DOI: https://doi.org/10.56712/latam.v6i1.3358

Escudo Digital - un curso interactivo de ciberseguridad para la Unidad Educativa Isaac Jesús Barrera

Digital Shield - an interactive cybersecurity course for the Isaac Jesús Barrera Educational Unit

Kevin Alexander Jiménez Hurtado
kevjimal24@gmail.com
https://orcid.org/0009-0005-2862-5306
Investigador independiente
Latacunga – Ecuador

Artículo recibido: 13 de enero de 2025. Aceptado para publicación: 27 de enero de 2025.
Conflictos de Interés: Ninguno que declarar.

Resumen

Este artículo presenta el desarrollo de un curso interactivo, MOOC (Massive Open Online Course) enfocado en ciberseguridad para los estudiantes de la Unidad Educativa Isaac Jesús Barrera, ubicada en Otavalo, Ecuador. El objetivo es fortalecer la conciencia y protección digital a través de materiales educativos digitales. Utilizando un enfoque de métodos mixtos, se diseñó un curso interactivo para mejorar la comprensión de los estudiantes sobre los riesgos digitales y las medidas prácticas de ciberseguridad. Los resultados muestran una mejora significativa en la conciencia de ciberseguridad de los estudiantes, con niveles de conocimiento que aumentaron del 25% al 85% después de completar el MOOC. El curso ayudó a los estudiantes a reconocer amenazas digitales como el phishing y a aplicar medidas de seguridad efectivas, demostrando que los MOOCs pueden ser una herramienta eficaz en la educación digital.

Palabras clave: MOOC, ciberseguridad, educación digital, protección en línea

Abstract

This paper presents the development of a cybersecurity-focused MOOC (Massive Open Online Course) for students at Isaac Jesús Barrera Educational Unit, located in Otavalo, Ecuador. The aim is to strengthen online awareness and protection through digital educational materials. Using a mixed-methods approach, an interactive course was designed to improve students' understanding of digital risks and practical cybersecurity measures. The results show a significant improvement in the students' cybersecurity awareness, with knowledge levels increasing from 25% to 85% after completing the MOOC. The course helped students recognize digital threats such as phishing and apply effective security measures, demonstrating that MOOCs can be an effective tool in digital education.

Keywords: MOOC, cybersecurity, digital education, online protection

Cómo citar: Jiménez Hurtado, K. A. (2025). Escudo Digital - un curso interactivo de ciberseguridad para la Unidad Educativa Isaac Jesús Barrera. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 6 (1), 554 – 560. https://doi.org/10.56712/latam.v6i1.3358*

INTRODUCCIÓN

La ciberseguridad se ha convertido en una preocupación global debido al aumento de los ataques cibernéticos y la creciente dependencia de las tecnologías digitales. Según el European Union Agency for Cybersecurity (ENISA, 2020), la educación en ciberseguridad es crucial para proteger a los usuarios de amenazas en línea. En el ámbito educativo, los estudiantes son especialmente vulnerables, ya que utilizan dispositivos digitales y acceden a plataformas en línea de manera cotidiana.

Bajo este contexto, la Unidad Educativa Isaac Jesús Barrera, ubicada en Otavalo, Ecuador, enfrenta desafíos significativos relacionados con la protección digital de sus estudiantes. La falta de formación específica en ciberseguridad aumenta la exposición a riesgos como el phishing, el ciberacoso y la pérdida de datos personales. Este proyecto busca abordar esta problemática mediante la implementación de un MOOC diseñado para educar y capacitar a los estudiantes en medidas de protección digital.

Un MOOC (Massive Open Online Course) es un curso en línea de acceso masivo que permite a personas de todo el mundo participar en programas educativos a través de plataformas digitales. Estos cursos ofrecen contenidos estructurados, incluyendo videos, evaluaciones y foros de discusión, lo que facilita el aprendizaje autónomo y flexible. Los MOOCs se han popularizado en los últimos años debido a su capacidad para llegar a un gran número de participantes y ofrecer educación de calidad a bajo costo, siendo una herramienta clave para democratizar el acceso al conocimiento en diversas áreas, incluida la ciberseguridad.

Diversos estudios han destacado la importancia de la educación en ciberseguridad para prevenir riesgos digitales. Clough (2015) subraya que la formación en ciberseguridad debe comenzar a una edad temprana para que los usuarios puedan reconocer y mitigar amenazas. Van Niekerk y von Solms (2010) sostienen que los programas educativos deben enfocarse en mejorar la conciencia de los usuarios sobre los riesgos cibernéticos y fomentar prácticas seguras en línea.

El marco de ciberseguridad del NIST (2018) proporciona una guía integral para identificar, proteger, detectar, responder y recuperarse ante amenazas digitales. Este marco ha sido adoptado en instituciones educativas para fortalecer la seguridad digital de estudiantes y personal. Además, Ponemon Institute (2022) destaca que las organizaciones que implementan programas de concienciación en ciberseguridad experimentan una reducción significativa en los incidentes de seguridad.

La Unidad Educativa Isaac Jesús Barrera no cuenta actualmente con un programa de formación en ciberseguridad, lo que expone a sus estudiantes a diversos riesgos digitales. Los estudiantes carecen de conocimientos prácticos sobre cómo protegerse en línea, lo que aumenta su vulnerabilidad ante ataques cibernéticos. Este proyecto busca responder a las siguientes preguntas de investigación: ¿Puede un curso MOOC mejorar la conciencia y las prácticas de seguridad digital en estudiantes de la Unidad Educativa Isaac Jesús Barrera?, ¿Qué riesgos digitales enfrentan los estudiantes de la Unidad Educativa Isaac Jesús Barrera?,¿Qué contenidos y estrategias educativas son más efectivos para enseñar medidas de protección digital?,¿Cómo influye el MOOC en la mejora de la conciencia y las prácticas de seguridad digital de los estudiantes?

El objetivo general de este proyecto es desarrollar un MOOC de ciberseguridad que fortalezca la conciencia y las prácticas de seguridad digital de los estudiantes de la Unidad Educativa Isaac Jesús Barrera. Este objetivo general se desglosa en tres objetivos específicos: analizar los riesgos digitales más comunes a los que están expuestos los estudiantes, diseñar materiales educativos interactivos que abordan medidas de protección digital y evaluar el impacto del MOOC en la mejora de la conciencia y las prácticas de seguridad digital de los estudiantes.

METODOLOGÍA

Este estudio adoptó un enfoque mixto, combinando métodos cualitativos y cuantitativos. El enfoque cualitativo permitió explorar las percepciones y experiencias de los estudiantes respecto a la ciberseguridad mediante entrevistas y debates. Por otro lado, el enfoque cuantitativo se utilizó para medir el impacto del MOOC a través de cuestionarios pre y post implementación del curso.

El diseño de la investigación fue cuasi-experimental, con un grupo de prueba que participó en el MOOC y completó evaluaciones antes y después de su participación. El curso se estructuró en módulos interactivos, incluyendo videos, actividades prácticas y foros de discusión para consolidar los conocimientos adquiridos.

Los participantes del estudio fueron 39 estudiantes del décimo año de educación básica de la Unidad Educativa Isaac Jesús Barrera, con edades entre 15 y 16 años. La selección se realizó de manera intencional, considerando su acceso a dispositivos tecnológicos y disposición para participar en el curso. El curso se desarrolló en formato SCORM y fue implementado en la plataforma Moodle de la institución educativa. Los estudiantes accedieron a los módulos de aprendizaje desde las salas de computación del colegio.

Se utilizaron diversos instrumentos para la recolección de datos, como entrevistas semiestructuradas, cuestionarios y observaciones directas. Las entrevistas fueron diseñadas para explorar las percepciones iniciales y finales sobre la ciberseguridad, mientras que los cuestionarios midieron el nivel de conocimiento antes y después de la implementación del MOOC. Las observaciones permitieron evaluar la participación activa de los estudiantes durante el curso.

El procedimiento de recolección de datos se llevó a cabo en varias etapas. Primero, se realizó una reunión introductoria con los participantes para explicar los objetivos del estudio y obtener su consentimiento informado. Luego, los estudiantes completaron un cuestionario inicial para evaluar su conocimiento previo. Posteriormente, participaron en el MOOC y al finalizar, completaron un cuestionario de evaluación y participaron en entrevistas de seguimiento.

Los datos cualitativos fueron analizados mediante análisis temático, identificando patrones y categorías clave relacionadas con las percepciones de los estudiantes sobre la ciberseguridad. Los datos cuantitativos se analizaron utilizando estadísticas descriptivas para medir los cambios en el nivel de conocimiento y conciencia antes y después de la implementación del MOOC.

Se tomaron en cuenta diversas consideraciones éticas para garantizar el bienestar de los participantes. Todos los estudiantes firmaron un consentimiento informado antes de participar en el estudio. Se garantiza la confidencialidad y anonimato de los datos recolectados, y se les informó que podían retirarse del estudio en cualquier momento sin repercusiones. Además, el estudio cumplió con las normativas éticas establecidas por la Universidad Internacional del Ecuador (UIDE) y las directrices internacionales para investigaciones educativas.

RESULTADOS

Los resultados obtenidos en este estudio se presentan en tres categorías principales: conocimiento previo de ciberseguridad, participación en el MOOC y cambios en la conciencia de ciberseguridad. Antes de la implementación del curso, solo el 25% de los estudiantes pudo identificar correctamente al menos una medida de seguridad digital básica, mientras que después del curso, el 85% mostró mejoras significativas en sus respuestas.

Durante el análisis de los datos, surgieron varias categorías clave:

Conocimiento Inicial Limitado: Muchos estudiantes mostraron un conocimiento limitado sobre conceptos como phishing, contraseñas seguras y protección de datos.

Participación Activa: La mayoría de los estudiantes participó activamente en las actividades del MOOC, lo que refleja un interés creciente en los temas tratados.

Mejora en la conciencia: Se observó un cambio positivo en la conciencia de los estudiantes sobre la importancia de la ciberseguridad y la necesidad de aplicar medidas de protección.

Algunos participantes expresaron sus percepciones durante las entrevistas de seguimiento:

"Antes del curso, no sabía que compartir mi contraseña podría ser peligroso. Ahora entiendo que es importante mantenerla segura" (Estudiante 1).

"El curso me ayudó a reconocer correos sospechosos y evitar caer en trampas de phishing" (Estudiante 2).

"Aprendí cómo crear contraseñas fuertes y cómo proteger mi información personal" (Estudiante 3).

Estas citas ilustran cómo el curso impactó positivamente en la comprensión de los estudiantes sobre los riesgos digitales y las medidas de seguridad necesarias.

DISCUSIÓN

Los resultados obtenidos en este estudio respaldan los hallazgos de investigaciones previas sobre la efectividad de los MOOCs en la educación digital. Como indican Clough (2015) y Van Niekerk y von Solms (2010), los programas educativos enfocados en ciberseguridad pueden mejorar significativamente la conciencia y las prácticas seguras en línea. El incremento del 25% al 85% en el conocimiento de medidas de seguridad digital demuestra que la formación específica es una estrategia efectiva para reducir la vulnerabilidad de los estudiantes ante riesgos cibernéticos.

Además, los participantes del MOOC mostraron una mejora notable en su capacidad para identificar riesgos como el phishing y tomar medidas preventivas. Esto coincide con los principios del marco de ciberseguridad del NIST (2018), que enfatiza la importancia de la educación en la prevención de amenazas digitales.

Los hallazgos de este estudio tienen importantes implicaciones teóricas y prácticas. Desde una perspectiva teórica, contribuyen a la literatura sobre educación digital y ciberseguridad, destacando la importancia de los MOOCs como herramientas educativas accesibles y efectivas. En términos prácticos, este estudio proporciona un modelo replicable para otras instituciones educativas que buscan mejorar la seguridad digital de sus estudiantes.

A pesar de los resultados positivos, este estudio presenta algunas limitaciones. En primer lugar, la muestra estuvo limitada a una sola institución educativa, lo que puede afectar la generalización de los resultados. Además, el acceso desigual a dispositivos tecnológicos podría haber influido en la participación de algunos estudiantes.

Futuras investigaciones podrían enfocarse en ampliar la muestra a diferentes contextos educativos y explorar el impacto de los MOOCs en diversos grupos etarios. También sería relevante investigar el uso de tecnologías emergentes, como la gamificación y la realidad aumentada, para mejorar la experiencia de aprendizaje.

CONCLUSIÓN

El desarrollo e implementación del curso MOOC de ciberseguridad en la Unidad Educativa Isaac Jesús Barrera ha demostrado ser una herramienta efectiva para mejorar la conciencia y las prácticas de seguridad digital de los estudiantes. Este proyecto ha permitido a los participantes identificar riesgos digitales y adoptar medidas preventivas, lo que refleja un avance significativo en su protección online.

Los hallazgos de este estudio confirman la relevancia de los programas educativos en ciberseguridad, especialmente en contextos educativos donde los estudiantes tienen acceso limitado a información sobre seguridad digital. La mejora del 25% al 85% en el conocimiento de medidas de protección es un indicador claro de que la educación digital puede marcar una diferencia significativa en la reducción de riesgos cibernéticos.

Desde una perspectiva teórica, este proyecto refuerza la literatura existente que enfatiza la importancia de la formación temprana en ciberseguridad. En términos prácticos, ofrece un modelo replicable para otras instituciones educativas que busquen implementar iniciativas similares.

Sin embargo, es importante reconocer las limitaciones de este estudio, como el acceso desigual a dispositivos tecnológicos y la limitada generalización de los resultados a otras instituciones. A pesar de ello, las implicaciones prácticas de este proyecto son claras: la educación en ciberseguridad es esencial para preparar a los estudiantes para los desafíos digitales del presente y del futuro.

Se recomienda que futuras investigaciones exploren la aplicación de MOOCs de ciberseguridad en diferentes contextos educativos y que se integren tecnologías emergentes, como la gamificación, para mejorar la experiencia de aprendizaje. Asimismo, es fundamental que las políticas educativas consideren la inclusión de programas de ciberseguridad como parte del currículo escolar, garantizando así una formación integral que permita a los estudiantes navegar de manera segura en el entorno digital.

REFERENCIAS

Arregui, L., & Lasso Ruiz, J. (2021). Ciberseguridad y protección de datos. Editorial Universitaria.

Clough, J. (2015). Principles of Cybersecurity: From Theory to Practice. Oxford University Press.

European Union Agency for Cybersecurity (ENISA). (2020). Cybersecurity in Education: Guidelines and Best Practices. Recuperado de [https://www.enisa.europa.eu].

Impulso06. (2023). La importancia de la educación en ciberseguridad. Recuperado de [https://impulso06.com].

NIST. (2018). Cybersecurity Framework. National Institute of Standards and Technology. Recuperado de [https://www.nist.gov/cyberframework].

Ponemon Institute. (2022). Global Trends in Cybersecurity. Recuperado de [https://www.ponemon.org].

UNIR Colombia. (2023). ¿Qué es la ciberseguridad? Recuperado de [https://colombia.unir.net].

Van Niekerk, J., & von Solms, R. (2010). The Role of Education in the Prevention of Cybercrime. Computers & Security, 29(7), 731-738.