runas
Journal of Education & Culture

Análisis de vulnerabilidades en entornos virtuales de aprendizaje. Caso Práctico: Instituto Superior Tecnológico Ismael Pérez Pazmiño

Vulnerability analysis in virtual learning environments. Case Study: Instituto Superior Tecnológico Ismael Pérez Pazmiño

Eduardo Rodolfo Tapia Noblecilla, Manuel Salvador Álvarez Vera, Miguel Santiago Andrade López

Resumen

En el Instituto Superior Tecnológico Ismael Pérez Pazmiño, se llevó a cabo una evaluación de seguridad en las plataformas virtuales de aprendizaje Moodle, Amauta y Atenea, con el objetivo de identificar posibles vulnerabilidades. La metodología incluyó escaneos de vulnerabilidades, pruebas de penetración, revisión de configuraciones, análisis de registros, entrevistas con personal y usuarios, revisión de incidentes anteriores y validación con expertos en ciberseguridad. Los resultados revelaron la existencia de vulnerabilidades críticas, tales como inyección SQL, ejecución remota de código, fallas de cross-site scripting (XSS), fuga de información, navegación de directorios, malas prácticas de programación, configuraciones inseguras y políticas de contraseñas débiles, comprometiendo la integridad y privacidad de los datos. Para mitigar estos riesgos, se recomienda aplicar parches de seguridad, fortalecer las políticas y configuraciones, implementar controles adicionales como sistemas de prevención y detección de intrusos, adoptar prácticas de programación segura, mejorar la gestión de identidades y accesos mediante autenticación multifactor, elevar la conciencia y capacitación en seguridad, establecer un programa de monitoreo y respuesta a incidentes, cumplir con las normativas y estándares pertinentes, y considerar la contratación de servicios de auditoría externa, abordando estas vulnerabilidades de manera proactiva e integral.

Palabras clave: Vulnerabilidades; Seguridad; Plataformas virtuales; Evaluación; Mitigación

Eduardo Rodolfo Tapia Noblecilla
Universidad Católica de Cuenca | Cuenca | Ecuador | eduardo.tapia.19@est.ucacue.edu.ec
https://orcid.org/0000-0002-1598-401X
Manuel Salvador Álvarez Vera
Universidad Católica de Cuenca | Cuenca | Ecuador | malvarezv@ucacue.edu.ec
https://orcid.org/0000-0002-2521-0042
Miguel Santiago Andrade López
Universidad Católica de Cuenca | Cuenca | Ecuador | msandradel@ucacue.edu.ec
https://orcid.org/0000-0002-6882-4204

https://doi.org/10.46652/runas.v5i10.199
ISSN 2737-6230
Vol. 5 No. 10 julio-diciembre 2024, e240199
Quito, Ecuador

Enviado: junio 16, 2024
Aceptado: agosto 27, 2024
Publicado: septiembre 17, 2024
Publicación Continua

Abstract

At the Ismael Pérez Pazmiño Higher Technological Institute, a security assessment was conducted on the virtual learning platforms Moodle, Amauta, and Atenea, with the aim of identifying potential vulnerabilities. The methodology included vulnerability scans, penetration testing, configuration reviews, log analysis, interviews with personnel and users, review of previous incidents, and validation with cybersecurity experts. The results revealed the existence of critical vulnerabilities, such as SQL injection, remote code execution, cross-site scripting (XSS) flaws, information leakage, directory traversal, insecure coding practices, weak configurations, and weak password policies, compromising the integrity and privacy of data. To mitigate these risks, it was recommended to apply security patches, strengthen policies and configurations, implement additional controls such as intrusion prevention and detection systems, adopt secure coding practices, improve identity and access management through multi-factor authentication, raise security awareness and training, establish an incident monitoring and response program, comply with relevant regulations and standards, and consider contracting external audit services, addressing these vulnerabilities proactively and comprehensively.

Keywords: Vulnerabilities; Security; Virtual platforms; Assessment; Mitigation

Introducción

Los entornos virtuales de aprendizaje han ganado una importancia crucial en la educación moderna, facilitando la impartición de cursos a distancia y mejorando la experiencia de enseñanza-aprendizaje (Al-Fraihat et al., 2020). El Instituto Superior Tecnológico Ismael Pérez Pazmiño ha adoptado plataformas como Moodle, Amauta y Atenea para aprovechar los beneficios de estas tecnologías. Sin embargo, a medida que la dependencia de estos sistemas aumenta, también lo hace la necesidad de abordar los desafíos de seguridad asociados con su uso (Vega-Oyola et al., 2022).

A pesar de sus ventajas, los entornos virtuales de aprendizaje pueden ser vulnerables a diversas amenazas cibernéticas, como ataques de inyección de código, secuestro de sesiones y acceso no autorizado, lo que compromete la privacidad y la integridad de los datos de los usuarios (Costinela-Luminiţa y Nicoleta-Magdalena, 2012). Este artículo aborda la necesidad de evaluar la seguridad de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño para identificar y mitigar las vulnerabilidades existentes.

Numerosos estudios han destacado la importancia de la seguridad en los entornos virtuales de aprendizaje y han explorado diferentes técnicas y enfoques para evaluar y mejorar la seguridad de estas plataformas (Gutiérrez-Oquendo y Luz-O Giraldo, 2022). Sin embargo, la naturaleza dinámica de las amenazas cibernéticas y la evolución constante de las tecnologías requieren evaluaciones periódicas y adaptadas a entornos específicos (Rendón Ortiz y Aldana García, 2015).

Este artículo evalúa la seguridad de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño mediante escaneos de vulnerabilidades, pruebas de penetración, revisión de configuraciones y análisis de registros, con el objetivo de identificar vulnerabilidades, evaluar los riesgos asociados y proponer medidas de mitigación. La importancia de

esta investigación radica en la creciente dependencia de los entornos virtuales de aprendizaje y la necesidad de garantizar la seguridad de los datos de los usuarios (Martínez Escobar et al., 2016). Los resultados permitirán al Instituto proteger la información confidencial y ofrecer un entorno de aprendizaje seguro.

Este artículo estará organizado de la siguiente manera: después de la introducción, se presentará la metodología utilizada en el artículo, seguida de los resultados y hallazgos. Luego, se discutirán los resultados y se proporcionarán recomendaciones detalladas para mitigar los riesgos identificados. Finalmente, se presentarán las conclusiones y las implicaciones del artículo.

Metodología

La investigación desarrollada fue de tipo descriptiva, debido a que se enfocó en evaluar y describir el estado actual de la seguridad de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño, identificando vulnerabilidades y brechas de seguridad existentes. Por lo que Baroja Llanos y Narváez Erazo (2018), indican que este enfoque permite obtener una comprensión detallada de los riesgos de seguridad presentes en estas plataformas y sentar las bases para futuras mejoras.

Se utilizaron fuentes de información primaria y secundaria para recopilar los datos necesarios para el artículo. Como fuentes primarias, se realizaron escaneos de vulnerabilidades, pruebas de penetración, revisión de configuraciones y análisis de registros de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño. Según OWASP (2021), menciona que estas técnicas permiten obtener información de primera mano sobre las debilidades de seguridad presentes en los sistemas.

Por otro lado, en la recolección secundaria de datos, se revisó literatura científica relevante sobre seguridad en entornos virtuales de aprendizaje, en la cual García y Pesantez (2023), indican que se deben incluir artículos de investigación, informes técnicos y guías de mejores prácticas. Esta revisión proporcionó un marco teórico sólido y permitió comparar los hallazgos del artículo con investigaciones previas en el campo.

Los instrumentos de investigación principales fueron herramientas de escaneo de vulnerabilidades ampliamente reconocidas y utilizadas en la industria, como Nessus, y OpenVAS (OpenVAS, 2021; Tenable, 2021). Estas herramientas automatizadas permitieron identificar de manera eficiente las vulnerabilidades presentes en las plataformas objetivo. Además, se emplearon técnicas manuales de pruebas de penetración siguiendo metodologías reconocidas como OWASP Testing Guide. En la cual OWASP (2021), menciona que estas pruebas proporcionan una evaluación más profunda y detallada de las debilidades de seguridad, complementando los resultados de las herramientas automatizadas.

La población del artículo comprendió todas las instancias de las plataformas Moodle, Amauta y Atenea desplegadas en el Instituto Superior Tecnológico Ismael Pérez Pazmiño. Dado que evaluar

exhaustivamente todas las instancias sería un proceso excesivamente laborioso y prolongado, se aplicó un muestreo intencional para seleccionar las instancias más críticas y representativas de cada plataforma (Martínez Cornelio, 2022).

La muestra se determinó considerando factores como el número de usuarios, la sensibilidad de los datos almacenados y la importancia para los procesos educativos. Esta estrategia de muestreo permitió obtener resultados significativos y generalizables, al tiempo que optimizaba los recursos y el tiempo dedicado a la evaluación de seguridad.

Los datos recopilados se analizaron utilizando herramientas especializadas de gestión de vulnerabilidades, que permitieron consolidar y priorizar los hallazgos de seguridad de las diferentes plataformas. Este enfoque de análisis combinado proporcionó una visión integral de la seguridad de las plataformas Moodle, Amauta y Atenea, permitiendo extraer conclusiones significativas y formular recomendaciones prácticas para la mitigación de riesgos.

Resultados

Los resultados de la investigación sobre la seguridad de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño revelaron varias vulnerabilidades y brechas de seguridad que requerían atención. La Tabla 1 presenta un resumen de los hallazgos más significativos, clasificados por plataforma y nivel de riesgo.

Tabla 1. Resumen de vulnerabilidades identificadas por plataforma y nivel de riesgo

Plataforma	Vulnerabilidades Críticas	Vulnerabilidades Altas	Vulnerabilidades Medias	Vulnerabilidades Bajas
Moodle	2	2	4	6
Amauta	1	2	3	5
Atenea	0	3	3	3
Total	3	7	10	14

Fuente: elaboración propia

Como se observa en la Tabla 1, Moodle presentó el mayor número de vulnerabilidades críticas y altas, seguido de Amauta y Atenea. Estas vulnerabilidades incluyeron inyección de SQL, cross-site scripting (XSS) y configuraciones inadecuadas de seguridad, entre otras y la necesidad de implementar medidas de seguridad más sólidas.

Además, la categoría más prevalente fue las configuraciones inadecuadas en el control de acceso, en la cual las plataformas evaluadas carecían de controles adecuados para restringir el acceso no autorizado a recursos y funcionalidades sensibles. Otra de las vulnerabilidades técnicas, que se identificó fueron deficiencias en las prácticas de gestión de parches y actualizaciones de seguridad. La Tabla 2 muestra el porcentaje de instancias de cada plataforma que se encontraban desactualizadas en el momento de la evaluación.

Tabla 2. Porcentaje de instancias desactualizadas por plataforma

Plataforma	Instancias Desactualizadas
Moodle	35%
Amauta	42%
Atenea	28%

Fuente: elaboración propia

Estos resultados destacan la importancia de mantener las plataformas actualizadas con los últimos parches de seguridad para mitigar los riesgos asociados con vulnerabilidades conocidas. En cuanto a las pruebas de penetración manual, se logró obtener acceso no autorizado a datos sensibles en el 15% de las instancias evaluadas, lo que demuestra la criticidad de las vulnerabilidades identificadas.

Los resultados de este artículo proporcionaron una visión integral del estado de seguridad de las plataformas Moodle, Amauta y Atenea en el Instituto Superior Tecnológico Ismael Pérez Pazmiño. Los hallazgos señalaron la necesidad de abordar las vulnerabilidades identificadas, fortalecer las prácticas de gestión de parches y fomentar una cultura de seguridad en toda la organización.

Discusión

Los resultados obtenidos en este artículo revelan vulnerabilidades significativas en las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño. La presencia de vulnerabilidades críticas y altas en todas las plataformas evaluadas indica un riesgo considerable para la privacidad de los usuarios y seguridad de los datos. Estos resultados coinciden con estudios anteriores que han subrayado la importancia de abordar las vulnerabilidades en los entornos de aprendizaje virtuales (Broncano y Pesantez, 2021).

La prevalencia de vulnerabilidades relacionadas con la pérdida de control de acceso y la exposición de datos sensibles sugiere deficiencias en los mecanismos de autenticación y autorización implementados en las plataformas. Estas debilidades pueden permitir a usuarios no autorizados acceder a información confidencial y comprometer la integridad del sistema (OWASP, 2021). Además, Espejo et al. (2020), indican que la falta de actualizaciones regulares y la presencia de configuraciones de seguridad incorrectas contribuyen a un mayor riesgo de explotación de vulnerabilidades conocidas.

Los resultados de este artículo son consistentes con investigaciones previas que han evaluado la seguridad de plataformas de aprendizaje en línea. Por ejemplo, un artículo realizado por Zúñiga Paredes et al. (2021), encontraron vulnerabilidades similares en instancias de Moodle en la Universidad de los Andes, incluyendo inyección de SQL y XSS. Asimismo, Arias Paredes (2019), identificó deficiencias en las prácticas de gestión de parches y actualizaciones en los servidores virtuales de la ESPOCH.

Sin embargo, este artículo se distingue por su enfoque integral, que abarca no solo las vulnerabilidades técnicas, sino también las brechas en los procedimientos y políticas de seguridad de los datos. Esta perspectiva más amplia permite una comprensión más completa de los desafíos de seguridad en los entornos virtuales de aprendizaje (Baroja Llanos y Narváez Erazo, 2018).

Si bien este artículo proporciona información valiosa sobre el estado de seguridad de las plataformas Moodle, Amauta y Atenea en el Instituto Superior Tecnológico Ismael Pérez Pazmiño, es importante reconocer algunas limitaciones. En primer lugar, el artículo se limitó a una sola institución educativa, lo que puede reducir la aplicabilidad de los resultados a otros contextos. Además, el artículo se centró en un momento específico en el tiempo y no abordó la evolución de las vulnerabilidades a lo largo del tiempo.

Otra limitación es que el artículo se basó principalmente en pruebas de penetración y análisis de vulnerabilidades técnicas, y no profundizó en aspectos como la ingeniería social o las amenazas internas. Futuras investigaciones podrían abordar estas limitaciones mediante la inclusión de múltiples instituciones, la realización de estudios longitudinales y la incorporación de un espectro más amplio de vectores de amenazas. Los resultados más importantes de este artículo incluyen:

- La presencia de vulnerabilidades críticas y altas en todas las plataformas evaluadas, lo que indica un riesgo significativo para la seguridad de la información.
- La prevalencia de vulnerabilidades relacionadas con la pérdida de control de acceso y la exposición de datos sensibles, lo que sugiere deficiencias en los mecanismos de autenticación y autorización (OWASP, 2021).
- La falta de actualizaciones regulares y la presencia de configuraciones de seguridad incorrectas, que contribuyen a un mayor riesgo de explotación de vulnerabilidades conocidas (Espejo et al., 2020).
- Brechas en los procedimientos y políticas de seguridad de la información, incluyendo deficiencias en la gestión de acceso y autenticación, gestión de parches y actualizaciones, capacitación y concienciación, y respuesta a incidentes

Estos resultados destacan la necesidad de abordar de manera proactiva las debilidades identificadas y fortalecer las medidas de seguridad en las plataformas de aprendizaje en línea del Instituto Superior Tecnológico Ismael Pérez Pazmiño. Con base en los resultados y las limitaciones de este artículo, se proponen las siguientes recomendaciones para futuras aplicaciones e investigaciones:

- Implementar medidas de seguridad más sólidas, como autenticación multifactor, políticas de contraseñas robustas y cifrado de datos sensibles, para abordar las vulnerabilidades identificadas (Navarrete et al., 2023; OWASP, 2021).
- Establecer un proceso formal de gestión de parches y actualizaciones para garantizar que las plataformas de aprendizaje en línea se mantengan actualizadas con los últimos parches de seguridad (Vallejo Ballesteros, 2022).

- Desarrollar y implementar políticas y procedimientos de seguridad de la información integrales, que abarquen aspectos como la gestión de acceso y autenticación, la capacitación y concienciación del personal, y la respuesta a incidentes (Alvarado Tapia y Montesdeoca Cabrera, 2017).
- Llevar a cabo evaluaciones de seguridad regulares y detalladas para identificar y corregir vulnerabilidades antes de que puedan ser aprovechadas por atacantes malintencionados (Broncano y Pesantez, 2021).
- Ampliar el alcance de futuras investigaciones para incluir múltiples instituciones educativas, realizar estudios longitudinales y abordar un espectro más amplio de vectores de amenazas, como la ingeniería social y las amenazas internas

Al implementar estas recomendaciones, el Instituto Superior Tecnológico Ismael Pérez Pazmiño y otras instituciones educativas pueden fortalecer la seguridad de sus plataformas de aprendizaje en línea, proteger los datos confidenciales y garantizar un entorno educativo seguro y confiable para estudiantes y profesores.

Conclusión

Este artículo evaluó la seguridad de las plataformas Moodle, Amauta y Atenea del Instituto Superior Tecnológico Ismael Pérez Pazmiño, identificando vulnerabilidades significativas y brechas de seguridad. Los hallazgos incluyen vulnerabilidades críticas y altas en todas las plataformas, debilidades en el control de acceso y exposición de datos sensibles, deficiencias en la gestión de parches y actualizaciones, y brechas en los procedimientos y políticas de seguridad de los datos.

Los resultados destacan la necesidad de abordar proactivamente las debilidades y fortalecer las medidas de seguridad en las plataformas de aprendizaje en línea. La implementación de medidas de seguridad sólidas, la gestión formal de parches y actualizaciones, y el desarrollo de políticas y procedimientos de seguridad integrales son cruciales para mitigar riesgos y garantizar un entorno educativo seguro.

Los resultados tienen implicaciones prácticas significativas para el Instituto Superior Tecnológico Ismael Pérez Pazmiño y otras instituciones educativas que utilizan plataformas de aprendizaje en línea. Los hallazgos destacan la importancia de realizar evaluaciones de seguridad periódicas, implementar medidas de seguridad robustas y establecer políticas y procedimientos de seguridad integrales.

Desde un enfoque teórico, este artículo aporta a la literatura sobre seguridad en entornos virtuales de aprendizaje, proporcionando evidencia empírica sobre vulnerabilidades y brechas de seguridad en plataformas específicas. Los resultados respaldan estudios previos y destacan la importancia de abordar los desafíos de seguridad desde una perspectiva integral, considerando tanto vulnerabilidades técnicas como brechas en políticas y procedimientos.

Referencias

Al-Fraihat, D., Joy, M., Masa'deh, R., y Sinclair, J. (2020). Evaluating E-learning systems success: An empirical study. *Computers in Human Behavior*, 102, 67-86. https://doi.org/10.1016/J.CHB.2019.08.004

Alvarado Tapia, A. C., y Montesdeoca Cabrera, R. A. (2017). *Análisis de vulnerabilidades del servidor e-learning de la espoch para la implementación de mejores prácticas de seguridad-acceso* [Tesis de licenciatura, Escuela Superior Politécnica De Chimborazo].

Arias Paredes, A. S. (2019). *Análisis de vulnerabilidades de servidores virtuales, caso práctico servicios web informativos de la Espoch* [Tesis de licenciatura, Escuela Superior Politécnica De Chimborazo].

Baroja Llanos, F. D., y Narváez Erazo, L. D. (2018). Metodología contra Vulnerabilidades en Ambientes de Aprendizaje Virtuales Methodology against Vulnerabilities in Virtual Learning Environments. *Revista Iberica de Sistemas e Tecnologias de Informacion, 15*(4), 282-291.

Broncano, M. P. E., y Pesantez, D. F. Á. (2021). Cybersecurity in learning management system (LMS*). Ecuadorian Science Journal, 5*(1), 46-54. https://doi.org/10.46480/esj.5.1.98

Costinela-Luminiţa, C., y Nicoleta-Magdalena, C. (2012). E-learning Security Vulnerabilities. *Procedia–Social and Behavioral Sciences*, 46, 2297-2301. https://doi.org/10.1016/J.SBSPRO.2012.05.474

Espejo, A. J. P., Bernal Reinoso, C. A., y Segura Greco, M. A. (2020). *Análisis de ciberseguridad para una empresa de educación virtual.* Universidad el Bosque. https://repositorio.unbosque.edu.co/handle/20.500.12495/8100

Garcia, P. A. P., y Pesantez, D. A. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectivas, 5*(1), 19-29. https://doi.org/10.47187/PERSPECTIVAS.5.1.179

Gutierrez-Oquendo, H., y Luz-O Giraldo. (2022). Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza – aprendizaje. *Publicaciones e Investigacion, 16*(1).

Martinez Cornelio, S. (2022). *Implementación de una metodología de pentesting haciendo uso de kubernetes en entornos virtuales* [Tesis de licenciatura, Benemérita Universidad Autónoma De Puebla].

Martinez Escobar, H. A., Dominguez Perez, D. A., y Perez Rul, M. N. (2016). La seguridad informática en las plataformas educativas que se utilizan en el nivel superior: una tarea pendiente. *Revista Multidisciplinaria de Avances de Investigacion, 2*(3), 15-33.

Navarrete, J., Sánchez, I., y Carpio, R. (2023). Vista de Actividades de evaluación de los aprendizajes en la modalidad de estudio en línea. Caso Instituto Superior Universitario Almirante Illingworth. *Revista Nexos Científicos, 7*(2), 29-40.

OpenVAS. (2021). Open Vulnerability Assessment Scanner. Open Vulnerability Assessment Scanner. https://lc.cx/rsMBXH

OWASP. (2021). Open Web Application Security Project. OWASP Top Ten. Open Web Application Security Project. https://owasp.org/www-project-top-ten/

Rendón Ortiz, O. L., y Aldana García, J. A. (2015). *Una aproximación a la identificación de riesgos tecnológicos presentes en sistemas virtuales de enseñanza y aprendizaje* [Tesis de licenciatura, Corporación universitaria minuto de Dios].

Tenable. (2021). Nessus Professional. https://lc.cx/gRYEpK

Vallejo Ballesteros, H. F. (2022). *Análisis de los servicios de red de los entornos virtuales de aprendizaje, para implementar un plan de mejora en la red de datos de la Universidad Estatal de Bolívar, 2021* [Tesis de maestría, Escuela Superior Politécnica de Chimborazo].

Vega-Oyola, C., Tapia-Noblecilla, E., y Gallardo-Gonzaga, F. (2022). Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL. *Espíritu Emprendedor TES, 6*(1), 70-88. https://doi.org/10.33970/eetes.v6.n1.2022.293

Zuñiga Paredes, R. M., Jalón Arias, E. J., Andrade Olmedo, M. E., y Giler Chango, J. L. (2021). Analysis of computer security in virtual environments of the autonomous regional university of the andes extension queve-do in times of Covid-19. *Revista Universidad y Sociedad, 13*(3), 454-459.

Autores

Eduardo Rodolfo Tapia Noblecilla. Ingeniero de Sistemas graduado en la Universidad Técnica de Machala, ha construido una carrera sólida y versátil en el desarrollo de software. Actualmente se desempeña como Coordinador del Programa de Desarrollo de Software en el Instituto Tecnológico Superior Ismael Pérez Pazmiño.

Manuel Salvador Álvarez Vera. Docente de la Maestría en Ciberseguridad

Miguel Santiago Andrade López. Docente de la Maestría en Ciberseguridad

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.