VOLUMEN 5, N˚1 / ENERO - JUNIO 2023 / e - ISSN: 2661

Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura

Analysis of cybersecurity in e-learning platforms: a systematic literature review

Paola Pillajo-García *	Paola.pillajo@pucesa.edu.ec
Diego Avila-Pesantez†	Davila@espoch.edu.ec

*Pontificia Universidad Católica del Ecuador, sede Ambato. Departamento de Posgrado, Ambato, Ecuador
†Escuela Superior Politécnica de Chimborazo (ESPOCH), Grupo de Investigación en Innovación Científica y Tecnológica (GIICYT), Riobamba, Ecuador.

RESUMEN

El análisis de ciberseguridad en plataformas e-learning es un proceso sistemático de evaluación y verificación de la seguridad de la información en una plataforma de aprendizaje en línea. Este proceso implica identificar los posibles riesgos y vulnerabilidades de la plataforma, evaluar la eficacia de las medidas de seguridad existentes y recomendar medidas adicionales para fortalecer la seguridad de la información y los datos confidenciales. Además, permite proteger la información confidencial, como los datos de los estudiantes y los profesores, garantizando la integridad de los cursos y materiales de enseñanza en línea, lo que asegura un aprendizaje sin interrupciones y confiable. El objetivo del trabajo es realizar una revisión sistemática de la literatura de los problemas de ciberseguridad en las plataformas e-learning de Moodle, Blackboard y Microsoft Teams, en el período 2016 hasta 2022, utilizando el protocolo definido por Kitchenham. Como resultados se detallan recomendaciones para mitigar vulnerabilidades como la encriptación de datos, autenticación de dos factores, actualización del software y políticas de seguridad, protección de datos sensibles y entrenamiento a los usuarios sobre ciberseguridad.

Palabras Clave: Ataques, Ciberseguridad, Plataformas E-learning, Revisión sistemática de Literatura, Vulnerabilidades.

ABSTRACT

Cybersecurity analysis of e-learning platforms is a systematic process of assessing and verifying information security on an e-learning platform. This process involves identifying potential risks and vulnerabilities of the platform, assessing the effectiveness of existing security measures, and recommending additional measures to strengthen the security of confidential information and data. In addition, it protects confidential information, such as student and teacher data, ensuring the integrity of online courses and teaching materials and ensuring uninterrupted and reliable learning. The work aims to perform a systematic literature review of cybersecurity issues in Moodle, Blackboard, and Microsoft Teams e-learning platforms, in the period 2016 to 2022, using the protocol defined by Kitchenham. The results detail recommendations to mitigate vulnerabilities such as data encryption, two-factor authentication, software updates and security policies, protection of sensitive data, and user training on cybersecurity.

Palabras Clave: Attacks, Cybersecurity, E-Learning Platforms, Systematic Literature Review, Vulnerabilities.

I. Introducción

Una plataforma de e-learning es una herramienta en línea que nace en los años 90, utilizada para ofrecer cursos o programas de formación a distancia. Estas suelen incluir una variedad de características y herramientas para facilitar el aprendizaje en línea, como contenido multimedia, foros de discusión, exámenes y evaluaciones, seguimiento del progreso, entre otros [1]. Los estudiantes pueden acceder a la plataforma a través de una conexión a Internet y utilizarla para completar tareas e interactuar con otros estudiantes y profesores.

Fecha de Recepción: 30/dic/2022. Fecha de Aceptación: 24/ene/2023 DOI: https://doi.org/10.47187/perspectivas.5.1.179

Las plataformas de e-learning son una forma conveniente y accesible de obtener educación y formación a distancia. En la actualidad, se ha perfeccionado el desarrollo de nuevas plataformas que den respuesta a procesos de aprendizaje para alcanzar el éxito. Por ejemplo, plataformas pagadas: Google classroom, Blackboard, E-ducativa, Edmodo, y Microsoft Teams. Plataformas gratuitas como Moodle, Chamilo, Claroline, entre otras.

Al ser plataformas que tienen una metodología flexible para el ingreso de cualquier usuario y disponibles en el internet, son vulnerables a múltiples amenazas de seguridad, y representan una oportunidad para ciberataques como el robo de identidad, el ciberfraude, extracción de datos o daños a los sistemas informáticos [2]. Por esta razón, se debe crear conciencia sobre la importancia de la seguridad y protección de la privacidad en las plataformas e-learning, garantizando que la información almacenada, compartida y generada sea de carácter seguro [3]. Sin que afecte los procesos educativos y tenga un impacto perjudicial en el proceso de aprendizaje de los usuarios. De esta manera conserva la integridad, confidencialidad y disponibilidad de la información, utilizando barreras y procedimientos que resguarden el acceso a los datos e información [4].

El artículo tiene como objetivo el análisis de ciberseguridad en plataformas e-learning a través de una revisión sistemática de la literatura, enfocado en las plataformas más utilizadas por los usuarios: Moodle, Microsoft Teams y Blackboard. Además, se presentan algunas de las vulnerabilidades más comunes en las plataformas e-learning como: Denegación de servicios (DoS), Falsificación de solicitud entre sitios (CSRF), Secuencias de comandos entre sitios (XSS), Inyección de SQL, en las cuales se analiza los problemas, soluciones y las tres metodologías más utilizadas para las plataformas e-learning.

El trabajo se estructura con una introducción que describe el objetivo y contexto de la revisión. Luego, se detalla los criterios y procedimientos de la metodología. Posteriormente, se presenta los resultados obtenidos y la interpretación; finalmente, se muestra las conclusiones.

II. Método de investigación

En el presente trabajo se realiza una revisión sistemática de literatura, basado en el modelo propuesto por Kitchenham [5], el cual consta de tres fases principales: Planificación de la revisión, realización de la revisión y análisis.

A. Planificación de la revisión

Para el desarrollo del estudio se realizó una revisión sistemática de literatura desde el año 2016 hasta 2022, obteniendo información necesaria para realizar una verificación de documentos, que describen las vulnerabilidades y mecanismos de mitigación en la seguridad en plataformas e-learning, y se plantean 3 preguntas:

- RQ1. ¿Qué tipo de vulnerabilidades existen en la seguridad en plataformas E-learning?
- RQ2. ¿Cuáles son las soluciones de seguridad existentes para proteger la información y mitigar los riesgos en plataformas E-learning?
- RQ3. ¿Qué metodologías existentes son apropiadas para garantizar la seguridad en plataformas E-learning?

Se consideró las bases de datos científicas IEEE Xplore, Scopus y Proquest para la revisión bibliográfica. Los artículos se seleccionaron dianteuna búsqueda precisa utilizando palabras claves, términos o expresiones concernientes con (a) E-learning, (b) Plataformas educativas y (c) Ciberseguridad, relacionados con (Microsoft Teams, Moodle, Blackboard, ataques, vulnerabilidades o riegos, contra medidas). Para seleccionar los documentos obtenidos según la importancia se utilizó los criterios de inclusión y exclusión mostrados en la Tabla I.

B. Planificación de la revisión

Una vez obtenido los documentos, se realizó la extracción de la información en base a los criterios de inclusión y exclusión, analizando el contenido de los documentos de acuerdo con las preguntas planteadas. De los 285 documentos, se seleccionaron 64, que cumplen estos criterios. En la figura 1 se muestra un diagrama de aportes científicos entre los años 2016 a 2022, relacionados con las vulnerabilidades y ataques más comunes en las principales plataformas e-learning.

Tabla I. *Criterios de inclusión y exclusión*

Criterios de inclusión	Criterios de exclusión
Documentos que detallan los problemas de seguridad en plataformas e-learning	Publicaciones relacionadas en sitios web
Publicaciones de impacto acerca de soluciones de seguridad en Moodle, Blackboard y Microsoft Teams	Artículos científicos que detallan soluciones de seguridad general
Publicaciones relevantes acerca de las preguntas de investigación	Publicaciones, artículos científicos que hablan acerca de problemas de seguridad, pero no describen la forma de mitigación
Documentos que detallan metodologías, técnicas de mitigación en la seguridad de plataformas e-learning	Tesis, Libros, blogs y posters

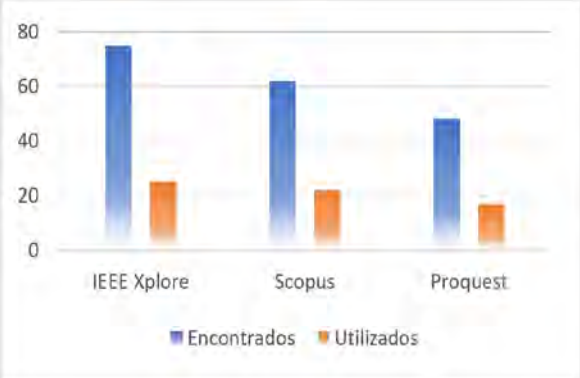

Fig 1. *Estudios encontrados y elegidos.*

A. Análisis

Una vez revisado detalladamente los documentos se procedió a responder las preguntas de investigación propuestas, con el fin de determinar los problemas, medidas de seguridad y metodologías existentes en las plataformas e-learning.

RQ1 ¿Qué tipo de problemas existen en la seguridad en plataformas E-learning?

Con el paso de los años, las aplicaciones y plataformas que se encuentran disponibles en internet se han actualizado y ampliado las herramientas y servicios. Esto permite mejorar los procesos educativos en línea. Sin embargo, están comprometidos a una variedad de vulnerabilidades y ataques, los cuales buscan sustraer datos exclusivos y provocar el colapso de los sistemas [6], afectando total o parcialmente la preservación de la confidencialidad, integridad y disponibilidad de la información. Regularmente, las amenazas en las plataformas e-learning se ven cubiertas como links de descargas en aplicaciones, correos de fuentes extrañas, con el fin de infiltrarse y afectar a los dispositivos y sistemas [7].

B. Planificación de la revisión

Una vez obtenido los documentos, se realizó la extracción de la información en base a los criterios de inclusión y exclusión, analizando el contenido de los documentos de acuerdo con las preguntas planteadas. De los 285 documentos, se seleccionaron 64, que cumplen estos criterios. En la figura 1 se muestra un diagrama de aportes científicos entre los años 2016 a 2022, relacionados con las vulnerabilidades y ataques más comunes en las principales plataformas e-learning.

Tomando el estudio de la gestión de seguridad realizado por Kaspersky en el año 2020 [8], que analiza las plataformas educativas, se encontraron múltiples amenazas en aplicaciones de videoconferencia y plataformas en línea, estimando un total de 168,550 casos de vulnerabilidades encontradas. Existen varios problemas de seguridad en las plataformas de e-learning como: a) Acceso no autorizado: Los hackers pueden acceder a la plataforma sin autorización y obtener información confidencial o cambiar la información; b) Phishing: Los estudiantes pueden recibir correos electrónicos falsos que les piden que inicien sesión en la plataforma con sus credenciales, lo que permite a los hackers acceder a sus cuentas; c) Malware: Los estudiantes pueden descargar malware al hacer clic en enlaces o descargar archivos de la plataforma, lo que puede dañar su computadora y exponer su información personal; d) Falta de privacidad: La plataforma puede recopilar y almacenar información sobre los estudiantes, lo que puede ser una violación de la privacidad si no se utiliza de manera responsable; e) Ataques DDoS: Los hackers pueden utilizar ataques de denegación de servicio (DDoS) para hacer que la plataforma deje de funcionar o sea inaccesible. En las tablas II, III, IV se detallan las vulnerabilidades más comunes en las plataformas e-learning.

Tabla II. *Problemas de ciberseguridad para moodle*

Problemas	Descripción
Ejecución de código	Afecta la Confidencialidad, Integridad Severidad critica Permite a atacantes tener privilegios de administrador a través de solicitudes HTTP que conduzca a la ejecución del comando y explotar la vulnerabilidad.
Inyección SQL	Afecta la Confidencialidad Severidad crítica Permite a los atacantes obtener acceso a modificar, eliminar datos y conseguir el control en la plataforma afectada [39].
Falsificación de solicitud del lado del servidor (SSRF)	Afecta la Integridad Severidad critica Permite a los atacantes conectarse con servicios de la infraestructura interna y filtrar información sensible de la plataforma.
Secuencias de comandos entre sitios (XSS)	Afecta la Confidencialidad Severidad media Permite a atacantes inyectar en las plataformas secuencias de comandos web por medio del parámetro de archivo [40].
Falsificación de solicitud entre sitios (CSRF)	Afecta la Confidencialidad Severidad media Permite realizar el ataque de manera remota mintiendo a la víctima para que visite una página web y ejecute diversas tareas en el sitio web vulnerable [41].
Denegación de servicio (DoS)	Afecta la Confidencialidad Severidad media Permite a atacantes que ingresan a las plataformas por vía remota provocar un consumo de disco e ingresar borradores con la función de guardado automático, afectando a los recursos de conectividad de Moodle [42].
División de respuesta HTTP	Afecta la Integridad Severidad media Permite a atacantes inyectar encabezados HTTP y realizar ataques de división de respuesta a través de vectores que involucran la variable url [43].
Recorrido de Directorio	Sin impacto Severidad media Permite a atacantes autenticados leer archivos arbitrarios a través de un (punto punto) en una ruta [44].

Tabla III. *Problemas de ciberseguridad para microsoft teams*

Problemas	Descripción
Secuencias de comandos entre sitios (XSS)	Afecta la Integridad Severidad baja El parámetro displayName contiene una secuencia de comandos, que se puede explotar en los clientes de Microsoft Teams, para obtener información confidencial, como tokens de autenticación, y ejecutar comandos arbitrarios [49].
Reproducción del protocolo de transporte en tiempo real (RTP)	Afecta la Confidencialidad Severidad media Intercepta y retransmite una transmisión multimedia válida entre dos usuarios con fines malintencionados.
Denegación de servicio (DoS)	Afecta la Disponibilidad Severidad media El atacante puede manipular un input desconocido causando una vulnerabilidad de clase denegación de servicio.

Tabla IV. *Problemas de ciberseguridad para blackboard*

Problemas	Descripción
Obtener privilegios	Afecta la Confidencialidad e Integridad Severidad critica Permite a los atacantes conseguir privilegios de administrador en blackboard, configurando el parámetro de contexto en "admin" [45].
Secuencias de comandos entre sitios (XSS)	Afecta la Integridad Severidad media Las secuencias de comandos entre sitios en Blackboard permiten a atacantes ejecutar secuencias de comandos web a través de los parámetros: Course_id, CTID en ProcessInfo.cgi o el parámetro Message en índice.cgi [46].
Obtener privilegios de omisión	Afecta la Confidencialidad e Integridad Severidad media Permite a los atacantes evadir la autenticación y obtener privilegios como otros usuarios a través de un parámetro user_id [47].
Intermediario	Afecta la Confidencialidad e Integridad Severidad media El atacante modifica los Servicios de dominio de Active Directory para agregar su servidor como un servidor de confianza o modifica la configuración de DNS o usa otros medios para que los clientes se conecten al servidor a través del atacante [48].

En la Fig. 2. se muestra la relación entre las plataformas Moodle, Blackboard y Microsoft Teams, con respecto a las vulnerabilidades encontradas.

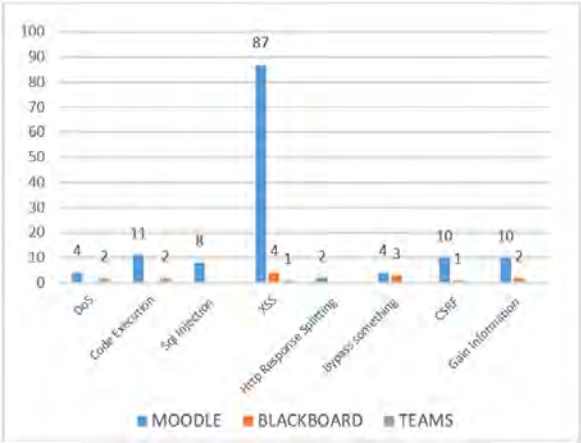

Fig. 2. *Vulnerabilidades más comunes en Plataformas e-learning.*

RQ2 ¿Cuáles son las soluciones de seguridad existentes para proteger la información y mitigar los riesgos en plataformas E-learning?

Actualmente, se utiliza varias herramientas dentro de las plataformas e-learning, que deben contar con mecanismos de seguridad y protección en la información, que se ingrese o se descargue. Además, la información con la que trabaja debe ser confidencial, por lo que es necesario protegerse de amenazas y ataques que puedan afectar el derecho a la privacidad e intimidad [9]. Por tal motivo, se presentan soluciones de seguridad para las vulnerabilidades encontradas y la forma de mitigarlos.

A. Suplantación de identidad (imitación de direcciones IP)

Para mitigar la vulnerabilidad de suplantación de identidad, se utiliza la seguridad en la capa de transporte (TLS), el cual imposibilita que el atacante ejecute la suplantación de direcciones IP en una conexión determinada. Sin embargo, en plataformas e-learning como Teams, Blackboard y Moodle se realiza la autenticación con certificados, el atacante no asumirá información legítima necesaria para reemplazar la identidad de una de las partes de la comunicación [10].

B. Intermediario

La vulnerabilidad de intermediario en plataformas e-learning participan entre dos puntos como: video, audio, y uso compartido de aplicaciones. Esta vulnerabilidad se evita utilizando el Protocolo de transporte en tiempo real seguro (SRTP), en el cual se cifra la secuencia multimedia [11]. Al realizar la conexión entre dos puntos se empiezan a negociar las claves de cifrado utilizando el protocolo de señalización de llamada que utiliza el canal de cifrado TCP, UDP de TLS.

C. Reproducción del Protocolo de transporte en tiempo real (RTP)

Para mitigar es ataque RTP, las plataformas e-learning utilizan SRTP, en conjunto con un protocolo de señalización segura, teniendo como objetivo proteger las transmisiones de los ataques. Esto permite que el receptor mantenga un índice de los paquetes RTP recibidos y compare el paquete nuevo con los paquetes que ya se encuentran en ese índice [11].

D. Seguridad en Autenticación

Existen varios métodos de autenticación, por ejemplo, la autenticación por defecto de las plataformas e-learning o la autenticación que utiliza plugins que son compatibles con Shibboleth [12]. Para una buena gestión de autenticación es recomendable seguir los siguientes pasos [13]:

- Realizar una buena construcción de la contraseña.
- Bloquear los dominios de correo de tipo sospechoso, de esta manera los usuarios que deseen autenticarse utilizando un determinado tipo de correo como, por ejemplo: @gmail.com, @yahoo.com, serán bloqueados automáticamente.
- Ocultar los campos que se suponga importantes como nombres de usuarios, contraseñas, dirección de correo.
- Revisar periódicamente los invitados no autenticados, determinando los permisos asignados y su rol.
- Implementar reCAPTCHA, obligando a que los usuarios que estén autenticados puedan ver la información de los demás usuarios y así mantener a los usuarios visitantes anónimos y motores de búsqueda alejados de la información del usuario.

E. Seguridad de contraseñas

Todos los usuarios que estén autenticados en las plataformas e-learning, deberán utilizar una contraseña segura para el inicio de sesión y así evitar el robo de contraseñas. A continuación, se presentan recomendaciones al momento de crearse una contraseña [14].

- Incluir mayúsculas y minúsculas.
- Incluir letras, números y caracteres especiales ($, %,&)
- Longitud mínima de 8 caracteres

F. Seguridad para Denegación de servicios (DoS)

El control de tráfico es la primera medida que se realiza a un ataque DoS, y consiste en eliminar todo el tráfico del ciberdelincuente. El rastreo del ataque se puede identificar el tráfico de los ciberdelincuentes que están ejecutando el ataque DoS, luego se trata de conseguir la identificación del atacante y finalmente se obtiene información para hacer el control de tráfico [15].

Microsoft Teams ofrece protección frente a estos

ataques mediante la ejecución de la protección de red Azure DDOS y la limitación de las solicitudes de los clientes desde los mismos puntos de conexión, subredes y entidades federadas [11]. Además, se debe implementar un sistema de prevención y detección de intrusos (IDS/IPS) para monitorear las conexiones y que se alerte la detección de intentos de acceso no permitidos [16]. Asegurarse de tener un dispositivo con funcionalidad mixta que incluya antivirus, antispam, antispyware y otras. Por ejemplo, un equipo de gestión de amanezcas (UTM, por sus siglas en inglés) ayuda a gestionar de manera unificada las ciber-amenazas.

G. Seguridad para Inyección SQL

Se debe tomar en cuenta algunos mecanismos para evitar los ataques de inyección SQL en las plataformas e-learning [17]:

- Emplear APIs, que mitigue la utilización de un intérprete y utilice una interfaz parametrizada como Mapeo Relacional de Objetos (ORMs)
- Utilizar el control SQL (LIMIT) dentro de las consultas para evitar la fuga masiva de registros.
- Cambiar las contraseñas que vienen por defecto, como root, evitando así tener permisos de modo privilegiado.
- Restablecer el ID de sesión cada cierto tiempo o cuando se cambie los privilegios del usuario.
- Finalizar después de un tiempo de inactividad la sesión.

H. Seguridad para Secuencias de comandos entre sitios (XSS)

Los principales métodos de prevención incluyen:

1) Frameworks: previene el ataque XSS codificando el contenido como React JS y Ruby 3.0.

2) Fuga de caracteres: es un problema técnico que ocurre cuando se utilizan caracteres especiales o acentos en el contenido del curso, y estos no se visualizan correctamente en la plataforma. Se debe evitar la inyección de código malicioso en la página web a través de la entrada de datos no validada. Esto puede permitir a los atacantes acceder a información confidencial, realizar acciones no autorizadas en el sistema o incluso dañar el sitio web [18]. Las consultas preparadas son una forma de proteger contra la fuga de caracteres al permitir que los datos del usuario sean enviados a la base de datos de manera segura sin posibilidad de ser interpretados como código.

3) Validación de datos: Se puede reducir los riesgos determinando que todo lo que ingrese por parte del usuario se debe validar con precisión, garantizando así la seguridad del sistema.

4) Filtración: El objetivo es buscar palabras clave peligrosas en la entrada del usuario y eliminarlas por cadenas vacías. Las palabras claves pueden ser [19]:
   - Etiquetas <script> </script>
   - Marcado HTML
   - Comandos Javascript

5) XSS Cheat Sheets: Es una guía que detalla cómo mitigar los ataques XSS. Se puede encontrar en OWASP [20].

I. Seguridad para División de respuesta HTTP

Para mitigar los riesgos de división de respuesta HTTP, se analiza y verifica la entrada para la combinación de dos códigos de control (CRLF) o cualquier otra forma de codificación de caracteres antes de procesarlos [21]. Se recomienda utilizar mecanismos de codificación con scripts o caracteres de entrada especial, que permiten transformar los caracteres codificados a una cadena especial de juegos de caracteres, de esta manera no se puedan ejecutar en el servidor web o en aplicaciones Java. Además, elimina la división de respuesta HTTP y los intentos de ataque XSS relacionados a la inyección de scripts y código malicioso. Se debe validar y verificar la entrada por parte del servidor si las plataformas e-learning se basan en la validación de datos por parte del cliente [22].

RQ3 ¿Qué metodologías existentes son apropiadas para garantizar la seguridad en plataformas E-learning?

Las plataformas virtuales de aprendizaje son evaluadas por marcos normativos que rige la constitución de páginas web, estableciendo procesos que regulan el manejo de sus operaciones, definiendo sus políticas de seguridad, procedimientos y procesos que guíen su actuar. Coelho [23] define a la metodología como un

conjunto se técnicas y métodos de carácter científico, que se aplican durante un proceso, funcionando como un soporte conceptual que rige la forma en que se aplica un procedimiento. Por tal motivo, se presentan las tres metodologías más utilizadas para la protección de información y sistemas de seguridad, que han llevado a varias plataformas a tener éxito al desarrollar sus proyectos [32].

A. OWASP

OWASP (Open Web Application Security Project, por sus siglas en inglés) es una organización sin fines de lucro que tiene como objetivo mejorar la seguridad de la información y proteger a los usuarios de Internet. OWASP proporciona documentación, herramientas e ingeniería complementaria para generar estabilidad al sitio web. Por ende, las plataformas e-learning han adoptado OWASP como una herramienta primordial para detectar vulnerabilidades implementado una metodología de pruebas de intrusión, que se basa en el enfoque de caja gris [25]. En donde no se tiene conocimiento o se tiene poca información sobre la aplicación que se va a probar. La metodología OWASP se divide en 2 fases [26]:

Fase pasiva: Se ejecutan pruebas para comprender la lógica de la aplicación que está en fase de auditoría, donde se analiza a profundidad los elementos que arrojen posibles vulnerabilidades.

Fase activa: En la presente fase se prueba los procesos encomendados por la metodología OWASP, siguiendo una metodología estándar de Ethical Hacking.

En la fase activa se puede encontrar el informe Top Ten de OWASP, el cual incluye la descripción de cada vulnerabilidad, recomendaciones para los desarrolladores, tester, todo esto para mitigar las vulnerabilidades que se puedan presentar, asegurándonos la prevención y una gestión más efectiva al momento de tratar las vulnerabilidades [26].

En la Tabla V, se muestra las principales vulnerabilidades de OWASP, se muestra que parte de ellas fueron encontradas como vulnerabilidades en las plataformas e-learning, además de las doce categorías de la metodología de pruebas de penetración de OWASP, se puede observar que ocho de ellas cuentan con pruebas para evaluar los diez riesgos del Top Ten de OWASP 2022

Tabla V. *TOP TEN 2021 VS. PRUEBAS DE PENETRACION DE OWASP*

Vulnerabilidades Owasp 2021	Pruebas de penetración Owasp
Control de acceso roto	Pruebas de autorización
Fallas criptográficas	Criptografía débil
Inyección	Pruebas de validación de entrada
Diseño inseguro	Recopilación de información Manejo de errores
Configuración incorrecta de seguridad	Pruebas de gestión de configuración e implementación
Componentes vulnerables y desactualizados	Recopilación de información
Fallas de identificación y autenticación	Pruebas de gestión de identidad Pruebas de autenticación
Fallas de integridad de datos y software	
Fallas de registro y monitoreo de seguridad	
Fallas de registro y monitoreo de seguridad	Pruebas de validación de entrada
	Pruebas de gestión de sesiones
	Pruebas de lógica de negocios
	Pruebas del lado del cliente
	Pruebas de API

B. NIST

En el ámbito de la ciberseguridad, NIST (National Institute of Standards and Technology, por sus siglas en inglés) juega un papel importante en la definición y promoción de estándares y prácticas recomendadas para la seguridad de la información y la protección de la infraestructura crítica. Esto incluye la publicación de guías y estándares para la seguridad de la información, la evaluación de la seguridad de productos y servicios de tecnología, y la investigación en ciberseguridad y tecnologías emergentes. En plataformas e-learning se utilizan como una guía para realizar evaluaciones de riesgos [27]. Esta guía incluye un procedimiento de buenas prácticas para tratar vulnerabilidades y riesgos en ámbitos de ciberseguridad, desde la gestión de riesgos de aplicaciones web, plataformas en línea, hasta procedimientos del sistema de gobierno de ciberseguridad. Además, realiza pentesting o gestión de incidentes. A continuación, se presenta las fases de una evaluación de seguridad para plataformas en línea [28].

1) Técnicas de revisión: son métodos pasivos que se basan en la revisión sistematizada del sistema, aplicaciones, redes y guías para detectar vulnerabilidades de seguridad en

plataformas en línea. Son esenciales para recopilar información y desarrollar técnicas como los test de intrusión avanzados, revisión de la documentación, revisión del conjunto de reglas, revisión de configuración de sistemas, escaneo de la red y comprobación de la integridad de los archivos que se suban o se descarguen de las plataformas. [29].

2) Técnicas de identificación y análisis de objetivos: Los usuarios encargados de la ciberseguridad deben identificar los servicios asociados, puertos, dispositivos activos para analizar y detectar las vulnerabilidades, descubrimiento de la red, escaneo de vulnerabilidades, y escaneo inalámbrico [30].

3) Técnicas de validación de la vulnerabilidad del objetivo: con la información encontrada en la identificación y análisis del objetivo se planifica e implementa técnicas que exploren a fondo la vulnerabilidad implementando pruebas de pentesting o test de intrusión avanzados.

4) Evaluación de seguridad: La guía NIST dedica dos secciones a las pruebas de seguridad. La primera se centra en la planificación y la segunda en la ejecución. La ejecución de la evaluación de seguridad se sustenta sobre cuatro fases, definidas en la guía NIST (Coordinación, Evaluación, Análisis Gestión de los datos: recolección, almacenamiento, transmisión y destrucción) [27]. A continuación, se describe 19 prácticas de las 4 categorías anteriormente vistas [31].

- Especificar requisitos de seguridad para el desarrollo de plataformas web.
- Efectuar roles y responsabilidades.
- Efectuar cadenas de herramientas de apoyo.
- Utilizar los criterios para las comprobaciones de seguridad.
- Efectuar y conservar entornos seguros para el desarrollo de plataformas.
- Proteger el código del acceso.
- Verificar la integridad de la versión del software utilizado.
- Proteger cada versión de software.
- Crear un software que cumpla con los requisitos de seguridad.
- Revisar el diseño del software y verificar los requisitos de seguridad.
- Reutilizar el software existente y utilizarlo cuando sea factible, en lugar de duplicar la funcionalidad.
- Crear un código fuente basándose a la codificación segura.
- Configurar el entorno de desarrollo integrado y la compilación.
- Analizar que el código sea legible para identificar vulnerabilidades.
- Probar el código ejecutable para identificar vulnerabilidades.
- Configurar el software para tener configuraciones seguras por defecto.
- Identificar vulnerabilidades de manera continua.
- Evaluar, priorizar y remediar vulnerabilidades.
- Analizar vulnerabilidades para identificar su causa raíz

C. MAGERIT

MAGERIT es una metodología de gestión de la seguridad de la información, la cual puede ser implementada en varias plataformas educativas en línea y aplicaciones web. Esta proporciona un marco para la planificación, implementación y evaluación de medidas de seguridad. Junto con OWASP, es una de las metodologías más utilizadas debido a su gestión prudente de las medidas de seguridad y la confianza de los usuarios con sus servicios [32]. En el estudio de Seguridad en entornos virtuales propuesta por Santiso, Koller, y Bisaro [33], definen los métodos más comunes para determinar los riesgos que pueden afectan a la infraestructura y las aplicaciones web educativas [34]. Se presenta a través de la metodología MAGERIT, algunas reglas para tener éxito al momento de implementar el análisis de gestión de riesgos, los cuales se describen a continuación [35].

1) Identificar los activos más relevantes de la organización y describir los servicios e información que maneja, realizándolo de forma cualitativa, teniendo en cuenta la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad y el valor por interrupción del servicio.

2) Definir las vulnerabilidades, dividiéndose en: vulnerabilidad natural, vulnerabilidad de hardware y software, vulnerabilidad de dispositivos y vulnerabilidad humana.

3) Definir las amenazas del sistema: sistemas de comunicación (de origen natural, causadas por personas, defectos de aplicaciones).

4) Valoración del riesgo: se valora el riesgo a la medida del daño probable sobre una plataforma o un sistema, se conoce el impacto de las amenazas sobre los activos, determinando las siguientes zonas.

   Zona 1: Riesgos muy probables y de muy alto impacto.

   Zona 2: Se genera desde situaciones improbables, impacto medio, hasta situaciones muy probables de impacto bajo.

   Zona 3: Riesgos improbables y de bajo impacto.

   Zona 4: Riesgos improbables, pero de muy alto impacto[36].

III. Resultados y discusión

De acuerdo con la información recopilada y el análisis de diferentes documentos, se puede argumentar que todas las investigaciones efectuadas acerca de la ciberseguridad en plataformas e-learning buscan como principal objetivo implementar medidas de seguridad y métodos adecuados cuyos patrones estén basados en la protección de datos y seguridad de información. Las vulnerabilidades más destacadas según diversos autores hacen referencia a la Denegación de servicio (DoS), Inyección SQL, División de respuesta HTTP y secuencia de comandos en sitios cruzados (XSS), siendo los principales problemas para las plataformas, produciendo sabotajes en los servicios o desencadenando situaciones peligrosas.

Las principales limitaciones de los estudios analizados se basan en que no existe la suficiente tecnología para detectar los riesgos y amenazas latentes en las plataformas e-learning, las cuales van surgiendo a medida que avanza la tecnología, además las metodologías analizadas se basan en una serie de pasos y protocolos los cuales deben ser evaluados y puestos a investigación para su implementación y su aplicabilidad puede ser limitada.

En relación con los problemas de seguridad existentes, es importante mencionar que Moodle ha desarrollado un software de seguridad llamada Bugcrowd, el cual se encarga de monitorear el código fuente para detectar los errores, reduciendo el impacto en las vulnerabilidades y agilizando la manera que se corrige los problemas [37]. Por otra parte, Blackboard para identificar problemas de seguridad utiliza pruebas de penetración de empresas externas y así proceder a su reparación. Además, se guía por el estándar CVSSv2 (Sistema común de puntuación de vulnerabilidades, versión 2.0) en el que se utiliza los puntajes de gravedad como indicaciones para clasificar el impacto de los problemas de seguridad [38]. Finalmente, Microsoft Teams ofrece protección de problemas a través de la ayuda de red Azure DDOS y la limitación de las solicitudes de los clientes [11].

Por otro lado, OWASP cuenta con una guía de pruebas de penetración en aplicaciones web, aunque no cuenten con pruebas para dos vulnerabilidades (fallas de integridad y fallas de registro y monitoreo), es la metodóloga más completa para ser utilizada. En cambio, la metodología NIST considera que la seguridad en plataformas web es un tema complejo, haciéndolo inadecuado para ser empleada en pruebas de penetración. Finalmente, MAGERIT por si sola desde el punto de vista de las plataformas web, no realiza pruebas de penetración, por lo que es inadecuada para ser empleada, pero al unirse MAGERIT con OWASP se convierte en una de las metodologías más adecuadas para tomarse como base en una prueba de penetración.

V. Referencias

1 R. H. Rodríguez and V. A. Vaca, "Importancia de las herramientas y entornos de aprendizaje dentro de la plataforma e-learning en las universidades del Ecuador," Edutec. Revista Electrónica de Tecnología Educativa. no. 65, pp. 68-92 (396), 2018.

2 M. Andrés, L. Díaz, P. Guía, David, and A. R. Zúñiga, “Universidad Nacional Andrés bello Facultad de Ingeniería. Predicción de áreas con usuarios vulnerables a ciberataques.”

3 P. I. Morales-Paredes and R. P. M. Chicaiza, "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua-Ecuador," TIC: cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 2, pp. 49-75, 2021.

4 G. Bustamante Maldonado, J. Andrés, and O. Cano, “Methodology of Information Security as a Measure of Protection Small Business,” 2014.

5 G. Tebes, D. Peppino, P. Becker, and L. Olsina, "Especificación del Modelo de Proceso para una Revisión Sistemática de Literatura," CIbSE.

6 M. M. Olmedo and V. J. Chaves, "Seguridad de la información en plataformas e-learning en tiempos de pandemia COVID-19," Revista UNIDA Científica.

7 C. A. Santamaría Calucho, "Control de Seguridad en una Plataforma Educativa Institucional," Pontificia Universidad Católica del Ecuador, 2022.

8 latam.kaspersky.com, “Casos de éxito Kaspersky,” CompanyAccount, 2022.

9 P. Lluzar Martí, "Ciberseguridad y E-learning: Hacia una transferencia tecnológica sostenible entre España y el Perú ,2019.

[10 A. S. Flórez, J. G. Chacón, R. A. Chía, A. E. Flórez, and J. E. J. I. e. I. Rodriguez, "Política De Seguridad Hsts O Seguridad De Transporte Http Estricta Y Su Implementacion En Entornos Web," 2021.

11 “Seguridad y Microsoft Teams,” learn. microsoft.com, Dec. 12, 2022.

12 R. Rodriguez, “Interoperabilidad Matefun-Moodle,” 2021.

13 A. C. Alvarado Tapia and R. A. Montesdeoca Cabrera, "Análisis de vulnerabilidades del servidor e-learning de la ESPOCH para la implementación de mejores prácticas de seguridad-acceso," Escuela Superior Politécnica de Chimborazo, 2017.

14 L. M. Romero-Moreno, “La seguridad informática en el trabajo con la plataforma Moodle,” 2018.

15 R. S. Yesquen Rodriguez, "Prototipo de Detección y Mitigación de Ataques de Denegación de Servicios (DoS), en Servidores Web," 2018.

16 INCIBE, “Medidas de prevención contra ataques de denegación de servicio,” Instituto Nacional de Ciberseguridad, Jul. 09, 2019.

17 M. P. Echeverria Broncano and D. F. Ávila Pesantez, “Ciberseguridad en los sistemas de gestiónde aprendizaje (LMS),” Ecuadorian Science Journal, vol. 5, no. 1, pp. 46–54, Mar. 2021, doi: 10.46480/esj.5.1.98.

18 “Vega Vulnerability Scanner Application in Web Applications.” [Online]. Available: http://www.trabajo.gob.ec/

19 N. Segundo and C. Jimenez, “HACKING WEB (ANÁLISIS DE ATAQUES SQL Inyección, XSS),” 2019.

20 W. Ajayi, O. E. Ibeto, O. Ibeto, T. Olomola, and M. Madewa, “Analysis of modern cybersecurity threat techniques and available mitigating methods analysis of modern cybersecurity threat techniques and available mitigating methods,” International Journal of Advanced Research in Computer Science, vol. 13, no. 2, doi: 10.26483/ijarcs.v13i2.6815.

21 F. D. Salimovna and Y. N. Salimovna, "Security issues in E-Learning system," in 2019 International Conference on Information Science and Communications Technologies (ICISCT), 2019, pp. 1-4: IEEE.

22 Fabian Coelho, “Definiciones En: Signifiados.com. ,” significados.com/metodologia, 2018.

23 Metodologíassdee E-learning. [Online]. Available: www.fao.org/publications

24 El “Copyright y Licencia Tabla de Contenidos Sobre OWASP,” 2003. [Online]. Available: https://github.com/OWASP/Top10/issues

25 J. Vinicio, B. Guerrero, I. David, and O. Guevara Aulestia, “Análisis de seguridad de la información aplicando la metodología NIST SP 800-30 y NIST SP 800-115 para la empresa textiles jhonatex línea de investigación: Normas y Estándares.”

26 “00004875”.

27 E. Ortiz and M. M. Toro-Alvarez, “IRETE resultado preliminar del estudio comparativo de metodologías de pruebas de intrusión informática,” 2018, doi: 10.13140/RG.2.2.19947.18728.

28 "RISK ANALYSIS IN SECURITY OF INFORMATION."

29 E. coordinación de contenidos, D. General de Modernización Administrativa, and P. Impulsode la Administración Electrónica, "Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método." [Online]. Available: http://administracionelectronica.gob.es/

30 H. Santiso, J. Matías Koller, and M. G. Bisaro, "Seguridad en Entornos de Educación Virtual Security in Virtual Education Environments," Memoria Investigaciones en Ingeniería, núm, vol. 14, 2016.

31 P. I. Morales-Paredes and P. Medina-Chicaiza, "Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador," 3C TIC: Cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 2, pp. 49–75, Jun. 2021, doi: 10.17993/3ctic.2021.102.49-75.

32 Seguridad de la información, "Estudio comparado de metodologías de análisis de riesgos para TI y Seguridad de la Información", vol. 01, 2021.

33 P. Sharma, K. Agarwal, and P. J. I. J. Chaudhary, "E-Learning Platform Security Issues and Their Prevention Techniques: a Review," vol. 6, no. 8, 2021.

34 F. Andres and M. Becerra, "Análisis de las vulnerabilidades asociadas a la plataforma de e-learning moodle".

35 Metodología de Ciberdefensa para Organizaciones Versión 1.0: Mejores Prácticas en Ciberseguridad

36 A. Scerbakov, F. Kappe, and N. Scerbakov, "Security vulnerabilities in modern LMS," in Multi Conference on Computer Science and Information Systems, MCCSIS 2019 - Proceedings of the International Conference on e-Learning 2019, 2019, pp. 282–286. doi: 10.33965/el2019_201909c038.

37 M. Rabie, "Cybersecurity vulnerability assessment in learning cyber security vulnerability assessment in learning management systems management systems," 2021. [Online]. Available: https://scholarworks.lib.csusb.edu/etd/1376

38 A. E. M. Elsawy and O. S. Ahmed^, "International Journal of Current Engineering and Technology E-Learning using the Blackboard system in Light of the Quality of Education and Cyber security," 49| International Journal of Current Engineering and Technology, vol. 9, no. 1, doi: 10.14741/ijcet/v.9.1.7.

39 H. Ibrahim, S. Karabatak, and A. A. Abdullahi, "A Study on Cybersecurity Challenges in E-learning and Database Management System," in 8th International Symposium on Digital Forensics and Security, ISDFS 2020, Jun. 2020. doi: 10.1109/ISDFS49300.2020.9116415.

40 R. Ali, H. Zafar, A. Security, and R. Ali Humayun Zafar, "A Security and Privacy Framework for e-Learning Recommended Citation A Security and Privacy Framework for e-Learning." [Online]. Available: https://digitalcommons.kennesaw.edu/facpubs/4137