales significativas: falta de recursos tecnológicos, escasez de personal especializado, carencia de protocolos internos unificados y una baja conciencia digital entre estudiantes y docentes. Estas vulnerabilidades refuerzan la necesidad de fortalecer tanto la infraestructura tecnológica como la formación transversal en competencias digitales.

En segundo lugar, la comparación regional revela que América Latina presenta un panorama heterogéneo. Mientras países como Chile y Colombia han logrado avances notables con políticas inclusivas y marcos normativos sólidos, otros como Ecuador y México aún muestran debilidades en la implementación de estrategias nacionales articuladas con el sector educativo (Urbanovics & Guajardo, 2022; Tiglla Tumbaico, 2024). Este contraste refleja la urgencia de promover una agenda regional de ciberseguridad, capaz de reducir las brechas y fomentar la cooperación interinstitucional.

En tercer lugar, las buenas prácticas institucionales identificadas —manuales de seguridad, autenticación multifactor, actualización periódica de software, creación de CSIRT universitarios y programas de sensibilización— se consolidan como herramientas efectivas para reducir riesgos. No obstante, su impacto depende de la sostenibilidad en el tiempo, del compromiso institucional y de la integración de estas prácticas en una cultura organizacional sólida (Edwards, 2024).

CONFLICTO DE INTERESES

Los Autores declaran que no existe conflicto de intereses, o lo que corresponda.

CONTRIBUCIÓN DE AUTORÍA

En concordancia con la taxonomía establecida internacionalmente para la asignación de créditos a autores de artículos científicos (https://credit.niso.org/). Los autores declaran sus contribuciones en la siguiente matriz:

	Jiménez V.	Tipanluisa R.	León C.
Participar activamente en:			
Conceptualización	X	X	
Análisis formal	X	X	X
Adquisición de fondos		X	X
Investigación	X	X	
Metodología	X		X
Administración del proyecto		X	X
Recursos	X	X	
Redacción –borrador original	X		X
Redacción –revisión y edición			X
La discusión de los resultados	**X**	**X**	**X**
Revisión y aprobación de la versión final del trabajo.	**X**	**X**	**X**

REFERENCIAS BIBLIOGRÁFICAS:

Aguilar, C. E., Hernández, T. H., & Soto, S. I. (2024). Buenas prácticas de ciberseguridad en educación superior. South Florida Journal of Development, 5(12), 1–10.

Aldaz López, W. H. (2019). Vulnerabilidad de seguridad informática en la administración zonal norte "Eugenio Espejo" a través del phishing (Tesis de maestría). Universidad Central del Ecuador.

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. International Research Journal of Engineering and Technology (IRJET).

BBC. (2020, 29 de junio). University of California pays $1.14 m ransom to hackers. BBC News.

Chérrez, W. E. M., & Pesantez, D. F. A. (2021). Ciberseguridad en las redes sociales: una revisión teórica. Revista UNIANDES Episteme, 8(2), 211–234. https://doi.org/10.26807/epi.v8i2.367

Edwards, J. (2024). Mastering cybersecurity: Strategies, technologies, and best practices.

Fonfría, A., & Duch-Brown, N. (2020). Elementos para una política de ciberseguridad efectiva. Análisis del Real Instituto Elcano (ARI), (127).

Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

González, J. M., Albornoz, M. M., & Ramírez, M. S. M. (2023). Ciberseguridad: estado de la cuestión en América Latina. RIS, 9.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill.

Herrera Carpintero, P. (2020). El enfoque de género en la Política Nacional de Ciberseguridad de Chile. Revista Chilena de Derecho y Tecnología, 9(1), 5–31.

Hobbs, J. (2023). Cybersecurity awareness in higher education. Issues in Information Systems, 24(1), 159–169.

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologías de Información, (E62), 16–31.

Maan, A. (2021). Cybersecurity: The definitive guide to security and privacy.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2021). National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework (NIST SP 800-181 Rev. 1).

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585.

Ojeda, C. E. A., Omaña, T. H. H., & Ortíz, S. I. S. (2024). Buenas prácticas de ciberseguridad en educación superior. South Florida Journal of Development, 5(12), e4879-e4879.

Ruiz, J. G. (2012). Metodología de la investigación documental. Editorial Trillas.

Singh, P., Gupta, M., & Kaur, S. (2021). Cybersecurity threats: Emerging trends and solutions. Springer.

Stallings, W. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Suárez, G., Bolino, P., Pretto, J., Venosa, P., & Queiruga, C. (2021). CTFs en escuelas: una plataforma para acercar la ciberseguridad a la educación secundaria. JADICC, 54, 1–9.

Susilo, A., Huda, M., & Yusof, N. (2022). Collaborative approaches in cybersecurity training: Bridging gaps between academia and industry. Journal of Information Security Education, 1(2), 45–58.

Taylor, S. J., & Bogdan, R. (1998). Introduction to qualitative research methods: A guidebook segurity dates.

Tiglla Tumbaico, B. D. (2024). Ciberseguridad en educación y política: Desafíos éticos y tecnológicos. Horizon International Journal, 2(1), 28–39.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.

Urbanovics, A., & Guajardo, R. (2022). Estrategias de ciberseguridad en los países latinoamericanos: Un análisis comparativo. Acta Hispanica, (IV), 89–104.

Yadav, S., & Gupta, R. (2021). Best practices in cybersecurity: Strategies and solutions for a secure future. Academic Press.