Artículo original

OWASP como marco de referencia para la seguridad informática en el sector azucarero

OWASP as a reference framework for information security in the sugar sector

Luis David Narváez Erazo: Pontificia Universidad Católica del Ecuador Ibarra, Máster en Seguridad Informática,
https://orcid.org/0009-0004-2758-6360

Galo Hernán Puetate Huera: Pontificia Universidad Católica del Ecuador Ibarra, Máster en Diseño y Gestión de Proyectos Tecnológicos,
https://orcid.org/0009-0000-4986-9477

José Luis Ibarra Estévez: Pontificia Universidad Católica del Ecuador Ibarra, Máster en Ingeniería de software y Sistemas Informáticos,
https://orcid.org/0009-0005-3159-4977

Diego Fernando Guerra Olmedo: Pontificia Universidad Católica del Ecuador Ibarra, Ingeniero en Tecnologías de la Información,
https://orcid.org/0009-0004-5300-6542
Autor de correspondencia: ldnarvaez@pucesi.edu.ec

Recibido: 9 septiembre 2025
Publicado: 25 septiembre 2025

DOI: https://doi.org/10.64424/rcu42202591

Resumen:
Este estudio de caso analiza la aplicación de la metodología OWASP como marco de referencia fundamental para fortalecer la seguridad informática en el sector azucarero ecuatoriano, enfocándose específicamente en la empresa IANCEM. El objetivo principal consistió en evaluar la postura de ciberseguridad de sus sistemas informáticos, identificando vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de sus activos digitales críticos. Mediante la utilización de herramientas especializadas como OWASP ZAP, se realizó una evaluación exhaustiva de vulnerabilidades, incluyendo inyección SQL y Cross-Site Scripting (XSS), lo que reveló brechas de seguridad potencialmente explotables por ciberatacantes. A partir de estos hallazgos, se desarrollaron recomendaciones específicas y aplicables, alineadas con las operaciones y regulaciones particulares del sector azucarero. Estas recomendaciones incluyen la implementación de controles de validación más rigurosos y mejoras en las políticas de gestión de riesgos, adaptadas específicamente al contexto del entorno agroindustrial ecuatoriano. El caso de IANCEM demuestra cómo OWASP trasciende su función como estándar técnico para convertirse en un aliado estratégico en el enfrentamiento de amenazas cibernéticas emergentes. Esta investigación no solo contribuye al conocimiento académico en el área de ciberseguridad, sino que también proporciona un modelo metodológico valioso para otras empresas que enfrentan desafíos similares en el campo de la seguridad informática empresarial.

Palabras clave: OWASP, ciberseguridad, sector agroindustrial, vulnerabilidades web, auditoría de seguridad

Abstract:
This case study examines the application of the OWASP methodology as a foundational framework for enhancing cybersecurity in the Ecuadorian sugar sector, with a specific focus on IANCEM. The main objective was to evaluate the cybersecurity posture of its computer systems, identifying vulnerabilities that could compromise the confidentiality, integrity, and availability of its critical digital assets. Using specialized tools such as OWASP ZAP, a comprehensive vulnerability assessment was conducted, including SQL injection and cross-site scripting (XSS), which revealed security gaps that could potentially be exploited by cyberattackers. Based on these findings, specific and applicable recommendations were developed, aligned with the specific operations and regulations of the sugar sector. These recommendations include the implementation of more rigorous validation controls and improvements to risk management policies, specifically tailored to the context of the Ecuadorian agro-industrial environment. The IANCEM case demonstrates how OWASP transcends its role as a technical standard to become a strategic ally in addressing emerging cyber threats. This research not only contributes to academic knowledge in the field of cybersecurity but also provides a valuable methodological model for other companies facing similar challenges in the field of corporate cybersecurity.

Keywords: OWASP, cybersecurity, agribusiness sector, web vulnerabilities, security audit

Como citar la obra: Narváez Erazo, L., D., Puetate Huera, G., H., Ibarra Estévez, J., L. y Guerra Olmedo, D., F. (2025). OWASP como marco de referencia para la seguridad informática en el sector azucarero. *Revista Científica Unanchay*, 4(2), 47-62
doi: https://doi.org/10.64424/rcu42202591

Introducción

En la era digital actual, la ciberseguridad se ha consolidado como un pilar esencial para el éxito y la sostenibilidad de las organizaciones en todos los sectores productivos, transcendiendo su percepción tradicional como un simple componente técnico. La ubicuidad de sistemas informáticos y plataformas en línea ha ampliado considerablemente la superficie de ataque, exponiendo a las empresas a una variedad de amenazas cibernéticas cada vez más sofisticadas (Espinoza, 2020). Este entorno, caracterizado por la interconexión global y la dependencia crítica de la infraestructura digital, demanda un enfoque holístico en la gestión de la seguridad de la información, que abarque desde la protección de los activos más sensibles hasta la creación de una cultura organizacional consciente de los riesgos cibernéticos (Olarte, 2023).

En el sector agroindustrial, la ciberseguridad adquiere una relevancia aún mayor, debido a su rol fundamental en la economía global y la seguridad alimentaria. La agroindustria enfrenta desafíos únicos derivados de la convergencia entre tecnologías operativas (OT) y tecnologías de la información (IT) (Guevara-Vega et al., 2023). El creciente uso de tecnologías como sistemas de control industrial, sensores IoT y plataformas de gestión de datos en la nube ha mejorado la eficiencia y productividad, pero también ha introducido nuevas vulnerabilidades susceptibles de explotación por parte de ciberdelincuentes (Bermúdez et al., 2022). Es notable que la digitalización en este sector amplifica su vulnerabilidad ante ataques cibernéticos, ya que muchos dispositivos conectados carecen de una preparación adecuada en ciberseguridad, convirtiéndose en objetivos atractivos para los atacantes (Berruz, 2022). Las amenazas más comunes incluyen ataques de ransomware dirigidos a empleados, explotación de sistemas de control mal configurados y vulnerabilidades en aplicaciones web obsoletas, con consecuencias que van desde la interrupción operativa hasta la pérdida de datos críticos y el daño reputacional (Sánchez, 2022).

El Ingenio Azucarero del Norte Compañía de Economía Mixta "IANCEM", líder en la comercialización de azúcar en el norte de Ecuador, se encuentra en una encrucijada donde la modernización tecnológica y la ciberseguridad deben alinearse para preservar la integridad de sus operaciones. A pesar de haber actualizado sus instalaciones para optimizar la producción y cumplir con rigurosas normativas ambientales, IANCEM enfrenta vulnerabilidades en la seguridad de sus sistemas informáticos. Es de vital importancia destacar que la falta de validación exhaustiva de las medidas de seguridad implementadas genera un riesgo considerable,

 ISSN: 2953-6707

susceptible de explotación por parte de ciberatacantes, lo que podría comprometer la integridad de los datos y la continuidad operativa (Murillo, 2022).

La presente investigación responde a la necesidad urgente de evaluar y fortalecer la postura de ciberseguridad de IANCEM en el entorno digital actual. El objetivo primordial de este estudio es realizar un análisis exhaustivo de los sistemas informáticos de IANCEM, fundamentándose en la metodología OWASP (Open Web Application Security Project). Esta elección se justifica por el reconocimiento de OWASP como estándar de facto en la industria de la seguridad informática, que ofrece un enfoque actualizado y estructurado para identificar, evaluar y mitigar riesgos de seguridad (Lucas et al., 2023). Esta metodología no solo guiará la detección de vulnerabilidades, sino que también proporcionará un marco para priorizarlas según su impacto potencial y probabilidad de explotación. Para ello, se emplearán herramientas especializadas como OWASP ZAP y Nmap para identificar riesgos y configuraciones incorrectas (Narváez et al., 2018).

El análisis se focalizará en la detección de una amplia gama de vulnerabilidades, destacando aquellas críticas en entornos empresariales similares, tales como inyecciones SQL, ataques de Cross-Site Scripting (XSS), configuraciones inseguras y exposición de datos sensibles. Además, se evaluarán las configuraciones de seguridad de aplicaciones web y la infraestructura de red, buscando identificar posibles vectores de ataque y configuraciones inadecuadas. Este estudio no se limita al descubrimiento de vulnerabilidades; su propósito también incluye categorizar y priorizar estos riesgos en función de su gravedad e impacto potencial en las operaciones de la empresa (Miranda, 2021).

La relevancia de este estudio trasciende un simple análisis de vulnerabilidades, ya que los hallazgos y recomendaciones pueden servir como modelo para otras empresas del sector agroindustrial que enfrentan desafíos similares en la protección de sus activos digitales. Al abordar proactivamente las vulnerabilidades de seguridad, IANCEM no solo reforzará su postura de ciberseguridad, sino que también establecerá un precedente de buenas prácticas en un sector cada vez más tecnificado. El propósito de este esfuerzo es no solo preservar los activos digitales críticos de IANCEM, sino también fomentar una cultura de ciberseguridad proactiva dentro de la organización, contribuyendo a la elevación de los estándares de seguridad en la industria. Al adoptar un enfoque basado en estándares internacionales como OWASP, IANCEM garantizará la protección de sus activos y reafirmará su compromiso con la innovación y la responsabilidad corporativa en la era digital. Esto posicionará a IANCEM no solo como líder en la producción de azúcar, sino también en la adopción de prácticas avanzadas de ciberseguridad en el sector agroindustrial ecuatoriano (Guerra & Narváez, 2025).

 ISSN: 2953-6707

Finalmente, es crucial reconocer que la seguridad no se limita a la infraestructura tecnológica, sino que también comprende la protección de información sensible mediante métodos de encriptación adecuados y la gestión apropiada de identificadores de red. La concienciación y capacitación de los empleados resultan fundamentales para la protección de los activos empresariales. La realización de pruebas de intrusión (ethical hacking) permitirá identificar vulnerabilidades y mejorar la gestión de riesgos, asegurando así una defensa robusta frente a las amenazas cibernéticas (Tejedor et al., 2023).

Metodología

La presente investigación se fundamentó en un enfoque metodológico mixto que combinó la rigurosidad de la metodología OWASP (Open Web Application Security Project) con la flexibilidad y profundidad del análisis cualitativo. Esta combinación estratégica no solo permitió identificar y clasificar las vulnerabilidades en los sistemas informáticos de IANCEM, sino que también proporcionó una comprensión integral del contexto operativo y las implicaciones empresariales asociadas con estas debilidades de seguridad. Este enfoque mixto respondió a la naturaleza compleja de los sistemas de información modernos, los cuales requieren evaluaciones tanto técnicas como organizacionales para asegurar una protección eficiente y completa.

El núcleo de la metodología se centró en la aplicación meticulosa de los principios y directrices de OWASP, reconocido como el estándar de facto en la industria de la seguridad informática. OWASP proporcionó un marco exhaustivo y actualizado para evaluar la seguridad en aplicaciones web, que abarcó desde la identificación de vulnerabilidades hasta la implementación de medidas correctivas. En este análisis, se siguió la OWASP Testing Guide, enfocándose en las vulnerabilidades más comunes del OWASP Top 10, tales como inyecciones SQL, fallos de autenticación, ataques de Cross-Site Scripting (XSS), configuraciones inseguras y el uso de componentes vulnerables (Narváez et al., 2018)

Adicionalmente, se complementó esta metodología con un enfoque cualitativo que permitió contextualizar los hallazgos técnicos y comprender su impacto en los procesos empresariales de IANCEM (Molina & Orozco, 2020). Este enfoque se basó en la recopilación de información a través de diversas fuentes, que incluyeron entrevistas con personal técnico, revisión de documentación interna y observaciones de las prácticas de seguridad implementadas. La integración de este análisis cualitativo enriqueció la investigación, ofreciendo una comprensión más amplia de los factores humanos y organizacionales que influían en la postura de seguridad de IANCEM. Asimismo, facilitó la comprensión de las implicaciones de las

vulnerabilidades en el contexto contexto específico de la empresa, considerando aspectos como la criticidad de los sistemas afectados, el valor de los datos comprometidos y el impacto potencial en la continuidad del negocio.

Descripción Detallada del Proceso

El proceso metodológico de esta investigación se estructuró en varias etapas interrelacionadas, como se ilustra en la figura 1. Proceso de aplicación de OWASP.

Figura 1

Proceso de aplicación de OWASP

a. Planificación y Alcance

En esta etapa inicial, se definieron claramente los objetivos y límites del análisis. El objetivo principal consistió en evaluar exhaustivamente la seguridad de los sistemas informáticos de IANCEM para identificar las vulnerabilidades existentes. El alcance se delimitó a los sistemas en uso dentro de la empresa, excluyendo dispositivos personales y redes externas, pero abarcando aquellos sistemas que gestionaban información crítica en la producción azucarera. También se desarrolló un cronograma de actividades y se asignaron los recursos necesarios para ejecutar la investigación de manera eficiente.

b. Identificación de Activos

La segunda etapa se centró en la identificación y documentación de todos los activos de información en uso en IANCEM. Esto implicó crear un inventario detallado de sistemas informáticos, aplicaciones web, bases de datos y dispositivos de red. Esta identificación resultó crucial para establecer el alcance del análisis y asegurar que no se omitieran componentes críticos del ecosistema tecnológico.

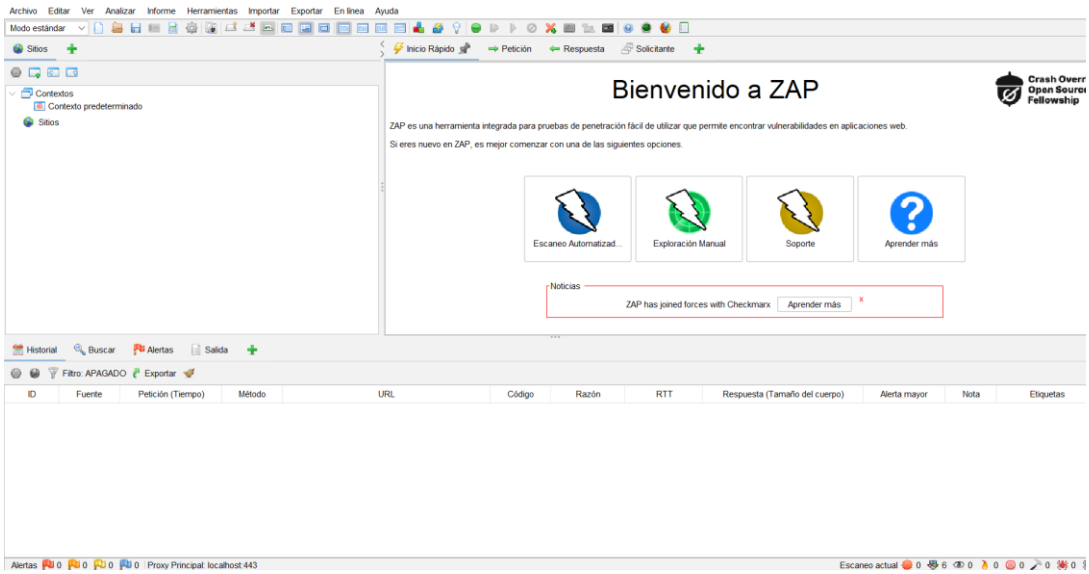
ISSN: 2953-6707

c. Análisis de Vulnerabilidades con OWASP ZAP

En esta fase central se aplicó la metodología OWASP y se utilizó la herramienta OWASP ZAP (Zed Attack Proxy) para detectar vulnerabilidades en los sistemas de IANCEM, cuya interfaz se puede observar en la Figura 2. OWASP ZAP es un proxy de interceptación y escáner de seguridad de código abierto, diseñado específicamente para evaluar la seguridad de aplicaciones web. La herramienta permitió realizar pruebas tanto automatizadas como manuales, abarcando vulnerabilidades como inyecciones SQL, ataques de XSS y fallos en la autenticación (Maniraj et al., 2024). Durante el análisis, se emplearon diversas técnicas: spidering para descubrir páginas y recursos, escaneo activo para detectar vulnerabilidades conocidas, y fuzzing para identificar errores en el manejo de entradas. También se realizaron pruebas manuales para obtener una evaluación más exhaustiva y precisa de la seguridad de los sistemas, complementadas con el uso de la herramienta Nmap para el reconocimiento de red.

Figura 2

Interfaz de OWASP ZAP



d. Evaluación de Riesgos

Una vez identificadas las vulnerabilidades, se evaluaron los riesgos asociados con cada una de ellas. Esta evaluación se basó en clasificaciones de severidad y probabilidad de explotación, considerando tanto el impacto técnico como el empresarial. Se utilizó el marco de OWASP para clasificar la severidad de las vulnerabilidades en críticas, altas, medias y bajas. La probabilidad de explotación se estimó considerando factores como la facilidad de implementación de ataques y la disponibilidad de exploits públicos.

ISSN: 2953-6707

e. Documentación de Vulnerabilidades

En esta etapa, se documentó detalladamente cada vulnerabilidad identificada, incluyendo descripciones precisas, ubicación específica, nivel de severidad y recomendaciones de mitigación. Esta documentación resultó esencial para facilitar la toma de decisiones informadas y permitir la implementación de medidas correctivas efectivas.

f. Acciones Correctivas Propuestas

Basándose en la evaluación de riesgos y la documentación de vulnerabilidades, se propusieron acciones correctivas específicas para fortalecer la seguridad y mitigar los riesgos identificados. Estas acciones se fundamentaron en las mejores prácticas de la industria y se adaptaron al contexto operativo específico de IANCEM.

g. Estrategias de Mitigación

Posteriormente, se desarrollaron estrategias integrales de mitigación, alineadas con las mejores prácticas de seguridad informática y adaptadas a las necesidades específicas de IANCEM. Estas estrategias incluyeron la implementación de firewalls de aplicaciones web, sistemas de detección de intrusiones y programas de concienciación en seguridad, todo con el objetivo de garantizar la protección continua de los activos de información de IANCEM.

Este enfoque metodológico permitió realizar un análisis detallado y sistemático de las vulnerabilidades en los sistemas de IANCEM, identificando riesgos específicos y planteando medidas correctivas para fortalecer su postura de seguridad y asegurar la protección de sus activos digitales. La documentación de los hallazgos se llevó a cabo utilizando las funcionalidades de generación de informes de OWASP ZAP (Maniraj et al., 2024), proporcionando un resumen completo de cada vulnerabilidad, su nivel de severidad y recomendaciones específicas para su mitigación.

Resultados

Tras la aplicación de cada una de las fases de la metodología propuesta, se identificaron diversas vulnerabilidades en los sistemas informáticos de IANCEM. Estas vulnerabilidades fueron clasificadas y priorizadas según su impacto potencial y probabilidad de explotación, siguiendo las directrices de OWASP y considerando tanto aspectos técnicos como empresariales (Zambrano et al., 2022). A continuación, se presenta una síntesis de los hallazgos más relevantes, organizados por nivel de riesgo.

 ISSN: 2953-6707

Tabla 1

Clasificación de Vulnerabilidades por Nivel de Riesgo

Nivel de Riesgo	Vulnerabilidad	Impacto Potencial
Alto	Exposición de Metadatos Sensibles en la Nube	Acceso no autorizado a información confidencial, comprometiendo la confidencialidad e integridad de los datos.
Alto	Ausencia de Cabeceras de Seguridad Críticas	Inyección de código, ataques de Clickjacking, comprometimiento de la integridad de las aplicaciones y datos de usuarios.
Medio	Configuraciones de Seguridad Incorrectas	Inyección de código, ejecución de scripts maliciosos, comprometimiento de la confidencialidad, integridad y disponibilidad.
Bajo	Falta de Encabezado X-Content-Type-Options	Posible ejecución de código malicioso debido a la interpretación incorrecta de archivos.

a. Vulnerabilidades de Alto Riesgo

Exposición de Metadatos Sensibles en la Nube: Se detectó una filtración de metadatos en la infraestructura de nube que podría exponer información sensible de la organización. Esta vulnerabilidad se clasificó como de alto riesgo, dado que existe una posibilidad significativa de que atacantes obtengan acceso no autorizado a información confidencial, comprometiendo tanto la confidencialidad como la integridad de los datos empresariales.

Ausencia de Cabeceras de Seguridad Críticas: La falta de implementación de cabeceras de seguridad como Content Security Policy (CSP) y Anti-Clickjacking expuso las aplicaciones web de IANCEM a riesgos significativos, incluyendo inyección de código y ataques de Clickjacking. Considerando el impacto sustancial que estos ataques podrían tener en la integridad de las aplicaciones y la confidencialidad de los datos de usuarios, esta vulnerabilidad también fue clasificada como de alto riesgo.

b. Vulnerabilidades de Riesgo Medio

Configuraciones de Seguridad Incorrectas: Se identificaron configuraciones de seguridad inadecuadas en varios sistemas que podrían facilitar diversos tipos de ataques, tales como inyección de código o ejecución de scripts maliciosos. Estas configuraciones deficientes incluyeron la falta de validación de entradas, el uso de contraseñas débiles y la exposición innecesaria de servicios de red.

Falta de Encabezado X-Content-Type-Options: La ausencia de este encabezado puede permitir que los navegadores interpreten incorrectamente los tipos de archivos, lo cual podría resultar en la ejecución no intencionada de código malicioso.

c. Vulnerabilidades de Bajo Riesgo

Aplicación Web No Actualizadas: Se identificó que algunos sistemas no utilizaban características de seguridad de aplicaciones web modernas, lo que podría limitar tanto su seguridad como su funcionalidad operativa.

d. Análisis Detallado por Servidor

El análisis presenta un desglose específico de las vulnerabilidades encontradas en cada uno de los servidores evaluados, incluyendo el servidor de nómina, el servidor RP y el servidor de archivos:

- ***Servidor de Archivos:*** Se identificaron vulnerabilidades críticas como la exposición de metadatos en la nube, la falta de la cabecera Content Security Policy (CSP), la ausencia de la cabecera Anti-Clickjacking y la carencia del encabezado X-Content-Type-Options. En la Figura 3 se pueden observar las diferentes vulnerabilidades encontradas en el servidor de archivos, clasificadas por nivel de riesgo.

Figura 3

Vulnerabilidades del servidor de archivos

Alert type	Risk	Count
Metadatos de la Nube Potencialmente Expuestos	Alto	1 (20,0 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	3 (60,0 %)
Falta de cabecera Anti-Clickjacking	Medio	3 (60,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Aplicación Web Moderna	Informativo	3 (60,0 %)
Total		5

- ***Servidor de Nómina:*** Se identificaron servicios activos como SSH y MySQL, además de otros servicios relacionados con la gestión de aplicaciones web ejecutándose en puertos no estándar, los cuales requieren evaluación adicional para garantizar su seguridad operativa (Ver figura 4).

Figura 4

Vulnerabilidad en el Puerto 10000 del Servidor de Nomina

```
PS C:\WINDOWS\system32> nmap -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-18 15:09 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 192.168.1.7
Host is up (0.0026s latency).
Not shown: 65354 filtered tcp ports (no-response), 174 filtered tcp ports (admin-prohibited)
PORT      STATE  SERVICE
22/tcp    open   ssh
3306/tcp  open   mysql
8080/tcp  closed http-proxy
8086/tcp  open   d-s-n
8087/tcp  closed simplifymedia
9090/tcp  closed zeus-admin
10000/tcp open   snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 170.72 seconds
```


ISSN: 2953-6707

- ***Servidor RP:*** Se detectaron servicios esenciales como FTP, Telnet y LDAP, que también requieren evaluación y fortalecimiento de seguridad debido a su naturaleza crítica en la infraestructura (Ver figura 5).

Figura 5

Vulnerabilidades del servidor RP

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	4 (133,3 %)
Falta de cabecera Anti-Clickjacking	Medio	1 (33,3 %)
Falta encabezado X-Content-Type-Options	Bajo	1 (33,3 %)
Total		3

e. Vulnerabilidades Críticas que Amenazan la Privacidad de los Usuarios

Se identificaron vulnerabilidades específicas que podrían comprometer significativamente la privacidad de los usuarios, tales como la falta de protección adecuada de datos personales y la ausencia de controles de acceso robustos. Estas vulnerabilidades podrían permitir que atacantes accedan a información personal sensible de los usuarios, incluyendo nombres, direcciones, números de teléfono y datos financieros. La deficiencia en configuraciones de seguridad adecuadas, como cabeceras de seguridad y protección contra Clickjacking, evidencia la necesidad urgente de adoptar mejores prácticas de seguridad en el desarrollo y mantenimiento de sistemas web (Ver figura 6).

Figura 6

Vulnerabilidades del servidor DNS y Vulnerabilidades del servidor de Base de Datos y Aplicaciones

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	15 (300,0 %)
Falta de cabecera Anti-Clickjacking	Medio	2 (40,0 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	16 (320,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (40,0 %)
Total		5

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	15 (300,0 %)
Falta de cabecera Anti-Clickjacking	Medio	2 (40,0 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	16 (320,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (40,0 %)
Total		5

ISSN: 2953-6707

f. Análisis de las causas y consecuencias

El análisis de las causas subyacentes de las vulnerabilidades identificadas reveló que, en la mayoría de los casos, estas se originaron por la falta de implementación de prácticas de desarrollo seguro, la carencia de actualizaciones regulares de seguridad y la insuficiente concienciación en materia de ciberseguridad. Las consecuencias potenciales podrían ser severas, incluyendo pérdida de datos confidenciales, interrupciones en los servicios críticos, daño significativo a la reputación empresarial y pérdidas económicas considerables.

En síntesis, los resultados de este análisis revelaron la presencia de múltiples vulnerabilidades en los sistemas informáticos de IANCEM, las cuales representan un riesgo significativo para la seguridad de la información y la continuidad operativa de la empresa, como se detalla en la Tabla 2. Es fundamental que IANCEM implemente medidas correctivas inmediatas para mitigar estos riesgos y fortalecer su postura general de ciberseguridad.

Tabla 2

Resumen Cuantitativo por Nivel de Riesgo

Servidor	Alto	Medio	Bajo	Informativo	Riesgo total
Servidor RP	0	2	1	0	3
Servidor de Nómina	1	3	2	0	6
Servidor de Base de Datos y Aplicaciones (Backup)	2	4	2	0	8
Servidor Virtualizado	2	3	3	0	8
Servidor de Archivos	1	2	1	1	5
Servidor DNS	0	2	2	1	5
Active Directory	0	2	2	1	5
	3	6	3	2	14
Servidor Replicado (Esxi)	0	4	3	0	7
Servidor de Cámaras	0	1	2	4	7
Servidor Linux	1	1	3	0	5
Servidor de Aplicaciones Principal	0	2	5	2	9
Severidad Total	**17**	**32**	**29**	**11**	**83**

Discusión

Al contrastar este caso de estudio con investigaciones previas en ciberseguridad, se observa que se distingue por su enfoque específico en el sector agroindustrial ecuatoriano, particularmente en la industria azucarera. Aunque numerosos estudios han abordado las vulnerabilidades en sistemas informáticos y aplicaciones web, pocos han tratado los desafíos específicos que enfrentan las empresas de este sector en el contexto ecuatoriano.

Investigaciones como la de Yacelga (2024) sobre vulnerabilidades en servidores empresariales de Cubosoft y el trabajo de Ruíz (2024) sobre el sistema de inventarios Phoenix de una IPS de primer nivel, utilizan la

 ISSN: 2953-6707

metodología OWASP y el estándar ISO 27001:2022. Estas investigaciones han demostrado la relevancia de las auditorías de seguridad y la aplicación de metodologías estandarizadas para la detección y mitigación de riesgos. Sin embargo, es evidente que estos estudios se realizaron en contextos diferentes y no abordan las especificidades del sector azucarero ecuatoriano.

Este estudio se alinea con la tendencia actual de utilizar metodologías como OWASP para evaluar la seguridad de sistemas informáticos. No obstante, se distingue por su enfoque en un sector específico y en un contexto geográfico particular. Adicionalmente, no solo se identificaron vulnerabilidades, sino que también se propusieron acciones correctivas y estrategias de mitigación adaptadas al contexto operativo específico de IANCEM. Esta investigación presenta relevancia significativa por varios aspectos fundamentales:

- Relevancia para el sector agroindustrial ecuatoriano: El sector agroindustrial constituye un pilar fundamental de la economía nacional, y la seguridad de sus sistemas informáticos resulta crucial para garantizar su competitividad y sostenibilidad a largo plazo. Este estudio proporciona información valiosa sobre las vulnerabilidades que pueden afectar a las empresas de este sector y ofrece recomendaciones prácticas para mejorar su postura de ciberseguridad.
- Contribución al conocimiento académico y científico: Este estudio enriquece el conocimiento existente sobre la aplicación de la metodología OWASP en el contexto de la seguridad informática empresarial. Los resultados obtenidos pueden servir como base metodológica para futuras investigaciones en el sector agroindustrial y en otros sectores de la economía ecuatoriana.
- Implicaciones prácticas para IANCEM: Los hallazgos de esta investigación permitieron a IANCEM implementar medidas correctivas inmediatas para mitigar los riesgos identificados y fortalecer su postura integral de ciberseguridad. La implementación de las soluciones recomendadas mejoró sustancialmente la seguridad organizacional, protegiendo tanto la integridad de los datos como la confianza en los servicios proporcionados a sus stakeholders.
- Promoción de una cultura de ciberseguridad: Al ejecutar este estudio, IANCEM demostró su compromiso proactivo con la seguridad de la información y su disposición a adoptar mejores prácticas en ciberseguridad. Este precedente puede servir de modelo para otras empresas del sector agroindustrial ecuatoriano, fomentando el desarrollo de una cultura de ciberseguridad más robusta en toda la industria.

 ISSN: 2953-6707

Conclusiones

La evaluación de la seguridad de los sistemas informáticos de IANCEM mediante la metodología OWASP y la herramienta OWASP ZAP permitió validar la utilidad de OWASP como marco de referencia esencial para la seguridad informática en el sector azucarero ecuatoriano. No obstante, la efectividad de su implementación radica fundamentalmente en la adopción de buenas prácticas de desarrollo seguro, la priorización de la mitigación de vulnerabilidades de alto riesgo y la adaptación de las estrategias de mitigación al contexto operativo específico de cada organización. En este sentido, se concluyen los siguientes aspectos clave:

- OWASP como Marco de Referencia Fundamental: La aplicación sistemática de los principios y directrices de OWASP permitió identificar y clasificar una amplia gama de vulnerabilidades en los sistemas informáticos de IANCEM, demostrando de manera efectiva su capacidad para mejorar la seguridad en este sector crítico de la economía nacional.
- Déficit en Buenas Prácticas de Desarrollo Seguro: El análisis de las causas subyacentes a las vulnerabilidades identificadas reveló una notable carencia en la implementación de buenas prácticas de desarrollo seguro, así como deficiencias significativas en las actualizaciones de seguridad y la concienciación sobre ciberseguridad. Este hallazgo subraya la necesidad imperativa de que las empresas inviertan en capacitación especializada y adopten prácticas de desarrollo seguras para mitigar efectivamente los riesgos de seguridad.
- Riesgos Críticos Asociados con Vulnerabilidades de Alto Impacto: Se identificaron vulnerabilidades de alto riesgo, tales como la exposición de metadatos sensibles en la infraestructura de nube y la ausencia de cabeceras de seguridad críticas. Estas debilidades estructurales podrían comprometer severamente la confidencialidad, integridad y disponibilidad de la información empresarial. El abordaje prioritario de estas vulnerabilidades resulta fundamental para proteger los activos de información críticos de la organización.
- Relevancia de la Adaptación Contextual de Estrategias de Mitigación: Se desarrollaron estrategias de mitigación integrales, alineadas con las mejores prácticas internacionales de seguridad informática y adaptadas específicamente a las necesidades operativas de IANCEM. Este enfoque enfatiza que la personalización contextual de las estrategias de seguridad es esencial para garantizar su efectividad en el entorno operativo específico de cada organización.

 ISSN: 2953-6707

Adicionalmente, el estudio destaca la importancia crítica de realizar auditorías de seguridad periódicas y de adoptar un enfoque sistemático fundamentado en estándares internacionales para evaluar y mejorar continuamente la seguridad web. Se recomienda implementar cabeceras de seguridad esenciales, como Content Security Policy (CSP) y X-Frame-Options, y asegurar la configuración adecuada de cabeceras de seguridad y validación de entradas en todas las fases del ciclo de vida del desarrollo de software. Asimismo, es fundamental corregir vulnerabilidades específicas como la filtración de metadatos y fortalecer los controles de acceso.

Los resultados de esta investigación presentan implicaciones prácticas significativas para otras empresas del sector azucarero y diversos segmentos de la economía ecuatoriana. Al compartir las experiencias adquiridas y las recomendaciones desarrolladas, se aspira a contribuir sustancialmente a la mejora de la ciberseguridad a nivel nacional. La implementación sistemática de auditorías informáticas se presenta como una estrategia óptima para elevar los estándares de seguridad en los sistemas y redes institucionales del país.

En síntesis, este estudio no solo demuestra la relevancia metodológica de OWASP en el contexto empresarial ecuatoriano, sino que también evidencia la necesidad de un enfoque integral y proactivo hacia la ciberseguridad organizacional. Al adoptar buenas prácticas de desarrollo seguro, priorizar la mitigación de vulnerabilidades de alto riesgo, adaptar las estrategias de mitigación al contexto específico de cada empresa y fomentar una cultura organizacional consciente de los riesgos cibernéticos, las organizaciones pueden proteger efectivamente sus activos digitales críticos y garantizar su sostenibilidad operativa a largo plazo. La protección de metadatos y la capacitación continua del personal constituyen elementos esenciales para establecer una defensa robusta contra las amenazas cibernéticas en constante evolución que caracterizan el panorama digital contemporáneo.

 ISSN: 2953-6707

Referencias

Bermúdez Márquez, G., Caicedo Mateus, M. A., & González Pérez, J. F. (2022). *Análisis de vulnerabilidades en seguridad informática para la infraestructura tecnológica central de un sistema RIS-PACS*. https://hdl.handle.net/20.500.12495/8123

Berruz Gordillo, J. K. (2022). *Vulnerabilidades en el sistema de información en el soporte de inventario del distribuidor mayorista de productos de ferretería ¨ferrequim sa¨* [bachelorThesis, Babahoyo: UTB-FAFI. 2022]. http://dspace.utb.edu.ec/handle/49000/11703

Espinoza Araujo, C. O. (2020). Implementación de Ethical Hacking para mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/47290

Guerra Olmedo, D. F., & Narváez Erazo, L. D. (2025). *Análisis de Vulnerabilidades a los Sistemas Informáticos de la Empresa Ingenio Azucarero del Norte de Compañía de Economía Mixta "IANCEM" Basado en la Metodología OWASP*. https://repositorio.puce.edu.ec/handle/123456789/45467

Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información: Una revisión sistemática. *Revista Científica de Sistemas e Informática*, *3*(1), Article 1. https://doi.org/10.51252/rcsi.v3i1.461

Lucas, G. I. C., Rodríguez, E. L. F., Lucas, N. I. C., & Parrales, W. M. A. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. *Journal TechInnovation*, *2*(2), Article 2. https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

Maniraj, S. P., Ranganathan, C. S., & Sekar, S. (2024). Securing web applications with owasp zap for comprehensive security testing. *International Journal Of Advances In Signal And Image Sciences*, *10*(2), Article 2. https://doi.org/10.29284/ijasis.10.2.2024.12-23

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/20966

Molina Marin, Y., & Orozco Nott, L. G. (2020). *Vulnerabilidades de los Sistemas de Información: Una revisión*. https://dspace.tdea.edu.co/handle/tdea/1398

 ISSN: 2953-6707

Murillo Prado, K. P. (2022). *Analizar la metodología de gestión de vulnerabilidades para mejorar la seguridad en los sistemas informáticos en una institución financiera nacional.* [Thesis, Universidad Cenfotec]. https://repositorio.ucenfotec.ac.cr/handle/123456789/xmlui/handle/123456789/394

Narváez, L. D., Arciniegas, S. M., Guerra, L., & Echeverría, F. R. (2018). OWITest: Penetration test methodology in wireless networks. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E15*, 187-200. Scopus.

Olarte Quispe, P. B. (2023). SEGURIDAD INFORMÁTICA Y LA VULNERABILIDAD DEL SISTEMA DE INFORMACIÓN INALÁMBRICO EN LA MUNICIPALIDAD PROVINCIAL DE LA CONVENCIÓN, PERIODO 2020. *Repositorio institucional - ULP*. https://repositorio.ulp.edu.pe/handle/ULP/49

Ruíz Cortés, R. A., & Ruíz Cortés, J. C. (2024). Análisis de vulnerabilidades en el sistema de inventarios Phoenix en una IPS nivel 1. http://hdl.handle.net/11371/6627

Sánchez Paredes, V. M. (2022). *Políticas de seguridad informática y vulnerabilidades en el sistema para generar citas y pagos de facturación del concesionario Ambacar*. https://repositorio.uta.edu.ec/handle/123456789/35198

Tejedor, B. G. S., Castrellón, H. V., León, E. T. D., & Ayala, D. V. de. (2023). Seguridad de los Sistemas Informáticos Universitarios: : Retos Pendientes. *REICIT*, *2*(2), Article 2.

Yacelga Almeida, J. S. (2024). Análisis de vulnerabilidades en servidores de aplicaciones empresariales mediante técnicas de pentesting utilizando la metodología Owasp y Ptes: Estudio de caso empresa Cubosoft [masterThesis, Universidad Técnica del Norte]. https://repositorio.utn.edu.ec/handle/123456789/16080

Zambrano, K. B. Á., Vidal, W. E. B., & Vera, R. R. T. (2022). Vulnerabilidades en los sistemas informáticos owasp top 10: Revisión bibliográfica. *Journal Business Science - ISSN: 2737-615X*, *3*(2), Article 2. https://doi.org/10.56124/jbs.v3i2.0001

 ISSN: 2953-6707