ESCUELA DE INGENIERÍAS

Tema:

CIBERSEGURIDAD EN UNA PLATAFORMA EDUCATIVA A TRAVÉS DE HERRAMIENTAS ESPECIALIZADAS

Proyecto de investigación previo a la obtención del título de Ingeniero en Sistemas de la Información

Líneas de investigación:

SISTEMAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor:

John Israel Balseca Tagua

Directora:

Mg. Liliana del Rocío Mena Hernández

Ambato – Ecuador

Agosto 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JOHN ISRAEL BALSECA TAGUA**, con cedula de identidad **1805376207**, autor del trabajo de graduación titulado: "CIBERSEGURIDAD EN UNA PLATAFORMA EDUCATIVA A TRAVÉS DE HERRAMIENTAS ESPECIALIZADAS", previa a la obtención del título profesional de **INGENIERO EN SISTEMAS DE INFORMACIÓN**, en la escuela **de INGENIERÍAS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, agosto 2024

John Israel Balseca Tagua

CC. 1805376207

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

CIBERSEGURIDAD EN UNA PLATAFORMA EDUCATIVA A TRAVÉS DE HERRAMIENTAS ESPECIALIZADAS

Líneas de investigación:

SISTEMAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor:

John Israel Balseca Tagua

Liliana del Rocío Mena Hernández, Ing. Mg. f._____
CC. 1802729077
CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____
CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____
CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____
DIRECTOR ESCUELA DE INGENIERÍAS

Ana Cecilia Parra Ramos, Ab. Mg. f._____
SECRETARIA GENERAL PUCESA (S)

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Agosto 2024

DEDICATORIA

Quiero agradecer totalmente a mis padres que siempre estuvieron en las buenas y las malas, que me supieron apoyar en los momentos difíciles cuando todo parecía acabar y no poder finalizar la carrera ellos estuvieron presentes, me supieron decir con palabras lo que mi corazón sentía. A mi hermana que estuvo presente desde que empecé la carrera de sistemas de información fue justo el nacimiento de ella y desde ese entonces ella ha sido mi apoyo en mis noches y me ha hecho seguir adelante porque tengo ganas de darle el mundo entero a ella y a mis padres.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a todas las personas e instituciones que hicieron posible esta tesis. En primer lugar, agradezco de todo corazón a mi directora de tesis, la Mg. Liliana Mena, por su orientación, paciencia y apoyo constante a lo largo de todo el proceso. Su conocimiento y experiencia fueron esenciales para el desarrollo de este trabajo.

También agradezco a la institución educativa que participo en este estudio, proporcionando los datos necesarios para el análisis y facilitando el acceso a su plataforma educativa. A mis padres, por su amor, comprensión y sacrificios, y a mi hermana, por darme su apoyo emocional y animo en los momentos difíciles. Sin ustedes, este logro no habría sido posible. Por último, gracias a mis amigos por su constante ánimo y por creer en mí. Su apoyo incondicional me ha impulsado a superar este reto para que un futuro ser un gran profesional. A todos ustedes, mi más sincero agradecimiento.

RESUMEN

Antes de la llegada del COVID-19, el uso de plataformas educativas era escaso, lo que dejó al descubierto importantes brechas durante la transición a la educación en línea. La pandemia enfatizó la necesidad de plataformas seguras para gestionar la asistencia, las calificaciones y los exámenes, asegurando la continuidad del aprendizaje. Este proyecto tiene como objetivo evaluar los niveles de seguridad en una plataforma educativa para garantizar un entorno seguro. La metodología utilizada se basa en OWASP (*Open Web Aplicación Security Project*), empleando herramientas como OWASP ZAP, *Nikto, Uniscan, Qualys, HostedScan Security, Observatory, Security Headers Powered by Probely e ImmuniWeb* para detectar vulnerabilidades. Evaluar la seguridad de estas plataformas es esencial para proteger la información y reducir las interrupciones educativas

Los resultados identificaron varias vulnerabilidades, tales como la falta de protecciones contra CSRF (*Cross-site request forgery)*, configuraciones de seguridad incorrectas, inyección SQL (*Structured Query Language*), errores en los cifrados TLS (*Transport Layer Security*) y políticas de seguridad inadecuadas. También se observó la ausencia de encabezados de seguridad y configuraciones deficientes de subdominios. Se recomienda implementar configuraciones de seguridad adecuadas y mantener actualizados los sistemas y aplicaciones. La metodología OWASP demuestra ser efectiva para identificar amenazas y ofrecer una base para mejorar la seguridad de las plataformas educativas, asegurando un entorno educativo seguro y continuo.

Palabras clave: ciberseguridad, herramientas especializadas, plataformas educativas, OWASP, vulnerabilidades.

ABSTRACT

Before the arrival of COVID-19, the use of educational platforms was limited, which revealed significant gaps during the transition to online education. The pandemic highlighted the need for secure platforms to manage attendance, grades, and exams, ensuring continuity in learning. This project aims to assess the security levels of an educational platform to guarantee a safe environment. The methodology used is based on OWASP (Open Web Application Security Project), employing tools such as OWASP ZAP, Nikto, Uniscan, Qualys, HostedScan Security, Observatory, Security Headers Powered by Probely, and ImmuniWeb to detect vulnerabilities. Evaluating the security of these platforms is essential to protect information and reduce educational disruptions.

The results identified several vulnerabilities, such as the lack of protections against CSRF (Cross-Site Request Forgery), incorrect security configurations, SQL injection (Structured Query Language), errors in TLS (Transport Layer Security) encryption, and inadequate security policies. There was also a noted absence of security headers and poor subdomain configurations. Recommendations include the implementation of appropriate security configurations and maintaining updated systems and applications. The OWASP methodology proves effective in identifying threats and provides a foundation for improving the security of educational platforms, ensuring a safe and continuous educational environment.

Keywords: *cybersecurity, specialized tools, educational platforms, OWASP, vulnerabilities.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

INTRODUCCIÓN

Antes de la irrupción del COVID-19, el uso regular de plataformas educativas en las instituciones era limitado, lo que llevo a conocer varias brechas durante la transición hacia la educación en línea. Además, la seguridad de estas plataformas era motivo de preocupación debido a su falta de protección adecuada. Sin embargo, la necesidad de contar con una plataforma educativa es fundamental en la actualidad. La gestión de asistencias, calificaciones, exámenes y la calidad de aprendizaje se vio afectada a raíz de la pandemia, y las plataformas educativas ofrecen una solución. Es crucial evaluar los niveles de seguridad en una Plataforma Educativa para garantizar un entorno educativo seguro. Esto asegura que las interrupciones en la educación presencial puedan minimizarse, facilitando la continuidad del aprendizaje y promoviendo la colaboración entre estudiantes y profesores. Además, estimula la interacción y el intercambio de conocimientos a través de foros, chats y otras herramientas de comunicación en línea, esto ayuda a promover la conciencia de la seguridad en las plataformas.

Las herramientas digitales como las plataformas en línea según Martínez (2021) ayudan a las instituciones educativas a proporcionar recursos de aprendizaje adicionales y de enseñanza, mundialmente la educación se sometió a cambios tecnológicos, lo que ha llevado a la necesidad de impartir conocimientos y valores a través de métodos alternativos a los tradicionales, como las aulas virtuales.

En la actualidad, la **necesidad** de contar con una plataforma educativa es esencial. Las plataformas educativas brindan soluciones a la gestión de asistencia, calificaciones, exámenes y calidad de aprendizaje, acciones que se vio afectada a raíz de la pandemia. Para garantizar un entorno educativo seguro, es fundamental evaluar los niveles de seguridad de una plataforma educativa. Esto minimiza las interrupciones en la educación presencial, facilita la continuidad del aprendizaje y fomenta la colaboración entre estudiantes y docentes. Además, fomenta la interacción y el intercambio de conocimientos a través de foros, chats y otras herramientas de comunicación en línea, lo que ayuda a aumentar la conciencia sobre la seguridad en las plataformas.

Lo primero hoy en día como usuarios activos es seguridad, pero ya no solo seguridad al momento de salir a la calle o al momento de entrar al mundo de internet y a ello se le llama ciberseguridad, ¿pero que es la ciberseguridad?

En un contexto para organizaciones y empresas de acuerdo con Aguilar (2011) su punto de vista es la idea tradicional del puesto de trabajo está cambiando por completo. Los empleados utilizan computadoras portátiles que llevan a casa para escribir, ver la prensa o consultar sitios web relacionados con su trabajo, y una gran cantidad de empresas consultadas reconocen que sus empleados han dado acceso no autorizado a familiares o amigos. Además, la mayoría de las empresas no renuncian a acceder a las redes sociales desde su lugar de trabajo. Entonces es justo la zona en donde entra el cibercrimen es un negocio puro y duro, y los cibercriminales están aprovechando las innovaciones tecnológicas para agilizar sus propias operaciones y obtener rentabilidad.

Y como actualmente dentro del mundo del internet ya nada es completamente seguro, conforme a García (2023) las plataformas son blancos vulnerables a una variedad de amenazas de seguridad y representan una oportunidad para ciberataques como el robo de identidad, el ciber fraude, la extracción de datos o el daño a los sistemas informáticos. Por esta razón, se debe aumentar la conciencia sobre la importancia de la seguridad y protección de la privacidad en las plataformas de aprendizaje electrónico, asegurándose de que la información almacenada, compartida y generada sea segura.

En este contexto, la **importancia** de este proyecto es crucial porque ayuda a proporcionar a la institución una muestra de las vulnerabilidades de la plataforma educativa y los riesgos asociados con los ataques, evalúo los niveles de seguridad de la plataforma y creo un entorno educativo seguro. Estas herramientas aumentarán la seguridad de la plataforma de alta calidad y podrá brindar a los estudiantes un ambiente educativo más seguro.

La seguridad tiene una variedad de facetas en palabras de Aguirre (2018) hay muchas maneras de exponer las vulnerabilidades en las aplicaciones web, como

se indica en OWASP sobre una mala configuración de seguridad. Las técnicas OWASP ayudan a reducir los riesgos de privacidad al determinar si las pruebas de penetración son efectivas al encontrar vulnerabilidades en el estado de seguridad de las aplicaciones web.

Los responsables del tratamiento de datos personales están obligados, según la nueva Ley Orgánica de Protección de Datos Personales, a implementar todas las medidas de seguridad necesarias como indica Carvaca (2022) podrá ayudar en sus páginas web o aplicaciones para proteger los datos personales de cualquier peligro, amenaza o vulnerabilidad. Esto se puede hacer adoptando estándares, mejores prácticas, códigos de protección o cualquier otro mecanismo que se considere adecuado para el tratamiento de datos.

Por lo tanto, se considera que la realización de un análisis de seguridad OWASP ayudará a las organizaciones a tener una evaluación real de la seguridad de sus sitios web y a tomar medidas correctivas para prevenir incidentes de seguridad y pérdidas importantes de datos.

Además de las vulnerabilidades, el análisis de seguridad incluye una variedad de programas o sistemas que ayudan a prevenir ataques, tal como señala Carvaca (2022) ayudo a la institución a tener una evaluación real sobre la seguridad de la información web y poder ejecutar acciones correctivas que eviten sufrir incidentes de seguridad y pérdidas de información crítica como valorar los riesgos de seguridad encontrados para priorizarlos según su criticidad.

El análisis de riesgos, las pruebas de seguridad y la gestión de dependencias de los componentes principales de la **metodología** OWASP, que proporciona pautas prácticas para integrar la seguridad en todas las fases del ciclo de vida del desarrollo de software. El **resultado** esperado de la metodología OWASP es una evaluación de vulnerabilidades para mejorar la seguridad de una plataforma educativa y lograr prevenir posibles ataques y vulnerabilidades.

Objetivo general.

- Evaluar los niveles de Seguridad en una Plataforma Educativa que garantice un entorno educativo seguro

Objetivos específicos

1. Fundamentar teóricamente aspectos de ciberseguridad en una plataforma educativa a través de herramientas especializadas.
2. Diagnosticar las fases de la metodología aplicable para la evaluación del nivel de seguridad de una plataforma educativa.
3. Analizar mediante herramientas especializadas las vulnerabilidades en una plataforma educativa para recomendar aspectos de seguridad en sitios de educación.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Ciberseguridad: la protección de datos y seguridad digital

La ciberseguridad de acuerdo con Yagual (2022) es un conjunto de procesos y tecnologías que se utilizan para proteger computadoras, redes, programas y datos de actividades maliciosas, ataques, daños o acceso no autorizado, las soluciones de seguridad convencionales conocidas, como antivirus, firewall, autenticación de usuarios, cifrado, y más, ya no pueden ser efectivas de acuerdo con las numerosas necesidades actuales. Por consiguiente, es útil estar al tanto de las tendencias y avances en ciberseguridad, así como de cómo están mejorando con el tiempo, además, es ventajoso tener un enfoque proactivo y estratégico para garantizar la protección de sistemas y datos en un entorno digital en constante evolución.

Para conocer mejor la ciberseguridad basado en Ortega (2021) resulta útil considerar tres conceptos clave utilizados para guiar las políticas de seguridad de la información que son la confidencialidad (protección contra el acceso no autorizado), la integridad (protección contra modificaciones no autorizadas) y la disponibilidad de activos (protección contra interrupciones en el acceso a la información) son varios de los elementos esenciales para mantener un sistema seguro para de esta manera, mejorar la protección de nuestros datos aplicando estos conceptos correctamente.

Como comprender las expresiones de una falta de ciberseguridad a decir de Giant (2016) es fácil ver lo importante a considerar el acceso de los niños a la tecnología debido a sus limitaciones cognitivas para comprender plenamente los riesgos futuros como potencialmente peligrosas, no se pueden sorprender con tener pruebas de una falta de ciberseguridad así como pueden pasar en personas adultas, y poder conocer que la falta de seguridad cibernética es un problema común. De esta manera el problema de ciberseguridad y de donde se origina los ataques es un problema que afecta a todas las edades.

Las nuevas amenazas que conlleva la ciberseguridad como afirma García (2019) se enfocan en la protección efectiva de la información en el ciberespacio, especialmente en temas de continuidad, disponibilidad, robo, fuga, falseamiento o modificación, un gran porcentaje de sus ataques se dirigen no solo a las instituciones gubernamentales, sino también al sistema financiero, y ahora con más facilidad a los individuos que son un objeto atractivo. Por lo tanto, conocer de estas amenazas es muy importante para tomar medidas que protejan nuestra información y con ello poder reducir los riesgos en un entorno digital en constante evolución.

Desventajas al aplicar la ciberseguridad con el surgimiento de IA (inteligencia Artificial) según lo indicado por Rubio (2021) el sistema IA ofrece información automatizada mediante el análisis de grandes volúmenes de datos y el descubrimiento de patrones, esto mismo es utilizado por los ciberdelincuentes para un beneficio indebido sabiendo que son capaces de adaptarse y acceder a los datos de empresas. Por lo tanto, se debe desarrollar Inteligencia Artificial de alta calidad para evitar que los ciberdelincuentes se aprovechen del sistema y poder para reducir grandes números de ataques.

Ventajas al aplicar la ciberseguridad con el surgimiento de IA ha permitido que los profesionales de la ciberseguridad realicen tareas más complicadas, como administrar la gran cantidad de datos generados por las industrias según indicado por Guillermo (2021) que los analistas pueden identificar puntos de amenaza a través de la información recopilada por tecnologías de IA como el aprendizaje automático y el procesamiento del lenguaje natural. Por lo tanto, la incorporación de la inteligencia artificial en la seguridad cibernética ayuda a crear un entorno digital más seguro y protegido al mismo tiempo que frena los avances en la defensa contra las amenazas cibernéticas que están aumentando.

Llegado aquí es importante saber que ningún sistema es seguro, pero la gente siempre hará el intento por estar protegida. Con el paso del tiempo, se observa cómo Internet ha cambiado nuestra forma de ver y percibir el mundo, afirmando que las sociedades modernas no tienen en cuenta las múltiples ventajas de internet en ello se logra visualizar que niños, niñas y adolescentes son nativos digitales

porque su mundo está completamente conectado a internet desde que nacieron, sin embargo no tienen en cuenta sobre como comparten los datos ya sea en redes sociales o páginas web y la conciencia del riesgo y el peligro en su mayoría solo advierten del entorno digital sus bondades y no sus peligros y consecuencias. Este es un punto en contra, la juventud puede compartir información de su vivienda sin el darse cuenta de que tan arriesgado es.

La protección de datos según lo expuesto por Vivar (2022) se refiere al derecho de las personas a saber que los datos se han recopilado, guardado y procesado para corregir cualquier error, mientras que las personas tienen obligaciones legales y éticas con respecto a compartirlos, estos ya pueden ser registros o información que, por sí solas o en conjunto con otros datos, pueden revelar la identidad de una persona viva se denominan datos personales, estos son datos delicados como la ascendencia racial, las creencias religiosas, los grupos sindicales a los que pertenece, su salud física y mental, su orientación sexual, la participación en delitos, entre otros. De esta manera se toma en cuenta la facilidad de ser atacados con un poco de información.

El consentimiento como sostiene Pérez (2015) determina en particular el momento en que se recopilan los datos, una vez completada esta acción se espera que el siguiente paso sea el tratamiento en sí, que ya está autorizado por haber sido consentido mediante la entrega de los datos, aunque la ley admite excepciones a esta posibilidad. Además, el término tratamiento se refiere a la comprensión de todas las operaciones que pueden ocurrir con los datos.

Al entender de protección de datos, uno de los problemas más importantes es cuando se ingresa en sitios web y acepta los términos y condiciones sin saber lo que está aceptando junto con el consentimiento, como menciona León (2021) que es una manifestación de voluntad que debe solicitarse para obtener una respuesta, no capturada que da a entender que de nada sirve gastar energías, esfuerzos creativos y tecnológicos para capturar consentimientos que no son saludables y no servirán para justificar los tratamientos que se pretenden llevar a cabo. Por lo tanto, la persona que recibe el pedido de consentimiento está informada, lo que le permite

ejercer sus derechos frente al futuro responsable del tratamiento de sus datos.

En el ámbito profesional a juicio de Balaguer (2020) los avances tecnológicos han dado un cambio radical, han dado lugar a cambios en los procesos productivos y en la forma en que las empresas organizan su trabajo, así como a la elección de nuevas formas y técnicas de supervisión de la actividad laboral. Sin embargo, en ocasiones, estos métodos pueden chocar con los derechos fundamentales de los trabajadores, como el derecho a la protección de datos y el derecho a la intimidad. De esta manera la Ley de Protección de Datos actual regula cómo las empresas controlan y acceden a los dispositivos digitales de sus empleados.

La digitalización, un fenómeno económico y social, ha puesto a las empresas y a los usuarios en un entorno cada vez más complejo en palabras de García (2022) confuso y con un mayor peligro ante los diversos retos y desafíos. Contar con estrategias para diferentes situaciones puede ser lo que marque la diferencia entre abordar un problema con la mayor brevedad posible o que la empresa desaparezca. Por lo tanto, el desarrollo de las empresas debe estar relacionado con el aumento de la ciberseguridad y la protección de datos de carácter personal, debido a la creciente exposición al exterior.

La seguridad cibernética hoy en día es un componente vital para proteger la privacidad y la información en línea, en un mundo interconectado donde la tecnología se encuentra presente en todos los aspectos de nuestras vidas, esta es esencial para la protección contra una variedad de amenazas cibernéticas, que van desde el robo de datos hasta el espionaje digital y el sabotaje informático.

1.2. Plataformas educativas: explorando la seguridad virtual

Las plataformas educativas en un estudio reciente Hernández (2021) son herramientas cruciales que permiten el aprendizaje autónomo y la comunicación que cubren una variedad de enfoques tanto para estudiantes como para maestros, lo que facilita la planificación y evaluación, aunque son importantes, no deben reemplazar por completo la educación presencial porque permiten la transmisión

de emociones y un entorno positivo que ayuda al desarrollo del alumno, estas plataformas resuelven problemas actuales y ofrecen entornos virtuales para la formación en línea, sin requerir habilidades de programación avanzadas, lo que las hace accesibles para todos. Este en un punto es beneficio a las plataformas, su uso requiere solo habilidades básicas en informática y tiene menús fáciles de entender.

Como estudiante, es increíble observar cómo las plataformas educativas han cambiado la forma en que se aprende, las herramientas en línea brindan un acceso fácil con variedad de recursos educativos junto con formas muy distintas de aprender.

El uso de las plataformas educativas ha sido muy importante según lo argumentado por Hernández (2021) argumenta que las plataformas son programas que facilitan la organización de cursos en línea, la gestión de matrículas, la comunicación interactiva y la evaluación del progreso de los estudiantes, teniendo en cuenta la situación actual ha provocado una reflexión sobre la rutina y ha enfatizado la importancia de la educación, al mismo tiempo que se enfrentan las barreras geográficas con el uso de la tecnología el Internet se ha vuelto fundamental para satisfacer necesidades básicas y ha cambiado una variedad de servicios, como la educación. Por lo tanto, estas plataformas permiten evaluaciones e impulsan la educación a distancia, mejorando el proceso educativo.

Dentro de las plataformas educativas se cuenta con distintos módulos según Carillo (2021) tres componentes principales componen las plataformas educativas: gestión académica y administrativa, gestión de comunicación y gestión del proceso de enseñanza-aprendizaje, esto permite a los maestros ofrecer actividades que contienen información sobre temas específicos en una variedad de formatos, así como la ayuda de foros y la mensajería electrónica facilitan la colaboración entre estudiantes, incluso los maestros pueden usar rubricas para evaluar las tareas, y los estudiantes pueden autoevaluarse, junto con la asignación de permisos mediante autenticación de usuario y contraseña, con niveles de administrador, profesor y alumno. Tomando en cuenta la cita, mi perspectiva es que mejora la experiencia del aprendizaje al facilitar la organización de los módulos principales.

Dentro de la educación existe tipos principales de plataformas educativas como expone Carillo (2021) son las siguientes: comerciales, de software libre y de propiedad intelectual, comerciales que se actualizan con el tiempo y ofrecen funciones sofisticadas como *Blackboard*, de programa informático libre; como Moodle que ofrecen libertad de personalización, soporte comunitario proporcionadas gratuitamente y por ultimo plataformas propias; creadas por instituciones o grupos de investigación que satisfacen necesidades particulares y no tienen fines comerciales, ofrecen flexibilidad y control total sobre el código fuente y el contenido. Se considera que las plataformas libres garantizan control total sobre el contenido, plataformas comerciales ofrecen estabilidad y plataformas propias reaccionan a factores educativos.

Llegado a esto es importante saber que ante la aparición del COVID-19, los estudiantes de colegio y bachillerato no tenían conocimiento alguno sobre las plataformas educativas, y al ingresar a instituciones de educación superior afrontaron una nueva realidad en el ámbito de calificaciones y entrega de tareas al que ya estaban acostumbrados.

Las plataformas educativas más conocidas tienen dos tipos de accesos según Viñas (2021) se usan frecuente la accesibilidad abierta que permite a los usuarios usar, modificar y distribuir libremente los bienes que han comprado, lo que beneficia a la comunidad y por otro lado, la accesibilidad comercial; más difícil para adaptarse al mercado en línea en constante crecimiento, mejorando la funcionalidad y agregando características variadas para facilitar el aprendizaje y la comunicación. A continuación, se muestran los tipos de características de las plataformas con AA (Acceso Abierto) y AC (Acceso Comercial).

Tabla 1. Plataformas de AA: Características

	Moodle	**A Tutor**	**Claroline**
URL	https://moodle.org/?lang=es	https://atutor.github.io/	https://claroline.net/
autor	Martin Dougiamas	Desarrollado por el Centro de recursos tecnológicos adaptados (*Adaptative Technology Resource Centre*) de la Universidad de Toronto.	Universidad de Louvain, Instituto de Pedagogía y Multimedia.
País de origen	Australia	Canadá	Francia
Idioma	120	51	35
Accesibilidad	Posee etiquetas en todas las imágenes y los datos de las tablas están optimizados para el uso de la plataforma con *screen readers*.	Fue diseñado con la accesibilidad como prioridad. Estándares de accesibilidad WCAG7 1.0 AA. • W3C WCAG 1.0 • W3C WCAG 2.0 • W3C ATAG 2.0 • US Section 508 • Italy Stanca Act • IMS *AccessForAll* 2.0 • ISO/IEC 24751	100% accesible, ha sido adaptada a personas con discapacidad visual
Recursos Multimedia	La plataforma puede incorporar ficheros del tipo que sean, pero es el navegador el que tiene la capacidad de visualizarlos	Posee capacidad para introducir recursos multimedia integrados en las unidades de aprendizaje	La plataforma puede incorporar ficheros del tipo.
Interfaz	El sistema está provisto de diez plantillas de apariencia. Las instituciones pueden	Tanto los estudiantes como los profesores pueden configurar diferentes	La interfaz es funcional, intuitiva y con elementos básicos para una

	insertar sus propias imágenes institucionales, cabeceras y pies de páginas Interfaz simple, características de arrastrar y soltar, y recursos bien documentados.	características de la apariencia de los cursos. Posee una interfaz sin complicación y que además se puede configurar de diversas formas. Por una parte, la interfaz gráfica es distinta para el estudiante y el profesor lo que puede provocar algún error.	eficaz navegación. La plataforma se instala rápidamente y el uso de cualquier navegador web permite manejar las distintas partes del curso y la admisión de usuarios con fluidez.

Fuente: tomado a partir de Viñas (2021)

En síntesis, sobre la información de la tabla, las plataformas ofrecen una amplia gama de características y funcionalidades que pueden adaptarse a una variedad de necesidades educativas e institucionales.

Tabla 2. Plataformas de AC: Características

	Blackboard	**Educativa**	**Saba**
URL	https://www.blackboard.com/	https://www.educativa.com/	https://www.cornerstoneondemand.com/
Autor	Empresa norteamericana dedicada al desarrollo de servicios y tecnologías innovadoras para la educación y/o capacitación.	Empresa e-educativa.	Pertenece a la compañía Saba software, una compañía ubicada en California, Estados Unidos, productora de software.
País de Origen	Washington D. C	Rosario Argentina, y Alcalá de Henares, España.	California (Estados Unidos).
Idioma	El contenido de *Blackboard Open LMS* está disponible	Español regionalizado, inglés, portugués, catalán,	6 idiomas: inglés, español, japonés, francés, alemán.

	únicamente en inglés, finés y español. Los paquetes de idiomas le proporcionan a Blackboard Learn las normas culturales y de idioma adaptadas distintos públicos. Las preferencias del paquete de idiomas se definen en los niveles de sistema, curso u organización, y usuario.	italiano, francés, alemán, ruso, y otros bajo solicitud.	
Accesibilidad	Sí, Ally permite crear los formatos de audio, de braille electrónico. WCAG 2.1 AA. *Blackboard* ayuda a las instituciones a crear un entorno de aprendizaje más inclusivo y mejorar la experiencia de los estudiantes ayudándolos a tomar un control claro del contenido del curso teniendo en cuenta la usabilidad	Sí, posee elementos de accesibilidad.	Aprendizaje accesible, pero no se puede comprobar cómo lo realizan.
Interfaz	La plataforma es bastante intuitiva y amigable para recorrerla.	Es amigable e intuitiva. La interfaz o apariencia puede modificarse.	Se puede personalizar la interfaz del colaborador. La misma se encuentra bien diseñada estéticamente y su robustez dada su experiencia en el mercado.
Recursos Multimedia	*Blackboard Learn* admite los siguientes tipos de archivo multimedia:	Audio/video, imágenes.	Audio/video.

	Audio: AIFF, MP3, MIDI, MP y WMA. Video: ASF, AVI, MOV, MOOV.		

Fuente: tomado a partir de Viñas (2021)

En síntesis, sobre la información de la tabla, las plataformas pueden mejorar significativamente la calidad y la accesibilidad de la educación en diversos contextos, ofreciendo soluciones flexibles y sólidas.

Con respecto a la seguridad virtual, el uso de diversas TIC (Tecnologías de la Información y Comunicación) para apoyar la educación a distancia ha aumentado constantemente en los últimos diez años y ahora es una parte importante de la planificación y diseño de los programas educativos actuales, en un estudio reciente (Santiso, 2016) comenta que la incorporación de nuevos medios de comunicación en las plataformas de educación virtual, como el chat, video digital y los sistemas de voz sobre IP, así como la aparición de nuevas formas de interacción en línea, como las redes sociales y los teléfonos inteligentes, mejora la facilidad de uso para los usuarios, lo que facilita la integración más rápida y efectiva de los procesos educativos a las plataformas virtuales. A la luz de esto la incorporación de estas tecnologías conlleva nuevas amenazas que, si no se detectan, afectaran gravemente.

Es fundamental considerar según Echaiz (2009) la virtualización actual ha evolucionado de su origen como una herramienta de multiplexado a una solución para abordar problemas de seguridad, confiabilidad y gestión. La virtualización tiene efectos positivos y negativos, tanto la virtualización como sus métodos ayudan a solucionar diversos problemas de seguridad, en particular porque las máquinas virtuales funcionan en un solo sistema que puede establecer un sistema seguro multinivel con sistemas virtuales separados en cada nivel. Sin embargo, la virtualización crea oportunidades para nuevas vulnerabilidades que los

mecanismos de seguridad convencionales no están listos para abordar.

1.3. Metodología y herramientas esenciales para la seguridad cibernética: OWASP

Muchas de las entidades ya sean financieras, educativas o médicas como expone Perero (2022) funcionan a través de redes de información dando a entender que a medida la población supera en gran porcentaje el deseo de pasar más tiempo en línea, con el tiempo esto puede tener graves consecuencias para las organizaciones porque el usuario final es su punto más débil. Por lo tanto, la ciberseguridad es un tema que se fomenta en el esfuerzo que establece la responsabilidad de proteger estos sistemas de cualquier mal uso o uso no autorizado.

En Ecuador, el gobierno aún no tiene una mentalidad de ciberseguridad como lo menciona Dávila (2017) y en palabras de Arrillo (2019) , hace referencia a la publicación de un ranking de países, elaborado por la Unión Internacional de Telecomunicaciones (UIT), que clasifica a las naciones según su nivel de preparación en ciberseguridad:

> constan 193 países, cada uno con un rango específico de compromiso para enfrentar posibles ciberataques; y que se basa en cinco pilares básicos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación. [ ] Ecuador se encuentra en el sexto puesto de América Latina y ocupa el puesto 66 en el listado global de los países que formaron parte del estudio…

A diferencia de lo antes mencionado, en las empresas privadas han comenzado a prestar atención al tema de ciberseguridad, identificando prácticas de alto riesgo, un punto en contra es que la mayoría de la sociedad desconoce las amenazas cibernéticas a su alrededor o, a pesar de ser conscientes de ellas, no toma medidas proactivas para mejorar su propia ciberseguridad y por esta razón que es necesario que los programas educativos e informativos nacionales aumenten la conciencia

sobre la seguridad cibernética, enfocándose en la identificación de los peligros y amenazas, aunque el gobierno ecuatoriano no presta atención a la ciberseguridad, las compañías privadas están prestando atención. Tomando en cuenta la cita, la sociedad carece de información y es necesario aumentar la conciencia nacional sobre los peligros cibernéticos y las medidas de seguridad.

El avance tecnológico ha llevado a la aparición de nuevos eventos cibernéticos que amenazan la seguridad de los sistemas y redes, en un estudio reciente Lainez (2023) da a entender que la creación de nuevas herramientas defensivas para enfrentar la pérdida de grandes cantidades de datos, el robo de propiedad intelectual, el robo de identidad y la denegación de servicio se ha convertido en algo habitual así como existe un amplio acceso a estándares de seguridad, herramientas y tecnología, entrenamiento, certificaciones, bases de datos vulnerables, orientación, conjunto de mejores prácticas, catálogos de controles de seguridad e innumerables listas de verificación y recomendaciones de seguridad. A partir de esto, el principal objetivo es identificar las amenazas actuales y aplicar la mejor estrategia de defensa de seguridad sobre la infraestructura.

Dada la inmensidad de herramientas para la búsqueda de vulnerabilidades se encontró OWASP, el objetivo principal según Aguirre (2018) es expandir, comprar y mantener aplicaciones confiables para los dispositivos en los que se ejecutan, también años posteriores se lanzó un top 10, que permite establecer un margen de seguridad en las aplicaciones identificando y destacando los riesgos más importantes que amenazan la seguridad de las organizaciones, estas técnicas ayudan a reducir los riesgos al comparar si las pruebas de penetración son efectivas al encontrar vulnerabilidades en el estado de seguridad de las aplicaciones web de protección de la privacidad en las aplicaciones.

OWASP funciona como una protección contra el programa maligno para nuestros proyectos. Ofrece los recursos y consejos necesarios para proteger nuestras aplicaciones web de los programas maliciosos.

CAPÍTULO II. DISEÑO METODOLOGICO

2.1. Caracterización de la institución educativa

En el segundo capítulo de Diseño Metodológico, se discuten dos metodologías principales: la de investigación, que utiliza un enfoque cualitativo, y, la de desarrollo la metodología que utiliza el modelo OWASP o en español proyecto abierto de seguridad de aplicaciones web, así como también se realizan las fases de la metodología de creación de documentación para comprobar los varios factores que se va a investigar.

Para la descripción de la institución se toma como referencia la documentación recogida mediante la página web de la institución, en donde se menciona que: El Centro Educativo Integral Suizo fue establecido el 04 de agosto de 2003 por el Ministerio 002-DP-DPET-2003, CE, con una oferta educativa para Inicial II y Básica. Su objetivo es formar niños con valores éticos y morales que trasciendan en la sociedad, mostrando su pensamiento crítico, analítico y creador a través del saber, el hacer y el actuar.

Su objetivo es liderar y contribuir al desarrollo sociocultural, científico. En julio de 2005, se elevó el establecimiento a una Unidad Educativa por acuerdo ministerial 022-DP-DPET-2005, lo que se permitió ofrecer una nueva oferta educativa a la zona centro del país. Los niveles de educación inicial I, II y básica están disponibles en instalaciones modernas con nuevos espacios pedagógicos y recreativos, y los docentes están capacitados para promover una educación personalizada basada en valores como la autonomía, la tolerancia, la integridad. Con el tiempo y gracias al nivel académico, la atmósfera familiar y su carácter multicultural, se determinó en el año 2013 la necesidad de ofrecer el Bachillerato en Ciencias mediante el acuerdo 760-CZE3-2013, y desde entonces se han graduado 11 promociones, con un total de 177 estudiantes.

Figura 1. Exteriores de la institución

Fuente: elaboración propia

Una de las grandes metas ha sido fortalecer la parte humana y los valores para que los estudiantes aumenten su autoestima y puedan alcanzar los objetivos académicos propuestos durante todos estos años, aumentando las áreas deportivas y lúdicas. Desde hace 19 años, se ha educado a estudiantes con una perspectiva abierta, pensamiento crítico, investigación, innovación y creatividad, con una alta autoestima y valores éticos y morales.

Misión

Comprometidos con la formación integral de niñas, niños y adolescentes basados en los principios fundamentales de amor, solidaridad, con disciplina y responsabilidad; cumpliendo con estándares de calidad reconocidos a nivel nacional e internacional, lo que produce un alto nivel de pensamiento analítico, crítico y reflexivo; capaces de solucionar problemas y tomar decisiones en la vida cotidiana, contribuyendo al avance científico y tecnológico, la protección del medio ambiente y el desarrollo de una comunidad equitativa e inclusiva.

Visión

De la institución tiene un sistema de gestión educativa acreditado a nivel internacional, para ser un referente escolar innovador que combina una formación integral, la práctica de valores y el respeto por la naturaleza, lo que tendrá un impacto significativo en el crecimiento de una sociedad que sea justa y autosuficiente.

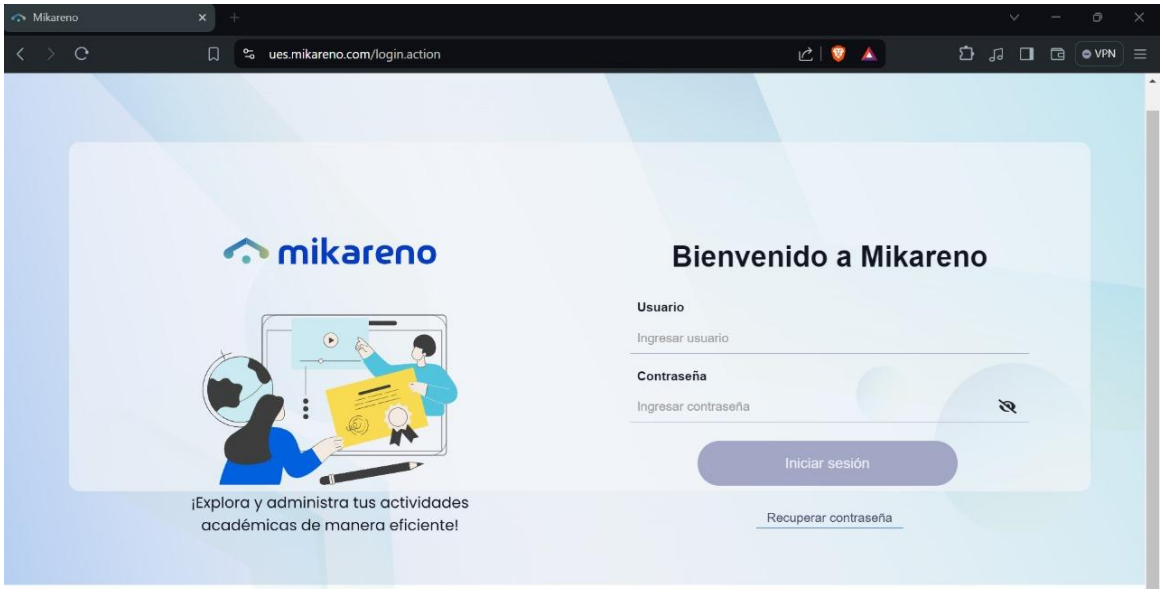
2.2. Metodología de la investigación

El enfoque cualitativo de la investigación aborda completamente el tema y permite el análisis de los datos. Para obtener información sobre el conocimiento de la ciberseguridad y el examen junto con herramientas especializadas para observar la eficacia en este, dentro del contexto educativo, se realizó entrevistas y encuestas al Gerente, Rector y jefe de sistemas a cargo de la plataforma educativa. Cuando se combinan estas técnicas, se puede obtener una comprensión completa de la situación actual.

Enfoque de la investigación

Nada en la actualidad es cien por ciento seguro y lo que la ciberseguridad ofrece es ser un escudo ante amenazas por parte de delincuentes que solo roban información para sacar beneficio personal es por eso por lo que la evaluación de la seguridad de la plataforma educativa requiere medición y análisis con herramientas especializadas.

Figura 2. Plataforma educativa para analizar



Fuente: elaboración propia

El análisis de la plataforma se llevó a cabo para comprender a fondo las vulnerabilidades detectadas y cómo podrían afectar la seguridad de la plataforma educativa. Esto permitió a la institución fortalecer las medidas de seguridad, lo que garantizo la protección efectiva de los datos de estudiantes y docentes frente a amenazas cibernéticas potenciales. Estas herramientas facilitan la identificación de fallas, la comparación con los estándares de seguridad, el análisis de riesgos y la eficacia de las medidas de seguridad implementadas. Se espera obtener una comprensión del conocimiento que tienen los directivos de la plataforma al momento que este interactúa dentro del mundo digital y si la seguridad brindada es eficiente.

Esto permitiría que la institución tenga conocimiento de su plataforma, sus vulnerabilidades y a que tipos de ataque se encuentra desprotegido.

Método de investigación

El método realizado es analítico sintético, este método permite obtener una comprensión profunda de la seguridad de la plataforma educativa y proporcionar sugerencias útiles sobre cómo mejorarla. Al momento de realizar el análisis, usando

herramientas especializadas, examina la seguridad de la plataforma educativa para encontrar posibles vulnerabilidades y áreas de debilidad en su estructura y configuración. Al momento de realizar la síntesis, para comprender los problemas importantes de seguridad, riesgos potenciales para la plataforma.

Tipo de investigación

El tipo de investigación que se llevó a cabo para la ciberseguridad en una plataforma educativa a través de herramientas especializadas se organizó como análisis cualitativo e investigación bibliográfica. Esta combinación permitió obtener una comprensión completa y fundamentada en evidencia tanto de los directivos que se encuentran a cargo como del contexto general del proyecto.

La investigación se caracterizó por ser descriptiva y empleó un enfoque cualitativo según lo descrito por Ramírez (2023) este tipo de estudio permite detallar un fenómeno social y profundizar en su problemática para identificar sus variables, causas y consecuencias. La investigación también es de tipo documental, citado por Reyes (2020) la investigación documental se refiere a un método de investigación que implica la recopilación, selección y análisis de información proveniente de diversas fuentes, como documentos, revistas, libros, grabaciones, filmaciones, periódicos, artículos de resultados de investigaciones y memorias de eventos. En este caso, la estrategia para la investigación será la recolección de información y el análisis será el análisis para la interpretación de datos, relacionados con el objeto de estudio.

Población

Para el propósito de esta investigación, la población objetivo se limita a los directivos principales y encargado de la plataforma que conforman la Unidad Educativa Suizo en la ciudad de Ambato, Provincia de Tungurahua, Ecuador. Esta cifra se basa en la última elección vigente para este período académico.

Porque la institución no se trabaja con una mayor muestra o porque la población se limita al rector y jefe de sistemas, esto debido a que estos encargados son los que manejan principalmente la plataforma y están a cargo de los cambios que se hace y que no dentro de la plataforma. A continuación, la población se detalla en el siguiente cuadro:

Cuadro 1. Población entrevistada

Entrevistado	**Cargo**	**N**
Carlos Escobar	Gerente Administrativo	1
Wilmer Paredes	Vicerrector de la Institución	1
Gabriel Valdivieso	Encargado de la Pagina Web	1
TOTAL		3

Fuente: elaboración propia

La tabla anterior se usó para conocer el número de población con las que se va a trabajar, y de igual manera para determinar si tienen conocimiento de ciberseguridad y como pueden estar propensos a robo de información o más sobre el tema de ciberseguridad.

Técnicas e instrumentos de recolección

Técnicas

Es necesario analizar un fenómeno que sucede dentro de un contexto particular según Mendoza (2020) afirma que además de la información disponible en los documentos, el investigador puede recurrir a las percepciones de las personas afectadas por el problema o que tienen conocimiento sobre él. Esta se considera información primaria, y las técnicas más relevantes para recopilarla son la observación, la encuesta y la entrevista.

Para comparar las estadísticas de OWASP a nivel nacional, la recopilación de datos de vulnerabilidades presentes en estas instituciones permitirá identificar las brechas de seguridad más comunes en instituciones educativas que trabajen con

plataformas educativas que se encuentra en la tabla 3, lo que permitirá hacer recomendaciones sobre su mejora y las vulnerabilidades a las que está en riesgo.

Instrumentos

Para obtener las opiniones de cada profesional, se optó por la técnica de entrevista en profundidad, es la más adecuada para recopilar este tipo de información en línea con lo mencionado por Roca (2021) la entrevista en profundidad consiste en una serie de preguntas diseñadas para filtrar las respuestas de los participantes, con el propósito de reunir los datos más pertinentes para el estudio. Este enfoque busca construir y analizar diversas cuestiones sociales interesantes desde la perspectiva de los entrevistados. La entrevista de interacción verbal asimétrico, a diferencia de la conversación cotidiana. El entrevistador hace preguntas para controlar el intercambio verbal, pero el entrevistado es el sujeto-objeto de la entrevista. De esta manera, las preguntas de las entrevistas en profundidad se definen con anticipación para abordar los temas relevantes para el desarrollo de la investigación.

En este estudio, las entrevistas fueron fundamentales para obtener datos precisos y detallados. Las entrevistas proporcionaron perspectivas valiosas de expertos y no expertos, generando una nueva visión sobre la ciberseguridad y sus impactos.

Fue por esto por lo que se eligió la entrevista en profundidad, para el presente trabajo se tomó en consideración 2 tipos de entrevistas, son diferentes cargos y por lo tanto tienen muy diferentes puntos de vista, la primera fue a la persona encargada de TI o la que lleva a cabo la plataforma, que se encuentra en el anexo 1 para poder recopilar la mayor cantidad de información que conoce acerca de la ciberseguridad, y sobre la cantidad de miembros con los que se puede llegar a trabajar. La siguiente entrevista junto con las mismas preguntas se realizó al vicerrector de la institución Wilmer Paredes y Carlos Escobar al gerente administrativo, quienes compartieron sus conocimientos sobre las diferentes medidas de seguridad que se puede llegar a implementar en las instituciones.

Las entrevistas utilizadas en este estudio han sido fundamentales para reunir datos precisos y detallados, proporcionando perspectivas valiosas de expertos y profesionales. Se permitió obtener una visión distinta sobre la ciberseguridad y sus implicaciones. A partir de las entrevistas, se describió el conocimiento de las personas responsables del sistema. Para la recopilación de la información, se realizaron a cabo dos entrevistas: una al encargado de TI (ver Anexo 1) y otra al gerente administrativo y vicerrector de la institución (ver Anexo 2).

Encargado de TI

El encargado de TI advierte sobre ataques de DDOS que pueden paralizar plataformas educativas al inundar los servidores con tráfico falso y menciona medidas de seguridad para evitar la ejecución de código malicioso y la pérdida de datos. Destaca que los sistemas con información personal son los más atacados por *hackers* que envían mensajes y enlaces fraudulentos para robar datos.

En relación con la pregunta sobre las medidas de seguridad implementadas en plataformas educativas para proteger datos, menciona que las medidas de seguridad normalmente incluyen:

- Cifrado de datos
- autenticación segura
- Contraseñas sólidas
- Políticas de bloqueo
- Monitoreo del sistema
- Manual del sistema
- Respaldo de datos anual
- Actualización de parches de seguridad
- Control de inicio de sesión con códigos captcha

Respecto a la gestión de actualizaciones de seguridad y parches de software, menciona que se sugiere implementar un proceso de gestión de cambios para manejar las actualizaciones de seguridad y parches de software. Es importante

tener un proveedor de hosting confiable con medidas de seguridad adecuadas, monitoreo constante, mantenimiento regular del servidor y control de tráfico para prevenir robos de información.

En cuanto a los procedimientos para detectar y responder a posibles incidentes de seguridad, se realiza monitoreo de seguridad en tiempo real del tráfico en el sistema para verificar la actividad de los usuarios y evitar posibles caídas o interferencias. Es importante implementar sistemas de alerta y realizar evaluaciones periódicas de seguridad, así como tener un plan de emergencia en caso de *hackeo*. También se recomienda tener *hosting* propio en lugar de compartirlo para reducir el riesgo.

Sobre la herramienta utilizada para detectar vulnerabilidades, menciona que el escaneo de vulnerabilidades se realiza con herramientas como:

- *Nexus*
- *OpenBast*
- Dinámica de Servidor
- AD
- Afomética
- DASK

Según el encargado de TI, la ciberseguridad en las instituciones educativas se refiere a proteger las herramientas tecnológicas y plataformas utilizadas, como redes sociales y bases de datos. Se mencionan varios riesgos, como el robo de información y plagio. Por lo tanto, es importante que las instituciones tengan su propia ciberseguridad para evitar posibles daños causados por terceros.

Segunda Entrevista - Encargados de la Institución

En relación con la pregunta sobre la importancia de la ciberseguridad en el entorno educativo actual, las autoridades no supieron responder que la ciberseguridad es crucial en el entorno educativo actual, protege contra el robo de información, datos personales y cuentas bancarias. La tecnología y herramientas actuales permiten

mantener actualizados y protegidos dentro de la institución.

Sobre los riesgos específicos de seguridad considerados relevantes para las instituciones educativas, las autoridades no supieron decir que los riesgos de seguridad considerados relevantes para las instituciones educativas son el robo de información y datos durante la transferencia de la base de datos, así como la posibilidad de destrucción de datos y alteraciones de contenido en la página. Además, hay riesgos asociados a la información personal de estudiantes y profesores, así como a las calificaciones y la parte contable de la institución, por lo que la ciberseguridad es fundamental para su protección.

En cuanto a los desafíos comunes en términos de ciberseguridad y cómo abordarlos, las autoridades dijeron que los desafíos comunes en ciberseguridad para las instituciones incluyen la necesidad de crear planes de seguridad, contratar paquetes de seguridad y utilizar antivirus y software para controlar el acceso a la información. Además, es importante concienciar a los trabajadores y estar actualizados con la tecnología para proteger las plataformas de posibles riesgos de terceros. También se mencionó la necesidad de realizar un análisis de riesgos mediante el uso de herramientas especializadas para detectar posibles fallos o vulnerabilidades que puedan afectar la información de la institución educativa.

2.3. Metodología de desarrollo

OWASP proporciona una variedad de métricas y preguntas tal como indica González (2020) para determinar la gravedad de las amenazas y distribuir de manera más efectiva los recursos disponibles para la seguridad de las aplicaciones. Sin embargo, esto es solo una recomendación; cada organización e institución tiene la libertad de establecer sus puntos clave y métricas para adaptarse al análisis.

La metodología de OWASP analiza cada amenaza desde dos perspectivas: la probabilidad de que ocurra y los efectos potenciales. Cada una de estas perspectivas se dividirá en tres etapas nuevas para clasificar las amenazas. Según el impacto de la amenaza, se asignarán valores a cada herramienta en una escala

de 1 a 5 con el nivel de impacto de lo que ocasiona la vulnerabilidad.

Utilizar esta metodología, es importante destacar que numerosos estudios científicos respaldan la efectividad y confiabilidad de esta metodología, lo cual añade un dato adicional relevante a nivel mundial a través del compendio OWASP TOP 10.

OWASP proporciona una variedad de métricas y preguntas como apunta González (2020) para determinar la gravedad de las amenazas y distribuir de manera más efectiva los recursos disponibles para la seguridad de las aplicaciones. Sin embargo, esto es solo una recomendación; cada organización e institución tiene la libertad de establecer sus puntos clave y métricas para adaptarse al análisis.

OWASP, proyecto de seguridad de aplicaciones web como apunta Suárez (2022) es un proyecto abierto que recopila y organiza pruebas de seguridad enfocadas en aplicaciones web. Esta guía se considera la más completa y abarcadora en el campo de las aplicaciones web en comparación con otras metodologías. La estructura de las pruebas de seguridad de aplicaciones web se divide en dos categorías: pasiva y activa. La pasiva se refiere a interactuar directamente con la aplicación para comprender su lógica, entradas y salidas. Para las pruebas de seguridad activas propone, pero no se debe seguirlas todas, se puede adaptar algunas para la proposición del proyecto al que se está realizando:

1. Recopilación de información.
2. Pruebas de gestión de configuración e implementación.
3. Pruebas de gestión de identidad.
4. Pruebas de autenticación.
5. Pruebas de autorización.
6. Pruebas de gestión de sesión.
7. Pruebas de validación de ingreso.
8. Manejo de errores.
9. Criptografía.
10. Pruebas de lógica del negocio.

11. Pruebas del punto de vista del cliente.

La necesidad basada en lo dicho por Ortega (2022) de implementar una estrategia de seguridad integral y adherirse a estándares y modelos de seguridad en el desarrollo de software, como OWASP, es crucial para prevenir futuras fugas y fallos en sistemas y sitios web. Esto se debe a que constantemente se desarrollan nuevos métodos que amenazan la seguridad de la información en las organizaciones e instituciones. Por lo tanto, es esencial que las organizaciones consideren los peligros a los que pueden enfrentarse, como el robo, la pérdida, la alteración o la interrupción de información y es esencial seguir los estándares y normas globalmente aceptados para proteger los activos de la empresa o institución mediante la seguridad de su sitio web, una vulnerabilidad se puede definir como una falla en el sistema que un atacante puede explotar.

La metodología OWASP lo que busca es mejorar la visibilidad de la seguridad de las aplicaciones según Rojas (2018) para que tanto organizaciones como individuos puedan tomar decisiones informadas sobre cuestiones de seguridad, respaldadas por datos fiables y verificados y otras características más que hacen de esta metodología la mejor, estos datos son:

1. Cualquier persona puede participar en OWASP y todos sus proyectos, materiales y documentación están disponibles gratuitamente.
2. Todos los productos y servicios recomendados no son productos comerciales, sino que son productos libres y de código abierto.
3. Realiza un informe periódicamente que compila las vulnerabilidades más frecuentes de las aplicaciones web.
4. Ofrecen herramientas de detección y orientación sobre cómo abordar dicha debilidad.

OWASP de acuerdo con Zambrano (2022) llama a los diez principales un documento de concientización y recomienda que todas las organizaciones incluyan informes en sus operaciones para reducir o reducir los riesgos de seguridad. La

Tabla 1 muestra los peligros de seguridad incluidos en el informe OWASP Top 10 de 2021:

Tabla 3. Vulnerabilidades OWASP Top 10 2021

OWASP Top 10 2021	
A01:2021	Pérdida de control de Acceso
A02:2021	Fallas Criptográficas
A03:2021	Inyección
A04:2021	Diseño Inseguro
A05:2021	Configuración de Seguridad Incorrecta
A06:2021	Componentes Vulnerables y Desactualizados
A07:2021	Fallas de Identificación y Autenticación
A08:2021	Fallas en el Software y en la integridad de los Datos
A09:2021	Fallas en el registro y Monitoreo
A10:2021	Falsificación de solicitudes de Lado del servidor (SSRF)

Fuente: tomado a partir de Kiuwan (2021); Zambrano (2022)

Una lista de las diez vulnerabilidades de seguridad web según OWASP (2021) más comunes y peligrosas, esta lista, conocida como OWASP TOP 10, se actualiza regularmente para reflejar los avances más recientes en seguridad cibernética.

A01:2021 - Pérdida de Control de Acceso ha ascendido de la quinta posición a ser la categoría con el mayor riesgo en la seguridad de aplicaciones web. Los datos indican que, en promedio, el 3,81% de las aplicaciones evaluadas presentaban una o más debilidades comunes CWEs (*Common Weakness Enumeration*), sumando más de 318.000 incidencias en esta categoría. Asociadas con la Pérdida de Control de Acceso se encontraron con mayor frecuencia que en cualquier otra categoría.

A02:2021 - Fallas Criptográficas ha subido un puesto, situándose en el segundo lugar. Anteriormente conocida como A3:2017-Exposición de Datos Sensibles, esta categoría ahora se centra en fallos relacionados con la criptografía, un aspecto que ya se insinuaba anteriormente. Las fallas criptográficas a menudo resultan en la exposición de datos confidenciales o en la vulnerabilidad del sistema.

A03:2021 - Inyección ha descendido al tercer lugar. El 94% de las aplicaciones fueron examinadas por algún tipo de inyección, mostrando una incidencia máxima del 19% y un promedio del 3,37%. Las 33 CWEs relacionadas con esta categoría tuvieron la segunda mayor cantidad de ocurrencias, con 274.000 casos. El XSS (*Cross-Site Scripting*) se incluye en esta categoría en la edición actual.

A04:2021 - Diseño Inseguro es una nueva categoría para 2021, enfocada en los riesgos asociados con fallos de diseño. Para avanzar como industria, incorporar actividades de seguridad en las primeras etapas del desarrollo. Se necesita más modelos de amenazas, patrones y principios de diseño seguro. Un diseño inseguro no puede corregirse mediante una implementación perfecta, los controles de seguridad necesarios no fueron creados para defenderse de ataques específicos.

A05:2021 - Configuración de Seguridad Incorrecta ha subido desde la sexta posición de la edición anterior. El 90% de las aplicaciones fueron examinadas por configuraciones incorrectas, con una tasa de incidencia promedio del 4,5% y más de 208.000 casos de CWEs relacionadas. Con el aumento de software altamente configurable, no es sorprendente que esta categoría haya ascendido. La categoría A4:2017-Entidades Externas XML (*Extensible Markup Language*), XXE (*XML external entity*) ahora forma parte de esta categoría.

A06:2021 - Componentes Vulnerables y Desactualizados, antes conocida como Uso de Componentes con Vulnerabilidades Conocidas, ocupa el segundo lugar en el Top 10 de la encuesta a la comunidad y también tuvo suficientes datos para estar en el Top 10 del análisis de datos. Esta categoría ha subido desde la novena posición en 2017. Es un problema conocido que es difícil de probar y evaluar el riesgo. Es la única categoría sin CVE (*Common Vulnerabilities and Exposures*), las vulnerabilidades y exposiciones comunes relacionadas con las CWEs incluidas, por lo que se considera una vulnerabilidad predeterminada con puntuaciones de impacto de 5,0.

A07:2021 - Fallas de Identificación y Autenticación, previamente denominada Pérdida de Autenticación, ha descendido desde la segunda posición y ahora incluye

CWEs más relacionadas con fallas de identificación. Esta categoría sigue siendo crucial en el Top 10, aunque el aumento de frameworks estandarizados parece estar ayudando.

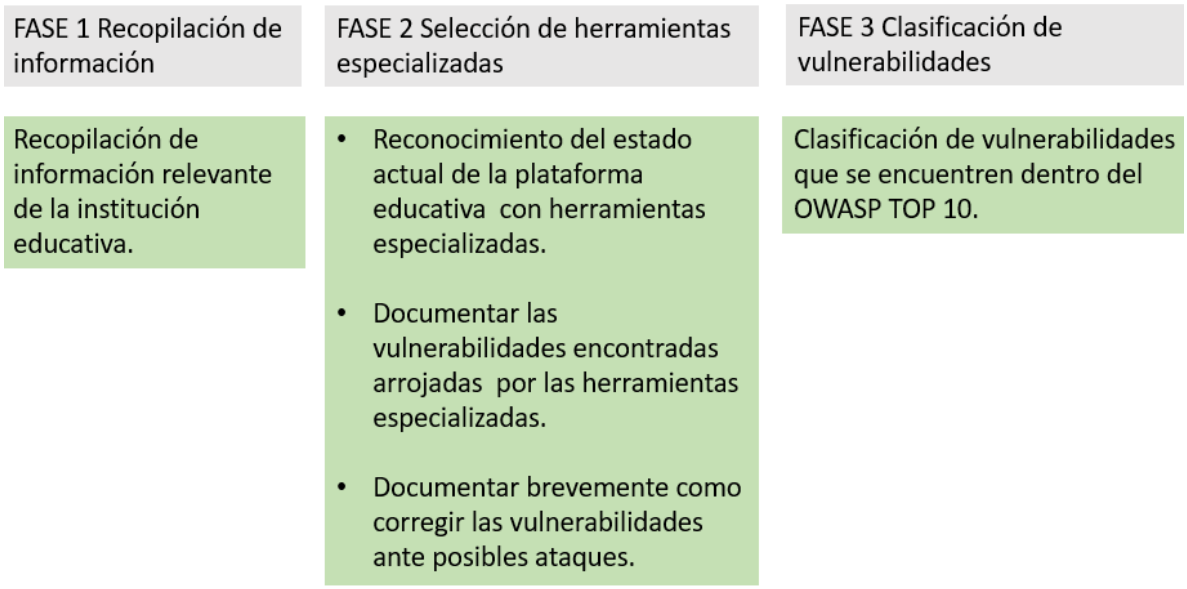
A08:2021 - Fallas en el Software y en la Integridad de los Datos es una nueva categoría para 2021, centrada en suposiciones relacionadas con actualizaciones de software, datos críticos y pipelines CI (*Continuous Integration*) y CD (*Continuous Distribution*) sin verificación de integridad. Representa uno de los mayores impactos según los sistemas de ponderación de vulnerabilidades (CVE) /CVSS (*Common Vulnerability Scoring System*), sistema de puntuación de vulnerabilidad común. La categoría A8:2017-Deserialización Insegura ahora forma parte de esta amplia categoría.

A09:2021 - Fallas en el Registro y Monitoreo, previamente A10:2017-Registro y Monitoreo Insuficientes, ha subido desde la décima posición y se ha ampliado para incluir más tipos de fallas. Es difícil de probar y no está bien representada en los datos de CVE/CVSS. No obstante, las fallas en esta categoría pueden afectar directamente la visibilidad, las alertas de incidentes y los análisis forenses.

A10:2021 - Falsificación de Solicitudes del Lado del Servidor ha sido incluida desde el Top 10 de la encuesta a la comunidad. Aunque los datos muestran una tasa de incidencia relativamente baja, esta categoría tiene una cobertura de pruebas y calificaciones altas para la capacidad de explotación e impacto. Esta categoría subraya la importancia de estos problemas, incluso si no están ampliamente representados en los datos actuales.

Se establecen tres fases basado en el trabajo de Herney (2020) y modificado para llevar a cabo el desarrollo del proyecto, detallándose cada una de ellas junto con las actividades correspondientes que se realizó para alcanzar los objetivos propuestos.

Figura 3. Fases metodología de desarrollo



Fuente: tomado a partir de Herney (2020)

Diagnostico basado en pruebas con herramientas especializadas

Esta fase es crucial, se llevará a cabo un análisis exhaustivo para obtener una visión completa del estado inicial del sitio web. Se cuenta con los permisos necesarios de la administración de la institución para utilizar la URL del sitio web en las actividades planificadas para esta etapa.

Primera fase: Recopilación de la información

Se realizo una consulta en el buscador de Google para acceder a la información general de la institución educativa "Unidad Educativa Suizo" para las pruebas de recopilación.

El Centro Educativo Integral Suizo, fundado el 4 de agosto de 2003, se dedica a formar niños con valores éticos y morales para impactar positivamente en la sociedad. Inicialmente ofreciendo educación para niveles de Inicial II y Básica, la institución se expandió a una Unidad Educativa en 2005, incorporando educación inicial y básica en modernas instalaciones. En 2013, comenzó a ofrecer el Bachillerato en Ciencias, con 177 estudiantes graduados hasta la fecha. La misión

de la institución es proporcionar una educación integral basada en principios de amor, solidaridad, disciplina y responsabilidad, promoviendo el pensamiento crítico y analítico. Su visión es ser un referente educativo innovador y acreditado internacionalmente, que fomente una formación integral y el respeto por la naturaleza, contribuyendo al desarrollo de una sociedad justa y autosuficiente.

Segunda fase: Reconocimiento y documentación del estado actual del sitio web y pruebas con herramientas especializadas

Se llevo a cabo pruebas especializadas para obtener información completa sobre el estado inicial de la plataforma educativa de la “Unidad Educativa Suizo”, utilizando las herramientas mostradas en la figura 2.

Figura 4. Herramientas especializadas

Fuente: elaboración propia

La metodología, como bien señala OWASP (2017) se centra en detectar riesgos cruciales para las organizaciones y ofrece datos sobre la probabilidad y el nivel de riesgo técnico de dichos riesgos para identificar problemas de seguridad en diversas fases, desde la etapa de diseño hasta la producción. Por eso se realizó un análisis del nivel del riesgo al que se expone la plataforma educativa, de acuerdo con la gravedad de la vulnerabilidad en las herramientas siendo estos los niveles que se describen en la siguiente tabla:

Tabla 4. Nivel de riesgo

Nivel de riesgo	Descripción
1. Muy Bajo	La vulnerabilidad afecta elementos de muy bajo riesgo, como la estética de la página o información pública de bajo valor.
2. Bajo	La vulnerabilidad afecta elementos de bajo riesgo, como información pública de bajo valor.
3. Medio	La vulnerabilidad afecta la usabilidad del sitio web o datos menos críticos, como perfiles de usuarios sin información sensible.
4. Alto	La vulnerabilidad compromete datos sensibles, como información personal de estudiantes, calificaciones, o credenciales de acceso.
5. Muy alto	La vulnerabilidad compromete datos sensibles o críticos, como información confidencial, accesos o parte de la infraestructura tecnológica de la institución.

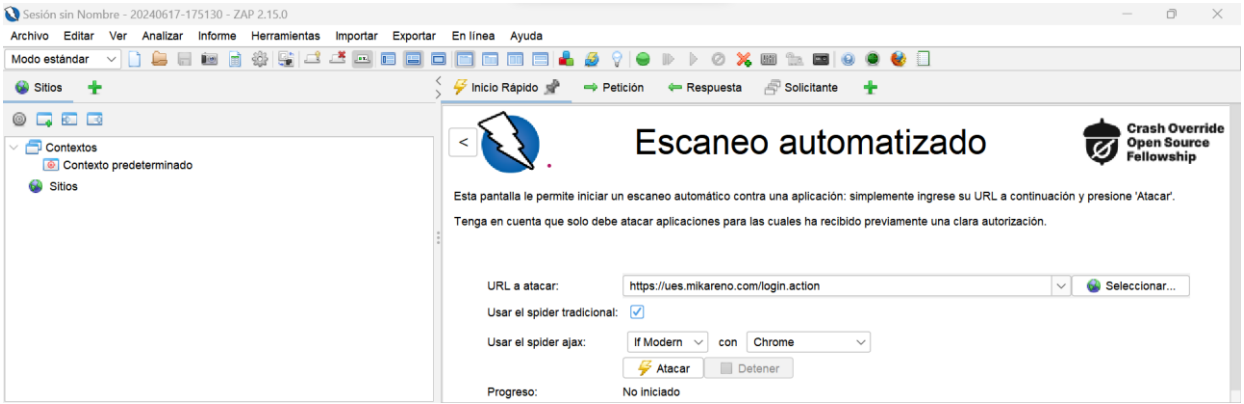
Fuente: elaboración propia

A continuación, se muestra las pruebas con la URL de la institución educativa SUIZO en las diferentes herramientas especializadas.

1. OWASP ZAP

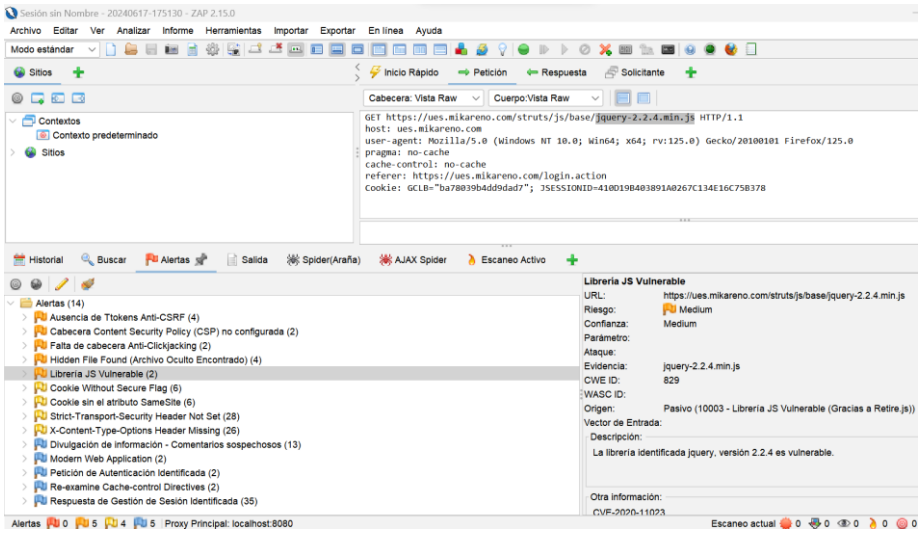
Es una herramienta de código abierto y multiplataforma que permite realizar análisis de vulnerabilidades en aplicaciones web.

Figura 5. Escáner con la herramienta ZAP 2.15.0



Fuente: elaboración propia

Figura 6. Escaneo con la herramienta ZAP 2.15.0



Fuente: elaboración propia

Resultado de las pruebas:

En la figura 5 se presenta el escaneo automatizado de vulnerabilidades en donde se ve como iniciar el ataque y en que navegador se lo prueba, en este caso Chrome, en la figura 6 se presentan tres vulnerabilidades principales: ausencia de *tokens anti-CSRF* (código que previene ataques), falta de configuración de la cabecera *Content Security Policy* (CSP), y ausencia de cabeceras *anti-clickjacking* (medida para prevenir engaños en clics de usuario). Estas vulnerabilidades permiten ataques como la ejecución de peticiones maliciosas, inyección de código y *clickjacking*, poniendo en riesgo la seguridad de los usuarios y la integridad de la aplicación. En el lado izquierdo del pie de página ZAP se muestra un recuento de las alertas encontradas durante el testeo donde se indica un nivel de riesgo medio y bajo, estos resultados en suceso de ataque no están a un peligro considerable pero igual se podría sacar una mínima información de ella, así como la ausencia de cabeceras *anti-clickjacking* permite que la aplicación sea cargada en *iframes* desde orígenes no autorizados, exponiendo a los usuarios.

Nivel de riesgo: 3 (medio)

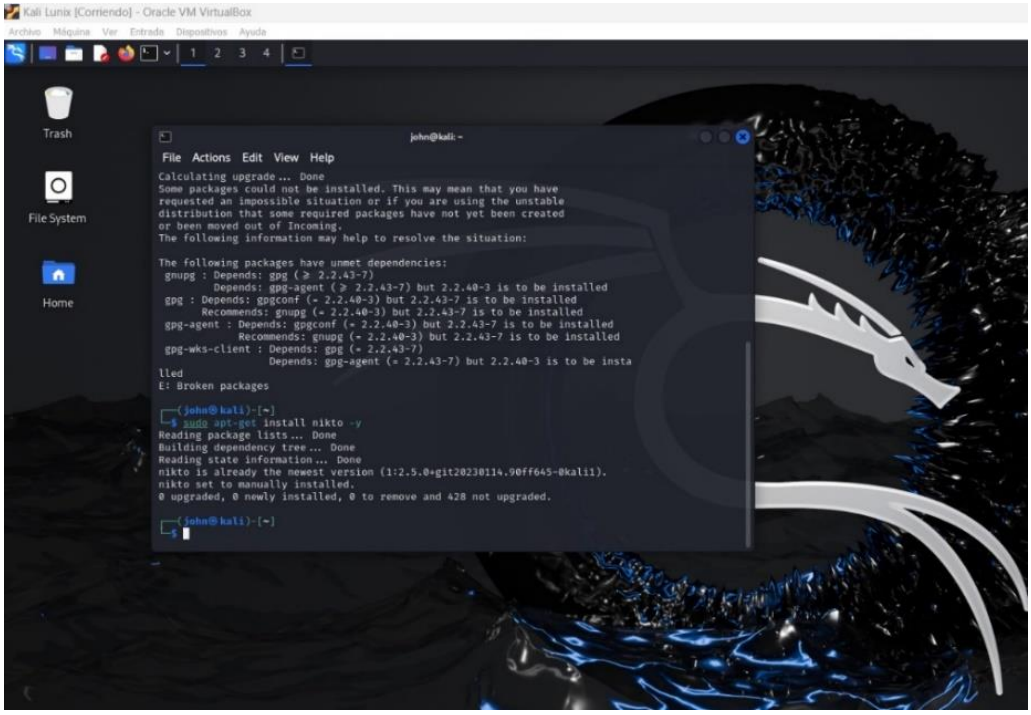
Prevención:

La ausencia de tokens anti-CSRF, lo cual se puede mitigar implementando y validando tokens anti-CSRF en los formularios. La falta de la cabecera CSP deja la aplicación vulnerable a ataques de inyección de código, por lo que se recomienda configurar una política de seguridad de contenido que restrinja los orígenes permitidos, esto controla qué dominios pueden acceder al servidor, protegiendo así contra ataques maliciosos como CORS (*Cross-Origin Resource Sharing*, mecanismo que usa cabeceras HTTP adicionales para permitir que un usuario obtenga permisos para acceder a recursos seleccionados desde un servidor en un origen diferente).

2. *Nikto*

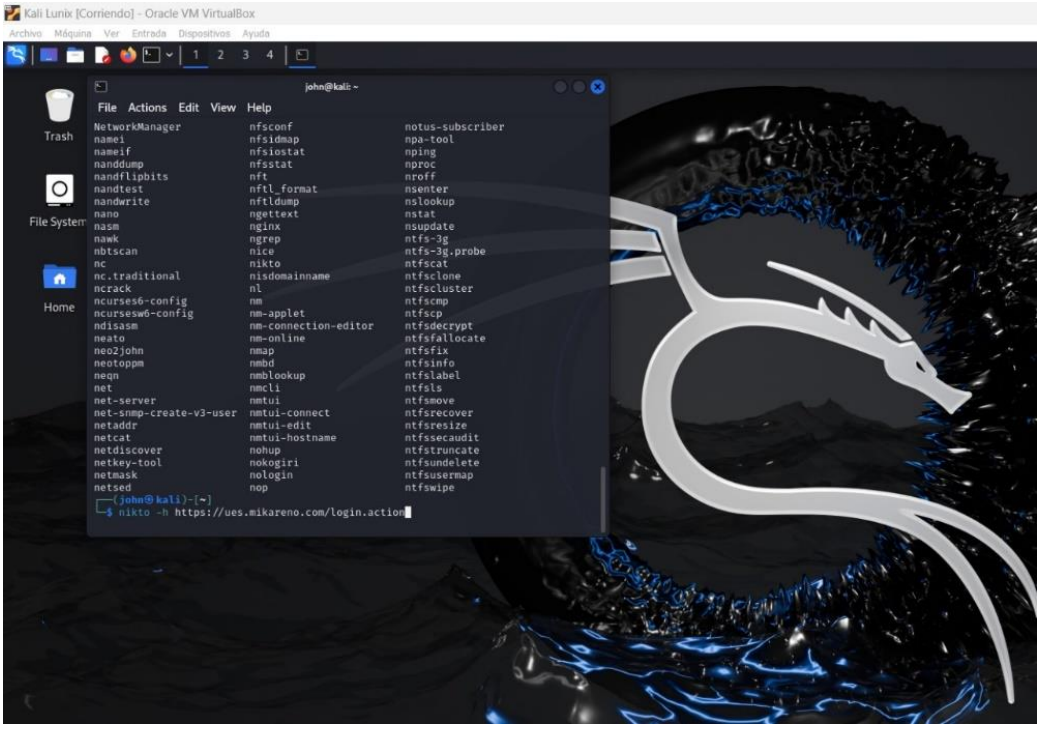
Nikto, es un escáner de servidor web gratuito y de código abierto (GPL) que realiza análisis de vulnerabilidades en múltiples proyectos de servidores *web*, incluidos archivos y programas peligrosos, y busca versiones de software obsoletas.

Figura 7. Instalación de escáner Nikto dentro de un Kali Linux



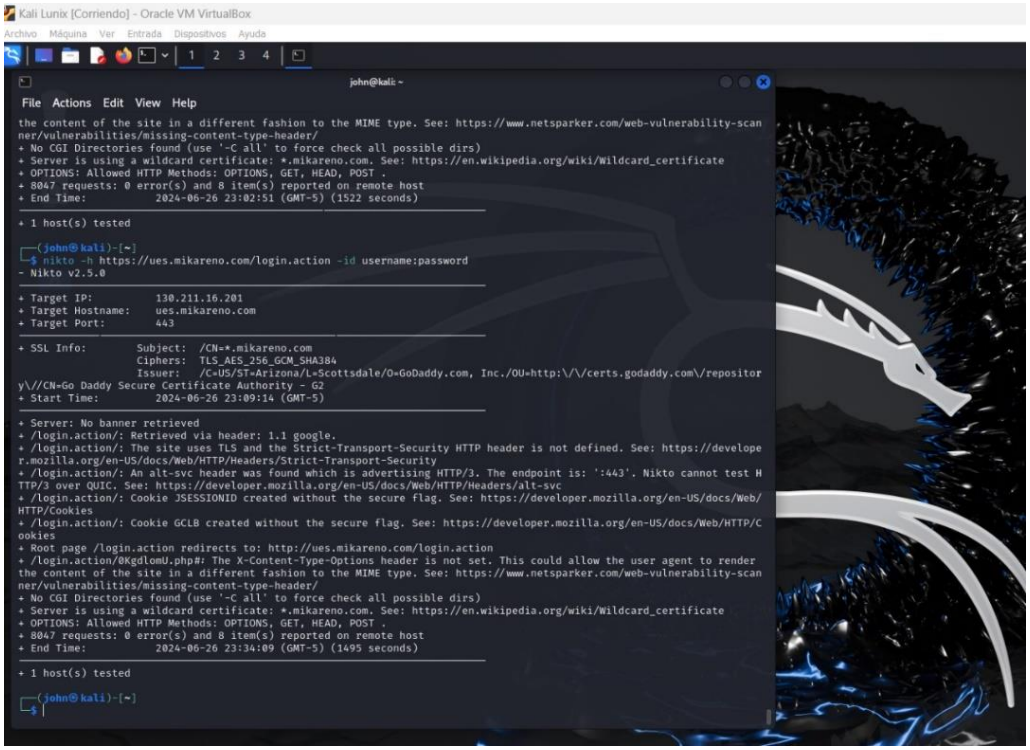
Fuente: elaboración propia

Figura 8. Incorporación de la URL para el escaneo con la herramienta



Fuente: elaboración propia

Figura 9. Escaneo completo con la herramienta Nikto



Fuente: elaboración propia

Resultado de la prueba:

En la figura 7 se presenta Instalación de Nikto dentro de un Kali Linux, en la figura 8 se incorpora de la URL para el escaneo con la herramienta y en la figura 9 el escaneo que ya ha sido completado arrojándome los siguientes resultados con un nivel de riesgo medio y alto que son:

Tabla 5. Identificación de debilidad y su vulnerabilidad

Debilidad	**Vulnerabilidad**
Falta de encabezado Estricta-Seguridad-del-Transporte (HSTS)	Cabecera para posibles ataques y secuestro de cookies en conexiones HTTPS.
Encabezado Alt-Svc que anuncia HTTP/3	Encabezado para usar incorrectamente y exponer la aplicación a vulnerabilidades
Cookie JSESSIONID sin el atributo *Secure*	La cookie sea enviada a través de conexiones no seguras (HTTP)
Falta de encabezado *X-Content-Type-Options*	Encabezado no configurado, posibles ataques de ejecución de scripts y otros tipos de inyección**.**
Falta de encabezado Estricta-Seguridad-del-Transporte (HSTS)	No se encontraron restricciones de directorios CGI, se puede permitir que se ejecuten scripts no deseados en el servidor.

Fuente: elaboración propia

Nivel de riesgo: 4 (Alto)

Prevención:

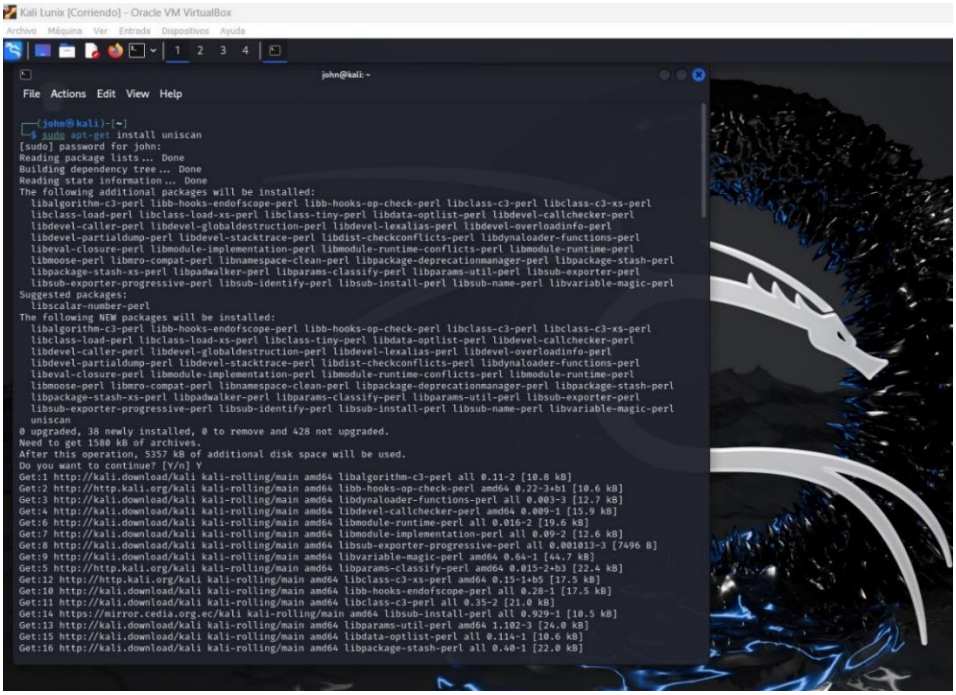
Según lo expuesto por OWASP (2024) proporciona recursos valiosos para el desarrollo seguro de aplicaciones web para las vulnerabilidades identificadas, es crucial configurar el servidor web para incluir la cabecera agregando *Strict-Transport-Security* para evitar ataques de *downgrade* (retroceso de versiones), al igual añadir la cabecera *X-Content-Type-Options*: nosniff (directiva de seguridad de navegador) para proteger contra ataques. Finalmente, configurar las cookies con el

flag secure garantizará que estas solo se transmitan a través de conexiones seguras, evitando su interceptación.

3. *Uniscan*

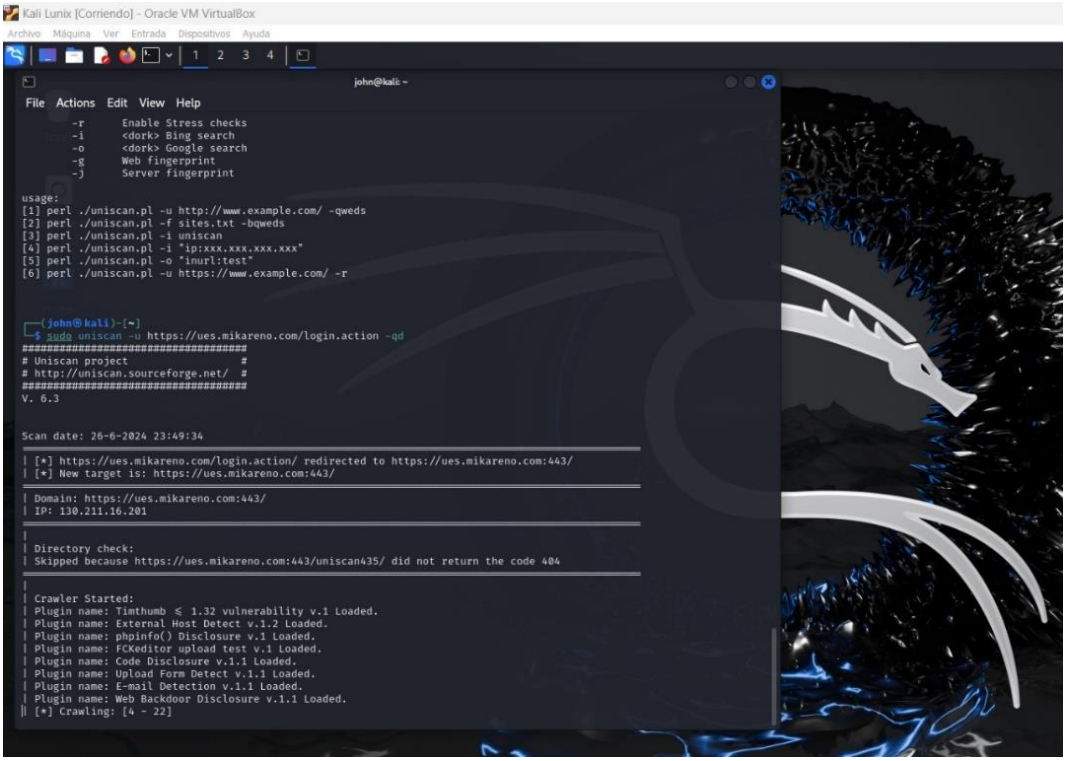
Puede identificar errores que van desde el acceso a archivos locales hasta la ejecución remota de código, e incluso puede cargar archivos de forma remota en sistemas vulnerables**.**

Figura 10. Instalación del escáner Uniscan dentro de un Kali Linux



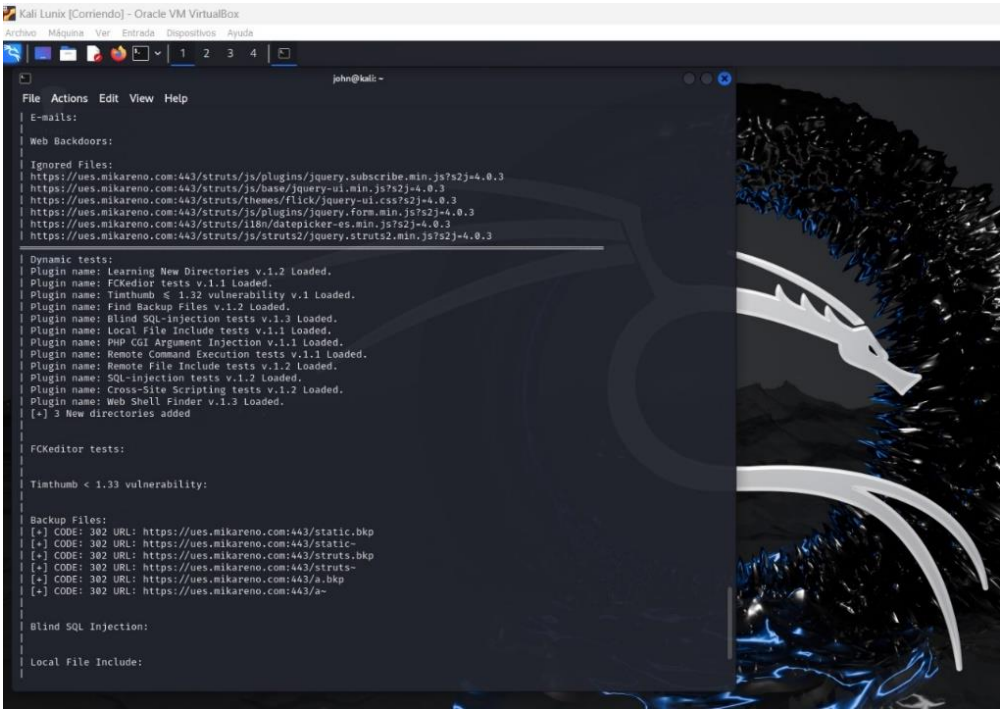
Fuente: elaboración propia

Figura 11. Incorporación de la URL para el escaneo con la herramienta Uniscan



Fuente: elaboración propia

Figura 12. Escaneo completo con la herramienta Uniscan



Fuente: elaboración propia

Resultado de la prueba:

En la figura 10 se presenta Instalación de Uniscan dentro de un Kali Linux, en la figura 11 se incorpora de la URL para el escaneo con la herramienta y en la figura 12 el escaneo que ya ha sido completado arrojándome los siguientes resultados que son vulnerabilidades como inyección SQL, ejecución remota de comandos, inclusión de archivos locales y remotos, exposición de archivos de respaldo, y *Timthumb* (abandonado) < 1.32. Estas vulnerabilidades representan un nivel de riesgo alto de comprometer el sistema.

Tabla 6. Identificación de debilidad y su vulnerabilidad

Debilidad	**Vulnerabilidad**
Timthumb < 1,32	Vulnerabilidad en el script anterior a la versión 1.32.
Archivos de respaldo	Archivos de respaldo expuestos que podrían contener información sensible.
Inyección SQL ciega	Permite a un atacante ejecutar consultas SQL**.**
Archivo local incluido	Permite que un atacante incluya archivos locales en el servidor.
Ejecución remota de comandos	Permite a un atacante ejecutar comandos en el servidor de forma remota.
Inyección SQL	Permite a un atacante manipular consultas SQL ejecutadas por la aplicación.

Fuente: elaboración propia

Nivel de riesgo: 5 (Muy Alto)

Prevención

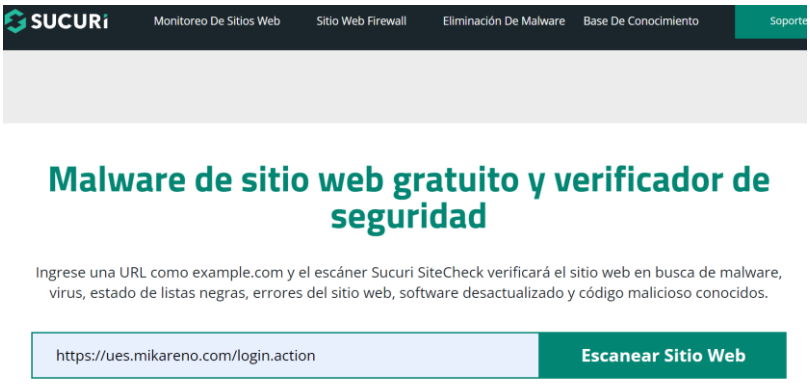
Para prevenir diversas vulnerabilidades, a partir de Saltzer (1974) se recomienda adoptar medidas de seguridad específicas. La actualización de *scripts* como *Timthumb* a la versión más reciente puede prevenir ataques, otro dato es asegurar

que los archivos de respaldo no sean accesibles públicamente y almacenar en ubicaciones seguras que sean cruciales para evitar inyecciones SQL, es fundamental usar consultas parametrizadas, así como implementar validaciones estrictas de entrada. Validar y sanitizar todas las entradas de usuario ayuda a evitar inclusiones de archivos locales y finalmente validar y desinfectar todas las entradas previene la ejecución remota de comandos y secuencias de comandos entre sitios (XSS).

4. *Sucuri*

Es un escáner gratuito para la seguridad de sitios web. Detecta programa maligno, comprueba listas negras, *spam* inyectado y desfiguraciones en plataformas como *WordPress, Joomla, Magento, Drupal* y otras más.

Figura 13. Escáner online Sucuri

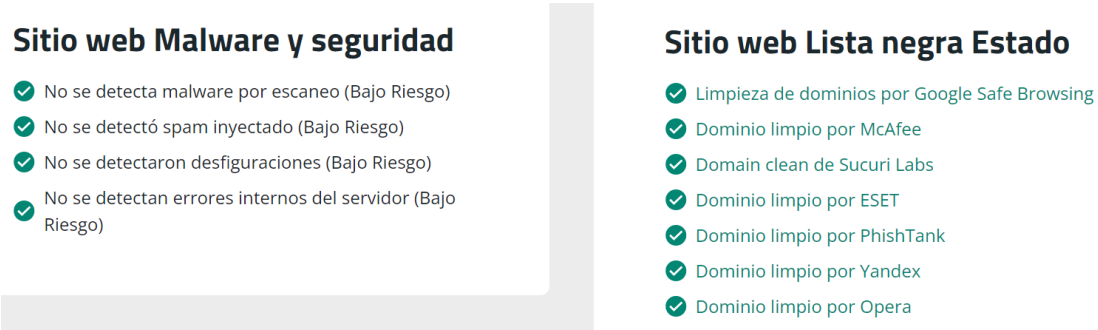


Fuente: elaboración propia

Figura 14. Escaneo de programa maligno y lista negra en la plataforma online Sucuri

Fuente: elaboración propia

Figura 15. Listado de pruebas verificados en el escáner online Sucuri



Fuente: elaboración propia

Resultado de la prueba:

En la imagen 13 se presenta el escaneo en la plataforma Sucuri con la URL de la institución, en la imagen 14 presenta el escaneo que ya ha sido completado donde se arrojó los resultados para detectar posibles programas malignos o si está dentro de la lista negra de dominios, en la figura 15 el reporte informa que el análisis ha arrojado un resultado completamente limpio. Ningún tipo de amenaza en la URL durante la prueba. El sitio web presenta un nivel de riesgo bajo de vulnerabilidad.

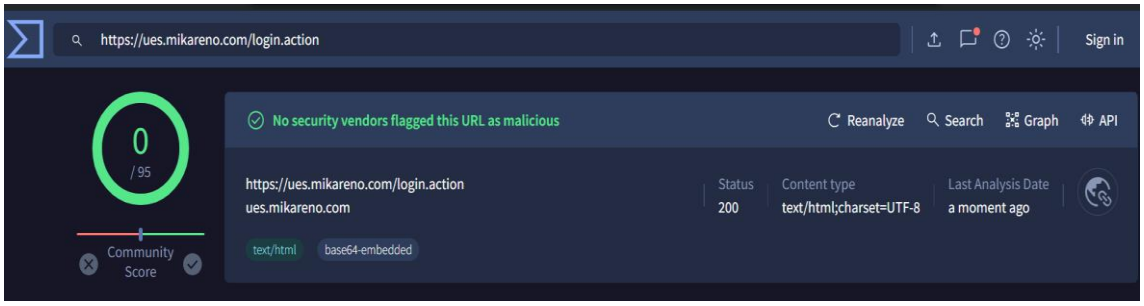
Nivel de riesgo: 2 (Bajo)

Prevención: No existe amenaza, pero se recomienda tener en cuenta errores que comúnmente sucede como la presencia de contenido mixto, donde recursos se cargan a través de conexiones no seguras (HTTP) en una página que utiliza HTTPS para la mayoría de su contenido, lo cual puede comprometer la seguridad al permitir que un atacante intercepte. A partir de (Keith, 2018) una configuración incorrecta de redireccionamiento de HTTP a HTTPS puede dejar a los usuarios vulnerables a ataques de intermediarios malintencionados. Es crucial implementar redirecciones 301 permanentes en el servidor, mejorando así la seguridad y la confianza del usuario en la integridad de los datos del sitio web.

5. Virus Total:

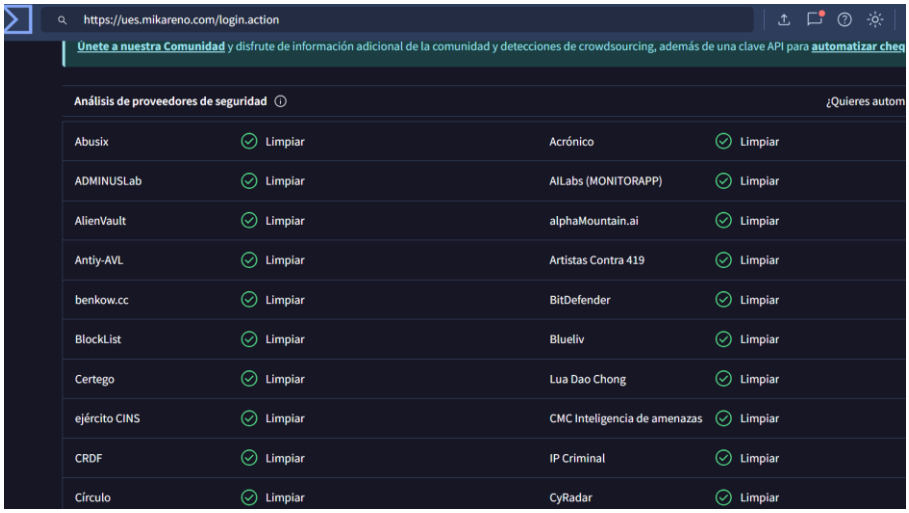
Plataforma integral para la seguridad informática que permite escanear archivos y URL en busca de programa maligno utilizando múltiples motores antivirus.

Figura 16. Escáner Online Virus Total



Fuente: elaboración propia

Figura 17. Análisis de proveedores dentro del escaneo de la plataforma Virus Total



Fuente: elaboración propia

Resultado de la prueba:

En la figura 16 se presenta el escaneo en la plataforma Virus Total con la URL de la institución, en la figura 17 presenta el escaneo que ya ha sido completado donde se arrojó los resultados para detectar posibles amenazas de seguridad, incluyendo programa maligno, phishing u otras vulnerabilidades y el reporte informa que el análisis ha arrojado un resultado completamente limpio. Ningún motor antivirus detectó ningún tipo de amenaza en la URL durante la prueba. El sitio web presenta un nivel de riesgo bajo de vulnerabilidad.

Nivel de riesgo: 2 (Bajo)

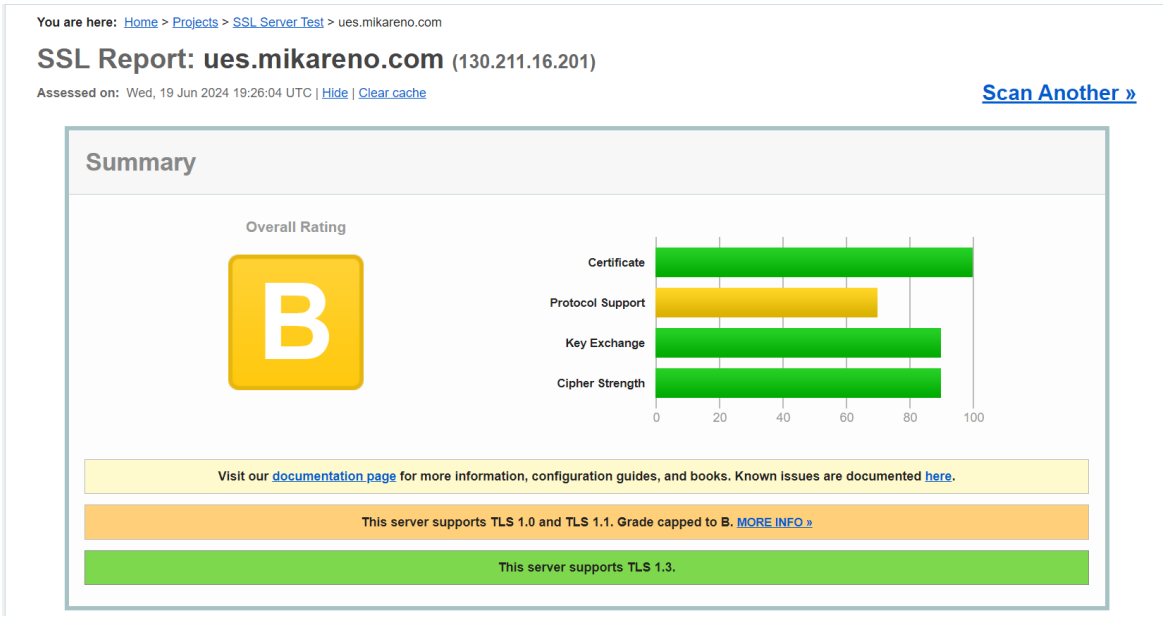
Prevención:
No existe amenaza, pero se recomienda seguir prácticas de seguridad sólidas, tales como emplear HTTPS y llevar a cabo auditorías de seguridad de forma periódica.

6. Qualys:

Escáner en el sitio web en busca de vulnerabilidades y errores de configuración SSL/TLS. Proporciona un análisis en profundidad de su URL https:// que incluye el día de caducidad, la clasificación general, el cifrado, la versión SSL/TLS y otro tipo

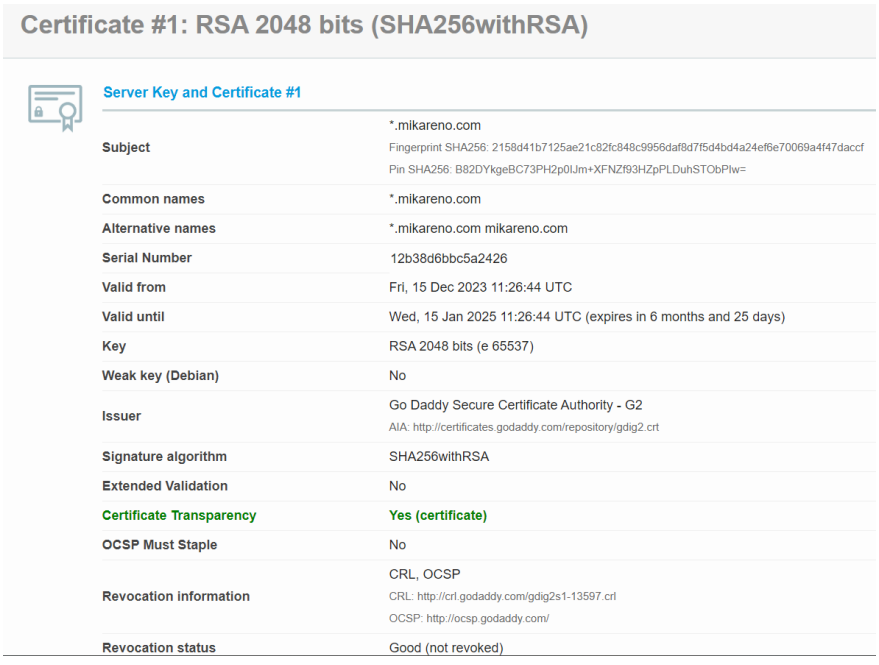
de datos que pueden ayudar a la investigación.

Figura 18. Calificación del escaneo de la URL con el escáner Online Qualys



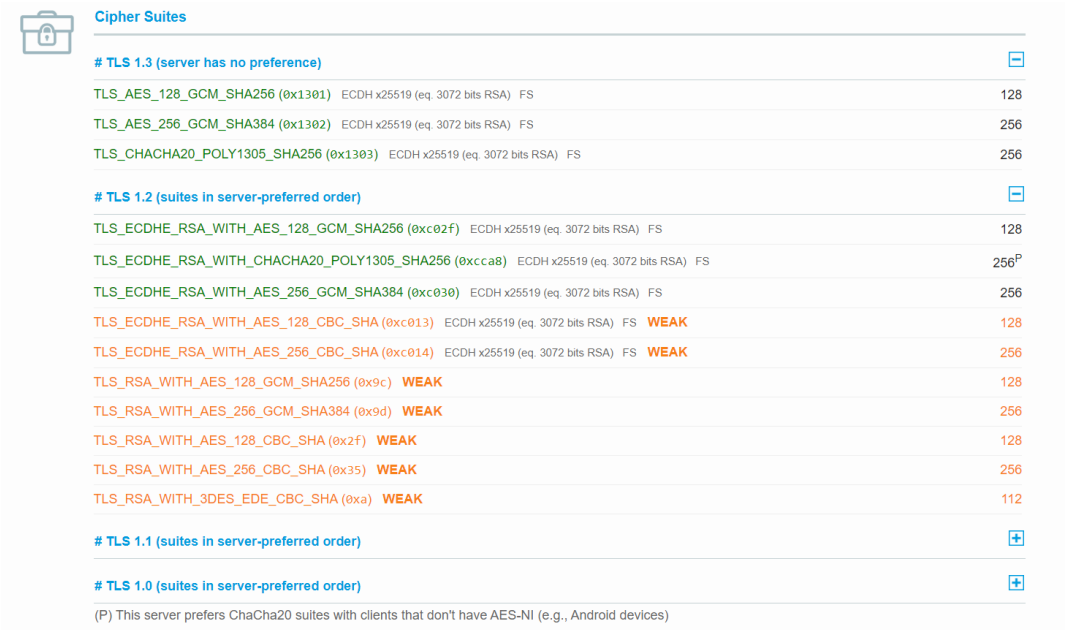
Fuente: elaboración propia

Figura 19. Resumen del escaneo con la plataforma Online Qualys



Fuente: elaboración propia

Figura 20. Vulnerabilidades en el escaneo con la plataforma Online Qualys



Fuente: elaboración propia

Resultado de la prueba:

En la figura 18 se presenta el escaneo en la plataforma *Qualys* con la URL de la institución, en la figura 19 los certificados con los que cuenta la página web y en la figura 20 los conjuntos de cifrado donde se arrojó los resultados para detectar posibles amenazas de seguridad. Los errores mencionados se refieren a la seguridad criptográfica y estándares de seguridad. Indica un nivel de riesgo medio y bajo, estos resultados en suceso de ataque no están a un peligro considerable pero igual se podría sacar una mínima información de ella.

Tabla 7. Identificación de debilidad y su vulnerabilidad

Debilidad	**Vulnerabilidad**
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	vulnerables a ataques como BEAST(vulneración de seguridad del navegador) debido a su corta clave y debilidades de SHA-1 (Algoritmo criptográfico utilizado para generar un hash único de los datos.)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	modo CBC y SHA-1 comprometen la seguridad, vulnerable a BEAST y debilidad de SHA-1
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	claves de 128 bits vulnerables a ataques de fuerza bruta avanzados
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	Uso de RSA sin *Perfect Forward Secrecy* (PFS) deja vulnerables las comunicaciones a largo plazo.
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	vulnerable a ataques como BEAST y debilidades de SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	CBC y SHA-1 comprometen la seguridad del cifrado.
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	3DES es obsoleto y vulnerable a ataques como Sweet32, tamaño de clave débil.

Fuente: elaboración propia

Nivel de riesgo: 3 (Medio).

Prevención:

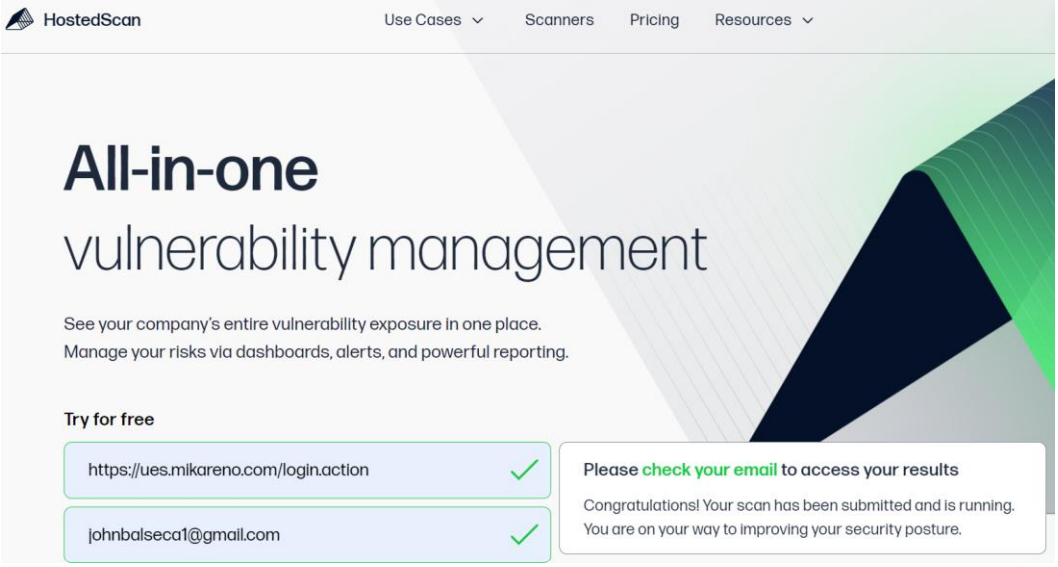
Es crucial adoptar estándares de seguridad más sólidos y actualizados para abordar las debilidades en los cifrados TLS. Según el *National Institute of Standards and Technology* (NIST), migrar a algoritmos de cifrado más fuertes como AES con claves de 256 bits y modos como GCM, que aseguran la integridad de los datos, es fundamental para mitigar riesgos significativos, a partir de (NIST, 2024), es posible adoptar protocolos que ofrecen Perfect Forward Secrecy (PFS), como ECDHE(protocolo de intercambio de claves) en lugar de RSA(algoritmo criptográfico de clave pública), es crucial para garantizar la confidencialidad a largo

plazo contra amenazas emergentes.

7. *HostedScan Security*

Ofrece un servicio en línea que automatiza la exploración de vulnerabilidades para empresas. Incluye escáneres para redes, servidores y sitios web, detectando vulnerabilidades como software obsoleto, inyecciones SQL, y problemas de configuración de red.

Figura 21. Escáner Online HostedScan



Fuente: elaboración propia

Figura 22. Escaneo con resultados arrojados del escáner Online HostedScan

Amenaza	Vulnerabilidad	Objetivo
Bajo	Declaración de Información de Marcas de Tiempo TCP CVSS: 2.6 QoD: 80%	https://ues.mikareno.com/login.action
Alto	SSL/TLS: Informe Vulnerable Cipher Suites para HTTPS CVSS: 7.5 QoD: 98%	https://ues.mikareno.com/login.action
Medio	SSL/TLS: Deprecated TLSv1.0 y TLSv1.1 Detección de Protocolo CVSS: 4.3 QoD: 98%	https://ues.mikareno.com/login.action
Medio	Falta 'Secure' Atributo a las Cookies (HTTP) CVSS: 5.0 QoD: 70%	https://ues.mikareno.com/login.action
Medio	Vulnerabilidad de Apache Tomcat XSS (Jun 2022) - Windows CVSS: 6.1 QoD: 80%	https://ues.mikareno.com/login.action

Fuente: elaboración propia

Resultado de la prueba:

En la figura 21 se presenta el escaneo en la plataforma HostedScan con la URL de la institución y el correo electrónico para que pueda ser llegado los resultados, en la figura 22 arroja ver riesgos recientes con los que cuenta la plataforma y se arrojó los resultados para detectar posibles amenazas de seguridad. Los errores mencionados se refieren a vulnerabilidades y configuraciones de seguridad específicas. Señala un nivel de riesgo medio con proyección a riesgo alto, estos resultados tienen diferentes temas de error como menciona (Nist, 2022) Estos datos permiten la automatización de la gestión de vulnerabilidades, la medición de la seguridad y el cumplimiento. En suceso de ataque están bastante vulnerables, como se mencionará en la siguiente tabla cada vulnerabilidad y su definición:

Tabla 8. Identificación de tabla de riesgos

Vulnerabilidad	**definición**
Declaración de información de marcas de tiempo TCP	Servidor que puede está revelando información sensible a través de marcas de tiempo en las respuestas TCP
SSL/TLS: Informe vulnerable clipher suites para-HTTPS	sitio web utiliza suites de cifrado SSL/TLS que son vulnerables
SSL/TLS: Deprecated TLSV1.0 y TLSV1.1. Detección de protocolo	protocolos de cifrado obsoletos y menos seguros
Falta *Secure* atributo a las *Cookies* (HTTP)	*cookies* están configuradas sin el atributo '*Secure*, riesgo de seguridad
Vulnerabilidad de *Apache Tomcat XSS* (JUN 2022)-Windows	vulnerabilidad de tipo *Cross-Site Scripting* (XSS), vulnerabilidad que podría permitir a un atacante ejecutar scripts maliciosos en el navegador de los usuarios del sitio web.

Fuente: elaboración propia

Nivel de riesgo: 3 (Medio)

Prevención:

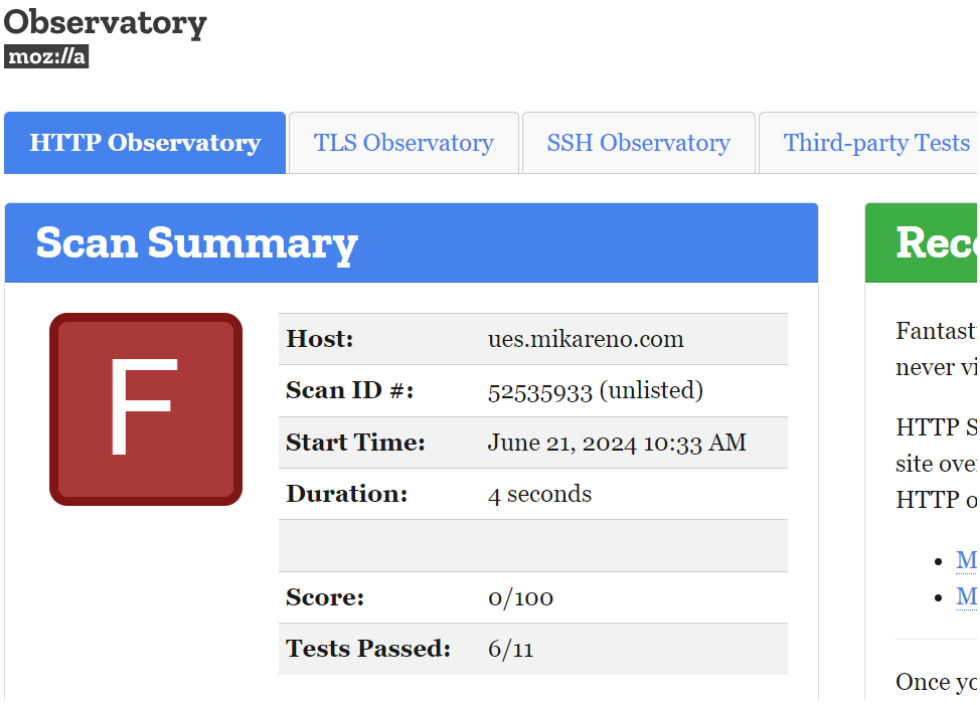
Como señala Helme (2015) "asegurar todas las comunicaciones y mantener las configuraciones actualizadas es fundamental para la protección contra amenazas

en línea", para prevenir estos errores de seguridad, es esencial implementar varias medidas como asegurar que todas las conexiones y recursos se carguen a través de HTTPS, eliminando contenido mixto y utilizando solo protocolos seguros, segundo, configure redirecciones 301 para forzar el uso de HTTPS y añada el atributo 'Secure' a las cookies para evitar que sean transmitidas a través de conexiones no seguras. Junto con esto se debe mantener software y bibliotecas actualizados para protegerse contra vulnerabilidades conocidas.

8. *Observatory*

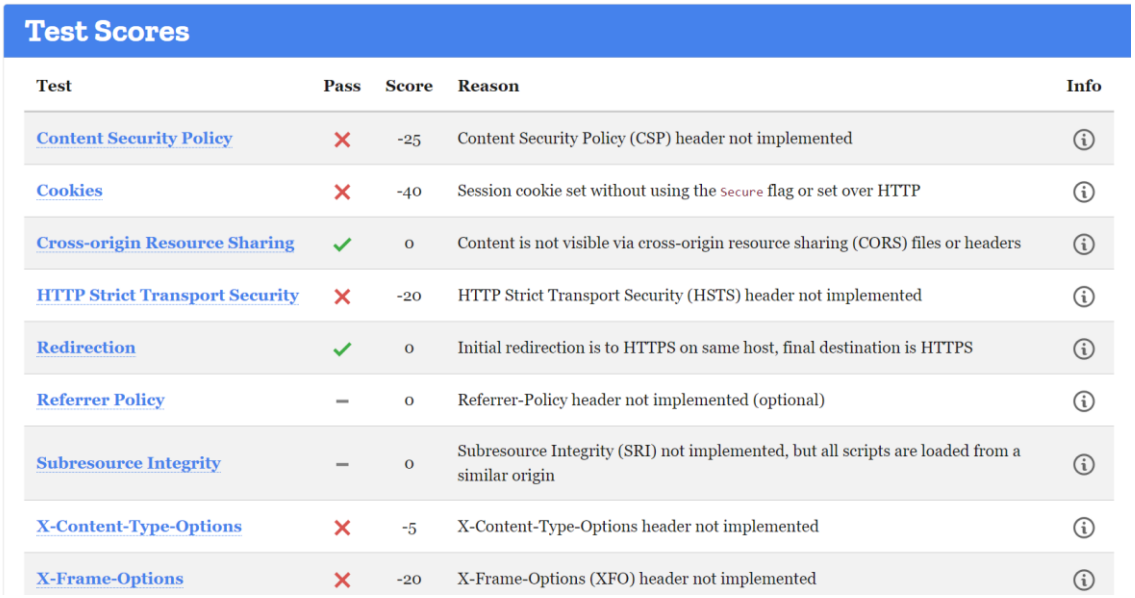
Ayuda a los propietarios de sitios a verificar la seguridad con validaciones de encabezados OWASP, prácticas TLS y pruebas de terceros como son SSL Labs, *High-Tech Bridge*, *Security Headers, HSTS Preload*, entre otros.

Figura 23. Escaneo realizado del escáner Online Observatory



Fuente: elaboración propia

Figura 24. Resultados arrojados en el escáner Online Observatory



Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✗	-40	Session cookie set without using the `Secure` flag or set over HTTP	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ

Fuente: elaboración propia

Resultado de la prueba:

En la figura 23 se presenta el escaneo en la plataforma Observatory con la URL de la institución donde llego a la calificación de F que es extremadamente inseguro y vulnerable (Observatory, 2024) según utilizan una escala de calificaciones que va desde A+ (excelente y seguro) hasta F (extremadamente inseguro y vulnerable), en la figura 24 muestra las vulnerabilidades con las que cuenta la plataforma. Los errores mencionados se refieren a falta de seguridad como se indica en la tabla x, así como indica un nivel de riesgo alto.

Tabla 9. Identificación de tabla de riesgos de la plataforma Observatory

Vulnerabilidad	**definición**
Content Security Policy (CSP)	Falta de implementación del encabezado CSP
Cookies	Cookies de sesión se establecen sin usar la bandera *Secure* o se configuran a través de HTTP, expuesto a ataques.
HTTP Strict Transport Security (HSTS)	Falta de implementación del encabezado HSTS
X-Content-Type-Options	Falta de implementación del encabezado *X-Content-Type-Options*
X-Frame-Options	Falta de implementación del encabezado *X-Frame-Options*

Fuente: elaboración propia

Nivel de riesgo: 4 (Alto)

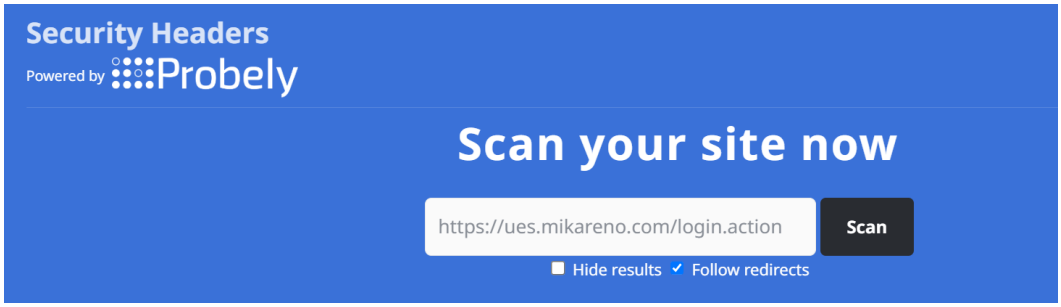
Prevención:

La seguridad informática se ha convertido en una preocupación primordial según Aharonov (2024) para empresas de todos los tamaños, la creciente sofisticación de los ataques cibernéticos exige una estrategia integral que proteja los activos digitales y minimice los riesgos de seguridad como la implementación *de Content Security Policy* (CSP) reduce los ataques XSS al limitar qué recursos pueden cargarse desde otras fuentes, así como configurar correctamente el *'Secure' Flag* en las *cookies* protege las sesiones de usuario contra la interceptación en redes inseguras, otra de las prevenciones para prevenir la vulnerabilidad es Activar HTTP *Strict Transport Security* (HSTS) que impide que los navegadores accedan al sitio a través de conexiones no seguras, además, como en las otras pruebas junto con las herramientas lo que predomina aquí son los fallos del encabezado los encabezados *X-Content-Type-Options* y *X-Frame-Options* evitan la ejecución de contenido malicioso y protegen contra ataques de *clickjacking*.

9. *Security Headers Powered by Probely*

Plataforma en línea diseñada para ayudar a las organizaciones a mejorar la seguridad de sus aplicaciones web.

Figura 25. Escáner Online Probely



Fuente: elaboración propia

Figura 26. Escaneo que arroja el resumen del informe de seguridad en la plataforma Online Probely

Fuente: elaboración propia

Resultado de la prueba:

En la figura 25 se presenta el escáner de la plataforma *Probley* con la URL de la institución donde llego a la calificación de F que es mala, en la figura 26 se observa las vulnerabilidades con las que cuenta la plataforma. Los errores mencionados se refieren a la ausencia de estos encabezados HTTP como se indica en la siguiente tabla 10, que aumenta vulnerabilidades potenciales del sitio web, indica un nivel de riesgo alto.

Tabla 10. Identificación de Encabezado faltante y su definición

Encabezado faltante	**Definición**
Estricto transporte de seguridad	Falta de implementación del encabezado HSTS, sirve para forzar a los navegadores a usar solo conexiones HTTPS.
Política de seguridad de contenidos	Falta de implementación del encabezado CSP, sirve para prevenir ataques como XSS.
X-Frame-Options	Falta de implementación del encabezado *X-Frame*, sirve para proteger contra ataques de clickjacking.
X-Contenido tipo opciones	Falta de implementación del encabezado *X-Content*, sirve para prevenir ataques de tipo MIME.
Referencia Política	Controla la información que se envía en el encabezado Referer.
Permiso Político	Controla las funciones y APIs disponibles en el navegador.

Fuente: elaboración propia

Nivel de riesgo: 4 (Alto)

Prevención:

En la siguiente tabla se mostrará los detalles que muestran los encabezados faltantes y cómo prevenir su vulnerabilidad, para ello un experto en seguridad y desarrollador web británico (Helme, 2024) da unas breves respuestas de cómo abordarlas:

Tabla 11. Identificación de Encabezado y su prevención

Encabezado faltante	**Como prevenir**
Strict-Transport-Security	*HTTP Strict Transport Security* (HSTS) refuerza TLS y obliga al uso de HTTPS.
Content-Security-Policy	La Política de seguridad de contenido (CSP) protege contra XSS, permitiendo solo recursos aprobados.
X-Frame-Options	*X-Frame-Options* decide si permitir el enmarcado del sitio para prevenir el clickjacking.
X-Content-Type-Options	*X-Content-Type-Options* evita que el navegador adivine el tipo MIME.
Referrer-Policy	Referrer Policy controla la información enviada con enlaces salientes.
Permissions-Policy	Política de permisos controla características y API permitidas en el navegador.

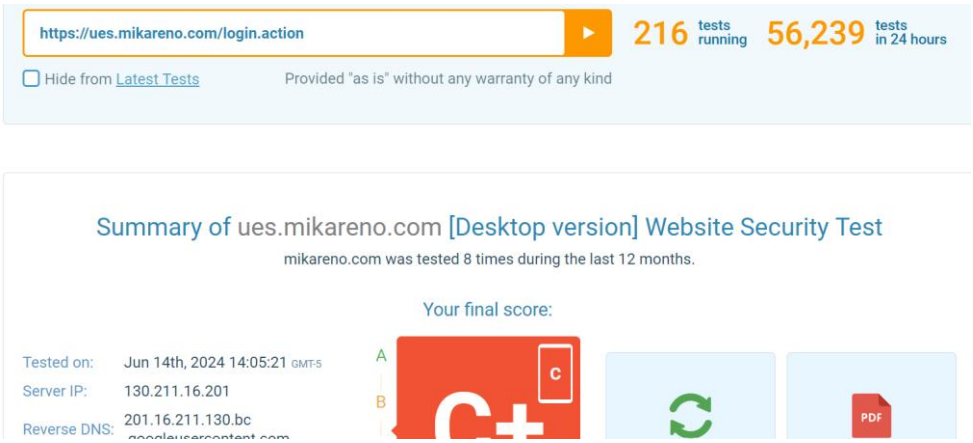
Fuente: elaboración propia

10. *ImmuniWeb*

Verifica que su sitio cumpla con las siguientes normas:

- Cumplimiento de PCI DSS y GDPR.
- Encabezados HTTP, incluyendo CSP (Content Security Policy).
- Pruebas específicas de CMS para sitios WordPress y Drupal.
- Identificación de vulnerabilidades en bibliotecas front-end.

Figura 27. Escáner online ImmuniWeb con informe de seguridad



Fuente: elaboración propia

Figura 28. Escaneo con Informe de subdominios descubiertos en el escáner online ImmuniWeb

Discovered Subdomains

Hostname	Protocol/Port	Certificate(s)	Tested on	Compliances	Grad
admisiones.mikareno.com	HTTP / 80	Not tested yet	Not tested yet	–	–
admisiones.mikareno.com	HTTPS / 443	The RSA certificate is valid till Aug 17th 2024	Not tested yet	–	–
planificaciones.mikareno.com	HTTP / 80	Not tested yet	Not tested yet	–	–
planificaciones.mikareno.com	HTTPS / 443	The RSA certificate is valid till Aug 13th 2024	Not tested yet	–	–

Fuente: elaboración propia

Resultado de la prueba

En la figura 27 se presenta el escáner de la plataforma *ImmuniWeb* donde llego a la calificación de C que es adecuado según (ImmuniWeb, 2024) las calificaciones de ImmuniWeb se expresan en una escala de letras, similar a la educativa: A (Excelente), B (Bueno), C (Adecuado), D (Deficiente) y F (Fallido), en la figura 28 se observa los subdominios descubiertos en la plataforma. Los errores mencionados se refieren a que los subdominios que operan en el puerto 80 no están cifrados y el puerto 443 son válidos hasta agosto de 2024, pero no se han realizado pruebas completas, cuenta con un nivel de riesgo bajo.

Nivel de riesgo: 2 (Bajo)

Prevención:

Para garantizar la seguridad de la comunicación web y la protección de los datos como menciona Apache (2024) es esencial establecer redirecciones automáticas de HTTP a HTTPS en el servidor web, utilizando redirecciones 301 en servidores como Apache o *Nginx*, o aplicando configuraciones de seguridad adicionales en servicios de alojamiento. Estas evaluaciones deben programarse de forma periódica, manteniendo los certificados actualizados y las configuraciones recomendadas para evitar el uso de cifrados obsoletos.

Tercera fase: Clasificación de vulnerabilidades dentro del OWASP top 10

Se han considerado para las pruebas las herramientas en base a la revisión bibliográfica, tomando en consideración aquellas herramientas gratuitas que permiten identificar las vulnerabilidades más frecuentes que menciona el OWASP Top 10, se basó en tal clasificación, refleja las últimas tendencias en ciberseguridad y proporciona un listado actualizado de las 10 vulnerabilidades más comunes y peligrosas que se pueden dar a nivel de la web, lo cual es tomado como referencia por varios autores expertos en ciberseguridad y a partir de ello se pueden generar buenas prácticas que permitan estar alertas ante los desafíos de la seguridad.

Para evaluar la seguridad de las aplicaciones web de la institución, se han utilizado diversas herramientas que identifican posibles vulnerabilidades. La siguiente tabla muestra estas vulnerabilidades y las clasifica según las categorías del OWASP Top 10. Esto facilita la comprensión de su importancia a nivel global.

Tabla 12. Herramientas utilizadas junto a sus vulnerabilidades que se encuentran dentro de la categoría del OWASP Top 10

Herramienta Especializada	**Vulnerabilidad**	**Dentro de la categoría OWASP Top 10**
OWASP ZAP	• Ausencia de *tokens anti CSRF* • Falta de configuración de la cabecera CSP • Ausencia de cabeceras *anti-clickjacking*	• *A5: Broken Access Control* • *A6: Security Misconfiguration* • *A08:2021 - Software and Data Integrity Failures* (CSRF)
Nikto	• Falta de encabezado *Strict-Transport-Security* (HSTS) • *Cookie JSESSIONID* sin el atributo *Secure* • Falta de	• *A6: Security Misconfiguration*

	encabezado *X-Content-Type-Options*	
Uniscan	• Ejecución remota de comandos • Inclusión de archivos locales • Inyección SQL	• *A1: Injection*
Qualys	• Vulnerabilidades de cifrados TLS	• *A03:2021 - Cryptographic Failures*
HostedScan Security	• *Cookies* sin el atributo *Secure* • Vulnerable *cipher suites* para HTTPS	• *A03:2021 - Cryptographic Failures* • *A05:2021 - Security Misconfiguration*
Observatory	• Falta de *Content Security Policy* (CSP) • Falta de *HTTP Strict Transport Security* (HSTS) • Falta de *X-Frame-Options*	• *A05:2021 - Security Misconfiguration*
Security Headers Powered by Probely	• Falta de encabezado *Strict-Transport-Security* (HSTS) • Falta de *X-Frame-Options* • Falta de *X-Content-Type-Options*	• A05:2021 - Security Misconfiguration
ImmuniWeb	• Subdominios no cifrados en puerto 80	• *A06:2021 - Vulnerable and Outdated Components*

Fuente: elaboración propia

La identificación de estas vulnerabilidades a través de diversas herramientas ayuda

a corroborar la necesidad de abordar los problemas de seguridad en las aplicaciones web, la clasificación según el OWASP Top 10 ayuda a priorizar las acciones correctivas dentro de la plataforma educativa para sus mejoras.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE INVESTIGACIÓN

3.1. Resultados

Resultados de las pruebas con herramientas especializadas

En la siguiente tabla se muestra la validación de resultados a partir de las pruebas de detección de vulnerabilidades realizadas con herramientas especializadas. Se detalla cada vulnerabilidad detectada, su descripción, la herramienta utilizada para su identificación y el nivel de riesgo asociado, lo que permite una rápida referencia y priorización de las acciones necesarias para mitigar los riesgos identificados.

Tabla 13. Resultados de las pruebas

Herramienta de Detección	**Vulnerabilidad**	**Descripción**	**Nivel de Riesgo**
OWASP ZAP	Vulnerabilidad 1: Ausencia de Protecciones contra CSRF, CSP y *Anti-Clickjacking*	Falta de *tokens anti-*CSRF, configuración de CSP y medidas *anti-clickjacking*. Estas debilidades permiten ataques como peticiones maliciosas e inyección de código.	medio
Nikto	Vulnerabilidad 2: Falta de Encabezado Estricta-Seguridad-del-Transporte (HSTS)	Ausencia de la cabecera HSTS y otras configuraciones incorrectas que podrían comprometer la seguridad de las conexiones HTTPS.	Alto
Uniscan	Vulnerabilidad 3: Inyección SQL y Ejecución Remota de Comandos	Inyección SQL, ejecución remota de comandos y exposición de archivos, representando un riesgo alto para la integridad del sistema.	Alto

Qualys	Vulnerabilidad 4: Errores en el uso de cifrado TLS	Errores en la configuración, incluyendo el uso de cifrados TLS vulnerables y debilidades en estándares como SHA-1.	Alto
HostedScan Security	Vulnerabilidad 5: Configuraciones de Seguridad Vulnerables	Marcas de tiempo TCP inseguras, cifrados SSL/TLS vulnerables y protocolos de cifrado obsoletos. Configuraciones incorrectas aumentan los riesgos de seguridad de la aplicación.	Alto
Observatory y Security Headers Powered by Probely	Vulnerabilidad 6: Políticas de Seguridad Inadecuadas	Ausencia de políticas de seguridad adecuadas como HSTS, CSP, X-*Frame-Options y X-Content-Type-Options*. Estas deficiencias exponen la aplicación a diversos tipos de ataques.	Medio
ImmuniWeb	Vulnerabilidad 7: Errores en Subdominios y Configuraciones de Seguridad	Subdominios operando en el puerto 80 no cifrados y certificados de seguridad caducados. Aunque el riesgo es bajo, es importante actualizar las configuraciones.	Bajo

Fuente: elaboración propia

Recomendaciones en aspectos de seguridad

En la tabla 14 se especifican algunas recomendaciones importantes para tener en cuenta a partir de las vulnerabilidades detectadas con las diferentes herramientas. Esto ayuda a proporcionar a la institución educativa pautas a considerar para evitar posibles ataques que pudieran comprometer la seguridad de la información.

Tabla 14. Aspectos de seguridad frente a sus vulnerabilidades

Herramientas Especializadas	**Vulnerabilidades**	**Recomendaciones de seguridad**
OWASP ZAP	• Ausencia de *tokens anti* CSRF • Falta de configuración de la cabecera CSP • Ausencia de cabeceras *anti-clickjacking*	• Implementar *tokens anti-CSRF* en todos los formularios para evitar ataques de falsificación de solicitudes entre sitios. • Configurar la cabecera *Content Security Policy* (CSP) para definir fuentes de contenido permitidas y prevenir ataques XSS.
Nikto	• Falta de encabezado Strict-Transport-Security (HSTS) • *Cookie JSESSIONID* sin el atributo *Secure* • Falta de encabezado *X-Content-Type-Options*	• Implementar el encabezado Strict-Transport-Security (HSTS) para asegurar que todas las comunicaciones se realicen a través de HTTPS. • Poner en seguro las *cookies* tengan el atributo Secure para protegerlas durante las transmisiones en redes no seguras.
Uniscan	• Ejecución remota de comandos • Inclusión de archivos locales • Inyección SQL	• Utilizar parámetros para prevenir la ejecución remota de comandos. • Implementar medidas de seguridad de archivos locales y la inyección SQL.

Qualys	• Vulnerabilidades de cifrados TLS	• Actualizar y configurar correctamente los cifrados TLS. • Deshabilitar protocolos obsoletos y vulnerables como SSLv3.
HostedScan Security	• Cookies sin el atributo *Secure* • Vulnerable *cipher suites* para HTTPS	• Configurar todas las *cookies* con el atributo Secure para protegerlas. • Actualizar la configuración de HTTPS para evitar el uso de *suites* vulnerables.
Observatory	• Falta de Content *Security Policy* (CSP) • Falta de HTTP *Strict Transport Security* (HSTS) • Falta de *X-Frame-Options*	• Implementar política de Content *Security Policy* (CSP) adecuada para prevenir ataques de inyección. • Configurar el encabezado HTTP *Strict Transport Security* para garantizar el uso de HTTPS.
Security Headers Powered by Probely	• Falta de encabezado *Strict-Transport-Security* (HSTS) • Falta *de X-Frame-Options* • Falta de *X-Content-Type-Options*	• Implementar el encabezado *Strict-Transport-Security* (HSTS) para forzar conexiones HTTPS. • Añadir el encabezado *X-Frame-Options* para prevenir ataques de *clickjacking.*

ImmuniWeb	• • • Subdominios no cifrados en puerto 80	• • Implementar redirecciones automáticas de HTTP a HTTPS para todos los subdominios.

Fuente: elaboración propia

Se destaca la importancia de mantener actualizados los sistemas y aplicaciones, así como la necesidad de implementar configuraciones de seguridad adecuadas para reducir los riesgos potenciales a la página web de la institución educativa.

Se detallan los resultados completos de la evaluación de seguridad, incluyendo las vulnerabilidades identificadas en las dependencias y las recomendaciones para su corrección. Las herramientas utilizadas: *OWASP ZAP, Nikto, Uniscan, Qualys, HostedScan Security, Observatory, Security Headers Powered by Probely e ImmuniWeb,* ayudaron a evaluar exhaustivamente la postura de seguridad de la plataforma educativa.

CONCLUSIONES

- Se fundamenta teóricamente los aspectos de ciberseguridad: la protección de datos y seguridad digital en una plataforma educativa mediante el uso de herramientas especializadas, lo cual permitió identificar vulnerabilidades potenciales que podrían comprometer la integridad, confidencialidad y disponibilidad de la información alojada en el sitio web de la institución educativa.

- Se revisó literatura referente a las fases de la metodología OWASP, las mismas que guiaron la aplicación de las herramientas especializadas para el desarrollo de la investigación.

- Aplicando la metodología se pudo diagnosticar la plataforma aplicable para evaluar el nivel de seguridad de la plataforma educativa. Este proceso permitió identificar vulnerabilidades potenciales y puntos críticos de mejora en la infraestructura y políticas de seguridad implementadas, así como también facilitó la recolección de datos relevantes para entender mejor los riesgos asociados con el manejo de información. Los resultados obtenidos son fundamentales para las recomendaciones a la institución de las mejoras futuras.

- Se analizaron las vulnerabilidades de la plataforma educativa, utilizando herramientas especializadas, y se identificó el nivel de riesgo al que se expone la misma. Este proceso reveló posibles accesos no autorizados, debilidades en la gestión de accesos y deficiencias en las políticas de seguridad y protección de datos. Como resultado, se formularon recomendaciones para fortalecer la seguridad de la plataforma y mejorar su integridad y protección frente a amenazas cibernéticas.

RECOMENDACIONES

- En vista que los temas de ciberseguridad se actualizan constantemente y cada vez aparecen nuevos tipos de ataques, se recomienda estar actualizados los conocimientos en herramientas especializadas para la detección del nivel de riesgo de plataformas educativas, que ayuden en la prevención de futuros ataques.

- Para la evaluación de nivel de seguridad de las plataformas educativas se debe adoptar una metodología aplicable que permita utilizar herramientas especializadas de forma periódica para identificar y corregir vulnerabilidades, asegurando la protección constante de datos sensibles de la institución.

- Se recomienda realizar las diferentes pruebas mediante herramientas especializadas, de forma periódica de tal manera que se puedan prevenir y mitigar riesgos, proporcionando un entorno seguro a todos quienes hagan uso de la plataforma educativa y tomar como base los resultados para a futuro implementar en la institución educativa las políticas de seguridad de la información, principalmente centrados en ofrecer una plataforma tecnológica educativa, que brinde las medidas preventivas para proteger la información personal y académica.

BIBLIOGRAFÍA

Aguilar, L. J. (2011). *Introducción. Estado del arte de la ciberseguridad. Cuadernos de estrategia,.* Obtenido de https://n9.cl/743zg

Aguirre, M. F. (2018). Obtenido de https://n9.cl/sqy8n

Aharonov, B. (20 de 01 de 2024). *Medium*. Obtenido de Cómo minimizar los riesgos en seguridad informática: https://n9.cl/jmlr8

Apache. (2024). *Redirecting and Remapping with mod_rewrite*. Obtenido de https://httpd.apache.org/docs/2.4/rewrite/remapping.html

Arrillo, J. J. (2019). *Ciberseguridad y su aplicación en las Instituciones de Educación Superior.* Obtenido de https://n9.cl/0hd9j

Balaguer, M. L. (2020). *Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos ya la intimidad.* Obtenido de https://n9.cl/ain1d

Browsing, G. S. (2005). *Hacer la información worldans seguro accesible.* Obtenido de https://safebrowsing.google.com/

Carrillo, M. V. (2021). *Plataformas Educativas y herramientas digitales para el aprendizaje.* Obtenido de https://n9.cl/5uqkr

Carrillo, M. V. (2021). *Plataformas Educativasy herramientas digitalespara el aprendizaje.* Obtenido de https://n9.cl/5uqkr

Carvaca Orrala, A. L. (2022). *“Análisis de seguridad controlado en aplicaciones web de una institucion financiera.* Obtenido de https://n9.cl/nfh3o

Carvaca, A. (2022). *Análisis de seguridad controlado en aplicaciones web de una institución financiera utilizando herramientas de ciberseguridad y buenas prácticas de OWASP.* Obtenido de https://n9.cl/nfh3o

Csirt. (07 de 10 de 2022). *Servicios y herramientas de ciberseguridad gratuitos.* Obtenido de https://www.csirt-epn.edu.ec/como-tener/331-servicios-y-herramientas-de-ciberseguridad-gratuitos

Echaiz, J. &. (2009). *Seguridad en entornos virtuales.* Obtenido de https://n9.cl/aqybe0

García, A. A. (2019). *Ciberseguridad:¿ Por qué es importante para todos?.* Mexico: Editores México.

Garcia, P. A. (08 de 02 de 2023). *Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura.* Obtenido de https://n9.cl/4qfij

Garcia, S. (2022). *Ciberseguridad y protección de datos en el entorno digital*. Obtenido de https://uvadoc.uva.es/handle/10324/63452

Giant, N. (2016). *Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones .* Madrid: Narcea Ediciones.

Gonzalez, V. (2020). *Estudio de los ataques contra website. OWASP.* Obtenido de https://n9.cl/8jq9d

Guillermo, R. (2021). *EL USO DE LA IA PARA CIBERSEGURIDAD.* Obtenido de https://revistas.rcaap.pt/uiips/article/view/26214/19289

Helme. (2024). *Scott Helme*. Obtenido de https://scotthelme.co.uk/

Helme, S. (24 de 03 de 2015). *Hardening your HTTP response headers*. Obtenido de https://scotthelme.co.uk/hardening-your-http-response-headers/

Hernández, L. (2021). Obtenido de https://n9.cl/tmzec

Hernández, L. (2021). *La importancia del uso de las Plataformas Educativas.* Obtenido de https://n9.cl/tmzec

ImmuniWeb. (2024). Obtenido de https://www.immuniweb.com/websec/

Keith, J. (10 de 04 de 2018). *Salir de Línea*. Obtenido de https://alistapart.com/article/going-offline/

Laínez, S. X. (2023). *Estudio de técnicas de ciberseguridad aplicado al desarrollo de aplicaciones web mediante el uso de la herramienta Damn Vulnerable Web Application DVWA.* Obtenido de https://repositorio.upse.edu.ec/handle/46000/9277

León, J. Á. (2021). *Ciberseguridad y protección de datos personales en el Perú.* Obtenido de https://n9.cl/xpz598

Machuca Vivar, S. A. (2022). *Habeas data y protección de datos personales en la gestión de las bases de datos.* Obtenido de https://n9.cl/vwqnkl

Marulanda Aguirre, M. F. (2018). *Aplicacion de la metodologia de pruebas OWASP para el mejoramiento de la seguridad en el sistema e-commerce siembraviva. com.* Obtenido de https://n9.cl/sqy8n

Mendoza, S. H. (2020). *Técnicas e instrumentos de recolección de datos. Boletín científico de las ciencias económico administrativas del ICEA.* Obtenido de https://n9.cl/x22k6

Moragues, F. R. (2020). *Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos ya la intimidad.* Obtenido de https://n9.cl/ain1d

Nist. (20 de 09 de 2022). *NATIONAL VULNERABILITY DATABASE*. Obtenido de https://nvd.nist.gov/

NIST. (2024). *https://www.nist.gov/search?s=Perfect+Forward+Secrecy*. Obtenido de https://www.nist.gov/

Observatory. (2024). Obtenido de https://observatory.mozilla.org/analyze/ues.mikareno.com

Ortega Candel, J. O. (2021). *Ciberseguridad. Manual práctico.* SANTIAGO DE COMPOSTELA: Ediciones Paraninfo, SA.

Ortega, J. C. (2022). *Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP.* Obtenido de https://n9.cl/v1yuq

Owasp. (2017). *DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES*. Obtenido de https://n9.cl/wikgn

Owasp. (2021). *OWASP Top 10:2021.* Obtenido de https://owasp.org/Top10/es/

OWASP. (2024). *Explore the world*. Obtenido de https://owasp.org/

Perero, G. (2022). *Análisis e implantación de técnicas y herramientas de ethical hacking para la Ciberseguridad.* Obtenido de https://n9.cl/ku2zf

Pérez, M. M. (2015). *El derecho fundamental a la protección de datos. Su contenido esencial. Nuevas Politicas Públicas: anuario multidisciplinar para la modernización de las administraciones Públicas.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=1396395

Quirumbay Yagual, D. I. (2022). *Una revisión del aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE.* Obtenido de https://n9.cl/o7hm5q

Ramírez, J. (Diciembre de 2023). *Retorno a la presencialidad en colegios públicos costarricenses: Opiniones del estudiantado y del profesorado.* Obtenido de https://n9.cl/csjy9

Raúl Efraín Serna Martínez, C. G. (26 de 12 de 2021). *Plataformas educativas: herramientas digitales de mediación de aprendizajes.* Obtenido de https://n9.cl/hptfy

Reyes, L. y. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio. [Documentary research for the ontological understanding of the object of study].* Obtenido de https://n9.cl/toc1

Roca, M. M. (2021). *Entrevistas en profundidad a docentes sobre el uso de contenido audiovisual infantil en las aulas. Comunicación & Métodos.* Obtenido de https://n9.cl/2z60y

Rojas, J. A. (2018). *Vulnerabilidades de aplicaciones web según owasp.* Obtenido de https://n9.cl/mj9zu

Rubio, G. (2021). *El uso de la IA para ciberseguridad. .* Obtenido de https://revistas.rcaap.pt/uiips/article/view/26214/19289

Saltzer. (1974). *The Protection of Information in Computer Systems*. Obtenido de https://www.cs.virginia.edu/~evans/cs551/saltzer/

Santiso, H. K. (2016). *seguridad en entornos de educación virtual.* Obtenido de https://n9.cl/5qqj8

Suárez, I. A. (Diciembre de 2022). *Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web.* Obtenido de https://n9.cl/juhgk

Viñas, M. (2021). *Plataformas educativas en el nivel superior en contexto de emergencia sanitaria por el COVID-19.* Obtenido de https://n9.cl/nuy03

Zambrano, K. B. (2022). *Vulnerabilidades en los sistemas informáticos owasp top 10: revisión bibliográfica: Vulnerabilities in computer systems owasp top 10: bibliographic review. Journal Business Science-ISSN: 2737-615X, 3.* Obtenido de https://revistas.uleam.edu.ec/index.php/business_science/article/view/221/308

ANEXOS

Anexo 1. Entrevista al encargado de la página Web

Cuestionario de preguntas para la entrevista al encargado de la página web

Pregunta 1. ¿Cuáles son las principales vulnerabilidades que podrían existir en una plataforma educativa en línea y cómo las aborda?

Pregunta 2. ¿Qué medidas de seguridad específicas se implementan actualmente en la plataforma educativa para proteger los datos de los usuarios?

Pregunta 3. ¿conoce que metodologías se aplican para la gestión de la seguridad de la información en la plataforma educativas?

Pregunta 4. ¿Cómo se gestionan las actualizaciones de seguridad y los parches de software en la plataforma para mantenerla protegida contra nuevas amenazas?

Pregunta 5. ¿Qué procedimientos se tiene en marcha para detectar y responder a posibles incidentes de seguridad cibernética en la plataforma educativa?

Pregunta 6. ¿Qué herramienta o herramientas ha utilizado para detectar vulnerabilidades en la plataforma educativa?

Pregunta 7. ¿Se han detectado amenazas o ataques dentro de la plataforma educativa en los últimos 6 meses?

Anexo 2. Entrevista a autoridades de la institución

Cuestionario de preguntas para la entrevista al Vicerrector de la institución y Gerente administrativo

Pregunta 1. ¿Qué entiende sobre ciberseguridad y cómo afecta a las instituciones educativas?

Pregunta 2. ¿Cómo describiría la importancia de la ciberseguridad en el entorno educativo actual?

Pregunta 3. ¿Qué riesgos específicos de seguridad cibernética considera más relevantes para una institución educativa?

Pregunta 4. ¿Ha oído hablar de incidentes de seguridad cibernética que hayan afectado a otras instituciones educativas?

Pregunta 5. ¿Cuáles son algunos de los desafíos comunes que enfrentan las instituciones educativas en términos de ciberseguridad y cómo podría abordarse?

Pregunta 6. ¿Qué debería conocer como institución para proteger la información y mejorar la seguridad cibernética?

Pregunta 7. ¿Qué iniciativas o políticas recomendaría implementar para mejorar la concienciación sobre seguridad cibernética entre los miembros de la comunidad educativa de su institución?