Evaluación de seguridad en Ambientes Virtuales de Aprendizaje AVA – Moodle y Dokeos

Alexander Barinas López[a], Helena Alemán Novoa[b]

[a] Ingeniero de Sistemas, Especialista en Telemática, Msc Maestría en Tecnología Informática. Universidad Pedagógica y Tecnológica de Colombia UPTC. Docente, Fundación Universitaria Juan de Castellanos (Tunja, Boyacá, Colombia), Integrante Grupo de Investigación MUISCA – línea de seguridad Informática y de la información. Correo electrónico: abarinas@jdc.edu.co

[b] Ingeniera de Sistemas, Especialista en Pedagogía, Msc Maestría en Seguridad Informática. Universidad Internacional de la Rioja. Docente, Fundación Universitaria Juan de Castellanos (Tunja, Boyacá, Colombia), Integrante Grupo de Investigación MUISCA – línea de seguridad Informática y de la información. Correo electrónico: haleman@jdc.edu.co

Resumen. Este artículo describe el procedimiento para la evaluación de seguridad de los ambientes de aprendizaje AVA en las plataformas de software libre y código abierto Moodle y Dokeos, inicialmente se presenta un estudio de guías, normas y estándares de seguridad, a partir de las cuales se establecen criterios y métricas para la evaluación de la seguridad de estas plataformas, posteriormente se analiza y selecciona herramientas para el análisis y evaluación de seguridad en los AVA y finalmente se propone un modelo de evaluación aplicado a los AVA que permite cuantificar su nivel de seguridad en cuanto a su confidencialidad, integridad y disponibilidad.

Palabras Clave: Ambientes virtuales de aprendizaje AVA, herramientas de evaluación de seguridad, criterios de seguridad, métricas de seguridad

1 Introducción

Actualmente la información es el activo más importante para las organizaciones, incluyendo el Sector Educativo, el cual implementa plataformas virtuales de aprendizaje AVA para apoyar los procesos académicos, en algunos casos, existen instituciones educativas que centran sus procesos de enseñanza - aprendizaje mediante el uso de dichas plataformas; estos ambientes son aplicaciones diseñadas para facilitar a los educadores la administración y gestión de cursos virtuales para sus estudiantes, funcionan generalmente en un servidor que permite guardar toda la información relacionada con los cursos, incluyendo contenidos, datos personales de docentes y estudiantes, calificaciones de actividades evaluadas; lo que implica que en un mismo ambiente se concentre información sensible que puede interesar a personal ajeno para realizar accesos no autorizados, suplantación de identidad, causando

alteraciones o pérdida de la información allí contenida, constituyéndose en un riesgo potencial que atenta contra la integridad, disponibilidad y confidencialidad de la información.

En este artículo se describen las actividades desarrolladas con el fin de diseñar un modelo de evaluación para los AVA, basado en criterios y métricas generadas a partir de normas y estándares de seguridad establecidos, como lo son la ISO 9126, ISO 25000, ISO 27001 y OWASP, igualmente se presentan el análisis y resultado de las pruebas de seguridad realizadas mediante el uso de herramientas de código abierto tales como: SQLmap, W3AF, OWASP ZAP, NESSUS, RIPS de donde se estructura el modelo que permite evaluar el nivel de seguridad en los AVA – Moodle y Dokeos, proporcionando un juicio de valor confiable a nivel cuantitativo y cualitativo en cuanto a la seguridad de los AVA.

2 Ambientes Virtuales de Aprendizaje (AVA).

Es un espacio de aprendizaje mediado por las tecnologías tales como Internet, sistemas satelitales, la multimedia, la televisión interactiva, entre otros, facilitando la comunicación, el procesamiento y distribución de la información, permitiendo nuevas posibilidades para el aprendizaje y facilitando las interacciones entre los diversos actores que intervienen en las relaciones del proceso enseñanza aprendizaje, así como la creación y mantenimiento de comunidades virtuales [1]. Algunas de las funcionalidades de los AVA son: Gestión administrativa (gestión de estudiantes, herramientas de monitorización, mecanismos de acceso a BD, elaboración de informes, administración cualitativa y funcional de flujos de trabajo), Gestión de Recursos (control de auditoría y edición de contenidos, objetos de aprendizaje, plantillas de ayuda en la gestión de contenidos, mecanismos de descarga y registro de contenidos, reutilización y compartición de objetos de aprendizaje), herramientas de comunicación (foros, chat, pizarra, email, wikis).

Los AVA también denominados Learning Management System (LMS), Sistema para la Gestión de Aprendizaje, es un software diseñado para facilitar la organización de materiales y actividades a profesores en cuanto a la gestión de cursos virtuales, llevar el control y seguimiento de procesos de aprendizaje a estudiantes, evaluarlos, comunicarse con ellos por medio de foros de discusión, chat o correo, permitiendo también funciones para administrar cursos de formación a distancia y presencial.

En la tabla 1 se muestra algunas herramientas LMS implementadas en Universidades Colombianas y el tipo de licencia que utilizan:

Tabla 1. Ambientes virtuales de aprendizaje utilizados por las principales Universidades de Colombia.

Herramienta LMS	Licencia Open Source (código libre)	Software privado	Universidades que utilizan LMS
Moodle	X		Universidad Nacional de Colombia Universidad de Antioquia Universidad del Valle Universidad del Norte Universidad Industrial de Santander Universidad Pontificia Bolivariana. Universidad de Caldas Universidad Pedagógica y Tecnológica de Colombia Universidad Externado de Colombia Universidad de Medellín Universidad Distrital Francisco José de Caldas
Blackboard		X	Universidad Nacional de Colombia Universidad de los Andes Universidad Javeriana

2.1 Plataforma Moodle.

Es un entorno dinámico de aprendizaje virtual, conformado por paquetes de software para la creación de cursos basados en web, permitiendo distribuir varios tipos de archivos como textos, hojas de cálculo, pdf, videos, imágenes, entre otros. Moodle es de libre distribución (bajo la Licencia pública GNU), es decir que este software tiene derechos de autor (copyright), pero se puede usar y modificar siempre y cuando se mantenga el código fuente abierto para todos [2].

El desarrollo de Moodle nace como parte del trabajo de investigación de Martin Dougiamas, en la Universidad de Curtin (Australia), cuyo principal objetivo de dicho proyecto era explorar las posibilidades que ofrece Internet, desde el punto de vista de la pedagogía construccionista social, en el proceso de enseñanza-aprendizaje [3]. La palabra Moodle es el acrónimo de Modular Object Oriented Dynamic Learning Environment (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular), el cual fue diseñado para poder desarrollar contenidos de acuerdo con la filosofía de los Objetos de Aprendizaje [4].

Características generales de Moodle [5]:

Moodle puede ser ejecutado en múltiples plataformas que soporten la tecnología PHP (Linux, UNIX, Windows, etc.)

Su diseño modular, ofrece una gran flexibilidad para añadir o eliminar funcionalidades en varios niveles.

Se puede actualizar de una versión a la siguiente, manteniendo la información original.

Permite definir varios niveles de acceso a los cursos, por ejemplo teniendo distintos niveles de acceso para profesores, esto hace que sea una plataforma segura.

Es una herramienta de colaboración, la pedagogía constructiva del aprendizaje tanto los estudiantes como profesores pueden contribuir a la experiencia educativa.

Es adecuado como herramienta de apoyo a la docencia tanto presencial como virtual.

Su interfaz simple, ligera y eficiente, es compatible con múltiples navegadores web (Internet Explorer, Mozilla, Opera, Safari, etc.)

Es de gran utilidad para impartir múltiples cursos, permitiendo que el profesor administre recursos del aula virtual e interactúe con los alumnos, invitados, e incluso con otros profesores.

2.1 Plataforma Dokeos.

Es un software libre bajo la licencia de General Public Licence (GPL), su desarrollo es internacional y colaborativo, su código está disponible para que cualquiera pueda hacer uso del mismo o para realizar cambios que se adapten a las necesidades específicas de un usuario, Dokeos es un Sistema de Gestión de Contenidos (CMS), el cual puede ser usado para la educación y por muchas organizaciones (empresas, universidades, institutos, administraciones públicas). Dokeos fue implementado por primera vez en la Université Catholique de Louvain (Belgica), siendo uno de los software más difundidos en más de 63 países y 34 idiomas, su principal objetivo es ser un sistema flexible y de fácil uso mediante un interfaz de usuario amigable [6].

Características principales de la plataforma Dokeos [7]:

Dokeos es una suite de aprendizaje en línea basada en software libre.

Está basado en PHP y usa bases de datos en MySQL

Permite publicar documentos (texto, pdf, HTML, videos)

Cuenta con una interfaz amigable al usuario, especialmente para quienes tengan pocas nociones en computación y mayor interés en los contenidos de los cursos.

Es una aplicación de administración de contenidos de cursos, permitiendo la gestión y seguimiento de actividades de enseñanza aprendizaje en la red.

Algunas de las principales herramientas que proporciona Dokeos son: Aprendizaje a través de lecciones SCORM[1], producción de documentos basados en plantillas, diferentes formas de realizar los cuestionarios, interacción por medio de chats y

[1] Del inglés (Sharable Content Object Reference Model) es una especificación que permite crear, integrar y enlazar objetos pedagógicos estructurados.

grupos, videoconferencia, encuestas, autentificación vía LDAP[2], sesiones de usuario, entre otros.

3 Guías, normas y estándares de seguridad

El marco normativo que constituye la seguridad web, en el caso particular de los ambientes virtuales de aprendizaje, fue el fundamento para la selección de criterios y métricas que se aplicaron al modelo de evaluación de los AVA, dentro de la selección de este referente normativo se encuentran:

3.1 Normas ISO / IEC 9126

Al hablar de calidad de producto software, se hace necesario contar con un estándar internacional para la evaluación de la calidad de dicho producto. Esta norma publicada en 1992 con el nombre de Information technology – Software product evaluation: Quality characteristics and guidelines for their use, establece criterios de calidad para este tipo de productos. El estándar 9126 establece que cualquier componente de calidad del software puede ser descrito en términos de una o más de seis características básicas, las cuales son: funcionalidad, confiabilidad, usabilidad, eficiencia, capacidad de mantenimiento y portabilidad; cada una de las cuales se detalla por medio de un conjunto de sub-características que permiten profundizar en la evaluación de productos software. Esta norma consta de cuatro secciones: modelo de la calidad, métricas externas, métricas internas y calidad en las métricas en uso. Para este trabajo se seleccionó como marco de referencia al primero (ISO/IEC 9126-1) por ser el que cuenta con el modelo de calidad que más se ajusta a los objetivos propuestos teniendo en cuenta la sub-característica de seguridad referente a la característica de funcionalidad como tema principal de la investigación [8].

3.2 ISO 25000

Calidad del producto software. Estas normas han sido el resultado de la evolución de normas ISO/IEC 9126 e ISO/IEC 14598. La nueva familia de normas ISO/IEC 25000, conocida como SQuaRE (Software product Quality Requirements and Evaluation), tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad de producto software sustituyendo a normas anteriores y convirtiéndose así en la piedra angular de la ingeniería de software. Actualmente la familia SQuaRE define tres modelos de calidad: el modelo de calidad del producto, el de calidad en uso y el de calidad de datos; para el desarrollo de este trabajo se hace énfasis en el primer modelo por ser el principal a la hora de implantar la evaluación del producto software, el cual a su vez se encuentra compuesto por ocho características de calidad como son: adecuación funcional, eficiencia de desempeño, compatibilidad, capacidad de uso,

[2] Del inglés (Lightweight Directory Access Protocol), es decir, Protocolo Ligero/Simplificado de Acceso a Directorios, un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

fiabilidad, seguridad, mantenibilidad, portabilidad. Dentro de estas características se toma como referencia la seguridad como tema central de esta investigación [8].

3.3 Norma ISO 27001

Siendo la información un activo intangible y primordial para el funcionamiento de cualquier organización, es indispensable ofrecerle mayor importancia al aseguramiento y conservación de la misma, para esto es necesario contar con una norma que de las pautas necesarias para abordar esta tarea de una manera clara, documentada y fundamentada en objetivos precisos de seguridad por medio de una valoración de los riesgos a los que está expuesta la información de la organización [9], [10].

La ISO 27001, es la norma principal de la serie 27000, la cual contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y su objetivo fundamental es proteger la confidencialidad, integridad y disponibilidad de la información en cualquier tipo de organización, identificando cuáles son los potenciales inconvenientes que pueden afectar la información (evaluación de riesgos) y estableciendo controles para evitar estos problemas (mitigación del riesgo). Dentro de los aspectos relevantes de la norma 27001, se toman como referentes la integridad con el fin de verificar que la información sea correcta y completa, la disponibilidad para comprobar que siempre esté a disposición de las instituciones educativas y la confidencialidad para velar que la información sea utilizada sólo por personas que tienen autorización para hacerlo. Además es importante aplicar esta norma por cuanto contiene las disposiciones y directrices necesarias para la implementación de un SGSI. Los controles y objetivos de control referente con las aplicaciones se encuentran relacionados dentro de la norma ISO 27001, Anexo A de la misma, sección A.12 (A.12.1.1 – A.12.2.4)

3.4 Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP)

Este proyecto es producto de la comunidad de código abierto y su objetivo se concentra en ayudar a mejorar la seguridad de las aplicaciones informáticas estableciendo estándares que conduzcan a fomentar la solidez de la seguridad de una aplicación.

En cuanto a las aplicaciones web, una de ellas los AVA, OWASP presenta una guía fundamental a tener en cuenta para la seguridad de este tipo de aplicaciones, ya que esta comunidad frecuentemente realiza estudios de vulnerabilidades y ataques más comunes, además plantea las formas de combatirlos. En los documentos más importantes presentados por OWASP está la guía de pruebas de seguridad, denominada “OWASP Testing Guide” [11], en donde se analizan las condiciones para realizar pruebas en aplicaciones web, el alcance de estas, los principios de una prueba exitosa y cómo realizar pruebas a vulnerabilidades específicas.

En el modelo de seguridad planteado para los AVA, se tuvieron aspectos de la Guía de pruebas de OWASP, los cuales corresponden a: Gestión de configuraciones,

codificación y validación de entrada, controles de acceso y autenticación, gestión de sesiones y de usuarios, gestión de errores y excepciones, gestión de datos sensibles.

4 Seguridad en Ambientes Virtuales de Aprendizaje AVA

Actualmente en Internet encontramos un sinnúmero de servicios y aplicaciones funcionando en la red, desde comercio en línea, transacciones que mueven enormes cantidades de dinero, búsquedas en la web, correo electrónico e igualmente sitios de redes sociales que contienen información importante y confidencial de sus miembros [12]. Los problemas de estas aplicaciones y repositorios de datos corresponden generalmente a: Problemas de diseño, de implementación y operación del software, estos problemas dan lugar a diferentes tipos de ataques que implican, por un lado, abordar el diseño seguro de una aplicación web con almacén de datos desde el comienzo del Ciclo de Vida de Desarrollo Seguro de Aplicaciones (SSDLC), y por otro lado, a afrontar la gestión de la seguridad una vez desplegada en la fase de producción de la aplicación.

La seguridad de una aplicación web y por ende de un AVA depende del cumplimiento de algunos objetivos de seguridad tales como: Autenticación, control de acceso, confidencialidad, integridad, disponibilidad, no repudio (proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, no pudiendo su receptor-transmisor negar que se haya producido) y trazabilidad (proporcionar los controles que determinen que en todo momento se podrá determinar quién hizo qué y en qué momento).

4.1 Métricas de seguridad

El uso de métricas de seguridad permiten cuantificar el nivel de seguridad de un producto software con el fin identificar posibles acciones de control y mejora frente a los riesgos a los cuales está expuesta la información, tomando decisiones oportunas para mitigar las amenazas, como lo expresa Cano, "las métricas en seguridad son valoraciones altamente riesgosas, pues al comprender mejor algo que previamente no se conocía se genera un mayor conocimiento de la situación y su correspondiente responsabilidad y obligación para actuar en conformidad" [13].

Con respecto a las métricas en seguridad el profesor Hyden citado por Cano, presenta tres lecciones a saber [13]:

Las métricas de seguridad y la toma de decisiones producto de la gestión de riesgos ayudarán a mejorar la seguridad, en cuanto a la capacidad de recolección, análisis y comprensión de los datos relacionados con la operación de la seguridad.

La seguridad es un proceso de negocio, ya que si no se mide ni controla el proceso no estará midiendo ni controlando la seguridad.

La seguridad es el resultado de una actividad humana, producto de una lista efectiva de métricas en seguridad, que darán cuenta de cómo comprender a las personas como a la tecnología.

4.2 Criterios de seguridad

El Diccionario de la lengua española (DRAE), define criterio como una regla o norma conforme a la cual se establece un juicio o se toma una decisión.

Teniendo en cuenta el enfoque de la investigación, se seleccionaron algunos aspectos de seguridad de mayor relevancia como se muestra en la tabla 2, desde los cuales se puede considerar un sistema seguro si cumple con los aspectos de integridad, confidencialidad y disponibilidad de la información. Se analizaron diversas normas y estándares, organizaciones certificadas e información propuesta por diversos autores, con el fin establecer los criterios más importantes a considerar al establecer las características de los instrumentos de evaluación.

De manera general para analizar y evaluar el nivel de seguridad en aplicaciones web, se tienen en cuenta los siguientes criterios.

Integridad: Es la propiedad que busca mantener la información exactamente cómo fue generada, protegiéndola de modificaciones accidentales y/o intencionales.

Disponibilidad: Es la cualidad, característica o condición que posee la información de encontrase disponible de quienes quieren acceder a ella.

Confidencialidad: Es la capacidad para prevenir la divulgación parcial o completa de la información sensible a terceros.

Tabla 2. Criterios de seguridad de acuerdo a normas y estándares.

	ISO 9126	**ISO 25000**	**ISO 27001**	**OWASP**
Confidencialidad	X	X	X	X
Integridad	X	X	X	X
Disponibilidad	X		X	X
Autenticación		X		
No repudio		X		
Responsabilidad		X		

4.3 Herramientas de evaluación de seguridad en AVA

Las herramientas que se describen en la tabla 3, son herramientas para análisis de seguridad en aplicaciones web, las cuales permiten automatizar el análisis de seguridad, ayudando tanto a los administradores como a los profesionales de seguridad a realizar un cubrimiento mayor de la superficie de ataque de una aplicación y a su vez mejorar la tomar de decisiones con el fin mantener protegida infraestructuras informáticas, aunque también pueden ser utilizadas por los hackers para fines ilegales.

Estas herramientas fueron analizadas y evaluadas mediante un proceso de estudio, de acuerdo a su funcionalidad, ranking de mejores herramientas y el objetivo de análisis, posteriormente se eligieron tres herramientas para aplicar las pruebas de seguridad a los AVA, SQLMap, W3AF y OWASP ZAP, por su características especificas, los criterios y métricas a evaluar y su adaptabilidad.

Tabla 3. Descripción de las herramientas de seguridad.

Herramienta	**Descripción**	**Licencia/ Versión**
SQLMap	- Herramienta de código abierto desarrollada en Python para realizar inyección de código SQL automáticamente. - Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web.	GNU Ver. 0.9-3758
W3AF	- W3AF: Web Application Attack and Audit Framework - Es un framework de test de intrusión web - Proyecto cuyo objetivo es desarrollar un Framework para ayudar a proteger las aplicaciones web mediante la búsqueda y explotación de vulnerabilidades - Tiene funcionalidad de scanner de vulnerabilidades.	GPL 2.0 Ver. 1.6
OWASP ZAP (Zed Attack Proxy Project)	- Herramienta libre escrita en Java proveniente del Proyecto OWASP para realizar, en primera instancia, tests de penetración en aplicaciones web - Herramienta para pruebas de penetración, permite encontrar diversos tipos de vulnerabilidades, tales como: * Inyección de código arbitrario (SQL, OS, PHP, etc.) * Cross-site scripting (XSS) * Inclusión remota y local de ficheros.	Apache 2.0 Ver. 2.3.1

4 Metodología

La metodología llevada a cabo para el desarrollo de esta investigación, sigue una serie de fases como se muestra en la figura 1, que incluyen investigación previa de guías, normas y estándares, que permitieron identificar los criterios de seguridad en las aplicaciones Web, posteriormente se eligieron herramientas las cuales se usaron para realizar pruebas de seguridad a los AVA (ver la tabla 3), se establecieron métricas para la evaluación de los criterios asignándoles valores de acuerdo al grado de importancia, se determinaron los pasos para la evaluación de los criterios y los métodos para la evaluación de los AVA, se realizó la evaluación de seguridad a los

AVA Moodle y Dokeos de acuerdo al modelo propuesto, se verificó el nivel de seguridad y finalmente se validó la funcionalidad del modelo.

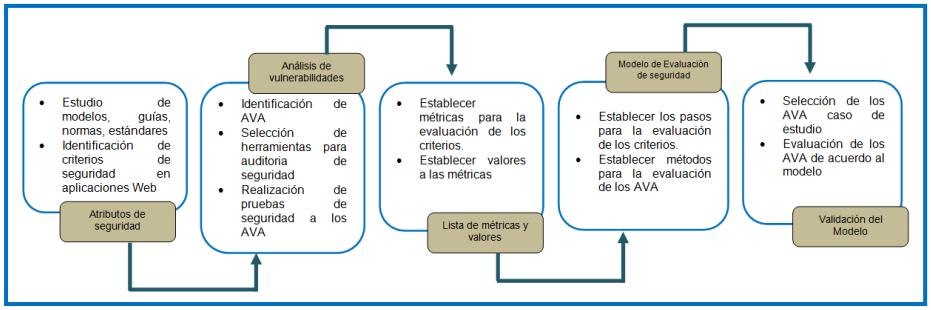

Fig. 1. Diseño metodológico

4.1 Análisis de vulnerabilidades

El proceso de análisis inicia con recolección de información pertinente a los aplicativos Dokeos y Moodle, seguido por las pruebas de seguridad y análisis de resultados.

El tipo de análisis de seguridad llevado a cabo fue el de pruebas de penetración (Penetration test) [14] [15], también denominado test de intrusión, cuyo propósito es detectar los puntos débiles, buscando explotar las vulnerabilidades de seguridad con el fin de quebrantar la integridad, confidencialidad y disponibilidad de la información.

Una vez aplicadas las pruebas de seguridad a estas plataformas virtuales, se presentaron los siguientes resultados como se muestra en la tabla 4.

Se realizó el análisis de vulnerabilidades a los AVA Moodle y Dokeos utilizando las herramientas SQLMap, W3AF y OWASP ZAP, generando resultados en los cuales la herramienta W3AF presentó falsos positivos como vulnerabilidades CSRF y click_jacking los cuales fueron inspeccionados manualmente; W3AF encontró vulnerabilidades de fuga de información sensible como rutas absolutas y configuraciones por defecto. OWASP ZAP, no reportó ningún falso positivo y logró también encontrar vulnerabilidades de fuga de información sensible como listado de directorios y errores en la gestión de las cookies, ya que Moodle ni Dokeos declaraba la directiva HttpOnly, la cual le indica al navegador que esa cookie no debe poder accederse directamente, esto puede permitir que un atacante pueda robar la sesión de un usuario, en el peor de los casos un administrador del sistema. SQLMap no reportó vulnerabilidades del tipo inyección de SQL, ni XSS, como se aprecia en la tabla 4.

Tabla 4. Vulnerabilidades identificadas en las plataformas Moodle y Dokeos

AVA	Total	Code execution	SQL injection	XSS	Bypass something	Gain information	CSRF	File inclusion	Flow control
Moodle	3	0	0	0	0	3	0	0	0
Dokeos	5	0	0	0	0	5	0	0	0

Es importante aclarar que para realizar esta comparación se tuvieron en cuenta diferentes criterios con el propósito de reducir la subjetividad de la evaluación, ya que los datos que se encuentran en la tabla pertenecen a vulnerabilidades verificadas bajo inspecciones manuales, por lo que no aparecen falsos positivos generados en las pruebas realizadas.

4.2 Diseño del modelo de evaluación de seguridad

El modelo de seguridad propuesto se basó en los criterios más relevantes en cuanto a normas y estándares de seguridad junto con la especificación de métricas de evaluación, las cuales permiten medir la seguridad de los AVA Moodle y Dokeos.

Los criterios definidos son: confidencialidad (C), integridad (I) y disponibilidad (D) de la información, y las métricas establecidas fueron resultado de guías de seguridad OWASP [18], como se presentan en la figura 2:

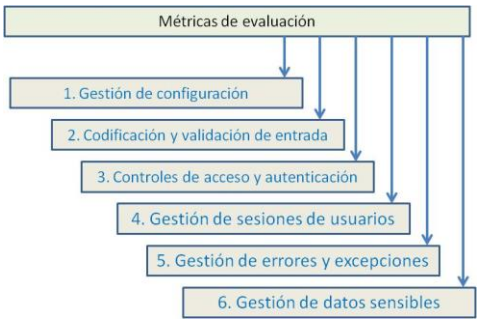

Fig 2. Métricas de evaluación de seguridad

Después de establecidas las seis (6) métricas para la evaluación junto con los criterios generales de seguridad (Integridad, Confidencialidad y Disponibilidad), fue necesario establecer valores con el fin de cuantificar dichos criterios y de esta manera tener como resultado final el nivel de seguridad de los AVA Moodle y Dokeos.

Para cuantificar la evaluación de la seguridad de la información, se definió que cada una de las seis métricas tendría una ponderación distinta como se muestra en la tabla 5. Estas ponderaciones asignadas a las métricas se especificaron de acuerdo al

impacto que tenía cada una en el negocio y este fue calculado con base en los valores de explotabilidad, prevalencia y detección de una posible vulnerabilidad.

Tabla 5. Tabla de ponderaciones a cada métrica

Métrica	**Ponderación**	**Valor individual máximo para sus criterios**	**Valor de acuerdo a OWASP**
Métrica de gestión de configuraciones	14%	14	0 - 14
Métrica de gestión de codificación y validación de entrada	25%	25	0 - 25
Métrica de gestión de control de acceso y autenticación	16%	16	0 - 16
Métrica de gestión de sesiones y usuario	16%	16	0 - 16
Métrica de gestión de errores y excepciones	6%	6	0 - 6
Métrica de gestión de datos sensibles	23%	23	0 - 23

La evaluación general de seguridad se obtiene de acuerdo a una escala de valores (ver tabla 6) con el fin de indicar diferentes niveles de seguridad en que puede estar una aplicación (AVA), así un valor cuantitativo en el rango (0 a 20), significa que el valor total de la evaluación de la aplicación se encuentra en un nivel cualitativo "bajo", de esta manera el Agente Evaluador (AE) puede tomar las decisiones respectivas para llevar a cabo un plan de mejoramiento o emitir un juicio de valor sobre las posibles fallas del sistema.

Tabla 6. Valores cualitativos y cuantitativos

Valor Cualitativo	Valor Cuantitativo
Bajo	0 – 20
Medio-Bajo	21 – 40
Medio	41 – 60
Medio-Alto	61 – 80
Alto	81 – 100

Cada métrica contiene una serie de preguntas a evaluar que se relacionan con los criterios de integridad (I), confidencialidad (C) y disponibilidad (D) como se muestra en el ejemplo de la siguiente tabla:

Tabla 7. Métrica de gestión de configuraciones.

Nº	Pregunta	I.	C.	D.	Valoración total
1.	¿Tiene algún software sin actualizar? Esto incluye el SO, Servidor Web/Aplicación, DBMS, aplicaciones, y todas las librerías de código.	8	4	8	20
2.	¿Están habilitadas o instaladas alguna característica innecesaria (p. ej. puertos, servicios, paginas, cuentas, privilegios)?	2	2	2	6
3.	¿Están las cuentas por defecto y sus contraseñas aun habilitadas y sin cambiar?	2	6	2	10
4.	¿Carece de configuraciones de seguridad en su framework de desarrollo (p. ej. Struts, Spring, ASP.NET)?	2	2	2	6
Total:		14	14	14	∑=42/3 = 14

Una vez elaboradas las demás métricas, estas son aplicadas para evaluar la seguridad de los AVA, cada pregunta se responde de manera afirmativa o negativa (SI/NO), dando como resultado final el nivel de seguridad de los AVA como se presenta en las figuras 3 y 4.

Establecidas las métricas y criterios para la evaluación de la seguridad de los AVA, se procede a definir cada uno de los pasos que ha de tener en cuenta el Agente Evaluador (AE) para realizar la evaluación de la seguridad.

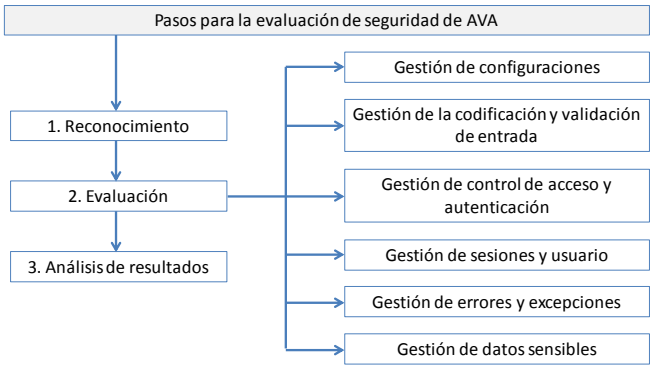

Fig 3. Pasos para la evaluación de seguridad

Etapa de reconocimiento. El primer paso es la etapa de reconocimiento, esta busca que el AE, logre conocer más acerca de los detalles y configuración técnica del AVA, y de las tecnologías que utiliza para que la evaluación sea más objetiva.

En este paso se requiere documentar la información técnica relativa al AVA tal como: versión del servidor Web, versión del sistema operativo, versión y arquitectura del AVA.

Etapa de evaluación. El segundo paso se refiere al proceso de evaluación de cada una de las métricas definidas, este se divide a su vez en seis (6) pasos diferentes, uno por cada métrica.

Los pasos para la evaluación de métricas se dividen en dos etapas cada uno, así:

Etapa de pruebas: En esta etapa se hacen inspecciones manuales o automatizadas que buscan recaudar la mayor cantidad de información posible y de esta manera contar con criterios base para responder a cada una de las preguntas planteadas.

Etapa de valoración de métricas: se responde cada una de las preguntas y el modelo implementado en Excel presenta resultados cuantitativos para su posterior análisis.

En esta etapa se plasma en la plantilla de evaluación el resultado de las pruebas, por medio de la respuesta a las preguntas de la métrica que se está evaluando.

Etapa de análisis de resultados. El tercer paso es el análisis de resultados, en este se analizan cada uno de los resultados de la evaluación de métricas, para poder cuantificar y calificar los criterios generales e individuales de seguridad, por ultimo basados en esto se dictamina el nivel de seguridad general que posee el AVA, con el fin de plantear estrategias de mejoramiento para esta característica de calidad de software (Seguridad).

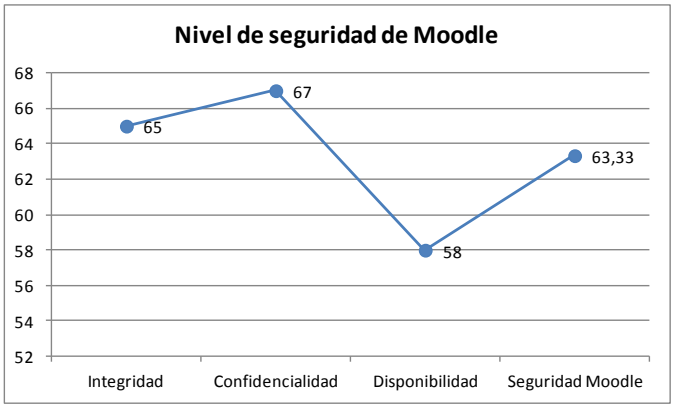

Fig 3. Resultado final de la seguridad de Moodle

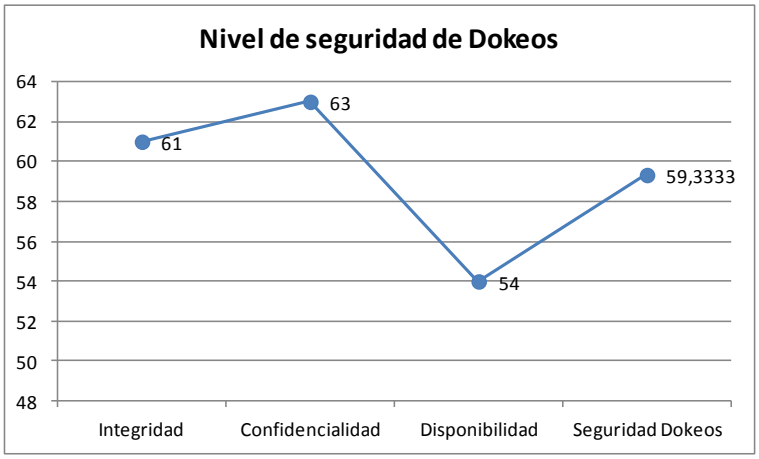

Fig. 4. Resultado final de la seguridad de Dokeos

Resultado general de la seguridad de Moodle y Dokeos aplicando el modelo de evaluación.

Tabla 8. Comparación de resultados de evaluación de seguridad de los AVA

Métricas de evaluación	**Valores en Moodle**	**Valores en Dokeos**
Pruebas para la gestión de la configuración	-2.66	-2.66
Pruebas para la codificación y validación de entrada	25	25
Pruebas de controles de acceso y autenticación	2	2
Prueba de gestión de sesiones y de usuarios	16	12
Prueba de gestión de errores y excepciones	6	6
Prueba de gestión de datos sensibles	17	17
Valor total:	63.33	59.33

Los resultados de evaluación de seguridad a los AVA Moodle y Dokeos con el modelo propuesto ha permitido establecer un valor cuantitativo y cualitativo del nivel de seguridad, por ejemplo, Moodle obtuvo una calificación de 63.33 puntos para una escala de nivel MEDIO-ALTO mientras que Dokeos obtuvo un valor de 59,33 puntos y su escala fue nivel MEDIO.

De acuerdo a lo anterior, los AVA Moodle y Dokeos obtuvieron un valor negativo en la métrica de "Gestión de la configuración", debido a que estas pruebas se han hecho con versiones antiguas, por tanto, esto afecta los valores generales de seguridad. En el caso de la métrica de Gestión de controles de acceso y autenticación los dos aplicativos se presentaron débiles en evitar ataques de fuerza bruta a sus mecanismos de autenticación, al igual que ninguno logró verificar la autenticidad de

las peticiones en sitios cruzados.

Haciendo la comparación de seguridad entre Moodle y Dokeos, se observa que ambas plataformas toman medidas en la gestión y codificación de entradas, que es un pilar de vital importancia para mantener el nivel de seguridad de las plataformas y aunque el aplicativo Dokeos obtuvo un valor inferior a Moodle en la métrica de Gestión de controles de acceso y autenticación, mantiene un nivel de seguridad confiable para su implementación en entornos de producción.

El modelo es útil para medir el estado de seguridad de una aplicación web de manera modular, permitiendo saber cuáles son los eslabones débiles del aplicativo (configuraciones, codificación y validación de entradas, etc.), de esta manera se puede analizar el costo beneficio al ejecutar medidas que mitiguen posibles riesgos de seguridad, es decir, teniendo en cuenta el análisis de seguridad de Moodle y Dokeos, se encuentra que los dos aplicativos son seguros y que requieren medidas para mitigar los riesgos en cuanto a sus configuraciones, controles de acceso y autenticación, lo que implica que el costo sea equitativo para ambos, la decisión de cual implementar en una entidad viene siendo condicionada por el que haya tenido el valor de seguridad más alto.

4 Conclusiones

El proceso de evaluación de seguridad permite establecer el grado de confiabilidad en los AVA evaluados mediante un estudio exhaustivo de criterios previamente analizados y cuyos resultados pueden convertirse en el insumo de apoyo a la toma de decisiones en entidades educativas interesadas en adquirir un AVA como recurso de apoyo para docentes e instructores.

Los chequeos eficaces por parte de las plataformas para comprobar la seguridad de las mismas, es una característica que se debería implementar en futuras versiones en estas plataformas. Adicionalmente los equipos de soporte y mantenimiento de Moodle y Dokeos deberían fortalecer sus herramientas de colaboración para poder conocer más rápidamente sus actualizaciones, buscando reducir las potenciales intrusiones o afectaciones de estas aplicaciones.

Aunque existen diversas guías, normas y estándares relacionados con la seguridad informática y de la información, a nivel general, es poco lo que existe respecto a normas de seguridad en aplicaciones Web, sin embargo, el proyecto OWASP es uno los más dedicados al estudio y prevención de las vulnerabilidades más relevantes descritas en el ranking top 10 del mismo, permitiendo que tanto arquitectos, desarrolladores y administradores de software y de redes estén a la expectativa para mejorar y aplicar buenas prácticas en la seguridad de los activos.

Los AVA Moodle y Dokeos fueron el fundamento de la investigación abordada, se aplicó el modelo de evaluación para identificar y comparar el nivel de seguridad en que se encuentran, así mismo evaluar el modelo establecido con el fin de verificar la consistencia del mismo.

Las métricas son un recurso útil al momento de medir y evaluar el aspecto de seguridad de un AVA, proporcionando una estimación del nivel de seguridad en que se encuentra, de tal forma que se pueda tomar decisiones oportunas con el fin de mantener la integridad, confidencialidad y disponibilidad de la información.

El proceso de validación del modelo permitió llevar a cabo una revisión cuidadosa de los criterios establecidos, ya que al momento de elaborarlo se pensó en la facilidad de uso, en la obtención de resultados propicios que ayuden al evaluador a la toma de decisiones que contribuyan al mejoramiento y protección de los activos de la organización, mitigando los riesgos de vulnerabilidad al que están expuestos los datos.

La propuesta del Modelo de evaluación de seguridad para Ambientes Virtuales de Aprendizaje (AVA), puede servir como referencia para el diseño y construcción de nuevos estudios en otros tipos de sitios Web, estableciendo diferentes criterios de seguridad y valores según el contexto de estudio sobre el cual se realice.

En el proceso de investigación se evidencia que gran parte de la responsabilidad y eficacia de las medidas para salvaguardar la seguridad de la información, radica en las tareas de administración del sistema, las configuraciones que se toman a la hora de instalar la plataforma, como la utilización de privilegios adecuados tanto en el sistema de ficheros y la base de datos; estos son factores relevantes a la hora de determinar el nivel de escalabilidad que puede llegar a tener un determinado ataque. Otro pilar fundamental, es la educación y capacitación en términos de seguridad a los usuarios de las plataformas; todas estas medidas juntas, permiten reducir el riesgo de sufrir ataques efectivos, y disminuir potencialmente los daños que pueden llegar a provocar alguno de ellos.

Referencias

1. Carmona, E., Rodríguez, E., 2009. Tecnologías de la información y la comunicación: ambientes web para la calidad educativa. Armenia: Ediciones Elizcom. http://books.google.com.co/books?id=TvPnYMT79FcC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
2. Escalona, P., Rodríguez, F., Concepción, R., 2008. El Moodle, una plataforma de apoyo al aprendizaje colaborativo en la Educación Superior Cubana: una experiencia en la Universidad de Holguín. En: 5º Congreso Internacional de la Educación Superior. Memorias. Cuba: Palacio de las Convenciones.
3. Pérez, M. et al., 2009. Innovación en docencia universitaria con moodle: casos prácticos. Alicante, España: Club Universitario. http://www.editorial-club-universitario.es/pdf/3333.pdf

4. Ávila, R., García, R., Barba, M., 2010. MOODLE y su integración a sistemas avanzados de intercomunicación basado en tecnologías Web 2.0. En: Memorias del programa científico Universidad 2010. Cuba: Editorial Universitaria.
5. Sierra, J., et al., 2011. Uso de estándares aplicados a TIC en educación. España: Ministerio de Educación.
6. Benítez, M., Barajas, J. 2010. Sistema de administración de contenidos para apoyar el desarrollo del modelo curricular de la Facultad de Contaduría y Administración de la Universidad Autónoma de San Luis Potosí, México. En: Distance Learning. 2010. vol. 7, no. 4, p. 1-9.
7. Sánchez, I., 2011. Plataforma educativa Moodle: administración y gestión. México: Alfaomega.
8. Sánchez, S., Sicilia, M., Rodriguez, D., 2011. Ingeniería del Software. Un enfoque desde la guía SWEBOK. ISBN: 978-84-9281-240-0 IBERGACETA PUBLICACIONES, S.L., Madrid. Primera edición, 568 p.
9. Norma ISO 27001. 27001 Academy. (s.f.). https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
10. Gómez, L., Andrés, A., 2012. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: AENOR - Asociación Española de Normalización y Certificación. ProQuest ebrary.
11. López, A., 2014. OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Owasp_4
12. Romero, A., 2011. Aspectos básicos de la seguridad en aplicaciones Web. México: Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx/documento/?id=17
13. Cano, J., 2013. Inseguridad de la información: una visión estratégica. México: Alfaomega. http://site.ebrary.com/lib/bibliojdcsp/docDetail.action?docID=10757910&p00=seguridad+inform%C3%A1tica
14. Sallis, E., Caracciolo, C., Rodríguez, M., 2010. Ethical hacking. Un enfoque metodológico para profesionales. Buenos Aires. Primera edición, Alfaomega grupo editor, 135 p.
15. Agé, M., Baudru, S., Crocfer, N., 2011. Seguridad informática: ethical hacking: conocer el ataque para una mejor defesa. Ediciones ENI. Disponible en: https://books.google.es/books?id=Caw7Ipl19KIC&printsec=frontcover#v=onepage&q&f=true