DOI: https://doi.org/10.46480/esj.5.1.98

Ciberseguridad en los sistemas de gestión de aprendizaje (LMS)

Cybersecurity in learning management system (LMS)

Mónica Echeverría Broncano[1], Diego Avila-Pesantez[2]

RESUMEN

Los Sistemas de Gestión de Aprendizaje (LMS) son aplicaciones software con múltiples herramientas que permiten canalizar el proceso de enseñanza-aprendizaje de manera online. Debido al crecimiento masivo de los LMS derivado por la situación de la pandemia, es necesario analizar las distintas vulnerabilidades y ataques que están expuestos estos sistemas. Por ello, este estudio platea una revisión sistemática de la literatura utilizando el protocolo definido por Kitchenham (2007), que se basa en tres fases: planificación, realización y análisis de resultados. Se identificaron 31 estudios potenciales, dentro del período 2014-2020, utilizando varias bibliotecas digitales. Pudiendo evidenciar también que existen varias políticas de mitigación presentes en los LMS, entre las más destacadas: establecimiento de roles, papel de los visitantes, rol para invitado, rol predeterminado para todos los usuarios, el papel de los creadores en los nuevos cursos entre otras; lo cuales permiten atenuar las vulnerabilidades existentes. Los resultados indican que ante las vulnerabilidades existentes es necesario la creación de procedimientos por parte de las instituciones educativas que permitan prevenir y mitigar los fallos que se presenten en los LMS.

Palabras clave: Ciberseguridad, Sistemas de Gestión de Aprendizaje, Moodle, Blackboard.

ABSTRACT

Learning Management Systems (LMS) are software applications with multiple tools to channel the teaching-learning process online. Due to the massive growth of LMS derived from the pandemic situation, it is necessary to analyze the different vulnerabilities and attacks that these systems are exposed to. Therefore, this study presents a systematic review of the literature using the protocol defined by Kitchenham (2007), based on three phases: planning, performance, and result in analysis. Thirty-one potential studies were identified within the period 2014-2020, using various digital libraries. They also showed that there are several mitigation policies present in the LMS, among the most prominent: establishment of roles, the role of visitors, role for guest, default role for all users, the role of creators in new courses, among others. ; which makes it possible to mitigate existing vulnerabilities. The results indicate that, given the current vulnerabilities, educational institutions must create procedures to prevent and minimize the failures that occur in the LMS.

Keywords: Cybersecurity, Learning Management Systems, Moodle, Blackboard.

Fecha de recepción: Enero 19, 2021.
Fecha de aceptación: Marzo 26, 2021.

Introducción

La falta de seguridad en el ciberespacio deteriora gravemente la confianza entre la comunidad TIC (tecnologías de la información y la comunicación) y sus usuarios. Por tanto, es necesario definir estrategias y procedimientos para mitigar los ataques y vulnerabilidades de estos recursos (Carlini, 2016). En la actualidad los Sistemas de Gestión de Aprendizaje (LMS, por sus siglas en inglés) juegan un rol principal en el contexto educativo. Es así, que con los últimos eventos ocurridos a nivel mundial y ante las medidas de distanciamiento social implementadas por la pandemia de COVID19, se han popularizado en su uso y accesibilidad por parte de estudiantes y docentes. Muchas instituciones educativas han integrado los LMS como un elemento académico fundamental, integrando las actividades de aprendizaje sincrónicas y asíncronas, que permite a los estudiantes intercambiar de ideas, conceptos y desarrollar tareas para el proceso de formación online (Bandara, Loras, Maher, 2014). En tal virtud los LMS (llamados también *e-learning)* cuentan con características como: interactividad, flexibilidad, escalabilidad, estandarización, usabilidad y funcionalidad (Clarenc, 2013). Estas particularidades permiten a los estudiantes aprender desde cualquier lugar y en cualquier momento, conduciendo al ahorro de costos sustanciales, y facilita el acceso a la información justo a tiempo sobre el plan de estudios.

[1] Ingeniera en Gerencia de Sistemas, Universidad Interamericana del Ecuador, Ecuador. E-mail: monica.p.echeverria.b@pucesa.edu.ec
[2] Ph.D. en Ingeniería en Sistemas e Informática, UNMSM. M.Sc. en Informática Aplicada, Profesor tiempo completo en la Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador. Profesor de postgrado en la Pontificia Universidad Católica del Ecuador Sede Ambato, Ecuador. E-mail: davila@pucesa.edu.ec

Como citar: Echeverria Broncano, M. P., & Ávila Pesantez, D. F. (2021). Ciberseguridad en los sistemas de gestión de aprendizaje (LMS). *Ecuadorian Science Journal*. 5(1), 46-54.
DOI: https://doi.org/10.46480/esj.5.1.98

Debido al aumento significativo de los LMS, estos son sujetos a distintas vulnerabilidades como XSS(*cross-site scripting, por sus siglas en inglés),* CSRF (*Cross Site Request Forgery, por sus siglas en inglés)* inyección directa de código SQL en la página web, inyección remota usando un archivo de virus/troyanos, ataques de destrucción de pilas, Inyección SQL en la dirección del sitio *(URL SQL injection)* (Costinela Luminiţa, Nicoleta Magdalena, 2012a), que afectan el normal funcionamiento de estas plataformas informáticas educativas.

Dentro de este contexto, los LMS más utilizados desde la perspectiva de la usabilidad de los usuarios son Moodle y Blackboard (Leon et al., 201, moodle, 2020). La gran demanda y la utilidad del sistema Moodle, no permiten tener un control absoluto en temas de seguridad. A partir de ello, es importante realizar una revisión sistemática de la literatura que permita comprender sobre las vulnerabilidades, ataques, políticas y mecanismos de mitigación que se dan frecuentemente, dado que en la actualidad existe pocos estudios enfocados a la ciberseguridad en los LMS. El objetivo del estudio fue identificar las diferentes vulnerabilidades que existen en los Sistemas de Gestión de Aprendizaje (LMS) más utilizados.

En la estructura del artículo, inicialmente se detalla los conceptos propios de la investigación, en la siguiente sección se especifica la metodología de investigación utilizada para el análisis de Ciberseguridad en los sistemas de gestión de aprendizaje. Finalmente, se presenta la discusión y conclusiones.

Materiales y Métodos

En el presente estudio se aplicaron las pautas generales propuestas por (Kitchenham, 2007), adaptando el proceso a la revisión sistemática de la literatura, lo que permitió recoger pruebas empíricas sobre las preguntas de investigación formuladas. Esta consta de tres fases principales: planificación de la revisión, realización de la revisión y análisis de resultados, las cuales se detallan a continuación.

A.- Planificación de la revisión

La revisión sistemática de la literatura se centra en la ciberseguridad aplicada a los LMS más utilizado por los usuarios, enfocándose en las vulnerabilidades, ataques, políticas y mecanismos de mitigación para lo cual se plantearon las siguientes preguntas de investigación:

- RQ1. ¿Cuáles son las vulnerabilidades y ataques más comunes en los principales Sistemas de Gestión de Aprendizaje?
- RQ2 ¿Se ven afectados los LMS por la falta de políticas y procedimientos de ciberseguridad adecuados?
- RQ3. ¿Qué mecanismos de mitigación y defensa se ha implementado en los Sistemas de Gestión de Aprendizaje más comunes?

En la búsqueda realizada se utilizaron las bases de datos electrónicas de Science Direct Elsevier, IEEE eXplorer, SpringerLink, ACM Digital Library, Proquest, y otros, en las cuales se incluyeron áreas asociadas a la Educación, Computación e Informática, Ingeniería y Tecnología. Se identificaron como fuentes de información revistas y conferencias publicadas entre los años 2014 hasta 2020. La estrategia de búsqueda se basó en los siguientes comodines: a) Políticas de los Sistema de Gestión de Aprendizaje, b) e-learning, c) seguridad cibernética, vulnerabilidades y ataques a los LMS más utilizados. La cadena de búsqueda fue: ("security") and ("security + "Learning Management System") and ("security + "cibernetics") and ("e-learning" +"security") and ("security"+ "moodle") and ("politics" "security"+ "moodle") and ("computer"+ "security") and ("security"+ "blackboard") Para depurar la selección de los estudios encontrados, se aplicaron los siguientes criterios de inclusión y exclusión señalados en la Tabla 1.

Tabla 1. Criterios de inclusión y exclusión

CRITERIOS DE INCLUSIÓN	*CRITERIOS DE EXCLUSIÓN*
Publicaciones científicas que tengan relación con vulnerabilidades y ataques de los LMS más utilizados	Publicaciones realizadas en foros
Publicaciones que mencionan los mecanismos de mitigación y defensa de los e-learning	Artículos que mencionan la ciberseguridad de los LMS, pero no definen tipos de vulnerabilidades existentes
Publicaciones relevantes que tengan temas en relación con las políticas de los LMS	Las publicaciones científicas que no aporten en lo referente a ciberseguridad.
Contenido de páginas web oficiales Moodle y Blackboard	Publicaciones de Moodle, en foros de páginas no oficiales.

B. Realización de la Revisión

En esta fase se estableció la selección de los artículos en base a los criterios de inclusión y exclusión, para lo cual se revisaron los títulos de las publicaciones encontradas en las bases de datos antes mencionadas. Asimismo, se realizó el análisis del contenido de los documentos seleccionados, lo que permitió determinar su relevancia y contribución, de acuerdo con las preguntas de investigación planteadas. Como resultado de la búsqueda se identificaron 300 documentos, de los cuales se seleccionaron 32 por cumplir con los criterios establecidos (véase la **Figura 1)**.

La **Figura 2** muestra el histograma de aportes científicos entre 2014 y 2020 en relación con las vulnerabilidades y ataques más comunes en los principales LMS. Uno de los trabajos más significados propuesto por (Ibrahim et al., 2020), quienes especifican varias estrategias para disminuir ataques a las bases de datos de los LMS, entre las que se encuentran los privilegios de la base de datos y controles de acceso, licencia de la base de datos, la seguridad de los datos utilizando el sistema almacenado, encriptación de datos, auditorías de seguimiento y control de acceso a la base de datos y copia de seguridad de los datos.

Figura1. Documentos identificados para la revisión

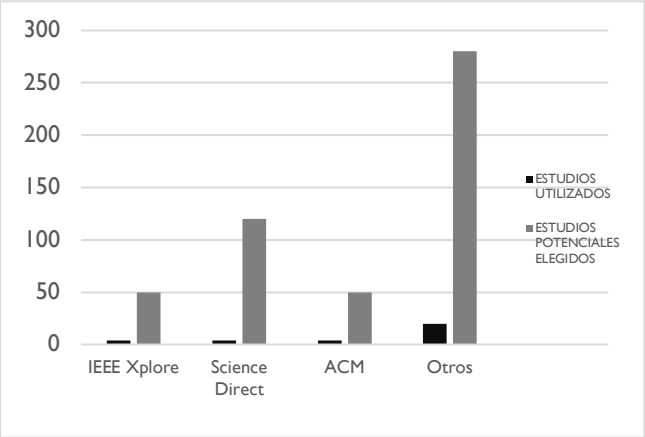
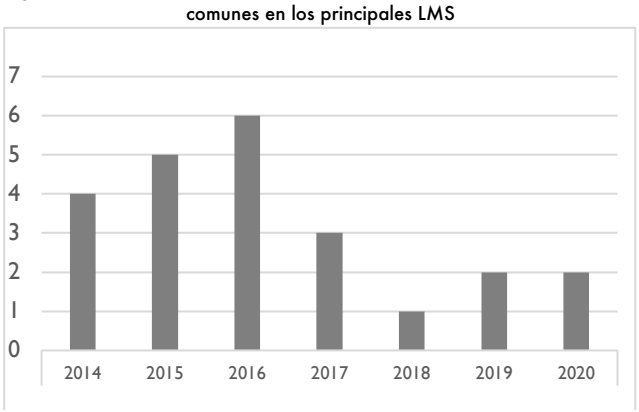


Figura 2. Actividad de investigación sobre vulnerabilidades y ataques más comunes en los principales LMS



C. Análisis

En base a los documentos analizados en este trabajo, se procedieron a responder a las tres preguntas de investigación destinadas a determinar las vulnerabilidades y riesgos; los ataques más frecuentes, los mecanismos de mitigación y defensa que se ha implementado en los Sistemas de Gestión de Aprendizaje.

RQ1. ¿Cuáles son las vulnerabilidades y ataques más comunes en los principales Sistemas de Gestión de Aprendizaje LMS?

Con el avance tecnológico, los Sistemas de Gestión de Aprendizaje se ha centrado en mejorar el aprendizaje colaborativo, dejando una brecha significativa en relación con la ciberseguridad, de ahí que las vulnerabilidades y ataques están presentes en Moodle, considerado uno de los LMS más populares (Violettas et al., 2013). En esta perspectiva, dichas vulnerabilidades y ataques se pueden manifestar en relación con los pilares fundamentales de la seguridad de la información (véase **Tabla 2).** En la **Tabla 3** se consideran los ataques de autenticación que existen en los LMS.

En los ataques de disponibilidad, la denegación de servicio (*DoS, por sus siglas en inglés)* también se encuentra presente en los sistemas de gestión de aprendizaje, haciendo que los servicios y datos se queden inaccesibles de manera brusca *hacia* un servidor determinado o servicio de red (Cloudflare, 2020), que se detalla en ***Tabla 4.***

Tabla 2. Ataques a Moodle

ATAQUES A MOODLE	
I Ataques de Autenticación	
1.1	Ruptura de la autenticación y gestión de sesión
1.2	Comunicación Insegura
II Ataques de disponibilidad	
2.1	Denegación de servicio
III Ataques de Confidencialidad	
3.1	Almacenamiento criptográfico inseguro
3.2	Referencia directa al objeto inseguro
3.3	Fuga de información y manejo inadecuado de errores
IV Ataques de Integridad	
4.1	Desbordamiento de búfer
4.2	Cross Site Request Forgery
4.3	Cross Site Scripting
4.4	Fallo en la restricción del acceso a la URL
4.5	Defectos de inyección
4.6	Ejecución de archivos maliciosos
V Ataques de Diseño	
5.1	Predicción de la contraseña
5.2	Predicción del nombre de usuario
5.3	Secuestro de sesión
5.4	Fijación de la sesión

Tabla 3. Ataques de Autenticación

Ataques Vulnerabilidades	Como se da el Ataque
Ruptura de la autenticación y gestión de sesión	El atacante puede fingir ser el usuario legítimo para hacer uso de las credenciales originales. Intercepta y roba la sesión autenticada mediante la opción de recuperación de contraseña, olvidar contraseña, o cambiar mi contraseña.
Comunicación Insegura	Durante la transmisión no se usa canales seguros, por ejemplo, una encriptación no adecuada, en la cual el atacante puede sacar ventaja de ello y hacerse pasar como si fuera el usuario legítimo para acceder a las conversaciones del usuario original.

Fuente: (Orehovački, 2008)

Tabla 4. Ataques de Disponibilidad a Moodle

Ataques Vulnerabilidades	Como se da el Ataque
Denegación de servicio (DoS)	Esta técnica de ataque apareció por primera vez en junio de 1998, consiste en enviar un alto número de solicitudes a los servidores, lo cual puede bloquear el servidor remoto o disminuir su rendimiento, así como también hacer mal uso del ancho de banda. y los recursos de conectividad de los sistemas LMS (Molina, Furfaro, Malena y Parise, 2015)
Denegación de servicio (DoS)	
Ataques lógico	Aprovechan las fallas existentes en los LMS para colapsar servidor remoto o disminuir significativamente el rendimiento (López, Aldana y Cuervo, 2014)
Ataques de inundación	Sobrecargan los LMS con un alto número de solicitudes hasta inhabilitar a los usuarios legítimos sin permitir el acceso a los sistemas de gestión de aprendizaje. (López et al., 2014)

Fuente: Elaboración propia (2021)

Los ataques de confidencialidad se originan mediante el almacenamiento criptográfico, referencia directa al objeto inseguro, así como, a la fuga de información y manejo inadecuado de errores, lo cuales se pueden observar en la **Tabla 5.**

Tabla 5. Ataques de Confidencialidad a Moodle

Ataques Vulnerabilidades	Como se da el Ataque
Almacenamiento criptográfico inseguro	Ocurre cuando la información sensible no dispone de una adecuada encriptación, por tanto, los LMS están sobre todo cuando la criptografía y algoritmos para poder proteger datos son débiles o no son utilizados.
Referencia directa al objeto inseguro	Los e-learning utilizan referencias a objetos directamente a interfaces web, sin que las comprobaciones de autorización se hayan implementado, estos objetos pueden ser archivos registros de las bases de datos y claves primarias los cuales están contenidos por parámetros URL.

Fuga de Información y manejo inadecuado de errores	Se da en cuanto a la divulgación involuntaria de datos sensibles e información mediante mensajes de error lo cual permite filtrar información sensible sobre su lógica, configuración y otros detalles internos como son la sintaxis del SQL, el código fuente, entre otros.

Fuente: Mohd Alwi & Fan (2010)

No obstante, la integridad también se ha visto afectada lo cual se pude verificar en la **Tabla 6,**

Tabla 6. Ataques de Integridad a Moodle

Ataques / Vulnerabilidades	Como se da el Ataque
Desbordamiento del buffer	Ocurre cuando las bibliotecas, controladores, componentes de servidores entre otros suelen almacenar datos en un buffer que se encuentre disponible sin previa validación de su tamaño, así como 900 caracteres en un campo de longitud determinada; ocasionando dicho desbordamiento.
Cross Site Request Forgery	Este ataque engaña a la víctima para poder interactuar con una página web o un script en un sitio de terceros con lo cual se generará una solicitud maliciosa al sitio del usuario; mediante el cual el servidor asume que es una solicitud del sitio web autorizado puesto que adquiere la identidad y los privilegios de la víctima para realizar una actividad no deseada en nombre de la víctima, como cambiar la dirección de correo electrónico, la dirección del domicilio o la contraseña de la víctima. (Lim & Jin, 2006). Se también cuando el usuario está conectado al LMS entonces el atacante puede engañar a su navegador haciendo una solicitud a una de las tareas del LMS, lo que causará un cambio en el servidor. (Arakelyan, 2013)
Cross site scripting	Posibilita al atacante inyectar un java script malicioso en páginas web vulnerables visitadas por otros usuarios y ejecutar dicho script para interceptar en el navegador de la víctima las sesiones iniciadas, ante lo cual se obtiene datos de la sesión del usuario cabe señalar que mediante este ataque para el usuario es imperceptible distingue código JavaScript inyectado. (Barhoom & Azaiza, 2016)
Fallo en la restricción del acceso a la URL	Permite a los atacantes tener la posibilidad de acceder a ciertos segmentos privilegiados y restringidos como es la gestión y administración a los LMS, mediante la intuición de la dirección de la URL y de esta manera realizar acciones no autorizadas sobre datos protegidos.
Inyección SQL	Se da en los servidores de bases de datos permitiendo a un posible atacante o intruso inyectar los comandos SQL y código malicioso para obtener información no autorizada de datos almacenados en las BD de los usuarios y sistemas (Keng, Chee, Mahinderjit & Hassan, 2014)
Ejecución de archivos maliciosos	Los LMS no tiene la capacidad para poder controlar o no permitir la ejecución de archivos subidos como puede ser el caso de archivos subidos como tareas, imágenes, entre otros.

Fuente: Elaboración propia a partir de autores (2021)

De la misma forma en los ataques de diseño las vulnerabilidades que se encuentran presentes son: la predicción de la contraseña, nombre de usuario, secuestro y fijación de sesión las cuales se detallan en la **Tabla 7.**

Tabla 7. Ataques de Diseño a Moodle

Ataques / Vulnerabilidades	Como se da el Ataque
Predicción de la contraseña & Predicción del nombre del usuario	En estos ataques se utiliza varias herramientas, de forma intuitiva o mediante fuerza bruta para poder probar las diferentes combinaciones de contraseñas y nombres de usuario, emitidas hacia el servidor web colocando un espacio en blanco para que el recuento de fallos de inicio de sesión se ponga en cero y así lograr descubrir las credenciales verdaderas para acceder a la cuenta o sistema. (Kumar & Dutta, 2011)
Secuestro de sesión	Es cuando atacante escucha la comunicación entre el cliente y el servidor en una solicitud HTTP, ante lo cual Moodle gestiona su sesión a través de dos valores para identificar una sesión activa: MoodleSession y MoodleSessionTest, estos valores se almacenan en la cookie que se envía en cada petición HTTP dentro de la cabecera del mensaje, Moodle usa túneles SSL en el servicio de acceso y algunos servicios administrativos. (Hernandez & Chavez, 2008)
Fijación de la sesión	El atacante intercepta la petición HTTP del usuario objetivo para acceder como usuario anónimo. (Hernandez & Chavez, 2008)

Fuente: Elaboración propia a partir de autores (2021

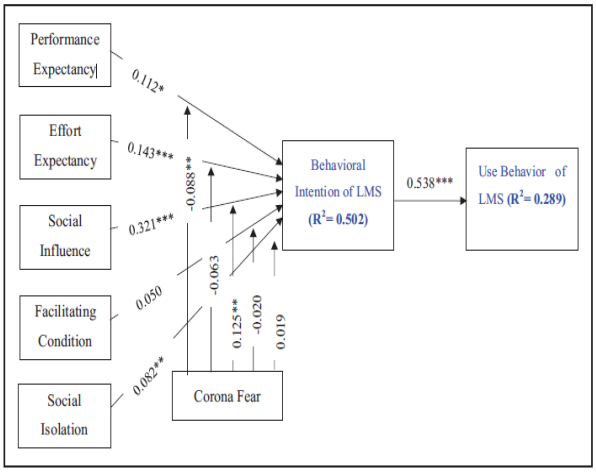
RQ2 ¿Se ven afectados los LMS por la falta de políticas y procedimientos de ciberseguridad adecuados?

En la actualidad, la formación virtual se está convirtiendo en una de las modalidades más utilizadas, debido al confinamiento por la pandemia del COVID-19, esto ha hecho que varias instituciones educativas tomen prioridad en la utilización del algún tipo de LMS, y así el aprendizaje no se vea interrumpido permitiendo alcanzar los objetivos en la enseñanza-aprendizaje. (Luo, Murray & Crompton, 2017)

En ese sentido, los autores (Raza, Qazi, Khan & Salam , 2020) desarrollaron una investigación para explorar la Teoría Unificada de Aceptación y Uso de la Tecnología (UTAUT), la cual está enmarcada en la observaron, el uso y comportamiento de Sistema de Gestión del Aprendizaje entre los estudiantes. Los datos fueron analizados usando el sistema de gestión de aprendizaje parcial. El análisis demostró que los temores por COVID 19, sólo moderan el vínculo de la expectativa de desempeño e influencia social con la intención conductual del LMS.

Por lo cual, se consideró como valor de R-cuadrado, a la medida de ajuste para los modelos de regresión lineal en la estadística aplicada lo cual se evidenció en el estudio, el porcentaje de la varianza en la variable dependiente, las variables independientes se explicaron colectivamente. El R2 de "Intención de Comportamiento de LMS" es 0,502, lo que implica que el 50,2% de la intención de comportamiento de usar LMS fue debido a la variable latente en el modelo. De manera similar, R2 para "Comportamiento de uso de LMS" es 0,289, lo que implicó que el 28,9% del comportamiento de uso de LMS fue por la intención conductual (Raza et al, 2020). Esto significó que la intención de comportamiento de los estudiantes para usar el LMS en las universidades de Pakistan, está influenciado por la expectativa de su utilidad, el esfuerzo requerido para invertir en su uso, y también la influencia social. Sin embargo, los hallazgos implican la necesidad de mejorar la experiencia del LMS, para aumentar su intención de comportamiento entre los estudiantes.

Figura 3. Resultados del estudio R-Cuadrado



Fuente: Raza et al. (2020)

Por otra parte, es importante destacar que en la actualidad no existen políticas de gestión de seguridad y riesgo informático en los LMS libres y comerciales (Santiso, Koller & Bisaro, 2016). Por su parte, Sánchez Freire & Parra Zamora (2018) mencionan que se debe mitigar o controlar los accesos no autorizados mediante la implementación o mejoramiento de las políticas de seguridad por parte de las instituciones que administran los LMS.

Con este antecedente, Santiso et al. (2016) desarrollaron una investigación donde lograron establecer un marco de gestión de la seguridad de la información aplicable a las plataformas de educación virtual, basado en estándares internacionales y enfocado específicamente en la actividad educativa. El Marco de Gestión definido, es de naturaleza abierta y sus definiciones no buscan ser para nada absolutas, sino que por el contrario, pretende ser un punto de partida para enmarcar la actividad de gestión de riesgo. Además, se lograron identificar y definir los aspectos necesarios para la puesta en práctica de dos tecnologías de seguridad que apuntan a proteger las plataformas educativas, como son: a) los sistemas Unificados de Gestión de Amenazas (UTM), orientados a la protección de las plataformas de cara a su interacción con Internet, y b) el uso de Infraestructuras de Clave Pública (PKI) para mejorar la autenticación y el no repudio de actividades a través del uso de certificados digitales.

Por su parte, Domínguez, Sepúlveda & Nuñez (2018) aplicaron una investigación orientada a los LMS vulnerables a ataques de sus administradores de bases de datos. Luego de las pruebas aplicadas a Moodle se determinó la carencia de un mecanismo para impedir que el administrador pueda realizar la suplantación no autorizada de identidad de un usuario cualquiera. Estas acciones tienen graves consecuencias, ya que el usuario víctima no posee ningún sistema de alerta para darse cuenta de que su cuenta fue utilizada por otra persona. Solamente Moodle posee registros de la actividad de autenticación dando como datos la fecha y la hora de la primera, y la última vez que se accedió al sitio, así como la dirección IP y la acción realizada. Si el usuario de Moodle tiene como costumbre revisar esta sección podría darse cuenta de que alguien accedió desde su sesión, pero si es olvidadizo o sencillamente no revisa esta sección, no se dará por enterado de que su cuenta fue usada por otra persona no autorizada

En contraste, Blackboard tiene un programa de seguridad sólido que no solo actúa para evitar los problemas de seguridad, sino que también determina sus causas. Así como también realiza pruebas continuas a la seguridad interna a nivel del código (análisis estático) y de la aplicación (análisis dinámico) para garantizar la satisfacción de las expectativas de los clientes, ratificando así que es el LMS comercial más popular utilizado por muchas universidades a nivel mundial (Blackboard Inc, 2018).

Un estudio realizado por Escobar, Perez & Rul (2016) mediante una auditoría informática realizada a la Universidad del Valle (México), se pudo determinar que al momento de revisar la documentación perteneciente al sistema de gestión de aprendizaje comercial Blackboard, el personal que se encontraba en su momento a cargo, no disponía de ningún documento o manual, por tanto el personal auditado desconocía de la política de seguridad de la plataforma, es así que, el auditor definió controles críticos de seguridad de la plataforma por riesgos que esta pudiera incurrir, así como también la importancia para las diversas actividades como es el control del acceso, protocolos y certificados de seguridad y por último documentación interna de la plataforma. En consecuencia, las recomendaciones emitidas por la auditoría realizada manifiestan que se debe realizar un manual de procedimientos de documentos para establecer políticas de seguridad para el sistema de gestión de aprendizaje.

A partir de esos aportes, es importante indicar que el sistema Moodle, siendo el más popular y utilizado a nivel educativo dispone de políticas de seguridad, para prever cualquier tipo de vulnerabilidad, que ocurriese. A continuación, se describen los tipos de políticas de acuerdo con:

a) Políticas de Usuario

Papel de los visitantes: Los usuarios que no hayan iniciado sesión en el sitio serán tratados como si tuvieran el rol especificado aquí, que se les otorga en el contexto del sitio. La función de invitado es la configuración predeterminada y recomendada para los sitios Moodle estándar (*MoodleDocs*, s/f).

- Rol para invitado: Esta opción especifica el rol que se asignará automáticamente al usuario invitado. Esta función también se asigna temporalmente a los usuarios no inscritos cuando ingresan a un curso que permite invitados sin contraseña.
- El papel de los administradores en los nuevos cursos. Moodle inscribirá automáticamente al usuario creando un nuevo curso en el curso con el rol especificado en esta configuración. Lo cual verifica que el rol utilizado para crear el curso. Por ejemplo, el "Administrador del curso", tiene el permiso de asignar el rol especificado en el nuevo curso. Si el rol de creador del curso no está configurado correctamente, el usuario se inscribirá en el curso sin ningún rol.
- Invitado de inicio de sesión automático: Si no está configurado, los visitantes deben hacer clic en el botón "Iniciar sesión como invitado" antes de ingresar a un curso que permite el acceso de invitados.
- Ocultar campos de usuario: Ciertos campos de usuario también se enumeran en la página de participantes del curso. Se puede aumentar la privacidad de los estudiantes ocultando los campos de usuario seleccionados.

Los siguientes campos de usuario aparecen en las páginas de perfil de los usuarios: descripción, ciudad, pueblo, país, página web, número ICQ, ID de Skype, ID de Yahoo, ID de AIM, ID de MSN, último acceso, mis cursos y primer acceso y grupos.

Los campos de usuario en las páginas de perfil de los usuarios están ocultos para todos los usuarios con la capacidad moodle / user: viewhiddendetails no establecida.

Los campos de usuario en la página de participantes del curso están ocultos para todos los usuarios con la capacidad moodle / course: viewhiddenuserfields no establecida.

- Mostrar la identidad del usuario: Cualquiera de los siguientes campos se puede mostrar a los usuarios con la capacidad moodle

site: viewuserientity al buscar usuarios y mostrar listas de usuarios: nombre de usuario, número de identificación, dirección de correo electrónico, número de teléfono, teléfono móvil, departamento, institución, ciudad –pueblo y país. Esta configuración es útil para sitios con una gran cantidad de usuarios, donde la probabilidad de que haya usuarios con el mismo nombre es alta.

- Asignaciones de funciones no admitidas: Las asignaciones de roles no admitidas son asignaciones de roles en contextos que no tienen sentido para ese rol, como el rol de creador del curso en el contexto de la actividad, o el rol del profesor en el contexto del usuario. Antes de Moodle 2.0, no existía la configuración de 'Tipos de contexto donde se puede asignar este rol' en el formulario de rol de edición, por lo que cualquier rol podía asignarse en cualquier contexto. Al actualizar un sitio desde la versión 1.9, las asignaciones de funciones en contextos que no tienen sentido para esa función se enumeran como asignaciones de funciones no admitidas.

En general, es seguro eliminar todas las asignaciones de funciones no admitidas, al hacerlo puede suceder que a un usuario se le anule la asignación de un rol personalizado; lo caul no se producirá ninguna otra pérdida de datos. (*MoodleDocs*, s/f).

b) Políticas de Referencia

Se puede establecer una política de referencia, el plugin de políticas proporciona un nuevo proceso para ingreso (identificación) del usuario, con habilidad para definir múltiples políticas (del sitio, privacidad, terceros), monitorear los acuerdos (consentimientos) del usuario y gestionar actualizaciones y versionado de las políticas, por lo mencionado existen políticas como: Referencia, Directivas, integracion con HTML, integracion con CSS y especificar una política de reservado (MoodleDocs, 2020) de detalla a continuación:

- Directivas: El Referer encabezado se omitirá por completo. No se envía información de referencia junto con las solicitudes.

No-referrer-when-downgrade (defecto)

Este es el comportamiento predeterminado si no se especifica ninguna política o si el valor proporcionado no es válido. El origen, la ruta y la cadena de consulta de la URL se envían como referencia cuando el nivel de seguridad del protocolo permanece igual (HTTP → HTTP, HTTPS → HTTPS) o mejora (HTTP → HTTPS), pero no se envía a destinos menos seguros (HTTPS → HTTP).

origin

Envíe únicamente el origen del documento como referente.
Por ejemplo, un documento en: https://example.com/page.html enviará la referencia https://example.com/

origin-when-cross-origin

Envíe el origen, la ruta y la cadena de consulta cuando realice una solicitud del mismo origen, pero solo envíe el origen del documento para otros casos.

same-origin

Se enviará una referencia para los orígenes del mismo sitio, pero las solicitudes de origen cruzado no enviarán información de referencia.

strict-origin

Solo envíe el origen del documento como referencia cuando el nivel de seguridad del protocolo sea el mismo (HTTPS → HTTPS), pero no lo envíe a un destino menos seguro (HTTPS → HTTP).

strict-origin-when-cross-origin

Envíe el origen, la ruta y la cadena de consulta cuando realice una solicitud del mismo origen, solo envíe el origen cuando el nivel de seguridad del protocolo se mantenga igual mientras realiza una solicitud de origen cruzado (HTTPS → HTTPS) y no envíe ningún encabezado a ningún sitio menos seguro destinos (HTTPS → HTTP).

unsafe-url

Envíe el origen, la ruta y la cadena de consulta al realizar cualquier solicitud, independientemente de la seguridad.

- Integración con HTML: También puede establecer políticas de referencia dentro de HTML. Por ejemplo, se puede establecer la política de referencia para todo el documento con un <meta>elemento con un nombre de referrer.

Integración con CSS: Puede recuperar recursos referenciados de hojas de estilo. Estos recursos también siguen una política de referencia: Las hojas de estilo CSS externas utilizan la política predeterminada (no-referrer-when-downgrade), a menos que se sobrescriba mediante un Referrer-Policyencabezado HTTP en la respuesta de la hoja de estilo CSS.

Para los <style> elementos o style atributos, se utiliza la política de referencia del documento del propietario.

- Especificar una política de reservado: Si desea especificar una política de reserva, en cualquier caso, la política deseada no tiene un soporte de navegador lo suficientemente amplio, use una lista separada por comas con la política deseada especificada al final:

Referrer-Policy: no-referrer, strict-origin-when-cross-origin

En el escenario anterior, no-referrer solo se utilizará si strict-origin-when-cross-originel navegador no lo admite. (Referrer-Policy, s/f)

c) Políticas de Contraseñas

La política de contraseñas incluye la opción de establecer la longitud mínima de la contraseña, el número mínimo de dígitos, el número mínimo de caracteres en minúsculas, el número mínimo de caracteres en mayúsculas y el número mínimo de caracteres no alfanuméricos.

La política de contraseña está habilitada de forma predeterminada. La configuración predeterminada (recomendada) es:

- Longitud de la contraseña: 8
- Dígitos - 1
- Letras minúsculas - 1
- Letras mayúsculas - 1
- Caracteres no alfanuméricos – 1

3. ¿Qué mecanismos de mitigación y defensa se ha implementado en los Sistemas de Gestión de Aprendizaje?

Ante los fallos y diversas vulnerabilidades existentes en los LMS es necesario contar con mecanismos de defensa que puedan mitigar y solucionar dichos ataques que van dirigidos a los pilares fundamentales de la información, a continuación, se describen algunos de los mecanismos planteados por varios autores:

MECANISMOS DE MITIGACIÓN Y DEFENSA

- Autenticación Biométrica

La autenticación biométrica desempeña un papel vital en la protección de la confidencialidad de los datos de los usuarios en los sistemas de gestión de aprendizaje, puesto que al momento de autenticarse en el LMS moodle éste considera únicamente usuario y contraseña y si son válidos accede, dejado una puerta abierta a la suplantación de identidad (Savulescu, Polkowski, Cosmin, & Blidaru, 2015).

- Modelos de Infraestructura Clave (PKI)

Según los autores Ibrahim et al. (2020) sugirieron la implementación de un sistema basado en el sistema de Modelos de Infraestructura Clave (PKI) que ofrecen seguridad esencial propiedades y servicios en el aprendizaje colaborativo en línea, que asegura la disponibilidad, integridad, autenticidad y confidencialidad de los datos y la información. La PKI consiste en hardware, software y procedimientos necesario para gestionar, almacenar y revocar los certificados digitales y claves públicas

- Modelo creado por Microsoft

Para los autores Mohd Alwi & Fan (2010) propusieron un modelo que fue creado por Microsoft en el diseño de la web para evaluar las amenazas a la seguridad en los sistemas de aprendizaje electrónico conocido como "IWAS". Este modelo proporciona cinco pasos en el cual se analizan a la seguridad de los LMS.

a. Identificar los objetivos de seguridad
b. Resumen de la aplicación
c. Aplicación de descomposición
d. Identificación de las amenazas

- Mitigación para el ataque de *cross site scripting*

Para la mitigación y defensa se considera lo siguiente:

a. Garantizar que las páginas del sitio web devuelvan las entradas del usuario sólo después de validarlas para cualquier código.
b. No confiar completamente en los sitios web que no sean HTTPS debido a que no cuentan con certificados digitales.
c. HTTPS asegura conexiones de tipo seguro, pero el procesamiento de los datos introducidos por el usuario es interno a la aplicación.
d. Convertir todos los caracteres no alfanuméricos en entidades de caracteres HTML antes de mostrar la entrada del usuario en los motores de búsqueda y los foros.
e. Utilizar ampliamente las herramientas de prueba durante la fase de diseño para eliminar esos agujeros XSS en el aprendizaje electrónico antes de que entre en uso (Costinela Luminița & Nicoleta Magdalena, 2012).

Dicha herramienta funciona del lado del servidor y tiene la capacidad de detectar y prevenir ataques XSS y superar las debilidades de los filtros seleccionados. RT_XSS_Cln ha sido conectado al servidor de Moodle. (Barhoom & Azaiza, 2016).

f. Según Al-azaiza, (2016)propone tres funciones PHP ampliamente utilizadas que pueden sanear los campos de los ataques XSS, estas funciones son strip_tags(), Htmlspecialchars() y Filter_Var() y, cuatro filtros XSS lo cual fue diseñado para evitar que los scripts XSS necesiten asegurar que todas las variables que se le dan al usuario debe ser codificada, este proceso sustituye al HTML con representaciones alternativas llamadas entidades y por último un filtro RT_XSS_Cln XSS mismo que se basa en la discusión previa de los cuatro filtros mencionados anteriormente.
g. Barhoom & Hamada (2014) propusieron dicha herramienta la cual puede ser usada en foros que toman la entrada del usuario como objetivo para detectar los ataques XSS mediante la inyección de código JavaScript malicioso del lado del cliente.

- Mitigación para el ataque de inyección SQL

Se debe tomar en cuenta algunos mecanismos de mitigación para evitar los ataques de inyección SQL:

a. Los programadores deben: usar un lenguaje o compilador que realice una comprobación automática de los límites para asegurar la entrada en la estructura de la memoria asignada; usar una biblioteca de abstracción para abstraer las APIs de riesgo; utilizar tecnologías que intenten proteger los programas contra estos ataques.
b. Los administradores de los sistemas deberían configurar las aplicaciones que vienen por defecto con usuario y contraseña *root,* para evitar tener permisos de modo privilegiado.
c. La identificación de la sesión debe ser adecuadamente larga e impredecible. (Al-azaiza, 2016)
d. Comprobar si el id de la sesión ha sido generado por la aplicación y no fue introducido manualmente por el usuario.
e. Regenerar el id de sesión después de un período de tiempo o cuando el nivel de privilegios del usuario haya cambiado.
f. Expirar la sesión después de un período de inactividad.
g. Eliminar la cookie de sesión cuando una sesión es terminada
h. Moodle usa la siguiente declaración de sql: UPDATE mdl_user SET apellido=? WHERE id=?; y luego pasa un array de valores array($lastname, $id) a la base de datos junto con el SQL.

- Capatcha

Mitigación para ataques de sesión, ataque de diseño y cierre de sesión de usuario, sesión no cerrada.
Kumar & Dutta, (2011) y otros sugieren se utilice la técnica CAPATCHA para evitar la fuerza bruta en la página de inicio de sesión que genera valores aleatorios que permiten al usuario introducir estos valores aleatorios durante su inicio de sesión.
Propone usar también Secure Socket Layer (SSL) el cual establece un enlace encriptado entre el servidor web y los navegadores.

- Encriptación de Datos

La encriptación es el proceso de ocultar datos en un formato que no es visible o común; existen varias técnicas de cifrado como son los algoritmos de clave secreta y algoritmos de llave pública los cuales proporcionan
Confidencialidad, autenticación, integridad y el no repudio de los datos.

- La Gestión de Derechos Digitales (DRM)

La aplicación de DRM en el aprendizaje electrónico permite controlar el acceso no autorizado a información, así como también los controles de edición, reenvío o intercambio, impresión, evitando la captura de pantalla de la información mediante la encriptación del contenido y sólo las personas autorizadas con las claves de desencriptación pueden tener acceso a la información. (Savulescu et al., 2015)

- Mitigación para secuestro de sesión, la fijación de la sesión y predicción de nombre de usuario y contraseña.

Según Hernández & Chávez (2008) proponen que la modificación de ciertas partes del código y la adición de nuevas funciones, como es el caso añadiendo un script PHP que cambia el contenido del objeto que contiene el entorno de configuración llamada CFG. Dentro de CFG hay las siguientes cuatro variables que son SSL relacionado.

a. Themewww. Esta variable contiene la ubicación de los recursos para construir la interfaz gráfica como una cadena de URL completa. El script tiene que cambiar el protocolo HTTP para HTTPS (solicitud SSL).
b. Wwwroot. Moodle usa esta variable para saber la URL asignada para una navegación rápida.

El script tiene que cambiar el protocolo HTTP para HTTPS.

c. Loginhttps. El valor de esta bandera se recupera de la base de datos y cuando está en el login encriptada a través de SSL. El guión lo enciende, incluso si las configuraciones principales dicen de lo contrario.
d. Httpstheme. Cuando se activa el loginthttps, el código fuente original cambia la URL de HTTP a HTTPS. Este script también cambia este valor a HTTPS, anulando el valor original de loginhttps.
e. El *script* también tiene que cambiar el valor de la bandera global HTTPSPAGEREQUIRED a true.

- Usar SSL en todo el sitio

Esta bandera es parte de la configuración por defecto de Moodle. Tales correcciones fueron implementadas en un script llamado buap_security que se invoca cuando el script principal de configuración config.php es llamado a cada solicitud de los usuarios.
La página de configuración del servidor de seguridad también fue cambiada se refleja la opción de cifrar todo el sitio modificando el

código fuente de la security.php, localizado dentro del paquete de administración (Arakelyan, 2013).

Resultados y Discusión

Las evidencias obtenidas luego de la Revisión Sistemática de la Literatura (RSL) permitieron identificar las vulnerabilidades y ataques más comunes en los LMS, las políticas de seguridad aplicadas a los sistemas de gestión de aprendizaje y los mecanismos de mitigación y defensa, lo cual dió respuesta a las preguntas de investigación formuladas. En relación con la primera pregunta se utilizaron diferentes aportes científicos, los cuales determinaron las vulnerabilidades más relevantes como son: Comunicación Insegura (Orehovački, 2008), Denegación de servicio (DoS) (López et al. 2014), fuga de Información y manejo inadecuado de errores (Mohd Alwi & Fan, 2010), inyección SQL (Keng et al., 2014).

Así mismo, según lo expuesto por los autores en relación con las vulnerabilidades existentes, permite inferir que estas afectan los principios básicos de la seguridad de la información; como es el caso del LMS Moodle, que tiene debilidades en cuanto a la inexistencia de un mecanismo para que el administrador de las bases de datos pueda detectar el acceso no autorizado o la suplantación de identidad de un usuario. No obstante, los LMS comerciales como Blackboard poseen un programa de gestión de vulnerabilidades que se rige por una política de divulgación y compromiso de gestión de vulnerabilidades. En caso de que se identifique una violación de la seguridad en un producto lanzado al mercado, el equipo de seguridad de Blackboard estará listo para tomar medidas al respecto.

En relación con la pregunta enfocada a la falta de políticas y procedimientos adecuados que afectan a los sistemas de gestión de aprendizaje, se considera pertinente la creación y aplicación de políticas para poder asegurar la información de los usuarios que en estos momentos tienen mayor interacción con los LMS debido a la situación de pandemia, lo que garantiza el éxito en el desarrollo de las actividades académicas.

Por otra parte, los mecanismos de mitigación y defensa más comunes implementados en los Sistemas de Gestión de Aprendizaje fueron: Mitigación para el ataque de inyección SQL se debe considerar que: a) los programadores deben usar un lenguaje o compilador que realice una comprobación automática de los límites para asegurar la entrada en la estructura de la memoria asignada; usar una biblioteca de abstracción para las APIs de riesgo; utilizar tecnologías que intenten proteger los programas contra estos ataques. b) los administradores de los sistemas deberían configurar las aplicaciones que vienen por defecto con usuario y contraseña *root,* para evitar tener permisos de modo privilegiado y c) la identificación de la sesión debe ser adecuadamente larga e impredecible (Al-azaiza, 2016).

De acuerdo con (Kumar & Dutta, 2011) sugieren utilizar la técnica CAPTCHA, al momento de que el usuario inicie sesión mediante la introducción de valores aleatorios, lo que permitirá proteger los LMS, garantizando la estabilidad y continuidad de los servicios. De la misma forma, la revisión de la documentación permite especificar, que la autenticación biométrica desempeña un papel vital en la protección de la confidencialidad de los datos de los usuarios en los sistemas de gestión de aprendizaje, puesto que al momento de autenticarse en el LMS Moodle éste considera únicamente usuario y contraseña, en el caso de ser válidos permite el acceso, dejado una puerta abierta a la suplantación de identidad, razón por la cual se sugiere otro mecanismo paralelo de autenticación.

Los resultados de la investigación muestran las vulnerabilidades y ataques se pueden manifestar en relación con los pilares fundamentales de la seguridad de la información de Moodle. Por ejemplo, ataques de autenticación, ataques de disponibilidad, ataques de confidencialidad, integridad de ataques y ataques de diseño, los cuales deben ser analizados y mitigados por el administrador del sistema e-learning.

Conclusiones

Mediante la revisión sistemática de la literatura, se pudo evidenciar las vulnerabilidades y las políticas de mitigación presentes en los LMS. Por tanto, se han desarrollado una serie de políticas, entre las más importantes se tiene el establecimiento de roles, papel de los visitantes, rol para invitado, rol predeterminado para todos los usuarios, el papel de los creadores en los nuevos cursos, invitado de inicio de sesión automático, ocultar campos de usuario, mostrar la identidad del usuario, formato de nombre completo, usuarios máximos por página, URL de imagen predeterminada de perfil, asignaciones de funciones no admitidas, entre otras.

Por otra parte, es pertinente mencionar que, Blackboard posee un programa de gestión de vulnerabilidades que se rige por una Política de divulgación y compromiso de gestión de vulnerabilidades. Ante las vulnerabilidades en los Sistemas de Gestión de Aprendizaje, específicamente uno de tanta usabilidad como Moodle, se considera necesario la creación e implementación por parte de las instituciones educativas de los mecanismos descritos que permitan prevenir los fallos que se presenten en los LMS, garantizando, la identidad de los usuarios, la integridad de la información transmitida o almacenada y también, la prosecución del aprendizaje colaborativo.

Trabajo Futuro

Este trabajo podría considerarse como una base para futuras investigaciones en determinar los ataques, vulnerabilidades y mecanismos, a futuro se podría definir las políticas internas en las instituciones educativas que dispongan de LMS para garantizar y precautelar la información de los usuarios, quienes entregan sus datos sensibles, y éstos al no estar protegidos de manera eficiente podrían ser expuestos a dichos ataques y vulnerabilidades existentes.

Referencias Bibliográficas

Al-azaiza, R. (2016). *Detection and Prevention of XSS Vulnerabilities in MOODLE*. https://iugspace.iugaza.edu.ps/handle/20.500.12358/20201

Arakelyan, V. A. (2013). *Vulnerable Security Problems in Learning Management System (LMS) Moodle*. 6.

Bandara, I., Ioras, F., & Maher, K. (2014). *CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION*. 7.

Barhoom, T. S., & Azaiza, R. J. (2016). Enhance MOODLE Security Against XSS Vulnerabilities. *International Journal of Computing and Digital Systems*, *05*(05). http://dx.doi.org/10.12785/IJCDS/050507

Barhoom, T, & Hamada, M. (2014). PalXSS: Client Side Secure Tool to Detect XSS Attacks. *Saba Journal Of Information Technology And Networking (SJITN)-ISSN: 2312-4989*, *2*(2), Article 2. http://www.ojs.sabauni.net/index.php/SJITN/article/view/14

Blackboard Inc. (2018). *Declaración de seguridad de los productos Blackboard | Ayuda de Blackboard*. https://help.blackboard.com/es-es/Product_Security

Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. *bie3: Boletín IEEE*, *2 (Abril-junio)*, 950–966. https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Clarenc. (2013). *Instrumento de evaluación de LMS, materiales educativos digitales y recursos de la WEB 3.0 | Tecnologia Educacional | Software*. Scribd. https://es.scribd.com/doc/175057118/Instrumento-de-evaluacion-de-LMS-materiales-educativos-digitales-y-recursos-de-la-WEB-3-0

Cloudflare. (2020). *What Is a Distributed Denial-of-Service (DDoS) Attack?* Cloudflare. https://www.cloudflare.com/es-la/learning/ddos/what-is-a-ddos-attack/

Costinela Luminița, C. (Defta), & Nicoleta Magdalena, C. (Iacob). (2012). E-learning Security Vulnerabilities. *Procedia - Social and Behavioral Sciences*, *46*, 2297–2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Costinela-Luminița, C. (Defta), & Nicoleta-Magdalena, C. (Iacob). (2012). E-learning Security Vulnerabilities. *Procedia - Social and Behavioral Sciences*, *46*, 2297–2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Domínguez, A. R. D., Sepúlveda, J. C. S., & Nuñez, Y. N. (2018). CMS y LMS vulnerables a ataques de sus administradores de bases de datos. *Revista Arquitectura e Ingeniería*, *12*(2), 2. https://dialnet.unirioja.es/servlet/articulo?codigo=6548141

Escobar, H. A. Q. M., Pérez, D. A. D., & Rul, M. N. P. (2016). La seguridad informática en las plataformas educativas que se utilizan en el nivel superior: Una tarea pendiente. *Revista Multidisciplinaria de Avances de Investigación*, *2*(3), 1–18. http://www.remai.ipn.mx/index.php/REMAI/article/view/21

Hernandez, J., & Chavez, M. (2008). Moodle security vulnerabilities. *2008 5th International Conference on Electrical Engineering, Computing Science and Automatic Control*, 352–357. https://doi.org/10.1109/ICEEE.2008.4723399

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). *A Study on Cybersecurity Challenges in E-learning and Database Management System*. 8th International Symposium on Digital Forensics and Security, ISDFS 2020. Scopus. https://doi.org/10.1109/ISDFS49300.2020.9116415

Keng, S., Chee, O., Mahinderjit Singh, M. (Mandy), & Hassan, R. (2014). SQL Injections Attack and Session Hijacking on E-Learning Systems. En *I4CT 2014—1st International Conference on Computer, Communications, and Control Technology, Proceedings*. https://doi.org/10.1109/I4CT.2014.6914201

Kitchenham. (2007). *Directrices para realizar revisiones sistemáticas de literatura en ingeniería de software—Buscar con Google*. https://www.google.com/search?sxsrf=ALeKk02CUNufUCplj5hgQXSRif0Af3V4og%3A1607394129516&source=hp&ei=UePOX7jdHZKD5wLM7YKICw&q=Guidelines+for+performing+Systematic+Literature+Reviews+in+Software+Engineering&oq=Guidelines+for+performing+Systematic+Literature+Reviews+in+Software+Engineering&gs_lcp=CgZwc3ktYWIQAzICCAAyAggAMgYIABAWEB4yBggAEBYQHjoHCCMQ6gIQJ1DmCljmCmDGFGgBcAB4AIABywGIAcsBkgEDMi0xmAEAoAECoAEBqgEHZ3dzLXdperABCg&sclient=psy-ab&ved=0ahUKEwj4yejgqb3tAhWSwVkKHcy2ALEQ4dUDCAc&uact=5

Kumar, S., & Dutta, K. (2011). Investigation on security in lms moodle. *International Journal of Information Technology and Knowledge Management*, *Vol4*(Issue 1), PP:233-238.

Leon, M. T., Larenas, F. P., & Fajardo, M. C. (2015). Comparación de los LMS Moodle y CourseSites de Blackboard usando el modelo de aceptación tecnológica TAM / Comparison of LMS Moodle and Blackboard CourseSites using the technology acceptance model TAM. *CIENCIA UNEMI*, *8*(16), 78–85. http://ojs.unemi.edu.ec/index.php/cienciaunemi/article/view/221

Lim, C. C., & Jin, J. S. (2006). *A Study on Applying Software Security to Information Systems: E-Learning Portals*. 6.

López, A. B., Aldana, A. C. A., & Cuervo, M. C. (2014). Vulnerabilidad de Ambientes Virtuales de Aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus [Vulnerability in Virtual Learning Environments using SQLMap, RIPS, W3AF and Nessus]. *Ventana Informatica*, *30*, Article 30. https://doi.org/10.30554/ventanainform.30.276.2014

Luo, T., Murray, A., & Crompton, H. (2017). Designing Authentic Learning Activities to Train Pre-Service Teachers About Teaching Online. *International Review of Research in Open and Distance Learning*, *18*(7). https://doi.org/10.19173/irrodl.v18i7.3037

Mohd Alwi, N. H., & Fan, I.-S. (2010). E-Learning and Information Security Management. *International Journal for Digital Society*, *1*(2), 148–156. https://doi.org/10.20533/ijds.2040.2570.2010.0019

Molina, V., Furfaro, A., Malena, G., & Parise, A. (2015). *Ataques Distribuidos de Denegación de Servicios: Modelación y simulación con eventos discretos*. https://doi.org/10.13140/RG.2.1.5123.5687

Moodle. (2020). *Estadísticas de Moodle*. https://stats.moodle.org/

Orehovački, T. (2008). Determination of optimal security settings for LMS Moodle. *Proceedings of the 31st MIPRO International Convention on Information Systems Security*. Recuperado el 24 de noviembre de 2020, de https://www.academia.edu/600843/Determination_of_optimal_security_settings_for_LMS_Moodle

Políticas de usuario—MoodleDocs. (s/f). Recuperado el 3 de diciembre de 2020, de https://docs.moodle.org/310/en/User_policies

Raza, S., Qazi, W., Khan, K., & Salam, J. (2020). Aislamiento social y aceptación del sistema de gestión del aprendizaje (LMS) en tiempos de la pandemia COVID-19: Una expansión del modelo UTAUT. *Journal of Educational Computing Research*, 0735633120960421. https://doi.org/10.1177/0735633120960421

Referrer-Policy. (s/f). MDN Web Docs. Recuperado el 3 de diciembre de 2020, de https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Sánchez, J., & Parra, P. (2018). *ANÁLISIS DE VULNERABILIDADES DE CREDENCIALES DÉBILES O POR DEFECTO EN APLICACIONES WEB LMS (HERRAMIENTAS DE GESTIÓN DE APRENDIZAJE)*. https://repositorio.pucesa.edu.ec/handle/123456789/2712

Santiso, H., Koller, J, & Bisaro, M. (2016). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*, *14*, 67–88. http://revistas.um.edu.uy/index.php/ingenieria/article/view/337

Savulescu, C., Polkowski, Z., Cosmin, D. I., & Elena, B. C. (2015). Security in e-learning systems. *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, WE-19-WE-24. https://doi.org/10.1109/ECAI.2015.7301225

Violettas, G, Theodorou, T, & Stephanides, G. (2013). E-Learning Software Security: Tested for Security Vulnerabilities & Issues. *2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity"* https://www.academia.edu/8066233/E_Learning_Software_Security_Tested_for_Security_Vulnerabilities_and_Issues