https://doi.org/10.69639/arandu.v12i1.859

Análisis de Vulnerabilidades en Moodle: Una Revisión Sistemática sobre Seguridad en LMS

Vulnerability Analysis in Moodle: A Systematic Review on LMS Security

Sandra Elizabeth Arias Calderón
se.ariasc@uea.edu.ec
https://orcid.org/0009-0004-9480-0857
Universidad Estatal Amazónica
Puyo – Ecuador

Fernando Javier Villarroel Córdova
fj.villarroelc@uea.edu.ec
https://orcid.org/0000-0002-8743-0171
Universidad Estatal Amazónica
Puyo – Ecuador

Byron Raúl Ureña Zúñiga
burena8566@uta.edu.ec
https://orcid.org/0009-0003-7404-5017
Universidad Técnica de Ambato
Ambato – Ecuador

Yajaira Beatriz Aman Collaguazo
yb.amanc@uea.edu.ec
https://orcid.org/0009-0005-3687-6113
Universidad Estatal Amazónica
Puyo - Pastaza - Ecuador

Artículo recibido: 10 enero 2025 - *Aceptado para publicación: 20 febrero 2025*
Conflictos de intereses: Ninguno que declarar

RESUMEN

Los sistemas de gestión de aprendizaje (LMS), como Moodle, han transformado la educación en línea, pero su uso masivo ha expuesto vulnerabilidades de seguridad. Este artículo realiza una revisión sistemática siguiendo la metodología PRISMA para identificar las principales vulnerabilidades en Moodle y otros LMS, así como las soluciones propuestas. Se analizaron 20 artículos publicados entre 2020 y 2025, identificando vulnerabilidades técnicas (filtraciones de datos, acceso no autorizado), humanas (falta de concienciación) y de configuración (gestión inadecuada). Entre las soluciones destacan el uso de blockchain, autenticación de dos factores (2FA) y auditorías de seguridad. Además, se enfatiza la importancia de la capacitación en ciberseguridad para usuarios. El estudio concluye que, aunque existen soluciones efectivas, su implementación requiere un compromiso continuo de las instituciones educativas para garantizar un entorno de aprendizaje en línea seguro.

Palabras clave: Moodle, seguridad, LMS, ciberseguridad, blockchain, 2FA

ABSTRACT

Learning Management Systems (LMS), such as Moodle, have transformed online education, but their widespread use has exposed security vulnerabilities. This article conducts a systematic review following the PRISMA methodology to identify the main vulnerabilities in Moodle and other LMS, as well as the proposed solutions. Twenty articles published between 2020 and 2025 were analyzed, identifying technical vulnerabilities (data leaks, unauthorized access), human factors (lack of awareness), and configuration issues (poor management). Among the proposed solutions are the use of blockchain, two-factor authentication (2FA), and security audits. Additionally, the importance of cybersecurity training for users is emphasized. The study concludes that, although effective solutions exist, their implementation requires ongoing commitment from educational institutions to ensure a secure online learning environment.

Keywords: Moodle, security, LMS, cybersecurity, blockchain, 2FA

INTRODUCCIÓN

Los sistemas de gestión de aprendizaje (LMS, por sus siglas en inglés) han revolucionado la educación en las últimas décadas, especialmente en el contexto de la digitalización acelerada por la pandemia de COVID-19. Plataformas como Moodle se han convertido en herramientas indispensables para instituciones educativas de todo el mundo, permitiendo la gestión de cursos, la evaluación del desempeño estudiantil y la facilitación de interacciones pedagógicas en entornos virtuales (Burchart et al., 2023). Sin embargo, este crecimiento exponencial en el uso de LMS ha traído consigo una serie de desafíos relacionados con la seguridad de la información, que amenazan la integridad, confidencialidad y disponibilidad de los datos almacenados en estas plataformas.

Las vulnerabilidades de seguridad en los LMS son un tema de creciente preocupación. Estudios recientes han identificado una variedad de amenazas, como ataques de inyección SQL, brechas de datos y problemas de autenticación, que exponen información sensible de usuarios, incluyendo datos académicos y administrativos (Mudiyanselage & Pan, 2020). Además, la falta de mecanismos robustos de seguridad ha permitido que actores malintencionados exploten estas vulnerabilidades, comprometiendo la privacidad de los usuarios y la confiabilidad de las plataformas (Khan & Naz, 2021). Por ejemplo, en el caso de Moodle, se han reportado incidentes en los que materiales didácticos protegidos fueron robados, credenciales de administradores fueron comprometidas, y resultados de exámenes fueron alterados sin autorización (Mudiyanselage & Pan, 2020).

En respuesta a estos desafíos, se han propuesto diversas soluciones tecnológicas y metodológicas para mejorar la seguridad en los LMS. Una de las más prometedoras es la implementación de tecnologías basadas en blockchain, que ofrecen un alto nivel de seguridad, inmutabilidad y trazabilidad de los datos. Khan y Naz (2021) proponen un sistema de gestión de aprendizaje descentralizado (BLMS) que utiliza contratos inteligentes y un mecanismo de permisos detallados para garantizar la seguridad contra ataques internos y externos. Este enfoque no solo protege los datos de los usuarios, sino que también asegura la integridad de los procesos académicos, como la evaluación y la certificación de resultados.

Otra solución destacada es la implementación de métodos avanzados de autenticación, como la autenticación de dos factores (2FA) y el uso de certificados digitales. Baneş et al. (2023) proponen un esquema de autenticación de dos factores para Moodle, que utiliza certificados digitales almacenados en dispositivos físicos o en la nube. Este enfoque ha demostrado ser efectivo para prevenir el acceso no autorizado a las cuentas de usuario, aumentando la confianza de los usuarios en la plataforma. Además, se han realizado esfuerzos para mejorar la seguridad mediante pruebas de penetración y análisis de vulnerabilidades, que permiten identificar y

corregir fallos en los sistemas antes de que sean explotados por actores malintencionados (Mudiyanselage & Pan, 2020).

A pesar de estos avances, la concienciación sobre seguridad entre los usuarios de LMS sigue siendo un tema crítico. Estudios como el de Sadikin et al. (2023) destacan que los estudiantes y profesores perciben de manera diferente los niveles de seguridad en plataformas como Moodle y Google Classroom. Mientras que los estudiantes tienden a confiar más en estas plataformas cuando perciben que sus datos están protegidos, los profesores suelen ser más críticos y exigen mayores garantías de seguridad. Esta discrepancia subraya la necesidad de implementar programas de capacitación y concienciación sobre ciberseguridad en las instituciones educativas, con el fin de fomentar un uso más seguro y responsable de los LMS.

En este contexto, el presente estudio tiene como objetivo realizar una revisión sistemática de las vulnerabilidades de seguridad en Moodle y otros LMS, utilizando la metodología PRISMA. A través de un análisis exhaustivo de la literatura reciente, se busca identificar las principales amenazas a la seguridad en estas plataformas, así como las soluciones tecnológicas y metodológicas propuestas para mitigarlas. Además, se explorará el impacto de estas vulnerabilidades en la confianza de los usuarios y se discutirán las implicaciones prácticas para las instituciones educativas. Los resultados de esta revisión no solo contribuirán a una mejor comprensión de los desafíos de seguridad en los LMS, sino que también proporcionarán una base sólida para futuras investigaciones en este campo.

METODOLOGÍA

Esta investigación se ha desarrollado siguiendo las pautas establecidas por PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), una metodología ampliamente reconocida por su rigor y transparencia en la realización de revisiones sistemáticas. PRISMA fue diseñada inicialmente para el ámbito de la salud, pero su versatilidad ha permitido su aplicación en diversas disciplinas, incluyendo la educación, la ingeniería y las ciencias sociales (Moher et al., 2009). Su objetivo principal es garantizar que los procesos de identificación, selección y síntesis de estudios se realicen de manera sistemática y libre de sesgos, proporcionando una base sólida para la toma de decisiones basada en evidencia.

La primera versión de PRISMA se publicó en 2009, y desde entonces ha experimentado actualizaciones significativas, la más reciente en 2020, para adaptarse a los avances en terminología y metodología. Estas actualizaciones han mejorado la capacidad de PRISMA para abordar revisiones sistemáticas en campos emergentes, como la seguridad en sistemas de gestión de aprendizaje (LMS) (Khan & Naz, 2021). Aunque PRISMA no evalúa la calidad metodológica de los estudios, sirve como una guía invaluable para garantizar que toda la información relevante sea recopilada y presentada de manera clara y estructurada (Page et al., 2021).

Preguntas de investigación

El diseño de esta revisión sistemática se guió por un conjunto de preguntas de investigación cuidadosamente formuladas, las cuales permitieron enfocar la búsqueda, selección y análisis de estudios relevantes. Estas preguntas surgieron de la necesidad de identificar brechas en la literatura existente y proponer recomendaciones prácticas para mejorar la seguridad en los sistemas de gestión de aprendizaje (LMS), con un enfoque particular en Moodle. Las preguntas de investigación que orientaron este estudio son las siguientes: *ver Tabla 1*.

Tabla 1

Preguntas de investigación

Código	Pregunta de investigación
PI1	¿Cuáles son las principales vulnerabilidades de seguridad en Moodle y otros sistemas de gestión de aprendizaje (LMS)?
PI2	¿Qué soluciones tecnológicas y metodológicas se han propuesto para abordar estas vulnerabilidades?
PI3	¿Cuál es el impacto de estas vulnerabilidades en la confianza de los usuarios y en la calidad del aprendizaje en línea?

Busqueda de documentos

La búsqueda de literatura se realizó exclusivamente en la base de datos Scopus, una de las plataformas más reconocidas y confiables para la búsqueda de literatura académica debido a su amplia cobertura de publicaciones revisadas por pares en áreas como la informática y la ingeniería (Mongeon & Paul-Hus, 2016). Scopus fue seleccionada por su capacidad para indexar revistas de alto impacto y proporcionar métricas de calidad, lo que garantiza la relevancia y rigurosidad de los estudios incluidos en esta revisión.

Para garantizar una búsqueda exhaustiva y sistemática, se utilizó la siguiente fórmula de búsqueda avanzada en Scopus: (TITLE-ABS-KEY("Moodle" OR "Learning Management System" OR "LMS") AND TITLE-ABS-KEY("security" OR "vulnerability" OR "cybersecurity" OR "attack" OR "data breach")).

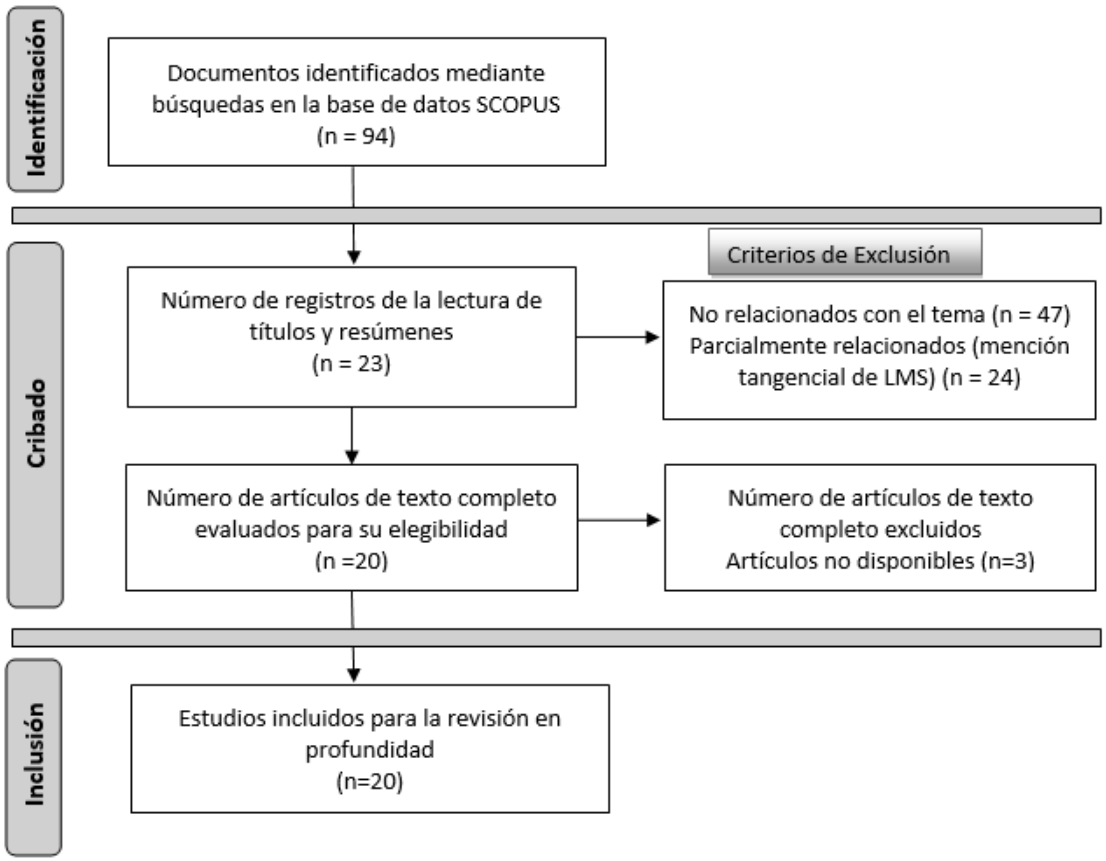
Esta fórmula de búsqueda avanzada en Scopus permitió identificar estudios que abordan tanto las vulnerabilidades de seguridad en Moodle como en otros sistemas de gestión de aprendizaje (LMS). La combinación de términos clave aseguró que se capturaran estudios relacionados con ataques cibernéticos, brechas de datos y otros riesgos de seguridad en estas plataformas. Además, se aplicaron filtros avanzados para limitar los resultados a artículos publicados entre 2020 y 2025, en idioma inglés, y en las áreas de Ciencias de la Computación e Ingeniería. Inicialmente, se identificaron 94 artículos que cumplían con estos criterios.

Selección de Estudios

Una vez identificados los 94 artículos iniciales a través de la búsqueda en Scopus, se procedió a aplicar un proceso riguroso de selección basado en criterios de inclusión y exclusión. Este proceso se llevó a cabo en dos etapas principales: cribado de títulos y resúmenes y evaluación de texto completo. El objetivo fue garantizar que solo los estudios más relevantes y de mayor calidad fueran incluidos en la revisión sistemática.

Figura 1

Diagrama de Flujo del procedimiento de selección de estudios



Nota: El diagrama presenta los datos recopilados en las distintas etapas de búsqueda, siguiendo el modelo establecido por la declaración PRISMA (Haddaway et al., 2022)

En la primera etapa, se revisaron de manera independiente los títulos y resúmenes de los 94 artículos identificados para determinar su relevancia en relación con las preguntas de investigación. Se aplicaron criterios de inclusión CI_n y exclusión CE_m. *ver Tabla 2.*

Tabla 2

Criterios de inclusión y exclusión

Criterio	Detalle
CI_1	Artículos que abordan vulnerabilidades de seguridad en Moodle y otros sistemas de gestión de aprendizaje (LMS).
CI_2	Estudios que proponen soluciones tecnológicas o metodológicas para mejorar la seguridad en LMS.
CI_3	Investigaciones publicadas en revistas revisadas por pares.
CI_4	Documentos disponibles en acceso abierto o a los que los autores tenían acceso.
CE_1	Artículos que no están relacionados con la seguridad en LMS.
CE_2	Estudios que no proporcionan datos relevantes o que carecen de rigor metodológico.
CE_3	Investigaciones con enfoque en hardware o infraestructura física
CE_4	Documentos que no están disponibles en inglés.

Tras aplicar estos criterios, se excluyeron 47 artículos por no estar relacionados con el tema y 24 por tener una relación parcial (por ejemplo, estudios que mencionaban LMS de forma tangencial sin centrarse en vulnerabilidades de seguridad). Como resultado, 23 artículos fueron considerados relevantes para la siguiente etapa de evaluación del texto completo.

En la segunda etapa, se evaluaron de manera independiente el contenido completo de los 23 artículos restantes para determinar su relevancia y calidad. Sin embargo, solo se pudo acceder al texto completo de 20 artículos, ya que 3 de ellos no estaban disponibles. Cada investigador realizó una revisión exhaustiva de los artículos, extrayendo información clave sobre las vulnerabilidades de seguridad, las soluciones propuestas y el impacto en los usuarios.

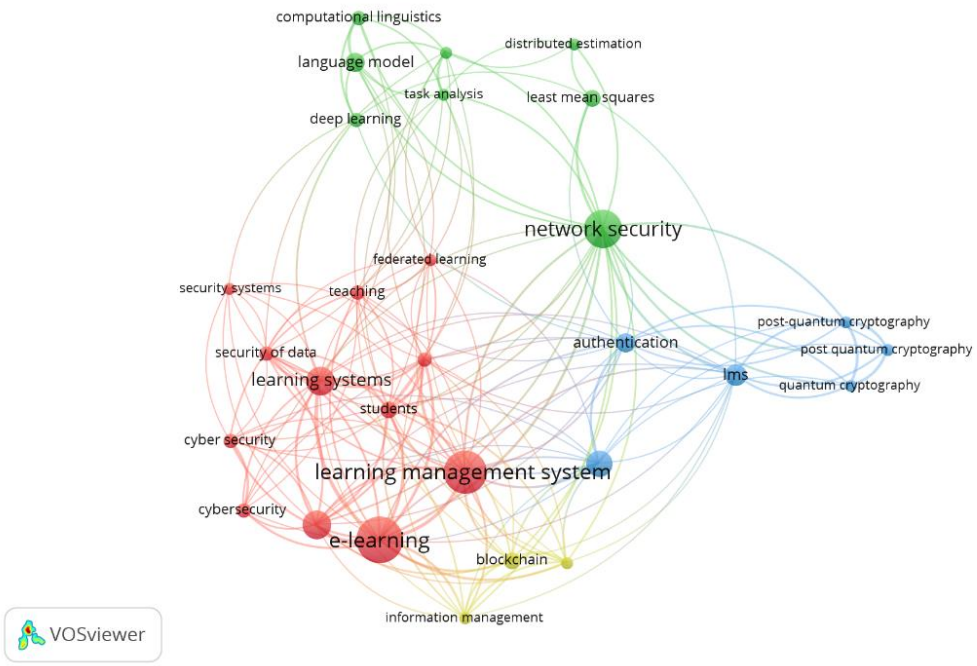
Posteriormente, se compararon los resultados para garantizar la consistencia y se resolvieron las diferencias mediante discusión y consenso. Este enfoque de revisión independiente y consenso es una práctica recomendada por PRISMA para minimizar el riesgo de sesgos y asegurar que solo los estudios más relevantes y de mayor calidad sean incluidos en el análisis (Page et al., 2021). Además, este proceso garantizó que la selección de estudios fuera transparente y reproducible.

Como parte del proceso de selección, se empleó la herramienta VOSviewer para llevar a cabo un análisis de co-ocurrencia de los términos más recurrentes en los artículos revisados. Este análisis, representado en la Figura 2, permitió identificar los temas centrales que predominan en la literatura, los cuales se enfocan principalmente en la seguridad de los sistemas de gestión de aprendizaje (LMS). Entre los aspectos más destacados se encuentran la ciberseguridad, los mecanismos de autenticación y la implementación de tecnologías innovadoras, como blockchain y la criptografía post-cuántica. Estos hallazgos sirvieron como referencia para evaluar la

pertinencia de los estudios durante la fase de selección, asegurando que los artículos incluidos abordaran las problemáticas más relevantes y actuales en el ámbito de la seguridad en LMS.

Figura 2

Coocurrencia de palabras clave



RESULTADOS

El análisis de las publicaciones por año muestra un incremento sostenido en la investigación sobre vulnerabilidades en Moodle y otros sistemas de gestión de aprendizaje (LMS). Este crecimiento puede atribuirse a la creciente adopción de plataformas de aprendizaje en línea, especialmente tras eventos globales como la pandemia de COVID-19, que impulsaron la digitalización de la educación. La Figura 3 ilustra un aumento progresivo en el número de publicaciones desde 2020 hasta 2024, con un pico notable en 2023.

Figura 3

Publicaciones durante el período de estudio

La Tabla 3 clasifica las palabras clave extraídas de los artículos revisados en categorías que abordan las principales vulnerabilidades de seguridad, las soluciones tecnológicas y

metodológicas propuestas, y el impacto de estas problemáticas en la confianza de los usuarios y la calidad del aprendizaje en línea. Cada categoría incluye su frecuencia y las palabras clave más recurrentes, lo que permite identificar los temas más relevantes y su importancia en la literatura analizada.

Tabla 3

Frecuencia de palabras recurrentes agrupadas

Nro.	Categoría	Frecuencia	Palabras recurrentes
1	Vulnerabilidades de seguridad en LMS	8	Cybersecurity vulnerabilities, Data breaches, Unauthorized access, Hacking, Exploits
2	Soluciones tecnológicas para LMS	10	Blockchain, Two-Factor Authentication, Encryption, Smart Contracts, AI Proctoring
3	Soluciones metodológicas para LMS	6	Risk Management, Penetration Testing, Security Audits, User Training, Best Practices
4	Impacto en la confianza de los usuarios	5	User Trust, Privacy Concerns, Data Integrity, Academic Integrity, User Perception
5	Impacto en la calidad del aprendizaje en línea	4	Learning Outcomes, Student Engagement, Academic Performance, Online Exam Reliability

La Tabla 4 resume los hallazgos de las investigaciones revisadas, organizando la información para identificar cómo los estudios abordan las vulnerabilidades de seguridad en LMS, las soluciones tecnológicas y metodológicas propuestas, y el impacto de estas problemáticas en la confianza de los usuarios y la calidad del aprendizaje en línea. Esta estructura facilita una comprensión clara y ordenada de los aportes de cada artículo, permitiendo una visión integral de los temas clave relacionados con la seguridad en entornos educativos digitales.

Tabla 4

Resumen de los hallazgos de los estudios seleccionados

Autores	Principal aporte
Burchart M.; Haake J.M.	Propone una solución tecnológica para mejorar la colaboración y seguridad en LMS.
Khan M.; Naz T.	Ofrece una solución tecnológica basada en blockchain para abordar vulnerabilidades de seguridad en LMS.

Abdelsalam M.; Shokry M.; Idrees A.M.	Sugiere una solución tecnológica para garantizar la integridad de los exámenes en línea.
Kepuska K.; Tomasevic M.	Identifica vulnerabilidades comunes en LMS. P2: Propone un marco metodológico para gestionar riesgos.
Cheriguene A.; Kabache T.; Adnane A.; Kerrache C.A.; Ahmad F.	Propone una solución tecnológica basada en blockchain para mejorar la seguridad en LMS.
Najm Y.A.; Alsamaraee S.; Jalal A.A.	Identifica vulnerabilidades en la nube. P2: Sugiere soluciones para mitigar riesgos en LMS basados en la nube.
Baneş V.; Ravariu C.; Appasani B.; Srinivasulu A.	Ofrece una solución tecnológica para fortalecer la autenticación en LMS.
Sadikin M.; Purnomo R.; Sari R.; Ariswanto D.A.N.; Wijaya J.; Vintari L.	Examina el impacto de las vulnerabilidades en la confianza de los usuarios.
Akacha S.A.-L.; Awad A.I.	Identifica vulnerabilidades en LMS. P2: Propone recomendaciones para mejorar la seguridad.
Amoako P.Y.O.; Osunmakinde I.O.	Ofrece una solución tecnológica para mejorar la autenticación en evaluaciones en línea.
Chatterjee P.; Bose R.; Banerjee S.; Roy S.	Propone soluciones tecnológicas para mejorar la seguridad de datos en LMS basados en la nube.
Tran T.M.; Beuran R.; Hasegawa S.	Propone una solución metodológica para mejorar la concienciación en ciberseguridad en LMS.
Al-Sherideh A.S.; Maabreh K.; Maabreh M.; Al Mousa M.R.; Asassfeh M.	Analiza el impacto de las medidas de seguridad en la confianza y participación de los usuarios.
Han Z.; Li X.; Xu G.; Xiong N.; Merlo E.; Stroulia E.	Identifica vulnerabilidades relacionadas con el control de acceso en LMS.
Korać D.; Damjanović B.; Simić D.	Propone una solución tecnológica para mejorar la gestión de identidades en LMS.

Alhazmi A.K.; Imtiaz A.; Al-Hammadi F.; Kaed E.	Identifica vulnerabilidades y factores de éxito en LMS.
Iliev O.; Yoshinov R.; Tsochev G.	Ofrece una solución tecnológica para mejorar la verificación de identidad y seguridad en LMS.
Fidas C.A.; Belk M.; Constantinides A.; Portugal D.; Martins P.; Pietron A.M.; Pitsillides A.; Avouris N.	Analiza el impacto de las soluciones de supervisión en la confianza y la integridad académica.
Mudiyanselage A.K.; Pan L.	Identifica vulnerabilidades específicas en Moodle.
Xenakis A.; Vlachos V.; Roig P.J.; Alcaraz S.	Propone una solución metodológica para mejorar la concienciación en ciberseguridad en LMS.

DISCUSIÓN

La revisión sistemática de los 20 artículos seleccionados permitió identificar las principales vulnerabilidades de seguridad en Moodle y otros sistemas de gestión de aprendizaje (LMS), así como las soluciones tecnológicas y metodológicas propuestas para abordar estos problemas. A continuación, se responde a las preguntas de investigación planteadas en el apartado de la metodología.

RPI1 El análisis de la literatura revela que las principales vulnerabilidades de seguridad en LMS, especialmente en Moodle, se pueden clasificar en tres categorías principales: vulnerabilidades técnicas, riesgos asociados al factor humano y problemas de configuración y gestión.

Entre las debilidades técnicas más recurrentes se encuentran las filtraciones de datos, que ocurren cuando los sistemas no cuentan con medidas adecuadas de cifrado o protección de la información (Najm et al., 2022). Además, se han identificado problemas de acceso no autorizado, donde usuarios malintencionados explotan fallas en los sistemas de autenticación para acceder a información confidencial (Kepuska & Tomasevic, 2024). Otro riesgo técnico destacado es la explotación de vulnerabilidades en sistemas basados en la nube, que son cada vez más utilizados para almacenar datos educativos (Chatterjee et al., 2023).

El factor humano sigue siendo una de las mayores fuentes de vulnerabilidad. Estudios como el de Tran et al. (2023) señalan que la falta de concienciación en ciberseguridad entre estudiantes

y profesores puede llevar a prácticas inseguras, como el uso de contraseñas débiles o la descarga de archivos maliciosos. Además, los ataques de phishing y la suplantación de identidad son amenazas comunes que aprovechan la desinformación de los usuarios (Fidas et al., 2023).

La configuración incorrecta de los sistemas LMS también representa un riesgo significativo. Por ejemplo, la falta de actualizaciones regulares o la implementación inadecuada de controles de acceso basados en roles (RBAC) pueden dejar brechas de seguridad expuestas (Han et al., 2020). Además, la ausencia de planes de respuesta a incidentes en muchas instituciones educativas agrava estos problemas (Kepuska & Tomasevic, 2024).

En conjunto, estas vulnerabilidades representan un desafío crítico para la seguridad de los sistemas LMS, especialmente en un contexto donde la educación en línea se ha convertido en una herramienta esencial para instituciones educativas de todo el mundo.

RPI2 En respuesta a las vulnerabilidades identificadas, se han propuesto diversas soluciones, tanto tecnológicas como metodológicas, que buscan fortalecer la seguridad de los sistemas LMS.

Entre las soluciones tecnológicas, destaca el uso de Blockchain esta tecnología ha emergido como una solución prometedora para garantizar la integridad y transparencia de los datos en LMS. Por ejemplo, Khan & Naz (2021) proponen un sistema descentralizado basado en blockchain (BLMS) que utiliza contratos inteligentes para gestionar permisos y proteger la información. Abdelsalam et al. (2024) también destacan el uso de blockchain para asegurar los resultados de exámenes en línea, evitando manipulaciones no autorizadas. Otra solución tecnológica efectiva es la autenticación de dos factores (2FA) que ha demostrado ser efectiva para reducir el riesgo de acceso no autorizado. Baneş et al. (2023) proponen un esquema de autenticación basado en certificados digitales, que mejora la seguridad en el acceso a plataformas como Moodle. Asimismo, para proteger los datos almacenados en la nube, Chatterjee et al. (2023) recomiendan el uso de técnicas criptográficas y esteganográficas, las cuales garantizan la confidencialidad e integridad de la información. Por último, en el ámbito de la supervisión Fidas et al. (2023) presentan un sistema de supervisión inteligente (TRUSTID) que utiliza reconocimiento facial y de voz para prevenir fraudes en evaluaciones en línea, mejorando la integridad académica.

En cuanto a las soluciones metodológicas, se ha destacado la importancia de la gestión de riesgos. Kepuska y Tomasevic (2024) proponen un marco ligero para la gestión de riesgos cibernéticos en instituciones educativas, que incluye la identificación de vulnerabilidades y la implementación de controles proactivos. Además, las pruebas de penetración y auditorías de seguridad son fundamentales para identificar y corregir vulnerabilidades en sistemas como Moodle, tal como lo destacan Mudiyanselage y Pan (2020). Por otro lado, la capacitación y concienciación juegan un papel crucial en la reducción de riesgos asociados con el factor humano. Tran et al. (2023) y (Xenakis et al., 2025) enfatizan la necesidad de programas de capacitación en

ciberseguridad dirigidos a estudiantes y profesores, con el fin de fomentar prácticas seguras y prevenir incidentes.

Estas soluciones, tanto tecnológicas como metodológicas, ofrecen un enfoque integral para abordar las vulnerabilidades de seguridad en LMS, aunque su implementación efectiva requiere un compromiso continuo por parte de las instituciones educativas.

RPI3 El impacto de las vulnerabilidades de seguridad en la confianza de los usuarios y la calidad del aprendizaje en línea es profundo y multifacético. Estas vulnerabilidades no solo comprometen la integridad de los sistemas, sino que también tienen consecuencias significativas en la percepción de los usuarios y en los resultados educativos.

En lo que respecta al impacto en la confianza de los usuarios, las brechas de seguridad, como las filtraciones de datos o los accesos no autorizados, erosionan la confianza en las plataformas LMS. Estudios como el de Sadikin et al. (2023) muestran que los estudiantes y profesores perciben un mayor riesgo cuando se enfrentan a incidentes de seguridad, lo que puede llevar a una disminución en el uso de estas herramientas. Además, la falta de transparencia en la gestión de datos también afecta negativamente la confianza. Por ejemplo, Al-Sherideh et al. (2023) encontraron que los estudiantes están más dispuestos a participar en actividades en línea cuando perciben que sus datos están protegidos y que las plataformas son seguras. Esto subraya la importancia de implementar medidas de seguridad robustas y comunicarlas de manera clara para mantener la confianza de los usuarios.

En cuanto a la calidad del aprendizaje en línea es igualmente significativo. Las vulnerabilidades de seguridad pueden afectar directamente la integridad académica. Por ejemplo, la manipulación de resultados de exámenes o la suplantación de identidad en evaluaciones en línea comprometen la validez de los procesos de evaluación (Fidas et al., 2023). Además, la falta de confianza en las plataformas puede llevar a una menor participación de los estudiantes en actividades colaborativas o en la entrega de tareas en línea, lo que afecta negativamente su rendimiento académico (Sadikin et al., 2023). Esto no solo perjudica a los estudiantes individualmente, sino que también puede socavar la credibilidad de las instituciones educativas que dependen de estas plataformas.

Por otro lado, la implementación de medidas de seguridad efectivas, como la autenticación biométrica (Amoako & Osunmakinde, 2020) y la supervisión basada en IA (Fidas et al., 2023), ha demostrado mejorar la confianza de los usuarios y garantizar la integridad académica. Estas soluciones no solo protegen los datos, sino que también fomentan un entorno de aprendizaje más seguro y confiable, lo que se traduce en una mayor participación y mejores resultados académicos.

CONCLUSIONES

La revisión sistemática realizada evidencia que las vulnerabilidades de seguridad en Moodle y otros LMS representan un desafío significativo para la educación en línea. Estas

vulnerabilidades se clasifican en tres categorías principales: técnicas, humanas y de configuración, cada una con implicaciones críticas para la integridad y confidencialidad de los datos. Las soluciones tecnológicas, como el uso de blockchain y la autenticación de dos factores, han demostrado ser efectivas para mitigar estos riesgos. Sin embargo, la implementación de estas soluciones debe ir acompañada de un enfoque metodológico que incluya la gestión de riesgos, auditorías de seguridad y programas de capacitación en ciberseguridad para usuarios. La confianza de los estudiantes y profesores en estas plataformas depende en gran medida de la percepción de seguridad, lo que subraya la necesidad de comunicar de manera clara y transparente las medidas de protección implementadas. En conclusión, aunque se han logrado avances significativos en la seguridad de los LMS, es fundamental que las instituciones educativas adopten un enfoque integral y proactivo para garantizar un entorno de aprendizaje en línea seguro y confiable en el futuro.

REFERENCIAS

Abdelsalam, M., Shokry, M., & Idrees, A. M. (2024). A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain. *IEEE Access*, *12*, 7719–7733. https://doi.org/10.1109/ACCESS.2023.3304995

Al-Sherideh, A. S., Maabreh, K., Maabreh, M., Al Mousa, M. R., & Asassfeh, M. (2023). Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study. *International Journal of Advanced Computer Science and Applications*, *14*(5), 158–164. https://doi.org/10.14569/IJACSA.2023.0140516

Amoako, Y. O., & Osunmakinde, I. O. (2020). Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments. In *Int. J. Technology Enhanced Learning* (Vol. 12, Issue 2).

Baneş, V., Ravariu, C., Appasani, B., & Srinivasulu, A. (2023). A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform. *Applied Sciences 2023, Vol. 13, Page 9675*, *13*(17), 9675. https://doi.org/10.3390/APP13179675

Burchart, M., Haake, J., & Haake, J. M. (2023). Supporting collaborative writing tasks in large-scale distance education. *Authorea Preprints*. https://doi.org/10.36227/TECHRXIV.24466321.V1

Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing Data Security of Cloud Based LMS. *Wireless Personal Communications*, *130*(2), 1123–1139. https://doi.org/10.1007/s11277-023-10323-5

Fidas, C. A., Belk, M., Constantinides, A., Portugal, D., Martins, P., Pietron, A. M., Pitsillides, A., & Avouris, N. (2023). Ensuring Academic Integrity and Trust in Online Learning Environments: A Longitudinal Study of an AI-Centered Proctoring System in Tertiary Educational Institutions. *Education Sciences*, *13*(6), 566. https://doi.org/10.3390/educsci13060566

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, *18*(2), e1230. https://doi.org/10.1002/CL2.1230

Han, Z., Li, X., Xu, G., Xiong, N., Merlo, E., & Stroulia, E. (2020). An Effective Evolutionary Analysis Scheme for Industrial Software Access Control Models. *IEEE Transactions on Industrial Informatics*, *16*(2), 1024–1034. https://doi.org/10.1109/TII.2019.2925422

Kepuska, K., & Tomasevic, M. (2024). A lightweight framework for cyber risk management in Western Balkan higher education institutions. *PeerJ Computer Science*, *10*, 1–23. https://doi.org/10.7717/PEERJ-CS.1958/SUPP-1

Khan, M., & Naz, T. (2021). Smart Contracts Based on Blockchain for Decentralized Learning Management System. *SN Computer Science*, *2*(4). https://doi.org/10.1007/s42979-021-00661-1

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J. A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J. J., Devereaux, P. J., Dickersin, K., Egger, M., Ernst, E., Gøtzsche, P. C., … Tugwell, P. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLOS Medicine*, *6*(7), e1000097. https://doi.org/10.1371/JOURNAL.PMED.1000097

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, *106*(1), 213–228. https://doi.org/10.1007/S11192-015-1765-5/METRICS

Mudiyanselage, A. K., & Pan, L. (2020). Security test MOODLE: a penetration testing case study. *International Journal of Computers and Applications*, *42*(4), 372–382. https://doi.org/10.1080/1206212X.2017.1396413

Najm, Y. A., Alsamaraee, S., & Jalal, A. A. (2022). Cloud computing security for e-learning during COVID-19 pandemic. *Indonesian Journal of Electrical Engineering and Computer Science*, *27*(3), 1610–1618. https://doi.org/10.11591/ijeecs.v27.i3.pp1610-1618

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*. https://doi.org/10.1136/BMJ.N71

Sadikin, M., Purnomo, R., Sari, R., Ariswanto, D. A. N., Wijaya, J., & Vintari, L. (2023). Information Security on Learning Management System Platform from the Perspective of the User during the COVID-19 Pandemic. *Journal of Information and Communication Convergence Engineering*, *21*(1), 32–44. https://doi.org/10.56977/jicce.2023.21.1.32

Tran, T. M., Beuran, R., & Hasegawa, S. (2023). Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning. *International Journal of Information and Education Technology*, *13*(4), 724–730. https://doi.org/10.18178/ijiet.2023.13.4.1859

Xenakis, A., Vlachos, V., Roig, P. J., & Alcaraz, S. (2025). Addressing the Necessity of CyberSecurity Literacy: The case of ETTCS CyberTeach Project. *Information and Computer Security*. https://doi.org/10.1108/ICS-04-2024-0095