UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Ciberseguridad en sitios web: auditoría de seguridad de una plataforma en línea

Website cybersecurity: security audit of an online platform

Autores

**** Juan Andres Jaramillo Barreiro***
jjaramillo26@utmachala.edu.ec

Joseph Camilo Reyes Sacaquirin
jreyes16@utmachala.edu.ec

Nancy Magaly Loja Mora
nmloja@utmachala.edu.ec

Universidad Técnica de Machala, Facultad de Ingeniería Civil, Machala, El Oro, Ecuador.
*Autor para correspondencia

Comó citar el artículo:
Jaramillo Barreiro, J.A., Reyes Sacaquirin, J.C. & Loja Mora, N.M. (2025). Ciberseguridad en sitios web: auditoría de seguridad de una plataforma en línea. *Informática y Sistemas, 9*(1), 93–103. https://doi.org/10.33936/isrtic.v9i1.7466

Enviado: 17/04/2025
Aceptado: 02/06/2025
Publicado: 09/06/2025

Resumen

Vivimos en un mundo digital cada vez más dependiente de plataformas en línea donde garantizar la seguridad se ha convertido en una de las grandes dificultades del día a día. Este trabajo muestra los resultados obtenidos de una auditoría de ciberseguridad sobre una plataforma web bajo este marco OWASP como marco de referencia técnico. En el análisis realizado se ha hecho énfasis en dos clases distintas de problemas: la configuración incorrecta de seguridad y los errores cometidos en la autenticación e identificación de los usuarios. En el proceso de evaluación realizado se detectaron una serie de vulnerabilidades destacada como pueden ser las cookies inseguras, los puertos abiertos con servicios sensibles expuestos o, la ausencia de autenticación multi-factor (MFA), entre otras. Si bien no se logró llevar a cabo la explotación de todas las vulnerabilidades detectadas debido a la existencia de mecanismos defensivos activos los hallazgos realizados permitieron proponer medidas de mitigación prácticas y aplicables. El estudio es capaz de validar como el marco OWASP se muestra útil para auditorías en la práctica y hace hincapié en que, a pesar de que ciertas técnicas informáticas limitan la transferencia de una serie de ataques, éstas no son capaces de sustituir la corrección de las configuraciones inseguras. Destacando también que se debe entender la ciberseguridad como un proceso cíclico y adaptativo. Estos resultados son de especial valía para organizaciones con escasos recursos, ya que ofrecen vías de trabajo aplicables para mejorar su postura de ciberseguridad a través de auditorías estructuradas y defensa en profundidad.

Palabras clave: Ciberseguridad; OWASP; Auditoría de seguridad; Vulnerabilidades.

Abstract

We live in an increasingly digital world that is highly dependent on online platforms, where ensuring security has become one of the major challenges of daily life. This paper presents the results of a cybersecurity audit conducted on a web platform using the OWASP framework as a technical reference. The analysis focused on two distinct categories of issues: misconfigured security settings and errors in user authentication and identification. During the evaluation process, several vulnerabilities were identified, including insecure cookies, exposed open ports with sensitive services, and the absence of multi-factor authentication (MFA), among others. Although it was not possible to exploit all detected vulnerabilities due to the presence of active defensive mechanisms, the findings allowed for the proposal of practical and applicable mitigation measures. The study demonstrates that the OWASP framework is effective in real-world audits and emphasizes that while certain technical barriers may limit the success of specific attacks, they cannot replace the correction of insecure configurations. It also highlights the importance of understanding cybersecurity as a continuous and adaptive process. These results are particularly valuable for organizations with limited resources, as they provide actionable strategies to improve their cybersecurity posture through structured audits and defense-in-depth approaches.

Keywords: Cybersecurity; OWASP; Security audit; Vulnerabilities.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

En nuestra sociedad actual, la conectividad universal ha impactado significativamente la forma de acceder a servicios y trabajar, así como también la manera de comunicarse. Las plataformas en línea han permitido mejorar estos procesos, pero por otro lado también han expuesto tanto a organizaciones como a individuos, a diferentes tipos de ciberamenazas que incluyen el secuestro de datos (ransomware), la suplantación de identidad (phishing), la inyección de código perjudicial (Guaña-Moya et al., 2022). Estos tipos de ciberamenazas que afectan directamente a la privacidad, a la integridad y a la disponibilidad de la información son un problema tanto para personas como para empresas (Altamirano et al., 2024). Por lo cual se ha vuelto un tema altamente priorizado en el ámbito mundial, en particular para sectores como la educación, la economía y los servicios públicos (Teins y Andrade-Love, 2024).

Pero para muchas organizaciones, y sobre todo en Latinoamérica, la falta de recursos económicos, la falta de conocimiento en la materia o la falta de un marco legal terminan por asfixiar cualquier posible estrategia sobre ciberseguridad (Ávila Niño, 2023; Decenzin-Martinez, 2024). En el Ecuador, por ejemplo, los ataques de phishing son muy frecuentes, se encuentran entre las primeras posiciones de la región, lo que manifiesta la necesidad urgente de establecer medidas de defensa cibernética y de erradicar la cibercriminalidad (Broncano y Heaviness, 2021; Pérez, 2022).

Este trabajo se centra precisamente en el problema referido a la implementación de la seguridad cibernética en plataformas web, y concretamente en aquellas utilizadas para el comercio electrónico, que están continuamente expuestas a actos perpetrados por ciberdelincuentes que llevan a considerables pérdidas económicas y a importantes daños en la reputación (Flores-Alava y Mena-Hernández, 2023; Uceda et al., 2024).

El éxito en la defensa contra este tipo de amenazas no solo depende de contar con tecnología avanzada, sino que también debe contemplar políticas educativas que sensibilicen y capaciten a los usuarios finales (Muñoz, 2024; Ospina Díaz y Sanabria Rangel, 2024). En el marco de esto, aunque la inteligencia artificial trae consigo muchos beneficios a la hora de detectar amenazas, también resulta útil para los atacantes que encuentran en esta una manera de automatizar ataques como el phishing avanzado y la suplantación de identidad (He et al., 2023; Dolores y Rendón, 2024).

El estudio se encamina a encontrar las vulnerabilidades más relevantes dentro de plataformas web y define técnicas de prevención y respuesta a partir de recomendaciones de uso internacionalmente reconocidas, las propuestas por OWASP (García y Pesantez, 2023; Parales et al., 2021). Es importante incluir las buenas prácticas en este tipo de situaciones, como son las pruebas de penetración (pentesting) y el análisis de explotación de vulnerabilidades, ya que estas permiten anticipar y contener posibles ataques, mejorando así los mecanismos de defensa (Nagata Bolivar et al., 2021; Ontiveros et al., 2024).

Es importante, sin embargo, no quedarse solo en un conocimiento práctico sobre los tipos de ataque; debe incluirse cómo se generan, qué métodos se emplean y qué puntos concretos de los desarrollos resulta más rentable explotar (Bermúdez-Bermúdez, 2024; Reyes et al., 2023). La progresiva evolución de la tecnología, incluyendo inteligencia artificial y deep learning, ha hecho que los métodos de ataque sean cada vez más sofisticados (Rivera et al., 2022), lo que requiere que las organizaciones se adapten a un entorno de amenazas cada vez en mayor evolución y peligro.

Sectores como el comercio y financiero, que tramitan información sensible y llevan a cabo operaciones críticas usando plataformas digitales, son especialmente vulnerables (García-Rojas et al., 2023; Vanegas Pineda y Ávila Quiceno, 2023). Ante esto, el análisis de casos concretos y la experiencia derivada de situaciones previas son prácticas necesarias para implementar soluciones integradoras donde se conjuguen tecnología, formación y marcos normativos en una actuación de ciberseguridad desde una perspectiva de integración.

De este modo, el objeto de este análisis es la identificación de las principales vulnerabilidades que son puestas de relieve por los ciberdelincuentes a partir de plataformas web, así como las soluciones tecnológicas y las políticas existentes con el fin de mitigar los riesgos derivados de aquellas. Esto se traduce en la pregunta de investigación central de este trabajo: ¿de qué forma, a partir de la identificación de vulnerabilidades, se puede fortalecer la seguridad de las plataformas web?

A raíz de que las amenazas evolutivas son cada vez más complejas, se hace evidente que herramientas tradicionales de defensa como los sistemas de detección y prevención de intrusos (IDS/IPS) y los firewalls no son suficientes para hacer frente a ellas (Capellino y Virgili, 2024; Hernández Domínguez y García, 2021).

En este sentido, en este trabajo se presentará un caso de auditoría de seguridad de aplicaciones web, un análisis en las vulnerabilidades detectadas y en las soluciones que se han implementado para corregirlas. Se persigue un objetivo general que no solo conlleva la necesidad de gestionar eficazmente el riesgo de un ciberataque sino que, además, construya los cimientos para desarrollar soluciones más robustas.

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

2. Materiales y Métodos

La metodología utilizada para la auditoría de seguridad en la plataforma de la aplicación web se encuentra estructurada siguiendo el estándar OWASP, un marco de evaluación de aplicaciones web reconocido internacionalmente. Esta estructura proporciona la oportunidad de ir llevando a cabo sistemáticamente las diferentes etapas del proceso de auditoría garantizando recubrimientos completos y profesionales respecto a las vulnerabilidades ya identificadas; su análisis y reducción de forma sistemática (Supriadi et al., 2024).

En este trabajo, la auditoría a partir de esta vulnerabilidad se basa en la configuración de seguridad incorrecta y error de identificación y autenticación, que son las dos críticas o críticas de OWASP.

• Configuración de seguridad incorrecta: está vulnerabilidad trata los errores de configuración que tiene la plataforma y por lo tanto pueden exponer información sensible, permitir características innecesarias o tener rutas críticas disponibles. Su análisis incluirá una revisión de los títulos de seguridad, la configuración del servidor y las políticas de acceso, proporcionando posibles puntos de exposición y recomendaciones de configuración para poder mitigar la seguridad (Supriadi et al., 2024).

• Errores de identificación y autenticación: se evaluará la resistencia de los mecanismos de autenticación y de gestión de sesiones para poder determinar si tienen carencias que pueden poner en peligro la identidad del usuario. La auditoría evaluará aspectos como la complejidad de la acreditación, la introducción de medidas de seguridad, como la autenticación multimodal, y la salida de sesión correcta (Supriadi et al., 2024).

A continuación, se detallan las fases específicas de la metodología que se utilizará, justificando de esta forma su importancia en el contexto de la auditoría de seguridad.

Figura 1. Fases de la Auditoría de Seguridad aplicando la Metodología OWASP.
Fuente: Los autores, basados en el estudio de Escobar Ávila y Rojas Amado (2021).

Planificación y Preparación

La figura 2 representa los pasos más relevantes que se producen en la etapa de planificación y preparación de la auditoría de seguridad, la cual es fundamental para sentar unas bases sólidas. En esta fase, se procederá a definir el ámbito de la auditoría y los objetivos, lo cual nos lleva a estipular que el análisis se va a centrar en la búsqueda de configuraciones incorrectas

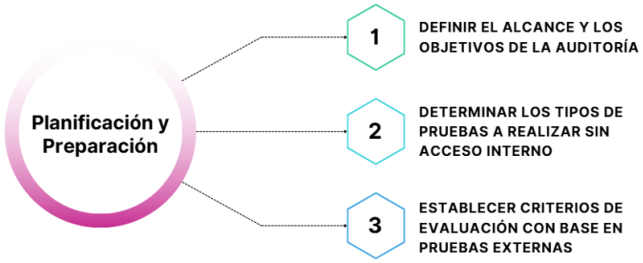

Figura 2. Actividades de la fase Planificación y Preparación.
Fuente: Los autores.

de seguridad y errores a la hora de identificar y confirmar la plataforma en línea.

Se elaborarán aspectos críticos activos para la evaluación como la configuración del servidor, los encabezados de seguridad, la gestión de sesiones o mecanismos de autenticación. También se seleccionarán los métodos más adecuados para analizar esta vulnerabilidad que nos permite asegurar un método estructurado, que identifica correctamente los riesgos.

Se procediendo a comprobar que las herramientas que se van a usar en las siguientes fases de la auditoría están actualizadas y con las que la infraestructura de la plataforma es compatible y funcionando correctamente durante la auditoría. En esta fase en particular, no se tiene en cuenta el rendimiento de las pruebas, sino que se orienta hacia la preparación de la estrategia para que determinados recursos y métodos puedan ser usados de una forma eficiente en el análisis de seguridad posterior.

Recolección de Información

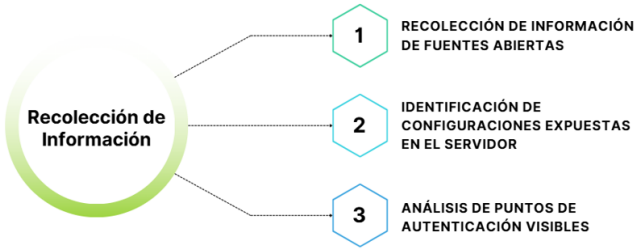

Figura 3. Actividades de la fase Recolección de Información..
Fuente: Los autores.

En la figura 3 se representará la fase correspondiente a la plataforma objetivo, es decir, el reconocimiento correspondiente a identificar las vulnerabilidades que tengan que ver con los mecanismos empleados por la aplicación web para la configuración y autenticación. En esta fase se emplearán técnicas para obtener información pública, tal como pueden ser direcciones IP, dominios, registros DNS y configuraciones de servidores, para poder detectar errores que puedan comprometer la seguridad de las infraestructuras que soportan dicha plataforma.Se espera que herramientas como WHOIS y NSLookup puedan comprobar el registro del dominio y la configuración del sistema DNS, lo que nos vendrá a mostrar ataques asociados a la administración

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

de un dominio y su resolución. Y, a su vez, estas herramientas nos pueden dar información clave de los servidores asociados al dominio (direcciones IP que posteriormente se analizarán).

Además, se utilizará NMAP para escanear puertos y servicios activos, ya que ello permitirá detectar posibles puertos abiertos (22 SSH, 80 HTTP, 443 HTTPS y demás) para descubrir si dichos puertos exponen algún servicio vulnerable. Se utilizará Shodan para identificar recursos públicos expuestos en internet mediante escaneos de puertos. Esto ayudará a dar contexto a los riesgos externos relacionados con la infraestructura tecnológica analizada. La información obtenida con estas herramientas será posteriormente utilizada en el análisis de vulnerabilidades con el que se podrá analizar la presencia de encabezados de seguridad HTTP mal configurados, exposición de información sensible, políticas de manejo de sesiones no seguras, y tokens mal gestionados. Estos resultados servirán como base técnica de propuestas orientadas a mitigar vulnerabilidades que se pudieran encontrar.

Análisis de Vulnerabilidades

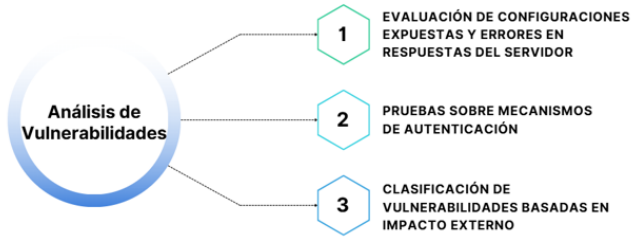

Figura 4. Actividades de la fase Análisis de Vulnerabilidades.
Fuente: Los autores.

En la Figura 4 se muestran las competencias que se ejecutarán en esta fase y que giran en torno a identificar y validar las vulnerabilidades de la plataforma, en especial aquellas que tienen que ver con la configuración y los errores inseguros en la autenticación. Las pruebas automáticas servirán para identificar los errores típicos de la autenticación, como podrían ser encabezados de seguridad mal configurados, permisos mal configurados, la ausencia de configuración de protocolos de autenticación débiles, etc. Pruebas manuales también se hacen prácticas para validar los resultados obtenidos con las pruebas automáticas, así como para explorar el espacio de vulnerabilidades que pueden comprometer la seguridad del sistema. También se analizará la autenticación y gestión de la sesión, evaluando la resistencia de las credenciales, la correcta implementación de la política de seguridad y la posibilidad de reutilizar sesiones. Para este análisis se utilizarán herramientas especializadas que permitan realizar peticiones y capturar las respuestas HTTP, especialmente al estudiar los procesos de autenticación.

Estas pruebas serán la base para localizar agujeros de seguridad y proponer contramedidas adecuadas a las vulnerabilidades identificadas.

Las vulnerabilidades que fueron identificadas en la configuración de las cookies y en los mecanismos de autenticación robusta, parecen verse, aunque sutilmente, reducidas por la presencia de defensas activas introducidas por la plataforma (como son los cortafuegos de perímetro y las limitaciones de escaneos automatizados), lo que muestra que a la hora de evitar la explotación de las posibles vulnerabilidades, la plataforma tiene una clara inclinación a la defensa en profundidad, de acuerdo con el estilo de las prácticas actuales de la seguridad adaptativa.

Explotación de Vulnerabilidades

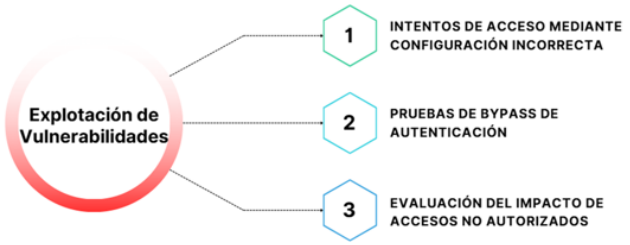

Figura 5. Actividades de la fase Explotación de Vulnerabilidades.
Fuente: Los autores.

La Figura 5 describe las actividades de esta fase, donde se evalúa las vulnerabilidades que se muestran en las pruebas controladas. En el caso de una plataforma en línea, se confirman vulnerabilidades asociadas con configuraciones y errores de seguridad inadecuados en los mecanismos de autenticación para determinar el nivel y el riesgo de su uso. Para evaluar la configuración de seguridad incorrecta, las pruebas controladas se realizan en los titulares de HTTP, y los permisos de acceso para determinar los posibles puntos de exposición que pueden poner en peligro la seguridad del sistema. También se analizarán configuraciones insuficientes en la gestión de sesiones, confirmando si permiten reciclar tokens o sesiones con vencimiento. Las pruebas se realizan en errores de identificación y autenticación para determinar las credenciales débiles y la ausencia de dicho mecanismo de protección, como la autenticación de factores múltiples (MFA). Los ataques controlados se simularán para evaluar la resistencia de los sistemas de autenticación a los intentos de acceso no autorizados que miden el posible impacto en la

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

seguridad de la plataforma. Y eventualmente, se analizarán las dificultades de las vulnerabilidades abiertas y se clasifican de acuerdo con su riesgo e impacto en el nivel de seguridad.

Documentación y Reporte

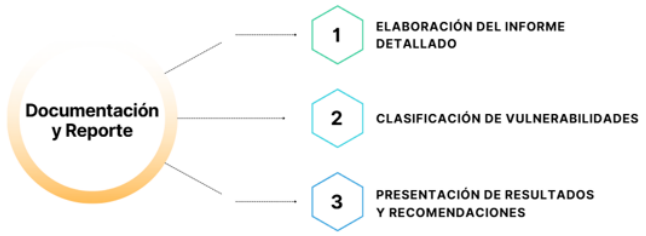

Figura 6. Actividades de la fase Documentación y Reporte. Fuente: Los autores.

La Figura 6 muestra lo que haremos al final de la auditoría, que será principalmente documentar todo lo que encontremos durante la revisión y ofrecer recomendaciones para disminuir los problemas de seguridad que identifiquemos. Prepararemos un informe completo para organizar bien los resultados. En cuanto a la seguridad que no esté bien configurada y los errores en cómo se identifica y se permite el acceso a los usuarios, determinaremos qué tan serios son estos problemas. Además, incluiremos todos los resultados en un informe, que contendrá la información que reunamos y los puntos débiles que encontremos. Proporcionaremos indicaciones para mejorar la configuración de seguridad y fortalecer los mecanismos de autenticación, para que sea menos probable que alguien se aproveche de los posibles problemas que se encuentren.

3. Resultados y Discusión

Planificación y Preparación

El ámbito de actuación del presente informe relativo a la auditoría de la seguridad se considera centrado en realizar la evaluación de la plataforma web desde un ámbito externo sin acceso interno al sistema. El análisis del dominio principal y de los subdominios se conducen para identificar y determinar configuraciones o errores difíciles de detectar en los mecanismos de autenticación y en los mecanismos de manejo de sesiones. El proceso de auditoría se informatizó a partir de la recogida de datos públicos y, para ello, se aplicaron técnicas OSINT, como quienes o el escaneado del dominio y el análisis de los puertos abiertos. Asimismo se evalúa la seguridad del servidor web revisando los encabezados HTTP, las políticas de seguridad y la verificación de los accesos.

El análisis se realizó en dos puntos muy importantes e interesantes como son errónea configuración de la seguridad; analizando cabeceras HTTP, políticas de seguridad web, archivos sensibles que pueden estar expuestos. Así como las fallas de Identificación y autenticación; analizando mecanismos de acceso, gestión de sesiones, políticas de control de credenciales.

Este alcance ha sido definido de un modo que permite proporcionar una primera aproximación a la seguridad de la plataforma desde un punto de vista externo e identificar qué puntos podrían estar expuestos y potencialmente comprometer la integridad o privacidad de los usuarios.

Los objetivos de esta auditoría son:

• Detectar configuraciones que no son válidas en la seguridad del servidor web, analizando encabezados HTTP, políticas de seguridad web, archivos sensibles que pueden estar en exposición.

• Detectar servicios y accesos que estén en exposición en la plataforma, analizando subdominios, puertos expuestos, o configuraciones DNS que pueden estar en la exposición.

• Detectar exposición pública de la información de autenticación, analizando credenciales pasadas por fuentes públicas utilizando OSINT o configuraciones mal protegidas.

Recolección de Información

Tabla 1. Resultados de la Fase de Recolección de Información.

Fuente: Los autores.

Herramienta	Hallazgos
NSLOOKUP	Servidor: dnsclt2.satnet.net Address: 200.25.144.1 Nombre: *******.com Address: 35.168.186.56
SUBLIST3R	www. *******.com aprendizaje. *******.com av. *******.com marketing. *******.com
HACKERTARGET	142.44.169.68 200.31.27.123 209.59.163.169
NMAP	**Puertos abiertos:** • 22/tcp: SSH • 80/tcp: HTTP • 443/tcp: HTTPS • 587/tcp: SMTP **Servicios detectados:** • Apache HTTP Server en puertos 80 y 443.
ANYMAILFINDER	atorres@*******.com jflores@*******.com dbasurto@*******.com

Análisis de Vulnerabilidades

Durante esta etapa se empezaron a detectar y validar las vulnerabilidades que posee la plataforma web a través de la combinación de herramientas automáticas con pruebas manuales. El análisis se realizó de forma selectiva a las categorías de Configuración de Seguridad Incorrecta y Fallas en la Identificación y Autenticación, y se han seguido los criterios del marco OWASP.

Se han empezado a utilizar herramientas como Nmap, Recon-NG, Sublist3r y WPScan, no obstante WPScan ha presentado ciertos problemas operativos como consecuencia de mecanismos

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

de protección anti-escaneo, lo cual ha llevado a la combinación con técnicas manuales.

Los principales hallazgos fueron los siguientes:

Explotación de Vulnerabilidades

no permitiendo obtener resultados de un primer análisis. Pese a que se volvió a realizar el análisis y se comunicó a WPScan que esta vez se ejecutaba mediante el protocolo HTTP, fue muy curioso que el programa comunicase que en este servidor no existía la aplicación WordPress. Este aspecto quedó refutado al

Tabla 2. Vulnerabilidades encontradas.
Fuente: Los autores.

Vulnerabilidad	Descripción
Cookies inseguras en la gestión de sesiones	Al revisar el sitio web, se encontró que algunas cookies no estaban bien protegidas. Una de ellas no tenía una medida de seguridad llamada HttpOnly, lo que permite que códigos maliciosos puedan leerla. También tenían una configuración llamada SameSite: None, que facilita ciertos ataques desde otras páginas. Aunque eran seguras para usar en conexiones protegidas, no se borraban al cerrar sesión, lo cual puede ser riesgoso.
Puertos abiertos con servicios sensibles	Usando una herramienta llamada Nmap, se descubrió que el sitio tenía abiertos varios "puertos" (puertas digitales por donde viaja la información), como el 22, 80, 443 y 587. Si esos puertos no están bien protegidos, pueden ser usados por atacantes para obtener información o intentar ingresar al sistema.
Debilidad en la autenticación	No se encontró el uso de autenticación en dos pasos (como pedir un código al celular), ni otras protecciones extra.

Durante esta fase, se procedió a intentar la explotación de las vulnerabilidades identificadas en la etapa anterior, con el objetivo de evaluar su impacto real sobre la plataforma objetivo. No obstante, los intentos de explotación fueron infructuosos debido a mecanismos de protección activos implementados en el sistema, los cuales bloquearon o limitaron el accionar de las herramientas de prueba utilizadas.

esfuerzo y obtención de resultados manuales de exploración del sitio objetivo que, al contrario, sí indicaban la presencia de las líneas de código que podrían servir para extraer o buscar vectores de explotación.

Este tipo de situaciones apuntan a la existencia de mecanismos activos de protección tendentes a evitar el reconocimiento automatizado del entorno tecnológico: técnicas de anti-fingerprinting o, como en este caso, detección de las respuestas

Tabla 3. Resultados de la Fase de Explotación de Vulnerabilidades.
Fuente: Los autores.

Herramienta	Objetivo	Acción realizada	Resultado	Indicador de protección
WPScan	HTTPS (35.168.186.56)	Escaneo de WordPress (SSL)	Abortado por error de certificado SSL	Rechazo de conexión segura
WPScan	HTTP (35.168.186.56)	Escaneo de WordPress (sin SSL)	Se rechazó identificación de WordPress	Mecanismo anti-fingerprint activo
Metasploit	SMTP - Puerto 587	Ejecutar exploit sobre WordPress	Falló por timeout, puerto inaccesible	Firewall o política de bloqueo de puertos

En una primera fase de explotación se optó por llevar un análisis de vulnerabilidades de la instalación de WordPress usando la herramienta WPScan.

El escaneo se perdió en este momento, ya que el servicio dio errores debido a la validez del certificado SSL del sitio objetivo,

que se obtienen por medio de la interacción con el servidor. Este último tipo de técnicas suelen ser bastante extensivas en cuanto a su utilidad, pues permiten dificultar la tarea de las personas atacantes que intentan el mapeo automatizado de tecnologías empleadas en la plataforma que se quiere atacar, limitando la posibilidad de identificar distintos vectores de ataque.

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

La segunda actividad que se realizó consistió en preparar un entorno de pruebas sobre la plataforma de Metasploit a fin de iniciar ataques controlados sobre aquellos puertos 22 (SSH), 80 (HTTP), 443 (HTTPS) y 587 (SMTP) que ya habían sido identificados como activos en el reconocimiento del entorno de la instalación.

Al llevar a cabo dicha tarea, hubo un intento de conexión al puerto 587, pero el resultado fue que la conexión al puerto 587 resultó fallida (error tipo Rex::ConnectionTimeout); si esto es correcto, se debería estar indicando que el inicio del servicio SMTP que nuestro escáner pensaba consultar podría estar deshabilitado, bloqueado o simplemente protegido por políticas restrictivas de acceso, siempre con la sospecha de estar bajo el control de un firewall perimetral o mediante reglas de control de tráfico de conexión muy restringidas.

Si bien estas barreras limitaron la posibilidad de validar de manera directa el verdadero impacto de las vulnerabilidades observadas, también pusieron de manifiesto que la plataforma contaba con un cierto grado de madurez en relación a las medidas defensivas. Lejos de asimilar estas barreras como vallas técnicas que impedirían la explotación de las vulnerabilidades ya detectadas, estas deberían ser entendidas como reflejo de una cierta madurez tanto en su postura de seguridad activa como reactiva.

El hecho de que estas vulnerabilidades no puedan ser explotadas no significa de ninguna manera que estas no tengan condiciones de riesgo reales, sino que el sistema tiene controles de seguridad suficientemente vigorosos que permitirán una mitigación temporal del riesgo operativo, lo cual se traduce en la utilización de una determinada defensa en profundidad , donde múltiples capas de controles de protección (como controles perimetrales de cortafuegos, detección automática de actividad sospechosa, limitación de escaneos automatizados) permitirán poner en marcha múltiples controles de protección para reducir la superficie de ataque de la que se dispone desde el exterior.

Aun así, también es importante concienciar que estas defensas, aunque funcionen en base al rechazo o mitigación de riesgo en el corto plazo, no suplen la existencia de una corrección de las configuraciones inseguras de base o de mecanismos de autenticación débiles.

Sin embargo, en entornos de recursos limitados, mantener y mejorar estas defensas puede convertirse en una estrategia sencilla y efectiva para elevar el nivel de ciberseguridad general y reducir la probabilidad de ataques automatizados. Por tanto, aquellas defensas observadas son determinantes para comprender que la plataforma tiene una arquitectura reactiva de seguridad, que a pesar de no eliminar vulnerabilidades subyacentes, sí que reduce considerablemente la exposición a amenazas externas.

Ello pone de manifiesto que estrategias proactivas de la corrección y reactivas de contención deben cruzarse, cuando la priorización de la ciberseguridad es reducida.

Documentación y Reporte

Una vez que completamos el trabajo técnico de revisar todo, nos enfocamos en algo crucial: organizar y entender bien todo lo que descubrimos. No nos limitamos a tomar nota de los pasos que dimos, sino que buscamos entender a fondo dónde nuestros intentos de ataque no funcionaron y dónde el sistema demostró ser fuerte y resistió bien.

Documentamos cada cosa que descubrimos en cada paso técnico. Esto incluyó la información básica que recabamos (ver Anexo A.1), la revisión de ajustes de seguridad que no eran seguros y posibles puntos de acceso expuestos (ver Anexo A.2), y las pruebas que realizamos para intentar vulnerar el sistema (ver Anexo A.3).

Durante la primera fase, la exploración inicial, realizamos el descubrimiento de las URLs secundarias públicas y de los registros de internet gracias a los programas de consulta de información WHOIS y Nslookup, que nos ofrecieron una visión de la estructura del dominio (véase Anexo A.1.1).

También comprobamos cuáles eran los puertos abiertos y qué servicios potencialmente vulnerables estaban en funcionamiento (gracias también a Nmap, véase Anexo A.1.3), y Localizamos las distintas direcciones de correo electrónico con las que engañar a la gente (phishing, véase Anexo A.1.4).

Posteriormente, en el momento de analizar la información correspondiente a las debilidades (consúltese el Anexo A.2.1) comprobamos que había configuraciones de seguridad que estaban mal definidas, así como caminos que eran importantes y que eran visibles desde el exterior dado que era fácil acceder, por ejemplo, a él (consúltese el Anexo A.2.2).

En la etapa de intentar entrar al sistema (explotación, ver Anexo A.3), usamos una herramienta llamada WPScan para buscar fallos específicos en la instalación de WordPress.

Pero el escaneo se detuvo dos veces: la primera por un problema con el certificado de seguridad del sitio (SSL, ver Anexo A.3.1), y la segunda porque el servidor actuó como si WordPress no existiera, aunque nosotros habíamos confirmado que sí estaba ahí. Esto nos dice que probablemente tienen defensas activas contra el reconocimiento automático de su sistema.

Propuestas de mitigación

A continuación, se presenta las ideas que salieron de revisar la seguridad de la plataforma. Estas propuestas están pensadas para bajarle el perfil a los riesgos que encontramos durante la auditoría.

4. Conclusiones

La auditoría de seguridad llevó a descubrir configuraciones inseguras y mecanismos de autenticación deficientes en la plataforma sometida a auditoría.

Uno de los resultados más destacados fue la relación que hallamos entre la presencia de vulnerabilidades presentes y la

e-ISNN 2550-6730 | **Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025** | **DOI: 10.33936/isrtic.v9i1.7466**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Tabla 4. Propuestas de mitigación para vulnerabilidades identificadas en la auditoría de seguridad.

Fuente: Los autores.

Vulnerabilidad	Propuesta
Cookies inseguras en la gestión de sesiones	Aconsejamos incluir el atributo HttpOnly con el fin de evitar que las cookies puedan llegar a ser leídas por scripts maliciosos. También debe permitirse que las cookies solo transporten el atributo Secure para ser transmitidas exclusivamente en conexiones cifradas (HTTPS). El atributo SameSite debe establecerse como Strict o Lax para que se detengan ataques CSRF. Por otro lado debe especificarse una caducidad clara y mecanismos de invalidación automática al cerrar sesión.
Puertos abiertos con servicios sensibles	Limitar el tráfico a través del puerto 22 - correspondiente a SSH- a solo aquellas solicitudes provenientes de direcciones IP consideradas como confiables. Utilizar autenticación basada en las claves públicas en vez de la que se basa en contraseñas, así como también cambiar el puerto por defecto. Habilitar o bien utilizar herramientas tales como Fail2Ban con la finalidad de prevenir ataques de fuerza bruta. Redirigir automáticamente el tráfico HTTP (puerto 80) hacia HTTPS (puerto 443) o configurar explícitamente su inutilización si el mismo no es necesario. Para el puerto 587 (SMTP), se recomienda implementar políticas de validación del correo tales como SPF (verifica que el correo se origina desde una IP autorizada), DKIM (añade una firma digital que permite comprobar que el contenido no ha sido modificado) y DMARC (indica como debe proceder la organización al recibir un mensaje que no ha pasado la validación de SPF o DKIM) para así reducir el riesgo de suplantación de identidad y de la llegada de correos no deseados.
Debilidad en la autenticación	Implementar autenticación multifactor (MFA) para agregar una capa extra de seguridad. Asegurarse de que los tokens de sesión no puedan reutilizarse y que expiren correctamente tras cierto tiempo o al cerrar sesión.

imposibilidad de explotarlas debido a controles defensivos en funcionamiento; esto es, a pesar de que la plataforma estudiada no cumple correctamente con las buenas prácticas de seguridad que marcos como OWASP dictan, sí que existen medidas reactivas suficientemente robustas como para ser un contendiente frente a tentativas de ciberataque desde el exterior.

Este hallazgo pone de manifiesto la necesidad de entender la ciberseguridad como un proceso fluido y evolutivo y no como una situación estática.

Una incorrecta puesta a punto estructural de ciertas debilidades puede ser en algún sentido subsanada temporalmente por capas suplementarias de defensa, tales como: firewalls perimetrales, políticas de acceso restrictivas, mecanismos anti-escaneo; pero con la posibilidad latente de que potencialmente estas vulnerabilidades pueden ser aprovechadas bajo diferentes condiciones, especialmente si los atacantes logran irrumpir en el perímetro interno o aplicar métodos de ingeniería social aventajados.

Desde un punto de vista científico, la investigación sirve a la validación empírica de metodologías ad hoc del marco OWASP en entornos reales de producción. Los resultados son indicativos de cómo las herramientas y fases del marco pueden ser utilizadas en la práctica real, hasta el punto de identificar riesgos incluso sobre aquellas plataformas con un nivel relativamente alto de protección.

Se aporta la idea de que, en esos escenarios, los mecanismos defensivos activos pueden actuar como mitigadores, en lugar de ceñirse estrictamente a estrategias preventivas fuertes por sí mismos.

Desde el punto de vista de la aplicabilidad práctica, los resultados son muy relevantes para aquellas organizaciones con recursos limitados, como por ejemplo: países en vías de desarrollo o sectores con poca inversión tecnológica; dado que en estos ámbitos insisto que la priorización de políticas reactivas —tales como: el monitoreo activo, el bloqueo de puertos sensibles y la detección de actividades sospechosas— puede llegar a ser una herramienta válida y económica para incrementar la ciberresiliencia.

El enfoque abordado en la investigación puede ser utilizado como un modelo replicable para aquellas instituciones que desean evaluar su propia exposición real sin comprometer la integridad operativa de sus sistemas.

Por último, más allá del análisis técnico propio, emerge una reflexión crítica: en un mundo donde la sofisticación y frecuencia de los ciberataques es creciente y exponencial, la verdadera fortaleza de una organización no reside únicamente en la infraestructura tecnológica que posee, sino en su capacidad de anticiparse ante el cambio, adaptarse ante el mismo, e incluso mantener una postura activa ante la amenaza cibernética.

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

Contribución de los autores.

Juan Andres Jaramillo Barreiro: Investigación, conceptualización, revisión y edición del artículo. **Joseph Camilo Reyes Sacaquirin:** Redacción-borrador, metodología, revisión y edición del artículo. **Nancy Magaly Loja Mora:** Revisión y edición del artículo.

Conflictos de interés

Los autores. declaran no tener ningún conflicto de interés.

Apéndice o Anexo

Anexo A. Informe detallado de evidencias obtenidas durante la auditoría

A.1 Recolección de Información

A.1.1 WHOIS y NSLOOKUP

Se realizó el análisis con Nslookup y Whois para la recuperación de la propiedad y la estructura del dominio, permitiendo así encontrar el proveedor, la dirección IP y unos datos de contacto asociados.

Resultado: Se detectó que el dominio estaba vinculado a la IP pública 35.168.186.56.

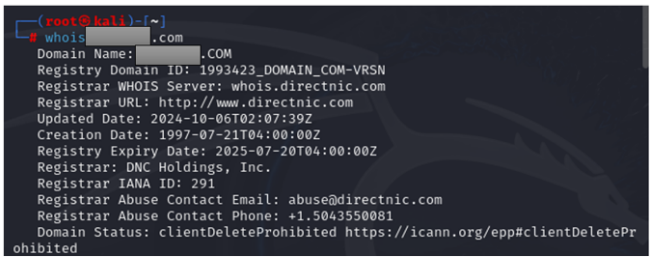

Figura 7. Búsqueda en WHOIS.
Fuente: Los autores.

A.1.2 Subdominios

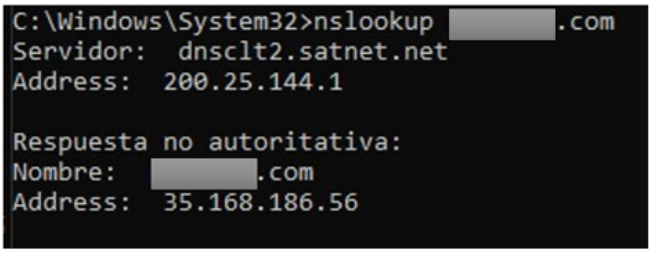

Figura 8. Búsqueda en NSLOOKUP.
Fuente: Los autores.

Con la herramienta de búsqueda de Sublist3r se obtuvieron un número de subdominios públicos del principal, lo que permitió aumentar la superficie a la vista para su análisis.

A.1.3 Puertos y Servicios

Con Nmap, se realizó un escaneo de puertos en el servidor,

Figura 9. Resultados de SUBLIST3R.
Fuente: Los autores.

encontrando servicios activos expuestos al público:

A.1.4 Recolección de Correos Públicos

A través de herramientas como AnyMailFinder, se localizaron

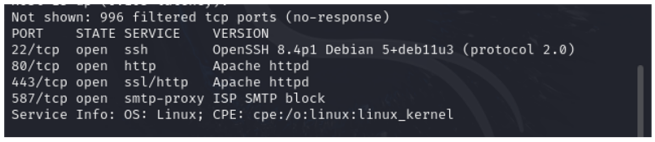

Figura 10. Resultados de NMAP.
Fuente: Los autores.

correos electrónicos pertenecientes al dominio objetivo, lo que podría usarse en ataques dirigidos como phishing o ingeniería social.

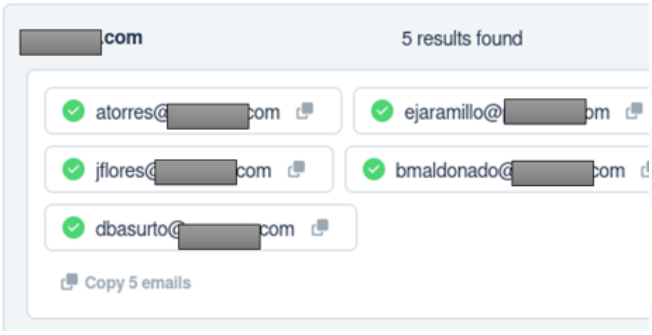

Figura 11. Resultados de ANYMAILFINDER.
Fuente: Los autores.

A.2 Análisis de Vulnerabilidades

A.2.1 Configuraciones inseguras del servidor

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
career4.successfactors.com	/	Session	119	false	true	None	Thu, 20 Mar 2025 15:55:56 GMT
career4.successfactors.com	/	Session	31	true	true	Strict	Thu, 20 Mar 2025 15:56:09 GMT
career4.successfactors.com	/	Session	55	true	true	None	Thu, 20 Mar 2025 15:55:56 GMT
career4.successfactors.com	/	Session	45	true	true	None	Thu, 20 Mar 2025 15:55:56 GMT

Figura 12. Cookies del sitio web.
Fuente: Los autores.

En esta fase se revisaron la seguridad de las cookies.

A.2.2 Rutas interesantes

Con Hackertarget, se analizaron rutas expuestas e información sensible potencial, útil para ataques posteriores si no están bien protegidas.

Figura 13. Resultados de HACKERTARGET.
Fuente: Los autores.

A.3 Explotación de Vulnerabilidades

A.3.1 Intento de escaneo con WPScan

El primer intento con WPScan fue bloqueado por un error con el certificado SSL.

Mensaje: "El escaneo fue abortado debido a un problema con el certificado SSL del sitio objetivo (https://35.168.186.56)."

El segundo intento, usando HTTP, fue rechazado porque WPScan no logró reconocer WordPress, a pesar de que sí estaba instalado.

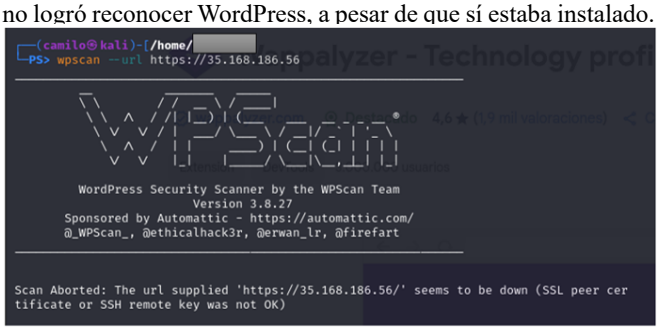

Figura 14. Resultado del Primer intento con WPSCAN.
Fuente: Los autores.

El sitio cuenta con protección activa contra fingerprinting o escaneos automáticos.

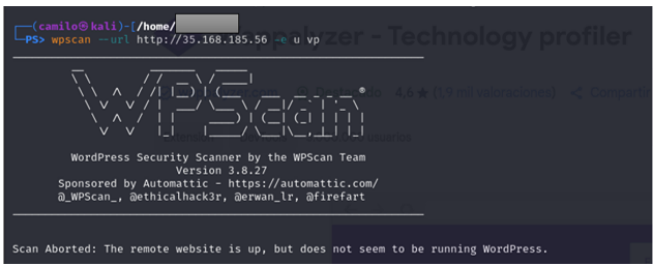

Figura 15. Resultado del segundo intento de WPSCAN.
Fuente: Los autores.

Referencias bibliográficas

Altamirano, C. W. F., Freire, M., Yamba Yugsi, M., & Ureta Arreaga, L. A. (2024). Prevención de ataques ransomware en entidades públicas y privadas en el Ecuador. *Polo del Conocimiento, 9*(8), 2710–2723. https://doi.org/10.23857/pc.v9i8.7850102

e-ISNN 2550-6730 | Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025 | DOI: 10.33936/isrtic.v9i1.7466

Ávila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes, 24*. https://doi.org/10.15517/isucr.v24i49

Bermúdez-Bermúdez, Y. A. (2024). El principio de proporcionalidad como límite de los ciberataques en los conflictos armados internacionales. En Problemas abiertos en torno al principio de proporcionalidad: un análisis desde el DIDH y el DIH (pp. 141–160). Escuela Militar de Cadetes General Jose María Córdova.

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

Escobar Ávila, M. E., & Rojas Amado, J. C. (2021). Beneficios del uso de tecnologías digitales en la auditoría externa: una revisión de la literatura. *Revista Facultad de Ciencias Económicas, 29*(2), 45–65. https://doi.org/10.18359/rfce.5170

García-Rojas, J., Vargas-Vega, T. J., Rodríguez-Aguilar, R., & Landeros-Valenzuela, K. (2023). Tecnología educativa de blockchain para prevenir ciberataques en ITSOEH. *593 Digital Publisher CEIT, 8*(2–1), 136–152. https://doi.org/10.33386/593dp.2023.2-1.1702

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. *Iberian Journal of Information Systems and Technologies*, 87–100.

He, Y., Zamani, E., Yevseyeva, I., & Luo, C. (2023). Artificial intelligence–based ethical hacking for health information systems: Simulation study. *Journal of Medical Internet Research, 25*, e41748. https://doi.org/10.2196/41748

Muñoz, A. B. (2024). Educar y proteger: análisis de la educación en ciberseguridad para combatir la ciberdelincuencia. *Education & Law Review / Revista de Educación y Derecho,* (30), 1–22. https://doi.org/10.1344/REYD2024.30.44082

Nagata Bolivar, T., Alemán Delgado, M. S., Toro Flores, Y. A., & Rivas Almonte, F. U. (2021). Análisis y optimización del proceso de validación de ataques de secuencia de comandos en sitios cruzados (XSS) empleando Burp Suite para evadir medidas de seguridad. *Iberian Journal of Information Systems and Technologies*, 414–432.

Ontiveros, J. M. B., Bailón Estrada, M., Flores Regalado, A., Benítez Guadarrama, J. P., & Cervantes Cardenas, S. A. (2024). Detecciones de vulnerabilidades web a través de la evaluación de pruebas de penetración. *Revista NeyArt, 2*(2), 46–63. https://doi.org/10.61273/NEYART.V2I2.49

Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2024). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*, 199–217.

Pérez, S. B. (2022). Moral hazard situations and misaligned incentives in cybersecurity. *Revista Chilena de Derecho y Tecnología, 11*(2), 103–120. https://doi.org/10.5354/0719-2584.2022.60821

Reyes, D. G., González Brito, H. R., Zulueta Veliz, Y., & Fernández Pérez, Y. (2023). Técnicas de aprendizaje automático para la detección y prevención de amenazas de ciberseguridad. Proyecciones futuras. *Revista Cubana de Ciencias Informáticas, 17*, 15–27.

Rivera, Y., Pinto Mangone, A. D., Castaño, S., Torres Tovio, J. M., Ibarra Hernández, F., & Guevara, P. (2022). Análisis bibliométrico sobre ciberseguridad: técnica de ataque de suplantación de identidad y evolución. *Iberian Journal of Information Systems and Technologies*, 21–35.

Supriadi, D., Suryadi, E., Muslim, R., Samsumar, L. D., & Universitas Teknologi Mataram. (2024). Implementasi vulnerability assessment OWASP (Open Web Application Security Project) pada website Universitas Teknologi Mataram. *Journal of Data Analytics, Information, and Computer Science, 1*(4), 232–240. https://doi.org/10.70248/JDAICS.V1I4.1368

Uceda, M. A. S., Varas Zurita, P. L., & Mendoza De Los Santos, A. C. (2024). Análisis de seguridad de bases de datos: Estrategias para la protección de datos. *Ingeniería: Ciencia, Tecnología e Innovación, 11*(1), 90–103. https://doi.org/10.26495/KZ3KYZ70

Vanegas Pineda, M., & Ávila Quiceno, A. M. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia. *Revista CIES, 14*, 221–241.

Zambrano Rendón, A. D. (2024). Impacto de la inteligencia artificial en los ciberataques. *Revista Científica Sinapsis, 24*(1), 2024–2030. https://doi.org/10.37117/S.V24I1.895

e-ISNN 2550-6730 | **Vol. 9, Núm. 1 (93-103): Enero-Junio, 2025** | **DOI: 10.33936/isrtic.v9i1.7466**