UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

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

Análisis de Vulnerabilidades en Sistemas Web Públicos de Ecuador bajo OWASP API Security Top 10:2023: Un Caso de Estudio

Vulnerability Analysis in Public Web Systems of Ecuador under OWASP API Security Top 10:2023: A Case Study

Autores

**Jaime Rubén Borja Ulloa*[1]
jborjau@mag.gob.ec

Rodrigo Cadena Martínez[2]
rodrigo.cadena@unade.edu.mx

[1]Universidad Americana de Europa (UNADE), Facultad de Informática, Ecuador, Quito.
[2]Universidad Americana de Europa (UNADE), Departamento de Informática, México, Cancún.

*Autor para correspondencia

Cómo citar el artículo:
Borja Ulloa, J.R. & Cadena Martínez, R. (2026). Análisis de Vulnerabilidades en Sistemas Web Públicos de Ecuador bajo OWASP API Security Top 10:2023: Un Caso de Estudio. *Informática y Sistemas, 10(1)*, 98–109. https://doi.org/10.33936/isrtic.v10i1.8463

Enviado: 26/05/2026
Aceptado: 29/06/2026
Publicado: 30/06/2026

Resumen

La creciente digitalización de los servicios del Estado ecuatoriano expone una superficie de ataque cuya postura de seguridad apenas ha sido evaluada empíricamente en la literatura académica. Este estudio analiza las vulnerabilidades identificables en nueve sitios web del sector público ecuatoriano, basándose en el marco de referencia OWASP API Security Top 10: 2023. En Python 3.12, se ha implementado una herramienta destinada a realizar análisis pasivos y no intrusivos de encabezados HTTP, cookies, configuraciones TLS, código fuente HTML accesible públicamente, así como archivos estándar como robots.txt y security.txt, y puntos finales de API de acceso público. Esta metodología no requiere pruebas de penetración activas, inyección de cargas ni acceso a recursos autenticados, por lo que se lleva a cabo dentro de los límites establecidos por el marco legal correspondiente, en particular el Artículo 232 del Código Orgánico Integral Penal (COIP) del Ecuador. Se identificaron 101 hallazgos, clasificados en cinco categorías según el marco OWASP. La categoría de configuraciones de seguridad incorrectas (API8:2023) constituye el 69,3 % de los resultados, mientras que los hallazgos de severidad alta representan el 20,8 % del total. Nueve portales carecían de los encabezados de seguridad necesarios, y ocho presentaron cookies con flags de seguridad incompletas. Los hallazgos ofrecen evidencia empírica replicable de deficiencias sistémicas en el fortalecimiento del sector público en Ecuador, indicando que intervenciones de bajo costo y alto impacto podrían formalizarse como requisitos mínimos en todos los portales gubernamentales.

Palabras clave: OWASP; seguridad web; portales públicos; análisis pasivo; vulnerabilidades web.

Abstract

The growing digitalization of Ecuadorian state services exposes an attack surface whose security posture has barely been empirically evaluated in academic literature. This study analyzes identifiable vulnerabilities in nine Ecuadorian public sector websites, based on the OWASP API Security Top 10: 2023 framework. We implemented a Python 3.12 tool to perform a passive, non-intrusive analysis of HTTP headers, cookies, TLS configurations, publicly accessible HTML source code, standard files such as robots.txt and security.txt, and publicly accessible API endpoints. Because this methodology requires no active penetration testing, payload injection, or access to authenticated resources, it remains within the boundaries set by the applicable legal framework, specifically Article 232 of Ecuador's Comprehensive Organic Criminal Code (COIP). A total of 101 findings were identified and classified into five OWASP categories. Security Misconfiguration (API8:2023) accounted for 69.3% of the results, and high-severity findings represented 20.8% of the total. Nine portals lacked the necessary security headers, and eight presented cookies with incomplete security flags. The findings provide replicable empirical evidence of systemic hardening deficiencies in Ecuador's public sector, indicating that low-cost, high-impact interventions could be formalized as minimum requirements across all government portals.

Keywords: OWASP; web security; public portals; passive analysis; web 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

La adopción de servicios de gobierno electrónico en Ecuador ha crecido de manera sostenida durante la última década. La plataforma central Gob.ec agrupa varios miles de trámites en línea de instituciones del Estado central, los gobiernos autónomos descentralizados y las entidades de la función ejecutiva. La digitalización abarca procesos que manejan datos personales sensibles, información tributaria, registros vehiculares, datos biométricos y registros académicos. Esta expansión, deseable desde la óptica de eficiencia y cobertura, también amplía la superficie de ataque disponible para actores maliciosos.

La preocupación por la seguridad de los portales gubernamentales no es nueva ni es exclusiva del contexto ecuatoriano. Awoleye et al. (2014) documentaron en un estudio empírico sobre 64 portales gubernamentales nigerianos que aproximadamente un tercio era susceptible a inyección de SQL o cross-site scripting, mientras que dos tercios presentaban enlaces rotos y casi la mitad transmitía credenciales sin cifrar. Weissbacher et al. (2014) realizaron un seguimiento longitudinal de la adopción de Content-Security-Policy en el Alexa Top 1M y mostraron que existe una brecha sostenida entre la velocidad de adopción de cabeceras de seguridad básicas y la de mecanismos más complejos como CSP, cuyo despliegue en modo enforcement era minúsculo. Calzavara et al. (2017) revisaron de manera exhaustiva el panorama de ataques contra sesiones web y concluyeron que la gestión inadecuada de cookies sigue siendo el principal vector de compromiso en aplicaciones modernas.

En el contexto latinoamericano, la transformación digital del Estado ha avanzado más rápido que las capacidades técnicas para asegurarla. Flor-Unda et al. (2023) identificaron como factores predominantes la baja conciencia de ciberseguridad, la ausencia de estándares y el uso de software desactualizado, mientras que Catota et al. (2019) documentaron brechas específicas en la formación profesional y el desarrollo institucional del Ecuador. Pellegrino et al. (2015) muestran que incluso las herramientas avanzadas de análisis dinámico tienen un alcance limitado cuando la instalación carece de controles de seguridad básicos, un requisito previo para que cualquier programa de evaluación sea efectivo y de alto impacto en organizaciones gubernamentales con presupuestos y personal técnico limitados.

En 2023, el Open Web Application Security Project (OWASP) lanzó su actualización API Security Top 10, que resume las amenazas más graves a las interfaces de programación de aplicaciones. Aunque la plataforma se diseñó originalmente para API, sus categorías, especialmente API8:2023 (seguridad mal configurada) y API2:2023 (autenticación rota), aún se aplican a cualquier sistema basado en web que proporcione puntos finales HTTP, administre sesiones de usuarios o maneje datos confidenciales. En general, la utilidad del marco de evaluación del portal en línea ha quedado demostrada en varios estudios empíricos del sector público en países en desarrollo, donde los patrones de vulnerabilidad identificados son similares a pesar de las diferencias contextuales (Awoleye et al., 2014).

Dentro del contexto de Ecuador, los estudios existentes han analizado los aspectos de gobernanza y gestión de la ciberseguridad organizacional. Cuzme et al. (2018) documentaron las vulnerabilidades estructurales del sector público ecuatoriano ante estos incidentes y diseñaron un sistema de gestión de incidentes utilizando los marcos de trabajo ITIL y MAGERIT. Navia y Zambrano-Romero (2021) identificaron una herramienta de prueba para la seguridad de redes de datos técnicas y observaron que aproximadamente el 80% de los ataques pueden mitigarse mediante controles de seguridad fundamentales. El marco legal, junto con datos técnicos reproducibles, ayuda a formular opciones distintas para fortalecer la seguridad. Sin embargo, según el mejor conocimiento del autor, no existe un informe empírico sobre el estado actual de las cabeceras HTTP, cookies, TLS y archivos estándares en el portal de intercambio del gobierno ecuatoriano, que haya sido documentado en una referencia internacional como OWASP.

Esta brecha técnica se inscribe en un marco de gobernanza de la ciberseguridad aún en consolidación. Ecuador cuenta con una Política de Ciberseguridad (Acuerdo Ministerial 006-2021) y con la Estrategia Nacional de Ciberseguridad 2022-2025, aprobada por el Comité Nacional de Ciberseguridad y coordinada por el MINTEL (MINTEL, 2022). La respuesta a incidentes se articula a través del EcuCERT, adscrito a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL); sin embargo, su mandato se circunscribe a los operadores de telecomunicaciones y no abarca de forma integral la red de servicios gubernamentales, una limitación reconocida en la propia Estrategia Nacional. A esta arquitectura se suma la Autoridad de Protección de Datos Personales creada por la Ley Orgánica de Protección de Datos Personales. La ausencia de visibilidad sistemática sobre la configuración de seguridad de los servicios del Estado, señalada como debilidad en la Estrategia, es precisamente el vacío empírico que este estudio busca documentar.

El objetivo de este estudio es abordar la siguiente interrogante: ¿Cuáles son los patrones de vulnerabilidades en los sistemas presentados por los portales web del sector público en Ecuador al ser evaluados en relación con el OWASP API Security Top 10:2023? A partir de la evidencia empírica internacional sobre portales gubernamentales (Awoleye et al., 2014; Buchanan et al., 2018), el estudio contrasta tres hipótesis operativas

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

independientes. H1: más del 50 % de los hallazgos se concentrará en la categoría de configuración insegura (API8:2023). H2: la mayoría de las cookies de sesión presentará flags de seguridad incompletas, por ausencia de Secure, HttpOnly o SameSite. H3: la adopción de cabeceras HTTP de seguridad será deficiente en la totalidad o la mayoría de los sistemas evaluados. Estas hipótesis se contrastan de forma explícita en la sección 3. El objetivo principal es evaluar la seguridad de una muestra representativa de portales en línea del Estado ecuatoriano mediante la determinación de los niveles de atributos críticos de rendimiento, los rangos de severidad observados y las características de posibles vectores de ataque. Como objetivos específicos se establecen: (i) construir una herramienta automatizada de análisis pasivo bajo OWASP API Security Top 10:2023; (ii) aplicarla sobre nueve portales web del sector público ecuatoriano; y (iii) caracterizar los hallazgos en función de severidad, categoría OWASP, vector de ataque, escenario concreto e impacto. El aporte específico del trabajo es la primera caracterización empírica y reproducible de la postura de hardening de portales del Estado ecuatoriano bajo un marco internacional, en un dominio donde la literatura previa ha sido predominantemente normativa.

2. Materiales y Métodos

2.1. Diseño del estudio

El estudio fue diseñado mediante un método de caso transversal y descriptivo, centrado en las plataformas en línea del sector público ecuatoriano que brindan servicios a la ciudadanía. Los datos se recolectaron en mayo de 2026 desde una conexión residencial en Quito (Pichincha). Los portales no aplican restricciones de acceso por ubicación geográfica dentro del Ecuador, por lo que el lugar de recolección no condiciona los resultados ni influyó en los criterios de exclusión aplicados (véase sección 2.2). El diseño metodológico adapta el trabajo de Awoleye et al. (2014) al contexto ecuatoriano.

La elección del OWASP API Security Top 10:2023 responde a tres consideraciones técnicas y se adopta reconociendo de forma explícita su solapamiento parcial con el OWASP Top 10 para aplicaciones web (2021). Primero, los portales analizados no son aplicaciones puramente presentacionales: exponen puntos finales HTTP que gestionan sesiones y transmiten datos personales, y al menos uno referencia de forma explícita un endpoint REST de integración en su código público (módulo 6, véase la sección 3.5). Segundo, para los hallazgos de cabeceras HTTP, cookies y TLS, la categoría API8:2023 (Security Misconfiguration) es conceptualmente equivalente a la categoría A05:2021 del marco web; elegir uno u otro no altera la sustancia de los hallazgos, sino la taxonomía con la que se etiquetan. Se opta por el marco API porque ofrece, para esta superficie concreta, una correspondencia más directa entre cada control verificado y su categoría, y porque alinea la línea base con la arquitectura API-first hacia la que evolucionan los servicios de gobierno electrónico. Tercero, el marco web no se descarta como referencia, pero buena parte de sus categorías solo son verificables con pruebas activas o acceso autenticado, condiciones que esta auditoría excluye por diseño. En síntesis, el marco API se emplea como lente de clasificación coherente y orientada al futuro, sin que ello implique que las debilidades detectadas sean exclusivas de arquitecturas API.

2.2. Selección de la muestra

Los portales se seleccionaron mediante muestreo intencional. Los criterios de inclusión fueron: (i) dominio .gob.ec del Estado central o de entidades autónomas; (ii) oferta de servicios transaccionales o de consulta a la ciudadanía; (iii) flujos que manejan datos personales o financieros. Se excluyeron los portales meramente informativos sin interacción del usuario y los sistemas que devolvieron códigos 5xx o no respondieron dentro del tiempo de espera configurado. De los 15 candidatos evaluados inicialmente, seis no superaron ese último criterio y fueron descartados. Estos seis portales, pertenecientes a cuatro instituciones del gobierno central, devolvieron códigos 5xx o superaron el tiempo de espera durante toda la ventana de medición. Su exclusión obedece a la imposibilidad de obtener respuestas HTTP estables para el análisis pasivo y no a una valoración de su postura de seguridad, ya que durante una medición puntual esos códigos suelen responder a geobloqueo, balanceo de carga o mantenimiento. No obstante, dado que un portal persistentemente indisponible podría reflejar también deficiencias operativas, su omisión introduce un posible sesgo de supervivencia que se discute en la sección 3.8.

Tabla 1. Portales del sector público ecuatoriano analizados en el estudio.
Fuente: Los autores, a partir del directorio Gob.ec.

N°	Sistema	URL
1	Servicio de Rentas Internas (SRI) - Servicios en Línea	https://srienlinea.sri.gob.ec/
2	Registro Civil - Portal Ciudadano	https://apps.registrocivil.gob.ec/
3	Sistema Oficial de Contratación Pública (SERCOP)	https://www.compraspublicas.gob.ec/
4	IESS - Gestión de Afiliados	https://app.iess.gob.ec/
5	Ministerio de Educación	https://educacion.gob.ec/
6	SENESCYT - Consulta de Títulos	https://www.senescyt.gob.ec/
7	ANT - Consulta de Licencias y Citaciones	https://consultaweb.ant.gob.ec/PortalWEB/
8	ANT - Sistema Virtual de Turnos	https://consultaweb.ant.gob.ec/SVT/
9	CNE - Consulta de Lugar de Votación	https://lugarvotacion.cne.gob.ec/

La muestra abarca siete instituciones del gobierno central ecuatoriano, que representan sectores de significativa importancia: tributación (SRI), Registro Civil, compras públicas (SERCOP),

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

seguridad social (IESS), educación básica y superior (Ministerio de Educación, SENESCYT), movilidad (ANT) y participación democrática (CNE). Los nueve portales analizados en conjunto atienden a millones de ciudadanos ecuatorianos, administran datos personales, financieros y biométricos, y representan infraestructura crítica del Estado. Desde una perspectiva técnica, la muestra presenta una heterogeneidad significativa, al abarcar sistemas con arquitecturas diversas, como portales informativos que ofrecen servicios transaccionales, sistemas de consulta ciudadana y plataformas para la gestión de turnos. Esta variedad posibilita la identificación de patrones de vulnerabilidad en distintos contextos de implementación.

2.3. Tipo de análisis y consideraciones éticas

Se aplicó análisis pasivo, entendido como la inspección de información que cualquier visitante regular del portal puede observar sin necesidad de credenciales, sin inyección de cargas maliciosas y sin enumeración por fuerza bruta. Esta delimitación cumple un doble propósito: hace el estudio reproducible por terceros sin riesgo legal ni operativo, y relaciona esto con el Artículo 232 del Código Orgánico Integral Penal (COIP) de Ecuador, que sanciona el acceso no autorizado a sistemas informáticos en los que se vulneran las medidas de seguridad con intención maliciosa. Ninguna de estas condiciones se aplica a una auditoría que simplemente lee respuestas HTTP estándar. La metodología también sigue las recomendaciones de divulgación responsable en el RFC 9116 (Foudil & Shafranovich, 2022).

El análisis pasivo es suficiente para lograr el objetivo previsto porque los errores de configuración que se investigan (encabezados, cookies, TLS y archivos de estándares) aparecen en la respuesta HTTP estándar sin requerir interacción de autenticación o inyección de carga útil. Las vulnerabilidades que requieren pruebas activas están fuera del alcance y se consideran limitaciones en la Sección 3.8.

Dado que el análisis se centra únicamente en la información pública que las instituciones ponen a disposición de la población en general, no fue requerido el consentimiento explícito de las instituciones examinadas. Toda la información procesada en este estudio puede ser observada por cualquier ciudadano usando un navegador estándar y herramientas de línea de comandos como cURL. Esta posición es coherente con el enfoque metodológico utilizado en estudios previos sobre portales gubernamentales en otros países (Awoleye et al., 2014).

2.4. Herramienta desarrollada

Se construyó una herramienta de auditoría en Python 3.12 que automatiza la inspección de los portales mediante ocho módulos independientes (Tabla 2). El código fuente fue puesto a disposición en un repositorio de acceso abierto bajo la licencia MIT con el fin de asegurar la reproducibilidad. Las dependencias técnicas incluyen: requests versión 2.31 para realizar solicitudes HTTP, BeautifulSoup4 versión 4.12 para el análisis de HTML, el módulo estándar ssl para la validación de certificados, así como pandas versión 2.0 junto con openpyxl versión 3.1 para la creación de informes en formato Excel. El diseño modular responde a las críticas de Doupé et al. (2010) a los escáneres tradicionales: cada módulo entrega hallazgos rastreables hasta el fragmento específico de la respuesta HTTP que los origina, en contraposición a un veredicto global no reproducible.

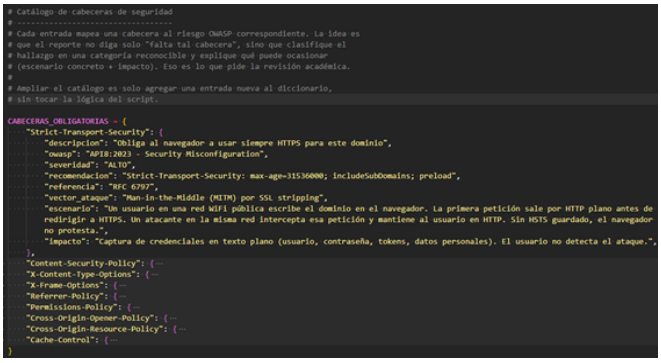

Figura 1. Estructura del catálogo CABECERAS_OBLIGATORIAS con clasificación OWASP, severidad, impacto y escenario de ataque.
Fuente: Los autores.

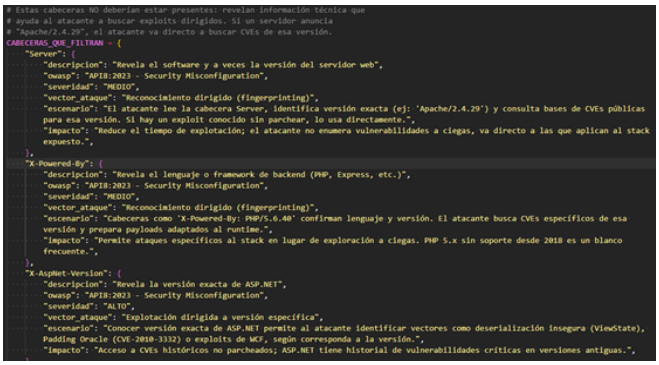

Figura 2. Catálogo CABECERAS_QUE_FILTRAN con clasificación de cabeceras que revelan información técnica del servidor y su impacto en el reconocimiento del atacante.
Fuente: Los autores.

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

Tabla 2. Módulos de análisis pasivo y categorías OWASP asociadas.
Fuente: Los autores, con base en OWASP Foundation API Security Top 10:2023.

N°	Módulo	Verificación realizada	Categoría OWASP
1	Cabeceras HTTP	Presencia de HSTS, CSP, X-Frame-Options, COOP, CORP y supresión de cabeceras que filtran versiones; control de cacheo de respuestas con datos sensibles (Cache-Control)	API8:2023 / API3:2023
2	Cookies	Validación de flags Secure, HttpOnly, SameSite y nombres reveladores de tecnología	API2:2023
3	CORS	Detección de Access-Control-Allow-Origin permisivo combinado con credenciales habilitadas	API8:2023
4	TLS/SSL	Versión negociada, vigencia del certificado, emisor y cipher suite	API8:2023
5	HTML público	Meta generator, comentarios sospechosos, formularios sin HTTPS, autocomplete en passwords, mixed content	API8 / API2
6	Endpoints API	Detección por expresiones regulares de rutas /api/v*, /graphql, /swagger, /openapi.json	API9:2023
7	Archivos estandarizados	robots.txt, sitemap.xml, .well-known/security.txt (RFC 9116)	API10:2023
8	Redirecciones	Cadenas largas y saltos por HTTP plano dentro de la cadena	API8:2023

2.5. Procedimiento de auditoría

La unidad de análisis es el hallazgo: una debilidad concreta en un sistema concreto. Si la ausencia de HSTS aparece en dos portales, son dos hallazgos, uno por portal. Dentro de un mismo portal, dos cabeceras ausentes solo cuentan como hallazgos distintos si corresponden a controles diferentes, cada uno con su propia categoría OWASP, severidad y recomendación de mitigación. Con este criterio se construyen los recuentos de las Figuras 3 a 8 y de la Tabla 4, y coincide con los dieciséis atributos que la herramienta registra por cada hallazgo.

La herramienta ejecuta los ocho módulos sobre cada portal de forma secuencial. Cada módulo opera de manera independiente: si un módulo falla por una respuesta atípica, el resto continúa, lo que evita la pérdida de toda la auditoría por un fallo aislado. Para cada hallazgo se registran dieciséis atributos: sistema afectado, URL, fecha, código HTTP, categoría OWASP, tipo de detección, elemento específico, valor observado, gravedad, descripción técnica, vectores de ataque, escenarios de uso específicos, impacto, recomendaciones de mitigación y referencias regulatorias. Este nivel de detalle es intencional: convierte cada punto en una unidad de cita directa en la discusión, en lugar de un punto agregado imposible de rastrear. La aproximación se inspira en las críticas de Doupé et al. (2010) sobre los escáneres de caja negra automatizados, que tienden a producir reportes voluminosos sin aportar trazabilidad por hallazgo.

2.6. Esquema de severidad

La severidad de cada hallazgo se asignó siguiendo un criterio cualitativo basado en el potencial daño descrito por OWASP, con cuatro niveles: Crítico (compromiso inmediato de confidencialidad o integridad), Alto (vector explotable con consecuencias graves bajo condiciones realistas), Medio (debilidad explotable bajo condiciones específicas) y Bajo (filtración de información o desviación de buenas prácticas sin impacto directo). Se construyó un puntaje de riesgo R agregado por sistema mediante la Ecuación (1):

$$R = \Sigma_i (s_i \times p_i) \qquad (1)$$

En la Ecuación (1), s_i representa el peso de severidad del hallazgo i, asignado según cuatro niveles: Crítico = 4, Alto = 3, Medio = 2 y Bajo = 1; mientras que p_i toma el valor 1 si el hallazgo está presente en el sistema evaluado y 0 en caso contrario. El nivel Crítico se incluye en la escala por completitud metodológica, aunque en la muestra analizada no se registraron hallazgos de esa categoría, dado que todos los portales contaban con cifrado TLS válido y certificados vigentes. Esta función genera un puntaje acumulado que permite comparar la postura relativa de seguridad entre sistemas. El esquema es deliberadamente simple frente a alternativas como CVSS porque busca expresar la severidad observable sin pretender estimar impacto comercial, atributo que solo el operador del sistema puede valorar adecuadamente.

El índice R es un indicador ordinal: sirve para comparar sistemas entre sí, no para estimar un riesgo absoluto. La suma ponderada asume aditividad por simplicidad operativa, pero algunos hallazgos se refuerzan entre sí y la suma no lo refleja. La ausencia conjunta de HSTS y de la flag Secure en cookies, por ejemplo, facilita los ataques de SSL stripping más de lo que cualquiera de las dos por separado lo haría. Esta limitación se asume de forma deliberada. R ordena la postura relativa de los portales con un criterio transparente y reproducible; no sustituye un análisis de riesgo formal.

2.7. Validación cruzada de la herramienta

Dado que la herramienta es de desarrollo propio, se hizo una validación manual cruzada sobre una submuestra de 25 hallazgos, el 24,8 % del total, repartida entre las cinco categorías OWASP detectadas (Tabla 3). De los 25, 18 coincidieron exactamente con lo que había reportado la herramienta. Los 4 casos sin coincidencia se explican por dos causas distintas. En tres (Cache-Control en SRI y SENESCYT, X-Content-Type-Options en SENESCYT) la cabecera que en mayo de 2026 se reportó ausente apareció presente al verificar en junio: más que un error de detección, esto

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

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

apunta a un cambio de configuración del servidor en ese mes. El cuarto, el endpoint /rest/conadisservicio del Registro Civil, no se reprodujo porque la verificación solo revisó el HTML de la página raíz; el hallazgo original probablemente proviene de un recurso JavaScript enlazado que esta comprobación puntual no llegó a descargar. Los 3 casos indeterminados, dos cookies de sesión y un campo de contraseña, tampoco aparecieron en una solicitud anónima a la página de inicio. Eso es coherente con elementos que solo se generan tras interacción de sesión o que se renderizan en el cliente, no con un fallo de la lógica de detección. En ningún caso de los siete la discrepancia se origina en la lógica determinista de los módulos pasivos: cuatro responden a cambios entre la fecha de auditoría y la de verificación o al alcance más estrecho de esta comprobación puntual, y tres a que esta verificación no abrió sesión ni ejecutó JavaScript.

Tabla 3. Resultado de la validación manual cruzada de una submuestra de hallazgos (n = 25, 24,8 % del total).
Fuente: Los autores, mediante verificación directa de las respuestas HTTP de los nueve portales (junio 2026).

Sistema	OWASP	Hallazgo verificado	Resultado	Observación
Registro Civil	API8	Filtración de información (X-Powered-By)	Coincide	-
SRI	API8	Cabecera ausente (Cross-Origin-Opener-Policy)	Coincide	-
Min. Educación	API8	Meta tag generator expone tecnología	Coincide	-
Min. Educación	API8	Cabecera ausente (Cross-Origin-Opener-Policy)	Coincide	-
IESS	API8	Filtración de stack vía cookie (JSESSIONID)	Indeterminado	La cookie no se generó en la solicitud anónima a la página de inicio; probablemente requiere interacción de sesión.
SERCOP	API8	Cabecera ausente (Referrer-Policy)	Coincide	-
Registro Civil	API8	Filtración de información (Server)	Coincide	-
SENESCYT	API8	Filtración de información (Server)	Coincide	-
ANT - Licencias	API8	Cabecera ausente (X-Content-Type-Options)	Coincide	-
ANT - Turnos	API8	Cabecera ausente (X-Frame-Options)	Coincide	-
Min. Educación	API8	Política CORS demasiado permisiva	Coincide	-
Registro Civil	API8	Cabecera ausente (Strict-Transport-Security)	Coincide	-
SENESCYT	API8	Cabecera ausente (X-Content-Type-Options)	No coincide	La cabecera está presente en la verificación (junio de 2026); posible cambio de configuración tras la auditoría de mayo de 2026.
ANT - Turnos	API2	Cookie con flags incompletas (JSESSIONID)	Coincide	-

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

SRI	API2	Cookie con flags incompletas (TS01ed1cee)	Coincide	-
SRI	API2	Cookie con flags incompletas (BIGipServerIntegra_statics)	Indeterminado	La cookie no apareció en la solicitud a la página de inicio; podría depender de una ruta o nodo de balanceo específico.
CNE	API2	Cookie con flags incompletas (visid_ incap_3214960)	Coincide	-
Registro Civil	API2	Input password sin autocomplete=off	Indeterminado	No se encontró ningún campo de contraseña en el HTML estático de la página raíz; el formulario podría estar en otra ruta o generarse con JavaScript del lado del cliente.
ANT - Licencias	API2	Cookie con flags incompletas (X-Oracle-BMC-LBS-Route)	Coincide	-
SRI	API3	Cabecera ausente (Cache-Control)	No coincide	La cabecera está presente en la verificación; posible cambio de configuración tras la auditoría original.
SENESCYT	API3	Cabecera ausente (Cache-Control)	No coincide	La cabecera está presente en la verificación; posible cambio de configuración tras la auditoría original.
Registro Civil	API3	Cabecera ausente (Cache-Control)	Coincide	-
ANT - Turnos	API10	Falta canal de divulgación (security.txt)	Coincide	-
ANT - Licencias	API10	Falta canal de divulgación (security.txt)	Coincide	-
Registro Civil	API9	Endpoint API referenciado (/rest/ conadisservicio)	No coincide	El patrón no apareció en el HTML de la página raíz; la verificación no inspeccionó los recursos JavaScript enlazados donde probablemente se origina el hallazgo.

3. Resultados y Discusión

3.1. Caracterización general de los hallazgos

La auditoría identificó 101 hallazgos distribuidos en los nueve portales analizados. Ninguno presentó hallazgos catalogados como Críticos en sentido estricto, lo que sugiere que los portales evaluados cuentan con cifrado TLS válido y certificados vigentes. Esta es una observación positiva: la infraestructura básica de cifrado en tránsito ha sido adoptada de manera generalizada. Sin embargo, sí se detectaron debilidades de severidad Alta que comprometen capas de defensa secundarias necesarias para un esquema de seguridad en profundidad. La distribución por severidad se muestra en la Figura 3.

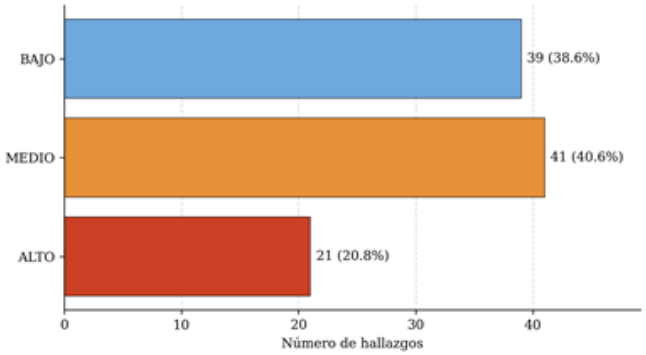

Figura 3. Distribución de hallazgos por severidad en la muestra (n = 101).
Fuente: Los autores.

De los 101 hallazgos, 21 (20,8 %) corresponden a severidad Alta, 41 (40,6 %) a Media y 39 (38,6 %) a Baja. La proporción de hallazgos Altos es significativa: indica que más de un quinto de las debilidades observadas en estos portales podrían explotarse bajo condiciones realistas con consecuencias relevantes para la confidencialidad o integridad de los datos ciudadanos. La distribución es similar a la reportada por Awoleye et al. (2014) en portales gubernamentales nigerianos, donde aproximadamente un cuarto de los hallazgos correspondía a categorías de alto riesgo.

3.2. Distribución por categoría OWASP

La distribución de hallazgos de OWASP API Security Top 10:2023 confirma un patrón sistemático en el cual la configuración insegura del servidor concentra la mayoría de los problemas detectados (Figura 4).

La categoría API8:2023 - Security Misconfiguration concentra 70 hallazgos (69,3 % del total). La segunda categoría más frecuente es API2:2023 - Broken Authentication, con 17 hallazgos (16,8 %), todos asociados a cookies de sesión sin las flags de seguridad apropiadas y a formularios que permiten autocompletado en

e-ISNN 2550-6730 | **Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026** | **DOI: 10.33936/isrtic.v10i1.8463**

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

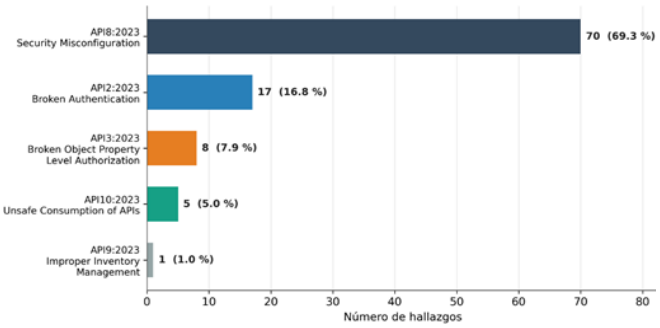

Figura 4. Distribución de los resultados según las categorías OWASP API Security Top 10:2023.
Fuente: Los autores.

campos de contraseña. Las categorías API3:2023 (Broken Object Property Level Authorization), API10:2023 (Unsafe Consumption of APIs) y API9:2023 (Improper Inventory Management) acumulan el 14 % restante. Esta distribución es consistente con los patrones reportados por Buchanan et al. (2018) y Calzavara et al. (2017): las vulnerabilidades de configuración del servidor y la gestión deficiente de cookies son las familias más persistentes en aplicaciones web modernas.

Para contrastar H1 de forma estadística, se aplicó una prueba binomial exacta de una cola sobre la proporción de hallazgos en API8:2023 (70 de 101) frente a la hipótesis nula de concentración aleatoria ($p_0 = 0{,}50$). La proporción observada (69,3 %) es significativamente superior al 50 % postulado ($p < 0{,}001$; intervalo de confianza del 95 % de Clopper-Pearson: 59,3 %–78,1 %). Dado que el límite inferior del intervalo supera el umbral del 50 %, H1 se confirma con respaldo inferencial y no por la mera superación nominal del umbral.

3.3. Análisis comparativo entre portales

La distribución de hallazgos por sistema (Figura 5) muestra una variabilidad considerable. El portal con menor número de hallazgos es SERCOP (5 hallazgos), mientras que el Registro Civil presenta el mayor volumen (16 hallazgos). Esta variabilidad, dentro de instituciones que pertenecen al mismo sector y operan bajo regulaciones similares, resulta informativa por sí misma: sugiere que los déficits de hardening no se explican únicamente por restricciones presupuestales globales y es consistente con la influencia de decisiones técnicas específicas de cada equipo. El diseño del estudio no permite, sin embargo, descartar factores como presupuestos diferenciados, proveedores de implementación distintos o la antigüedad de cada sistema.

Aplicando la Ecuación (1) al conjunto de resultados produce una estimación de riesgo R para cada sistema (Tabla 4). Cuatro portales superan R = 25 y se concentran en las instituciones que

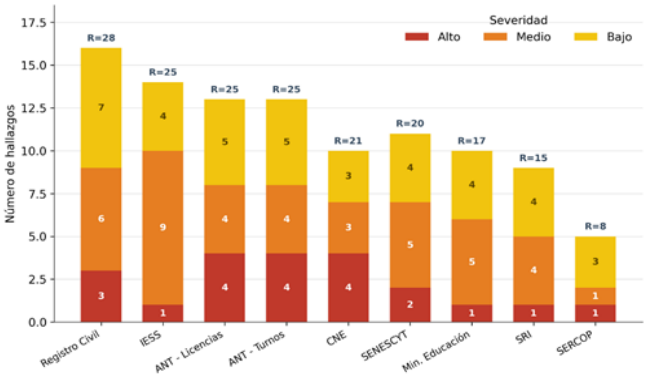

Figura 5. Distribución de hallazgos por sistema, segmentada por severidad.
Fuente: Los autores.

manejan datos personales identificables (cédula, dirección, datos vehiculares): los dos portales de la ANT, el portal del Registro Civil y el portal de afiliados del IESS. SERCOP, en cambio, presenta R = 8 a pesar de manejar también datos sensibles, lo que indica que es posible alcanzar una postura de hardening considerablemente mejor sin un costo desproporcionado.

Tabla 4. Puntaje de riesgo agregado R por sistema, ordenado de mayor a menor.
Fuente: Los autores. R = puntaje de riesgo agregado calculado mediante la Ecuación (1).

Sistema	Altos	Medios	Bajos	Total	R
Registro Civil - Portal Ciudadano	3	6	7	16	28
ANT - Consulta de Licencias y Citaciones	4	4	5	13	25
ANT - Sistema Virtual de Turnos	4	4	5	13	25
IESS - Gestión de Afiliados	1	9	4	14	25
CNE - Consulta de Lugar de Votación	4	3	3	10	21
SENESCYT - Consulta de Títulos	2	5	4	11	20
Ministerio de Educación	1	5	4	10	17
SRI - Servicios en Línea	1	4	4	9	15
SERCOP - Sistema Oficial de Contratación	1	1	3	5	8

3.4. Hallazgos predominantes

El tipo de hallazgo más frecuente fue “Cabecera de seguridad

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

ausente", con 67 ocurrencias (66,3 % del total). Las cabeceras omitidas con más frecuencia fueron Content-Security-Policy (CSP), Permissions-Policy, Cross-Origin-Opener-Policy y Cross-Origin-Resource-Policy, ausentes en los nueve portales evaluados. La cabecera Strict-Transport-Security (HSTS), en cambio, está ausente en cuatro de los nueve portales (Registro Civil, los dos portales de la ANT y el CNE): en esos casos, aunque el sitio sirve contenido por HTTPS, no instruye al navegador para que rechace conexiones HTTP futuras al mismo dominio. La especificación HSTS (Hodges et al., 2012) fue diseñada precisamente para cerrar esa ventana de exposición; De los Santos y Torres (2018) mostraron además que, incluso cuando HSTS está implementado, ciertas malas prácticas impiden alcanzar la protección esperada. Su omisión en esos cuatro portales deja al usuario expuesto a ataques de SSL stripping en redes inalámbricas no confiables. La ausencia de Content-Security-Policy expone al sitio a XSS sin contención, problema cuya complejidad práctica fue caracterizada por Weichselbaum et al. (2016), quienes encontraron bypasses en el 94,72 % de las políticas CSP desplegadas en la web. El mapa de calor de la Figura 6 visualiza el puntaje de riesgo agregado por sistema y módulo de análisis, permitiendo identificar de forma rápida las combinaciones de mayor concentración de hallazgos.

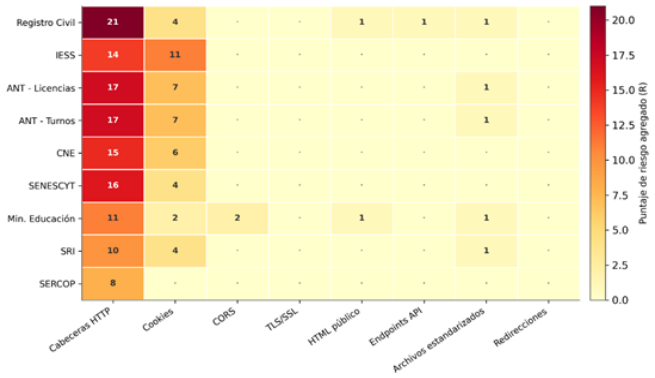

Figura 6. Mapa de calor del puntaje de riesgo agregado por sistema y módulo de análisis.
Fuente: Los autores.

El segundo tipo más frecuente fue "Cookie con flags de seguridad incompletas" (16 ocurrencias), seguido por "Filtración de stack vía nombre de cookie" (5 ocurrencias). Las cookies con nombres reveladores como JSESSIONID, observadas en el Registro Civil, el IESS, SENESCYT y los dos portales de la ANT, anuncian al atacante el stack tecnológico subyacente, en todos los casos Java sobre contenedores tipo Tomcat o JBoss, sin que este tenga que enumerar versiones. Este tipo de información reduce el tiempo de reconocimiento de horas a segundos en una fase de pre-ataque y constituye un ejemplo claro del principio de minimización de información atacable que la literatura ha defendido durante décadas (Calzavara et al., 2017). En cuanto a la flag SameSite, ausente en la mayoría de cookies de sesión observadas, Compagna et al. (2021) mostraron que su despliegue correcto puede mitigar de forma significativa los ataques de Cross-Site Request Forgery, aunque no constituye por sí solo una defensa completa.

3.5. Endpoints API detectados

El módulo 6 encontró un solo endpoint de integración en toda la muestra: /rest/conadisservicio/, visible en el código JavaScript público del portal del Registro Civil. Se clasificó como severidad Baja bajo API9:2023 (Improper Inventory Management): el endpoint no tiene documentación formal ni figura en ningún inventario público. En los otros ocho portales no apareció ninguna ruta /graphql, /swagger u /openapi.json accesible. La detección es pasiva, viene de leer el código y no de consultar el endpoint, así que no podemos decir si pide autenticación o no. Es poca evidencia, y la tratamos como tal. Confirma que al menos un portal de la muestra expone una superficie de integración programática, pero no alcanza para sostener que los nueve operan como APIs en sentido estricto. Por eso la elección del marco OWASP API se apoya en la equivalencia conceptual entre sus categorías y las del marco web para los controles auditados (sección 2.1), no en cuántos endpoints API aparecieron en la muestra.

3.6. Matriz de riesgo

La caracterización combinada de probabilidad e impacto se resume en la matriz de riesgo de la Figura 7, donde la probabilidad se aproxima por la frecuencia observada del tipo de hallazgo y el impacto corresponde a la severidad asignada según los criterios de la sección 2.6.

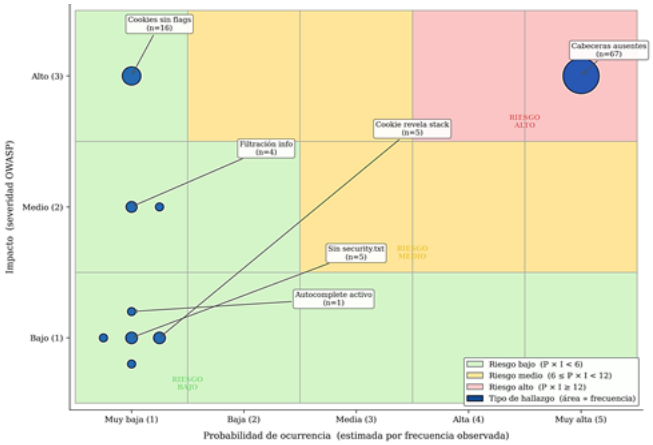

Figura 7. Matriz de riesgo de los principales tipos de hallazgo identificados. El área de los círculos es proporcional a la frecuencia observada del tipo de hallazgo.
Fuente: Los autores.

La matriz muestra que los hallazgos relacionados con las cabeceras de seguridad faltantes son de alto riesgo (alta probabilidad y alto impacto), lo que justifica su prioridad en cualquier plan de remediación. Las cookies sin indicadores apropiados, aunque menos comunes, también se encuentran en el área de alto impacto porque comprometen directamente la integridad de la sesión del usuario. Los hallazgos de filtración de información y la ausencia de canales de divulgación responsable

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

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

se ubican en la zona de riesgo medio.

3.7. Discusión

Los hallazgos apuntan a una conclusión que tiene implicaciones tanto académicas como operativas. Que el 69,3 % de los problemas se concentre en API8:2023 - Security Misconfiguration indica que la debilidad central de los portales públicos ecuatorianos no es técnicamente compleja: no se trata de cifrado insuficiente ni de funcionalidades expuestas, sino de configuraciones básicas del servidor que cualquier administrador puede aplicar en minutos. Su omisión sistemática confirma lo que Navia y Zambrano-Romero (2021) ya señalaban: hay una brecha entre el conocimiento técnico y su uso en el sector público.

Esa misma heterogeneidad de puntajes de riesgo agregado (Tabla 4) admite una lectura operativa: la coexistencia de sistemas con posturas de hardening dispares dentro del mismo sector abre la pregunta sobre los mecanismos de transferencia de buenas prácticas entre instituciones, más allá de los factores que el diseño no permite aislar (antigüedad del sistema, proveedor de implementación o presupuesto organizacional específico). Existen unidades técnicas dentro del Estado que ya han incorporado prácticas de hardening adecuadas, lo que da peso a esa posibilidad. A diferencia de la Figura 4, que organiza los hallazgos según la taxonomía OWASP, la Figura 8 los distribuye por módulo de análisis de la herramienta desarrollada, lo que permite identificar qué superficie técnica concentra mayor número de debilidades. Esta perspectiva complementaria confirma que los módulos de cabeceras HTTP y de cookies constituyen los vectores de exposición más frecuentes, con el 70,3 % (71 hallazgos) y el 20,8 % (21 hallazgos) del total respectivamente, resultado coherente con lo reportado por Buchanan et al. (2018) y Calzavara et al. (2017).

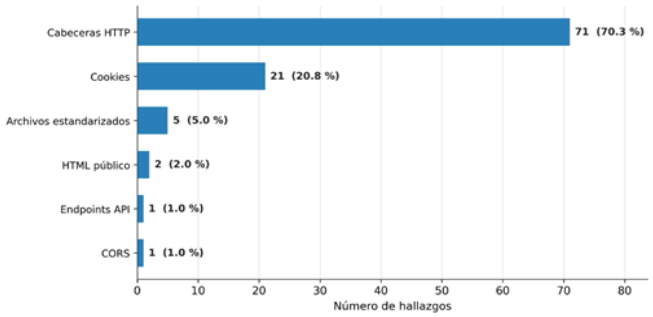

Figura 8. Porcentaje de hallazgos distribuido por módulo de análisis de la herramienta.
Fuente: Los autores.

Los resultados se alinean, además, con la literatura empírica internacional. Awoleye et al. (2014) reportaron en portales gubernamentales nigerianos una concentración similar de hallazgos en configuraciones inseguras y autenticación débil, con porcentajes equiparables a los aquí observados pese a la distancia contextual. Buchanan et al. (2018), en un análisis sistemático de las implementaciones de encabezados de seguridad HTTP documentaron que una proporción muy baja de sitios implementó conjuntos de recomendaciones, una observación consistente con el patrón que encontraron: la mayoría de los portales evaluados no implementaron ni siquiera los encabezados más básicos, como HSTS o X-Content-Type-Options. Pellegrino et al. (2015) han demostrado que los escáneres automatizados tienen un alcance limitado cuando los sitios carecen de controles de seguridad básicos, lo que refuerza la utilidad de las auditorías pasivas específicas como la que se presenta aquí. La aportación específica de este estudio es la caracterización empírica del fenómeno en el sector público ecuatoriano, que hasta la fecha contaba con literatura predominantemente normativa (Cuzme et al., 2018; Navia & Zambrano-Romero, 2021).

Una observación adicional surge al comparar los puntajes de riesgo entre instituciones que comparten infraestructura. Los dos portales operados por la Agencia Nacional de Tránsito, el de Consulta de Licencias y el Sistema Virtual de Turnos, presentan exactamente el mismo puntaje (R = 25) y la misma distribución por severidad. Esta concordancia indica que ambos heredan la configuración básica del mismo servidor o del mismo tipo de implementación, lo que tiene las correspondientes consecuencias operativas: una intervención en la configuración básica reducirá los riesgos en ambos sistemas al mismo tiempo. En la muestra no se observó la situación opuesta, donde sería más costoso reparar portales con diferentes configuraciones dentro de la misma organización, lo que sugiere una oportunidad para aumentar la eficiencia para el sector. Análogamente, el contraste entre el portal del Ministerio de Educación (R = 17) y el de SENESCYT (R = 20), ambos del mismo dominio sectorial, sugiere que las decisiones técnicas se toman institución por institución y no por área de gobierno, lo que refuerza la pertinencia de mecanismos de coordinación sectorial.

3.8. Limitaciones del estudio

El estudio reconoce limitaciones que conviene explicitar. El análisis pasivo no detecta vulnerabilidades de capa de aplicación inyección SQL, cross-site scripting persistente e IDOR, que solo se manifiestan ante interacción autenticada o cargas dirigidas; los hallazgos reportados son, por tanto, un subconjunto del riesgo total. Los nueve portales constituyen una muestra intencional y los resultados no pueden generalizarse estadísticamente a todo el sistema de Internet estatal ecuatoriano, especialmente al sistema de gobiernos autónomos descentralizados, que no fue incluido.

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

Además, los resultados hacen referencia a una fecha concreta (mayo de 2026); la configuración del portal puede variar de una auditoría a otra, especialmente después de mejoras de seguridad posteriores. La replicación del estudio en períodos sucesivos permitiría caracterizar la evolución de la postura de seguridad y contrastarla con el calendario de despliegue de medidas de la Estrategia Nacional de Ciberseguridad.

De manera similar, los seis portales excluidos por indisponibilidad durante la ventana de medición no fueron caracterizados, lo que introduce un posible sesgo de supervivencia: la muestra final podría sobrerrepresentar sistemas con mayor estabilidad operativa y, plausiblemente, con mayor madurez técnica.

4. Conclusiones

La auditoría pasiva de nueve portales web del sector público ecuatoriano bajo el marco OWASP API Security Top 10:2023 identificó 101 hallazgos, de los cuales el 20,8 % corresponde a severidad Alta. La categoría API8:2023 - Security Misconfiguration concentra el 69,3 % de los hallazgos, evidenciando un déficit transversal en prácticas de hardening que afecta a la totalidad de los sistemas evaluados. Ningún portal implementa el conjunto completo de cabeceras de seguridad recomendados por OWASP y ocho de los nueve portales presentan al menos una cookie con flags de seguridad incompletas. Las tres hipótesis operativas se confirmaron: la concentración en API8:2023 superó el 50 % de manera estadísticamente significativa (H1, $p < 0{,}001$), la mayoría de las cookies de sesión presentó flags incompletas (H2) y la adopción de cabeceras de seguridad fue deficiente en la totalidad de los sistemas (H3). En conjunto, existen patrones sistémicos de vulnerabilidades en el sector público ecuatoriano que pueden detectarse sin pruebas invasivas y son comparables a los reportados en estudios empíricos sobre portales gubernamentales de otros contextos.

Las consecuencias para los gestores públicos son directas. Implementar cabeceras de seguridad como HSTS con políticas de precarga, políticas estrictas de seguridad de contenido y configuraciones de cookies apropiadas (Secure, HttpOnly, SameSite) es un conjunto de medidas efectivas y económicas que deben formalizarse como requisito mínimo en todo portal gubernamental. La publicación de archivos /.well-known/security.txt bajo RFC 9116 facilitará la divulgación responsable de información por canales oficiales, algo que actualmente falta en seis de los nueve portales. Por el contrario, una herramienta desarrollada y publicada en un repositorio abierto puede servir como una herramienta de monitoreo continuo que se integra con los procesos de implementación para detectar regresiones de configuración antes de que se conviertan en problemas.

Las direcciones de investigación futuras incluyen ampliar el análisis a portales gubernamentales centralizados y descentralizados, el uso adicional de pruebas activas con consentimiento institucional y la evaluación longitudinal del impacto de las actividades de endurecimiento después de revelar responsablemente los resultados a las instituciones evaluadas. Establecer un observatorio público sobre la seguridad de los portales gubernamentales basado en métodos repetibles como el que aquí se presenta podría proporcionar evidencia continua para las decisiones de políticas públicas relacionadas con la ciberseguridad.

Además de sus aportes técnicos, este estudio también plantea interrogantes sobre el modelo de gobernanza de la seguridad informática en el estado de Ecuador. La uniformidad observada al abordar las brechas sugiere que las soluciones de las instituciones individuales no son suficientes: se necesita un mecanismo coordinado para distribuir plantillas de configuración, verificar su aceptación y publicar los resultados. La experiencia internacional indica que los observatorios independientes de seguridad y los programas de divulgación coordinada (Foudil & Shafranovich, 2022) son instrumentos efectivos para reducir la asimetría entre quien identifica un problema y quien tiene la responsabilidad de corregirlo. Adoptar instrumentos similares en Ecuador, alineados con el marco OWASP API Security Top 10:2023 y con las recomendaciones de la literatura empírica revisada, contribuiría a cerrar la brecha entre la legislación de protección de datos y la postura técnica real de los sistemas que los procesan.

Contribución de los autores

Jaime Rubén Borja Ulloa: Conceptualización, Metodología, Software, Investigación, Análisis formal, Redacción - borrador original del artículo. **Rodrigo Cadena Martínez:** Validación, Visualización, Revisión y edición del artículo, Supervisión.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Apéndice

A.1. Disponibilidad del código y datos

El código fuente de la herramienta de auditoría desarrollada para este estudio se encuentra disponible públicamente bajo licencia MIT en el repositorio: https://github.com/rubenborja/passive-security-audit. Los datos crudos generados durante la auditoría (formato JSON y reporte Excel con dieciséis columnas analíticas) se incluyen como material suplementario y permiten la replicación íntegra de los resultados aquí reportados.

A.2. Marco legal y ético del estudio

El estudio se enmarca en el Art. 232 del Código Orgánico Integral Penal del Ecuador, que tipifica el acceso no consentido a sistemas informáticos cuando media violación de medidas de seguridad y dolo. Ninguna de estas condiciones se configura en una auditoría pasiva que solo lee respuestas HTTP estándar. La

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463

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

metodología se alinea, además, con los principios de divulgación responsable establecidos en RFC 9116 (Foudil & Shafranovich, 2022) y con las recomendaciones generales sobre divulgación coordinada de vulnerabilidades.

Referencias bibliográficas

Awoleye, O. M., Ojuloge, B., & Ilori, M. O. (2014). Web application vulnerability assessment and policy direction towards a secure smart government. Government Information Quarterly, 31(S1), S118-S125. https://doi.org/10.1016/j.giq.2014.01.012

Buchanan, W. J., Helme, S., & Woodward, A. (2018). Analysis of the adoption of security headers in HTTP. IET Information Security, 12(2), 118-126. https://doi.org/10.1049/iet-ifs.2016.0621

Calzavara, S., Focardi, R., Squarcina, M., & Tempesta, M. (2017). Surviving the web: A journey into web session security. ACM Computing Surveys, 50(1), 13:1-13:34. https://doi.org/10.1145/3038923

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), tyz001. https://doi.org/10.1093/cybsec/tyz001

Compagna, L., Jonker, H., Krochewski, J., Krumnow, B., & Sahin, M. (2021). A preliminary study on the adoption and effectiveness of SameSite cookies as a CSRF defence. En 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 49-59). IEEE. https://doi.org/10.1109/EuroSPW54576.2021.00012

Cuzme, M., Pinargote, R., & Sabando, E. (2018). Plan de gestión de incidentes de seguridad informática mediante ITIL y MAGERIT. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 2(1), 24-30. https://doi.org/10.33936/isrtic.v2i1.1129

De los Santos, S., & Torres, J. (2018). Analysing HSTS and HPKP implementation in both browsers and servers. IET Information Security, 12(4), 275-284. https://doi.org/10.1049/iet-ifs.2017.0030

Doupé, A., Cova, M., & Vigna, G. (2010). Why Johnny can't pentest: An analysis of black-box web vulnerability scanners. En C. Kreibich & M. Jahnke (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2010) (LNCS, Vol. 6201, pp. 111-131). Springer. https://doi.org/10.1007/978-3-642-14215-4_7

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. Informatics, 10(3), 71. https://doi.org/10.3390/informatics10030071

Foudil, E., & Shafranovich, Y. (2022). A file format to aid in security vulnerability disclosure (RFC 9116). Internet Engineering Task Force. https://doi.org/10.17487/RFC9116

Hodges, J., Jackson, C., & Barth, A. (2012). HTTP Strict Transport Security (HSTS) (RFC 6797). Internet Engineering Task Force. https://doi.org/10.17487/RFC6797

Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). (2022). Estrategia Nacional de Ciberseguridad del Ecuador 2022-2025. Gobierno del Ecuador. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

Navia, M., & Zambrano-Romero, W. (2021). Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 5(2), 119-128. https://doi.org/10.33936/isrtic.v5i2.3952

Pellegrino, G., Tschürtz, C., Bodden, E., & Rossow, C. (2015). jÄk: Using dynamic analysis to crawl and test modern web applications. En H. Bos, F. Monrose, & G. Blanc (Eds.), Research in Attacks, Intrusions, and Defenses (RAID 2015) (LNCS, Vol. 9404, pp. 295-316). Springer. https://doi.org/10.1007/978-3-319-26362-5_14

Weichselbaum, L., Spagnuolo, M., Lekies, S., & Janc, A. (2016). CSP is dead, long live CSP! On the insecurity of whitelists and the future of Content Security Policy. En Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1376-1387). Association for Computing Machinery. https://doi.org/10.1145/2976749.2978363

Weissbacher, M., Lauinger, T., & Robertson, W. (2014). Why is CSP failing? Trends and challenges in CSP adoption. En A. Stavrou, H. Bos, & G. Portokalidis (Eds.), Research in Attacks, Intrusions and Defenses (RAID 2014) (LNCS, Vol. 8688, pp. 212-233). Springer. https://doi.org/10.1007/978-3-319-11379-1_11

e-ISNN 2550-6730 | Vol. 10, Núm. 1 (98-109): Enero-Junio, 2026 | DOI: 10.33936/isrtic.v10i1.8463