UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

ANÁLISIS DE SEGURIDAD EN LOS SITIOS WEB DE PLATAFORMAS DE COMERCIO DIGITAL: CASO ECUADOR

AUTORES:

CHRISTIAN GUILLERMO ACOSTA PATIÑO
FABIOLA LORENA LANDETA GUACHAMIN

DIRECTOR:

JUAN PABLO VÁZQUEZ LOAIZA

CUENCA – ECUADOR
2023

Autores:

Fabiola Lorena Landeta Guachamin
Ingeniera en Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
llandeta@est.ups.edu.ec

Christian Guillermo Acosta Patiño
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
acosta@ups.edu.ec

Dirigido por:

Juan Pablo Vázquez Loaiza
Ingeniero en Sistema
Magister en Ciencias de la Computación mención Aplicaciones Distribuidas.
Máster Universitario en planificación de Proyectos de Desarrollo Rural y Gestión Sostenible.
jvazquez@ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS
2023 © Universidad Politécnica Salesiana.
CUENCA – ECUADOR – SUDAMÉRICA
CHRISTIAN GUILLERMO ACOSTA PATIÑO
FABIOLA LORENA LANDETA GUACHAMIN
Análisis de seguridad en los sitios web de plataformas de comercio digital: caso Ecuador

DEDICATORIA

Dedico este proyecto primero a mi Dios que gracias a su misericordia y bendiciones me ha permitido culminar esta meta tan anhelada.

También dedico a mi Madre, mi Padre, mis Hermanos, quienes siempre me han brindado su apoyo y han confiado en mí. Además, dedico a mi amada Hija y mi compañero de vida mi Esposo quienes me han brindado su amor y me han dado fuerzas para no rendirme.

Finalmente, dedico este proyecto al esfuerzo de mi compañero Christian Acosta y el acompañamiento de nuestro Tutor Ing. Juan Pablo Vazquez Loaiza, quienes con su trabajo, conocimientos y apoyo culminamos nuestro proyecto de Titulación.

Fabiola Lorena Landeta Guachamin

Dedico y agradezco este proyecto de titulación primero a Dios, quien es el gestor de todos nuestros proyectos y propósitos. Luego a mi familia, base fundamental para ser mejores personas y poder contribuir con la sociedad. A mis docentes, profesores y compañera de proyecto Lorena Landeta, que supieron brindarme el apoyo en todo momento, pero en especial al docente tutor Juan Pablo Vázquez, extraordinario profesional, pero sobre todo mejor persona. Para todos aquellos que siempre de una u otra forma me han brindado sus palabras de aliento, gracias de corazón, ustedes también son parte de esto.

Christian Guillermo Acosta Patiño

AGRADECIMIENTO

Damos gracias a Dios por ser una parte fundamental en nuestra vida y quien nos ha llenado de sabiduría y fortaleza para culminar con éxito este gran paso importante en nuestras vidas y superarnos en el mundo profesional.

A nuestras familias por todo el apoyo para cumplir con nuestras metas, a nuestro tutor el Ing. Juan Pablo Vazquez Loaiza por su apoyo, guía y conocimiento brindado en la realización del proyecto de titulación.

A todos nuestros maestros y a la Universidad Politécnica Salesiana quienes han sido parte de este camino largo para nuestro crecimiento en el ámbito profesional y personal formándonos como buenos cristianos y honrados ciudadanos.

Indice

Análisis de seguridad en los sitios web de plataformas de comercio digital: Caso Ecuador

Autor(es):

FABIOLA LORENA LANDETA GUACHAMIN

CHRISTIAN GUILLERMO ACOSTA PATIÑO

Análisis de seguridad en los sitios web de plataformas de comercio digital: Caso Ecuador

Fabiola Lorena Landeta-Guachamin[1], Christian Guillermo Acosta-Patiño[2], Juan Pablo Vázquez-Loaiza[3]

[1] Universidad Politécnica Salesiana , Quito,
Ecuador

[2] Universidad Politécnica Salesiana , Quito,
Ecuador

[3] Universidad Politécnica Salesiana , Grupo de Investigación de la Gestión de las Mipymes, Cuenca,
Ecuador

cacosta@est.ups.edu.ec, llandeta@est.ups.edu.ec, jvazquez@ups.edu.ec

Resumen. Este documento presenta la investigación de la seguridad en los sitios web para comercio electrónico en el Ecuador al ser un foco importante para los ataques cibernéticos. La misma que permitió identificar y analizar las vulnerabilidades, con el fin de demostrar el riesgo de seguridad y la información que se encuentra expuesta en estas plataformas. De una población de 512 empresas que disponen comercio electrónico se aplicó la fórmula para calcular el muestreo probabilístico aleatorio simple, la cual se seleccionaron 220 empresas. A esta muestra se realizó pruebas de intrusión de seguridad basado en la metodología de OWASP utilizando diferentes herramientas para detectar vulnerabilidades relevantes, y posterior se evaluó el nivel de riesgo de las vulnerabilidades identificadas, donde la escala de valoraciones se determinó mediante la metodología de MARGERIT y de acuerdo con los resultados obtenidos del test de intrusión, se estableció valores cuantitativos y cualitativos en los riesgos encontrados con la finalidad de ver cuales tienen un impacto alto, y finalmente establecer recomendaciones para mejorar la seguridad de acuerdo a las buenas prácticas que sea aplicable en las plataformas web.

Palabras clave. Ciberseguridad, Seguridad, Vulnerabilidad, Margerit, Comercio Digital, OWASP.

Security analysis on the websites of digital commerce platforms: Ecuador Case

Abstract. This document presents the investigation of security on websites for electronic commerce in Ecuador. The same one that allowed to analyze the vulnerabilities, in order to demonstrate the security risk and the information that is exposed in these platforms. From a population of 512 companies that have electronic commerce, and by means of a simple random probabilistic sampling, 220 companies were selected. Intrusion tests were carried out on this sample based on the OWASP methodology using different tools to detect relevant threats, measure the security level of each website and define corrections to improve security. The scale of assessments was determined using the MARGERIT methodology and according to the results obtained from the intrusion test, quantitative and qualitative values were established in the risks found in order to see which ones have a high impact, and finally propose a plan. security and good practices that are applicable to web platforms.

Keywords. Cybersecurity, Security, Vulnerability, Margerit, Digital Commerce, OWASP.

1 Introducción

La tecnología digital ha ido evolucionando durante la pandemia y, más que todo, la entrada del Internet ha generado un gran cambio en el comercio electrónico favoreciendo así el uso de los sitios web para la compra, venta de productos y servicios en diferentes sectores que acompañan al mercado digital potenciado durante la pandemia [1].

Asimismo, de acuerdo con las estadísticas según [2] y [3] el 40% de las empresas crearon plataformas digitales para poder estar operativas durante la pandemia, ya que los consumidores empezaron a realizar sus compras por canales electrónicos suponiendo un incremento del 34% [4]. Por lo que, gracias a este fenómeno, el comercio electrónico experimentó un escenario de crecimiento y expansión atípico ofreciendo una nueva oportunidad para el desarrollo de falencias asociadas a la seguridad informática debido a la rápida implementación tecnológica en todo ambiente empresarial.

En el Ecuador, la transformación digital durante la pandemia ha provocado que las empresas opten por diferentes formas de negociación para la compra y venta de productos y/o servicios a través de sitios web de canales electrónicos, los mismos que hoy en día forman parte fundamental como matriz de negocios no solo a nivel local si no también mundial [4].

Por otro lado, desde la pandemia a través del fenómeno expuesto y a la fecha, la ciberseguridad ha tomado relevancia en el comercio digital ya que las principales características de estos sitios web suponen un gran atractivo para los ciberdelincuentes que aprovechan estos medios para el robo de información, ataques de Denegación de Servicio (DoS), Phishing y fraude directo con el fin de obtener beneficios de manera fraudulenta [5]. Siendo así, según [6] las pérdidas por ataques cibernético en los pagos online del comercio digital a nivel mundial aumentaron un 18% en 2021 hasta situarse por encima de los 20.000 billones de dólares, frente a los 17.500 del año 2020. Dentro de los siguientes años existe una tasa de crecimiento del 16% en 2023 con 48.000 billones de dólares, frente a los 41 mil millones del año 2022, de igual manera abra un crecimiento del 131.2% dentro de los próximos 5 años [7].

Sin embargo, el aumento de la actividad comercial por canales electrónicos desencadenó un incremento en el volumen de ciberataques en el 2022 según se ilustra en la Fig.1, a comparación del 2021 existe una tasa de crecimiento del 38% en ataques [8].

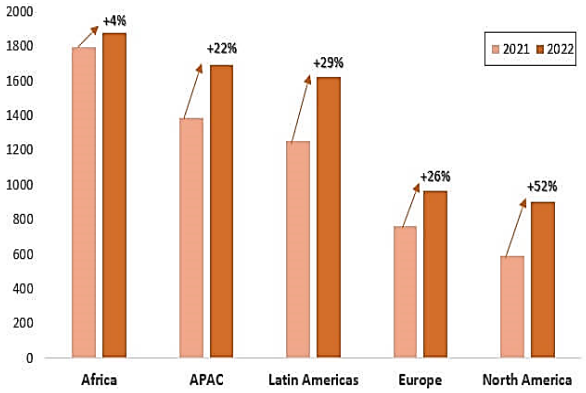

Fig. 1. Ataques cibernéticos

De acuerdo con los estudios, los principales ataques son los phishing con un 31% y el robo de contraseñas débiles con un 29% que se han convertido en un foco clave para aprovechar la vulnerabilidad de los sistemas de hardware y software [9]. Ante esta realidad, el Internet sigue evolucionando junto con los ciberdelincuentes y sus métodos de ataques, la causa del aumento de los ataques cibernéticos se debe principalmente al ámbito que aún no se ha podido controlar totalmente, y es el factor humano siendo el eslabón más débil de la ciberseguridad [10].

Y, sobre los escenarios de ciber delincuencia, existen ataques que, entre sus principales técnicas están [11]:

Fraude Directo: Este fraude es por medio de tarjetas de crédito robadas, chargeback, devoluciones forzosas y una vulnerabilidad en el web.

Robo de información: Los delincuentes obtienen una gran cantidad de información para causar una serie de estafas no solo de cuentas bancarias, sino también de bienes y negocios de los usuarios.
Malware: Las amenazas tecnológicas que se clasifican por diferentes ataques cibernéticos cuyo objetivo principal es infiltrarse en los sistemas de información sin autorización para causar daños.
Ataques Denegación de Servicios: Este ataque que se infectan servidores y se ponen a orden de los cibercriminales estos proceden de una forma retorica enviando miles de peticiones, los servidores no podrán contener estas solicitudes y hará que se encuentre fuera de servicio por el lapso que dure este proceso.
Phishing: Es uno de los métodos de estafas mediante la obtención de información de un tercero a través de correos maliciosos SPAM, o a su vez mediante ingeniería social con lo cual los cibercriminales una vez que obtiene la información deseada causan daños realmente importantes.
Ingeniería Social: Es la práctica de manipular a las personas para que divulguen información o realicen acciones que permitan el acceso a la misma, por parte de personas que cometen fraudes.
Scraping de cookies: También llamados cookies HTTP o cookies de navegador, que no son más que datos enviados por un servidor, encabezado de respuesta http al navegador de cualquier usuario que corresponda a Firefox, Edge o Chrome [12].

1.1 Ciberseguridad en Ecuador

En el Ecuador, la ciberseguridad garantiza 3 pilares de acción entendidos en confidencialidad, integridad y disponibilidad [13]. Así, en el modelo de madurez de la capacidad de ciberseguridad y en cuanto a rankings, el país Ecuador ocupa el puesto 98 mundialmente y el puesto 14 regionalmente. En donde se consideran varios aspectos como: a) iniciativas de ciberseguridad, b) marco legal, c) entidades regulatorias, e) programas de investigación y desarrollo d) Formación y cultura. Factores que, para la realidad local, la Fig.2. refleja la situación al año 2020 [14], sin embargo, desde 2022 Ecuador cuenta con la Estrategia nacional de ciberseguridad del ecuador que se encuentra vigente hasta el 2025 [15].

Fig. 2. Marcos Legales y Regulatorios

Información que, por otro lado, se complementa con lo expuesto en la Tabla 1. que refiere a las denuncias por ataques cibernéticos registradas en la Fiscalía General del Estado (FGE), en la que se observa que unos de los principales delitos cometidos con más frecuencia es la suplantación de identidad con un 43% [16] :

Tabla 1. Frecuencia de delitos informáticos reportados en Ecuador 2020

Ataque	Denuncias
Suplantación de identidad	2162
Falsificación y uso de documento falso	1448
Apropiación fraudulenta por medios electrónicos	1033
Acceso no concedido a un sistema informático, telemático o de telecomunicaciones.	175
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	85
Ataques a la integridad de sistemas informáticos	51
Intercepción ilegal de datos	45
Transferencia electrónica de activos patrimonial	31
Revelación ilegal de base de datos	18

Por otro lado, la seguridad que manejan hoy en día las organizaciones e industrias en Ecuador continúa en crecimiento exponencial al momento de asegurar los sistemas y plataformas. Sin embargo, a medida que aumenta la seguridad en las mismas, también existen cada vez métodos que pueden vulnerar dicha seguridad, la comprensión de estas, el cómo surge el robo de información de un tráfico de red y donde afecta más un ataque informático en la capa del modelo Open System Interconection (OSI) y cómo luchar contra ellas [17].

Siendo así, este estudio es significativo porque al identificar las amenazas más comunes en las plataformas digitales se establecerán métodos preventivos para reducir el riesgo de fraude cibernético en el ciberespacio y aumentar el nivel de seguridad de los sitios web que albergan estas plataformas.

Explicando brevemente las principales características del problema propuesto, la investigación se centra recomendar controles para aumentar el nivel de seguridad de los sitios web para las plataformas del comercio digital, a través del siguiente objetivo general:

Analizar la seguridad suscitadas en sitios web de comercio digital, mediante la validación de seguridad sobre la gestión de información ya que durante la pandemia fue uno de los objetivos principales de los ciberataques lo que, a su vez, exige cumplir con los siguientes objetivos específicos:

1. Identificar los diferentes tipos de amenazas y vulnerabilidades que existen en los sitios web de comercio digital con el fin de medir el nivel de seguridad existente y determinar los posibles ataques de ciberseguridad.
2. Analizar los resultados obtenidos de las vulnerabilidades para determinar los niveles de seguridad en las dimensiones de confidencialidad, integridad y disponibilidad .
3. Establecer recomendación y validación de propuestas para mejorar de prácticas de seguridad del contexto ecuatoriano.

1 Metodología y Técnicas

El presente apartado define la metodología para la identificación de vulnerabilidades, misma que se realizó a través de pruebas de intrusión basado en el enfoque Open Web Application Security Protect (OWASP) [18], marco de referencia que define fases de pruebas para verificar la seguridad en aplicaciones web y evaluar de las principales vulnerabilidades con un riesgo alto [19].

Para el cumplimiento del primer objetivo, se tuvo como fuente principal el ranking de empresas del Grupo Ekos que dispone estudios de las 5000 empresas más importantes del Ecuador resaltando su eficiencia e innovando al desarrollo empresarial, . El Grupo Ekos dispone información diferenciada y de alto valor para el uso de los diferentes lectores, con base a este listado de empresas, se validaron los siguientes aspectos, empresas que disponen página web y empresas que tienen comercio electrónico. Fuente que se usó dado a que no se identificó un registro legal y formal desde ninguna

entidad de control y regulación. Una vez validada las 5000 empresas se obtuvo un total de 512 empresas que tienen un sitio web con comercio electrónico.

Por lo tanto, una vez obtenido el tamaño de nuestra población (N), se calculó la muestra de las empresas aplicando la siguiente ecuación (1).

$$n = \frac{Z^2 p * q * N}{Ne^2 + Z^2 p * q} \quad (1)$$

Dónde:
N: 512 empresas
Z: 1.96% para el nivel de confianza 95%
P: Probabilidad de que el evento ocurra 0.5
Q: Probabilidad de que el evento no ocurra 0.5
E: Margen de error permitido 5%

$$n = \frac{1.96^2(0.5) * (0.5) * 50}{50(0.05)^2 + (1.96^2(0.5)) * (0.5)}$$

n= 220 empresas

A continuación, se exponen los métodos y técnicas aplicadas para las pruebas de intrusión como un método de evaluación de seguridad para la búsqueda de vulnerabilidades en las plataformas digitales, en la tabla II se encuentran las principales categorías basadas en OWASP donde se utilizó diferentes herramientas para recopilar información que se encuentra expuesta, para estas actividades se realizaron pruebas de tipo Caja Negra ya que no se dispone ninguna información de los sitios web con el fin de identificar las debilidades y poder evaluar de esta manera el nivel de riesgo de las amenazas.

Sin embargo, la metodología de OWASP define una variedad de pruebas de seguridad, tanto para caja negra y caja blanca, pero no se utilizó todas para evitar daños a los sitios web, es decir, no se va a realizar pruebas que dañen la integridad, confidencialidad y disponibilidad de la información, evitando así pruebas de ataques de fuerza bruta que provoque alguna denegación del servicio en la página web [20].

Tabla 2. Prueba de intrusión realizadas

Categoría	Prueba
Recopilación de información	Descubrimiento de Información expuesta con motores de búsqueda
	Identificar de puertos abiertos
	Identificar las IP de los servidores
	Identificar el servidor donde este alojado la plataforma web
	Identificar meta-archivos del servidor web y validar directorios o archivos expuestos
	Identificar aplicaciones que se encuentran en el servidor web.
	Identificar los puntos de entrada de la aplicación
	Detectar servicios utilizados en la página web
Gestión de configuración	Detección de la versión de las tecnologías utilizadas en el sitio web
	Validación de interfaces
	Validación de métodos http
	Seguridad en las cabeceras por http
Autenticación y autorización	Seguridad en cabeceras de autenticacion
	Validación de archivos que se encuentran en el sitio web alojado
Gestión de sesiones	Esquema de gestión de sesiones
	Renovación de las cookies
	Método TRACE
Errores comunes	Validación de Código de error 400
	Validación de cifrado SSL-TLS

2.1 Análisis de riesgos

Para el análisis de las vulnerabilidades se utilizó una matriz de escala de evaluación definida por la metodología de análisis y gestión de evaluación de riesgos MAGERIT [21], el cual permitió cuantificar el riesgo de las amenazas identificadas de acuerdo con las pruebas de intrusión realizados mediante OWASP. El uso de esta metodología permite evaluar cuantitativa y cualitativamente, es decir, para determinar los riesgos con más relevancia se categorizan de acuerdo con los principales aspectos de la seguridad que es la integridad, confidencialidad y disponibilidad.

Para identificar y comprender la valoración del riesgo se estableció la Tabla 3 con valores cuantitativos basado en la metodología de MARGERIT, para identificar la probabilidad de ocurrencia,

Tabla 3: Análisis de frecuencia – Vulnerabilidad

Comercio	Valor	Descripción	Probabilidad De ocurrencia
Muy frecuente	4	Ocurre de forma continua y permanente	75% - 100%
Frecuente	3	Ocurre más de una vez a la semana	50% - 75%
Frecuencia normal	2	Ocurre más de 1 vez al mes	25% - 50%
Poco frecuente	1	Insignificante posibilidad de ocurrencia o al menos 2 veces en un año.	0% - 25%

Mientras que, según se expone en la Tabla 4, se evaluó la valoración de impacto, así como confidencialidad, integridad y disponibilidad en función del daño técnico que las vulnerabilidades causan a una organización.

Tabla 4: Valoración de impacto

Comercio	Valor	Descripción
Crítico	5	I: Toda Información dañada C: Toda información expuesta D: Todos los servicios interrumpidos IMP: El daño que deriva la amenaza es grave
Alto	4	I: Gran información sensible dañada C: Informacion sensible expuesta D: Interrupción de servicios críticos IMP: El daño que deriva la amenaza genera un daño significativo
Medio	3	I: Gran información sensible dañada C: Gran información importante expuesta D: Gran interrupción de servicios IMP: El daño que deriva la amenaza es menor
Bajo	2	I: Mínima información sensible dañada C: Informacion relevante expuesta D: Mínima interrupción de servicios IMP: El daño que deriva la amenaza no genera consecuencias.
Muy Bajo	1	I: Poca información no sensible dañada C: Información no sensible expuesta D: Poca interrupción IMP: El daño que deriva la amenaza no genera consecuencias.

2.2 Evaluación de Riesgo

Así, para determinar el riesgo, se aplicó la ecuación (2) para considerar las variables impacto y probabilidad, con lo cual se obtiene un valor de consideración que se refleja en la Fig.4 permite evaluarlo en términos de escala cuantitativa y Fig.5 escala cualitativa.

$$R = Imp * Probabilidad \qquad (2)$$

Considerando que se estableció 4 niveles de riesgos categorizado su criticidad como muestra en la Fig. 3.

1	Bajo
2	Moderado
3	Alto
4	Extremo

Fig. 3. Niveles de riesgo

Riesgo			PROBABILIDAD				
			1	2	3	4	5
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
IMPACTO	5	Muy Alta	5	10	15	20	25
	4	Alta	4	8	12	16	20
	3	Moderada	3	6	9	12	15
	2	Baja	2	4	6	8	10
	1	Muy baja	1	2	3	4	5

Fig. 4. Nivel de Riesgo – cuantitativo

Riesgo			PROBABILIDAD				
			1	2	3	4	5
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
IMPACTO	5	Muy Alta	Moderado	Alto	Alto	Extremo	Extremo
	4	Alta	Moderado	Moderado	Alto	Extremo	Extremo
	3	Moderada	Bajo	Moderado	Alto	Alto	Extremo
	2	Baja	Bajo	Bajo	Moderado	Moderado	Alto
	1	Muy baja	Bajo	Bajo	Bajo	Moderado	Alto

Fig. 5. Nivel de Riesgo – cualitativo

3 Resultados

A interés de dar cumplimiento al propósito de la investigación sobre la existencia de vulnerabilidades en los sitios web, en primer lugar, se realizó la validación de seguridad de 220 empresas por lo que se ejecutaron 19 pruebas de intrusión con base a la guía que establece OWASP. Por lo tanto, las vulnerabilidades con más relevancia y que podrían poner en riesgo un sitio web se encuentran en la categoría de recopilación de información como se observa en la Fig.6.

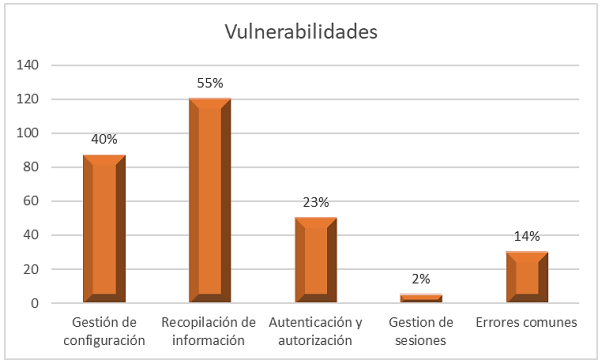

Fig. 6. Vulnerabilidades de sitios web - Empresas Ecuador

En las pruebas realizadas en la categoría de *Recopilación de Información* se utilizó la técnica de footprinting para acceder a la información pública mediante motores de búsqueda con el fin de encontrar información indexada y se utilizó las siguientes herramientas: Google, Shodan, Nslookup, Httprecon, Robots ,Nmap. Burp Suite, OWASP ZAP, Whatweb. En esta categoría se identificó que el 55% de empresas disponían información sensible expuesta como los puertos abiertos críticos tipo TCP y UDP, la vinculación de los sitios web a otros dispositivos, ubicación general del servidor y su dirección IP, ficheros con estado allow, exponiendo a los sitios web que sea víctima de ataques de intrusión.

En la Tabla 5 se muestra un resumen de las pruebas ejecutadas y las herramientas.

Tabla 5. Resumen pruebas ejecutadas Recopilación de Información

Prueba	Info	Herramientas	Vuln.
Identificar de puertos abiertos	URL	mnmap, Shodan	220
Identificar las IP de los servidores	IP	nslookup	220
Identificar el servidor donde este alojado la plataforma web	URL, IP	httprecon	67
Identificar meta-archivos del servidor web y validar directorios o archivos expuestos	URL	robots.txt	65
Identificar aplicaciones que se encuentran en el servidor web.	IP	Nmap	132
Identificar los puntos de entrada de la aplicación	URL	Burp Suite , Nmap	20
Mapear rutas de ejecución a través de la aplicación	URL	OWASP ZAP	58
Detectar servicios utilizados en la página web	URL	WhatWeb	220

En la Fig.7. se muestra las pruebas de intrusión con más porcentaje de vulnerabilidades encontradas.

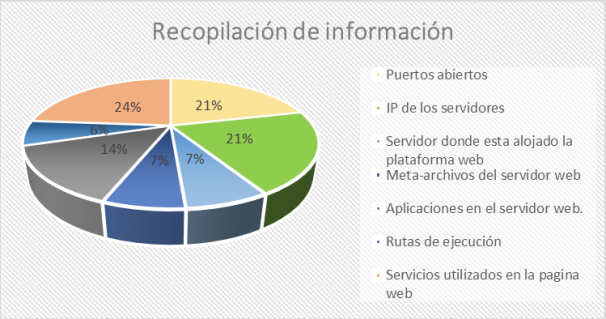

Fig. 7. Resumen pruebas ejecutadas Recopilación de Información

En las pruebas realizadas en la categoría de Gestión de configuración se utilizó herramientas como: Nikto, Interfaces de administración, Nmap y Curl, en esta categoría se identificó que el 40% de empresas tienen expuestas las versiones de las tecnologías utilizadas en los sitios web, cabeceras, métodos GET para recuperar recursos de un servidor web y métodos PUT que permitió enviar datos en el cuerpo del mensaje.

En la Tabla 6. se muestra un resumen de las pruebas ejecutadas y las herramientas.

Tabla 6. Resumen pruebas ejecutadas Gestión de configuración

Prueba	Info.	Herramientas	Vuln.
Detección de la versión de las tecnologías utilizadas en el sitio web	IP	nikto	150
Validación de interfaces	URL	/wp-admin /administrador /admin /user	36
Validación de métodos http	URL , IP	nmap --script http-methods	100
Seguridad en las cabeceras por http	URL	curl –I –s –k URL| grep Strict	62

En la Fig.8. se muestra las pruebas de intrusión con más porcentaje de vulnerabilidades encontradas

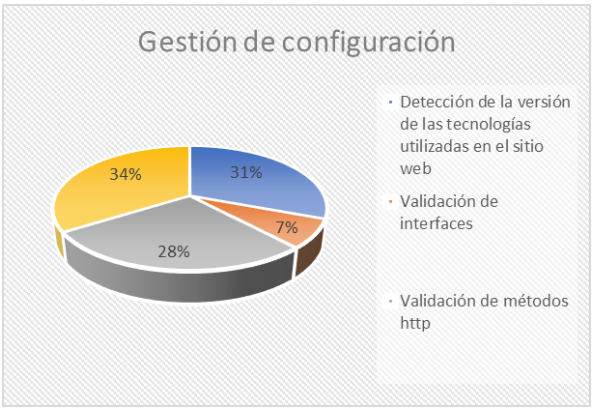

Fig. 8. Resumen pruebas ejecutadas Gestión de configuración

En la categoría de Autenticacion y Autorización se utilizó las herramientas Owasp ZA, se identificó que el 23% de empresas en sus cabeceras la información de autenticacion no tenían encriptada cuando se realizó las peticiones de GET y POST, de igual manera en la verificación de los archivos se encontró archivos alojados en los servidores web por lo que los sitios eran vulnerables ya que se puede redirigir a un sitio web principal.

En la Tabla 7 se muestra un resumen de las pruebas ejecutadas y las herramientas.

Tabla 7. Resumen pruebas ejecutadas Autenticación y autorización

Prueba	Info	Herramientas	Vuln.
Seguridad en cabeceras de autenticacion	URL	OWASP ZAP	67
Validación de archivos que se encuentran en el sitio web alojado	URL	Navegador site: ejemplo.com “php?id=”	38

En la Fig.9. se muestra las pruebas de intrusión con más porcentaje de vulnerabilidades encontradas

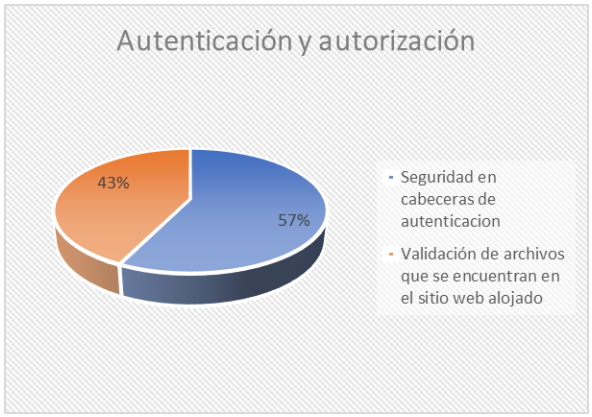

Fig. 9. Resumen pruebas ejecutadas Autenticación y autorización

En la *Gestión de sesione*s se realizó la validación de las cookies identificando si se crea de manera encriptada y no se pueda descifrar haciendo ingeniería inversa por lo que se validó el protocolo de transporte seguro HSTS.

En la Tabla 8 se muestra un resumen de las pruebas ejecutadas

Tabla 8. Resumen pruebas categoría Gestión de sesiones

Prueba	Info	Herramientas	Vuln.
Esquema de gestión de sesiones	URL	Scraping	2
Renovación de las cookie**s**	URL	Charles proxy	2
Método TRACE	URL	netcat	12

En la Fig.10. se muestra las pruebas de intrusión con más porcentaje de vulnerabilidades encontradas.

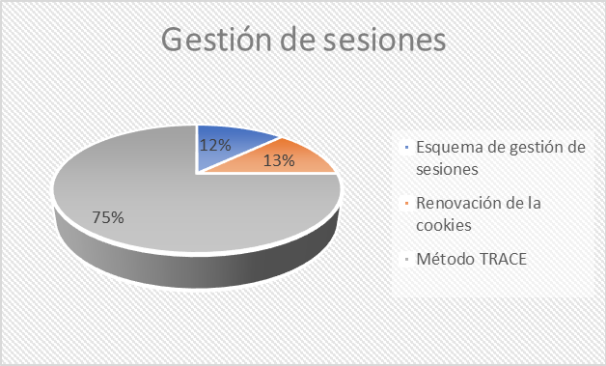

Fig. 10. Resumen pruebas ejecutadas Gestión de sesiones

En la categoría de *Errores comunes* se validó enlaces muertos mediante el código de error 400 lo cual contempla información de utilidad sobre el servidor web mediante la herramienta Telnet.

En la categoría de *Criptografía*, se identificó los servicios de seguridad SSL/TLS, mostrando protocolos y servicios que se encuentran dentro de la plataforma y a las que estarían expuestas los servicios web mediante la herramienta del Nmap como muestra en la Tabla 9.

Tabla 9. Resumen pruebas de Criptografía

Categoría	Prueba	Información	Herramientas
Criptografía	Validación de cifrado SSL-TLS	URL	nmap –sV –script ssl-enum-ciphers –p 443 <host>

A continuación, para identificar las amenazas, se estudió el catálogo de amenazas de la metodología de MARGERIT Libro II, apartado 5 [22], donde se consideraron amenazas que puedan vulnerar de acuerdo con las pruebas de intrusión.

Amenazas identificadas:

- Fuga de información
- Accesos no autorizados
- Explotar Cross-site tracing (TRACE)
- Informacion sensible expuesta
- Certificado para la página web

Una vez identificado las amenazas y las vulnerabilidades de cada prueba de intrusión ejecutada, se realizó un análisis de riesgo contemplando los tres pilares fundamentales de la Seguridad que es Confidencialidad, Integridad y Disponibilidad.

Para el análisis de riesgo en la Fig.11, se muestra el calculó del impacto y la probabilidad de los RF de las pruebas de intrusión, posterior, se evaluó los riesgos para identificar las pruebas que requieren ser tratados para establecer un método de reducción del impacto con el fin de aumentar la seguridad en los sitios web.

Categoría	RF	Prueba	Amenaza	Vulnerabilidad	I	C	D	Imp.	Prob.	Riesgo
Recopilación de información	Rf1	Identificar de puertos abiertos	Ingeniería social	Puertos críticos abiertos	5	4	5	5	4	20
	Rf2	Identificar las IP de los servidores	Ingeniería social	Direcciones IP	2	2	2	2	4	8
	Rf3	Identificar el servidor donde esta alojado la plataforma web	Acceso no autorizado a sistemas	Validación de tipo de servidores	3	3	4	3	3	9
	Rf4	Identificar meta-archivos del servidor web y validar directorios o archivos expuestos	Directorios con estado Allow	Intrusión de archivos con malware	3	5	1	3	4	12
	Rf5	Identificar aplicaciones que se encuentran en el servidor web.	Acceso no autorizado a sistemas	Datos del servidor, IP y dominio	1	1	1	1	3	3
	Rf6	Identificar los puntos de entrada de la aplicación	Acceso no autorizado a sistemas	Interseptar información mediante ataques de fuerza bruta	2	3	3	3	3	9
	Rf7	Mapear rutas de ejecución a través de la aplicación	Analisis de informacion de estructura de la platafoma	Interseptar información mediante ataques de fuerza bruta	3	3	2	3	3	9
	Rf8	Detectar servicios utilizados en la pagina web	Acceso no autorizado a sistemas	Versiones obsoletas	2	5	4	4	4	16
Gestión de configuración	Rf9	Detección de la versión de las tecnologías utilizadas en el sitio web	Acceso no autorizado a sistemas	Versiones obsoletas	4	5	3	4	1	4
	Rf10	Validación de interfaces	Acceso no autorizado a sistemas	Acceso a perfiles administrativos	2	4	1	2	2	4
	Rf11	Validación de métodos http	Acceso no autorizado a sistemas	Indisponibilidad de servicio	2	3	2	2	4	8
	Rf12	Seguridad en la cabeceras por http	Acceso no autorizado a sistemas	Información expuesta de fallas del servidor	3	4	4	4	4	16
Autenticación y autorización	Rf13	Seguridad en cabeceras de autenticacion	Acceso no autorizado a sistemas	Interceptar información sensible	2	1	5	3	3	9
	Rf14	Validación de archivos que se encuentran en el sitio web alojado	Acceso no autorizado a sistemas	Fuga de información	2	1	2	2	3	6
Gestión de sesiones	Rf15	Esquema de gestión de sesiones	Fuga de información	Protocolo de cifrado seguro HTTPS	3	1	4	3	3	9
	Rf16	Renovación de la cookies	Accesos no autorizados	Protocolo de cifrado seguro HTTPS	1	2	1	1	3	3
	Rf17	Método TRACE	Explotar Cross-site tracing (TRACE)	Métodos TRACE	2	1	4	2	3	6
Errores comunes	Rf18	Validación de Código de error 400	Informacion sensible expuesta	Divulgación de errores de los servidores web	2	4	4	3	4	12
Criptografía	Rf19	Validación de cifrado SSL-TLS	Certificado para la pagina web	Interceptar información sensible	4	1	1	2	3	6

Fig.11. Evaluación de riesgo - Margerit
I = Integridad C= Confidencialidad D= disponibilidad

En la siguiente Fig.12 , se presenta el mapa de riesgo de los RF (Requerimiento Funcional) ejecutadas, de los cuales 3 tenemos en zona Roja (Riesgo alto), 15 en zona amarilla (Riesgo medio) y 2 en zona verde (Riesgo Bajo).

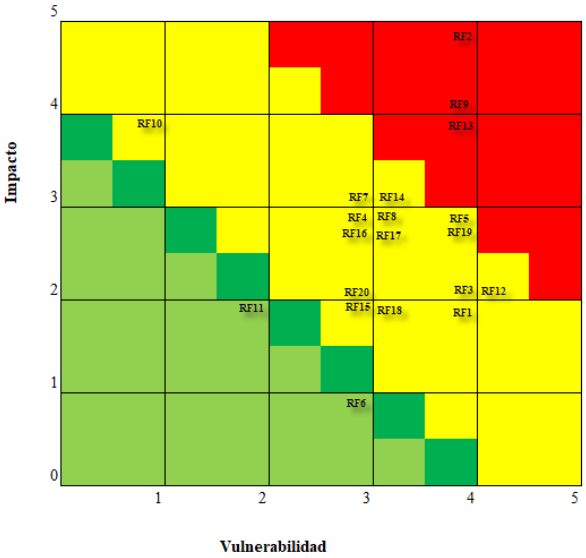

Fig. 12. Muestreo de mapa de riesgo

4 Recomendaciones

4.1 Buenas prácticas de seguridad en los sitios web

1 Forzar la finalización de sesión si se identifica que existe otro inicio de sesión con las mismas credenciales.
2 Utilización de certificado de seguridad SSL, utilizando protocolo seguro Https para que la información confidencial de los clientes y viaje de manera segura.
3 Para las empresas que manejan comercio digital es importante utilizar plataformas como PayPal para garantizar los pagos sea de manera segura.
4 Establecer actualizaciones permanentes de los servidores web como parchado virtual para mantener actualizada las versiones de los servicios utilizados.
5 Establecer un escaneo de vulnerabilidades con herramientas como el Nessus en los servidores donde este alojado los sitios web.
6 Analizar y validar las configuraciones existentes de cookies, con atracción especial a la configuración de las cookies JSESSIONID, basado en las mejores prácticas de seguridad.

4.2 Buenas prácticas de seguridad por expertos de Seguridad

Con el fin de validar nuestra investigación, se realizó una encuesta con cinco expertos de seguridad con los cargos Oficial de Seguridad de la información, Jefe De Riesgo Tecnológico–Proyectos, Especialista De Ciberseguridad, Gerente de Prevención de Fraudes, Gerente de riesgo operativo, sobre las buenas prácticas de seguridad en sitio web que tienen comercio electrónico, por lo que recomendaron los siguientes puntos:

Experto 1: Gerente De Prevención De Fraudes / Gerente de Riesgo Operativo

- Las páginas web que manejan diferentes tipos de comercio electrónico se recomienda implementar un software para antifraude y geolocalización con el fin de obtener los procesos fallidos mediante los pagos.

Experto 2: Gerente de riesgo operativo

- Se recomienda habilitar el protocolo EMV que se encuentra diseñado como una capa de seguridad adicional y permite que el cliente verifique que la transacción sea legitima con una autenticación.

Experto 3: Especialista De Ciberseguridad

- Para los usuarios que son administradores del sistema web se debería implementa una solución que permita Multi-Factor de autenticación (MFA), Doble factor de autenticación (2FA) en la administración de los equipos (servidores)

Experto 4: Oficial de Seguridad de la información,

- La arquitectura deberá considerar los estándares internos e internacionales de seguridad y buenas prácticas vigentes, a nivel de red, infraestructura, usuarios de conexión, base de datos, continuidad, ciberseguridad, etc.

5 Conclusiones

Las principales amenazas de seguridad cibernética que surgen en los sitios de comercio electrónico son aquellas que amenazan directamente la integridad de los datos del usuario, ya que los usuarios finales corren el mayor riesgo de vulnerabilidades potenciales de aplicaciones y sistemas.

Los errores internos dentro de un servidor web pueden corregirse lo suficiente como para que el sistema funcione de manera óptima utilizando tecnología y estándares internacionales que están fácilmente disponibles en esta era de globalización, sin embargo, los atacantes cibernéticos se aprovechan de la falta de conocimiento de la mayoría de usuarios para cometer sus robos y fraudes con una mayor destreza utilizando para dichos fines medios y técnicas tales como los robos tanto de identidad y de información.

En definitiva, en este documento se expone el crecimiento y la expansión del comercio electrónico en Ecuador lo cual ha supuesto una nueva problemática para los ciudadanos ya que al potenciarse el uso de Internet a la hora de comprar y vender productos y ofrecer servicios a través de la red, se ha abierto una nueva puerta a robos y fraudes informáticos que suponen un tráfico de información y datos personales y privados que las diferentes empresas obtienen mediante el acceso continuado de los usuarios a los diferentes sitios web.

En definitiva, a través de la investigación del comercio electrónico en Ecuador ha sido posible analizar las vulnerabilidades en los sitios web de lo cual favorecerá la realización de diferentes pruebas de intrusión para comprobar que tan vulnerables son los sitios web y que tan efectivas son las herramientas para combatirlos y asegurar el tráfico de datos en la red.

Finalmente, la validación de seguridad realizadas mediante la prueba de instrucción se limita a varios tipos de escaneo y detección en función de las vulnerabilidades encontradas en el sitio para otorgar recomendaciones de buenas prácticas que va a permitir reducir o mitigar el riesgo asociado con el ataque, permitiendo que el lector tenga conciencia y realice es estudio de sus plataformas y tomar acciones de mejora y levantar lineamientos de seguridad para desarrollo seguro de sitio web.

6 Referencias

[1] ESET, «Transformación digital: por qué el COVID-19 podría acelerar los procesos,» 202O. [En línea]. Available: https://www.welivesecurity.com/la-es/2020/05/11/transformacion-digital-por-que-covid-19-podria-acelerar-procesos/.

[2] U. d. E. E. Santo, «Comportamiento de Transacciones no presenciales en Ecuador,» 2022.

[3] C. E. d. C. Electrónico, «Comportamiento de Transacciones no presenciales en Ecuador,» 2022.

[4] M. D. TELECOMUNICACIONES, «ESTRATEGIA NACIONAL DE COMERCIO ELECTRÓNICO,» Quito, 2020.

[5] Tkanalytics, «La ciberseguridad en el ecommerce: ¿por qué es clave para tener éxito?,» 20 Noviembre 2021. [En línea]. Available: https://tkanalytics.es/la-ciberseguridad-en-el-ecommerce-por-que-es-clave-para-tener-exito/#:~:text=Todo%20ecommerce%20

debe%20cumplir%20con,en%20su%20defecto%2C%20se%20mitiguen..

[6] R. Jupiter, «ECOMMERCE LOSSES TO ONLINE PAYMENT FRAUD TO EXCEED $20 BILLION ANNUALLY IN 2021,» 26 Abril 2021. [En línea]. Available: https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-exceed-20bn.

[7] R. Juniper , «Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028,» 26 06 2023. [En línea]. Available: https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report.

[8] C. Point, «Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks,» 5 Enero 2022. [En línea]. Available: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/#:~:text=Global%20cyberattacks%20increased%20by%2038,%2Dlearning%20post%20COVID%2D19..

[9] M. R. Díaz, «La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad,» CEPAL, 2020.

[10] Ticpymes, «El 85% de los ataques contra activos digitales es consecuencia del error humano.,» 10 11 2022.

[11] F. Ureña Centeno, «CYBERATAQUE, LA MAYOR AMENAZA ACTUAL,» 16 enero 2015. [En línea]. Available: https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

[12] «Robo o Scraping de cookies – ¿Por qué los ciberdelincuentes quieren tus cookies?,» HACKWISE, 1 mayo 2021. [En línea]. Available: https://hackwise.mx/robo-o-scraping-de-cookies-por-que-los-ciberdelincuentes-quieren-tus-cookies/#:~:text=%C2%BFDiferentes%20m%C3%A9todos%20de%20robo%20de%20cookies%20y%20secuestro,Scripting-XSS%29%20...%204%204.%20Ataque%20de%20malware%20.

[13] «NORMA ISO 27001,» ISO, [En línea]. Available: https://normaiso27001.es/.

[14] O. d. l. ciberseguridad, «Ciberseguridad en America Latina y el Caribe,» 2020, [En línea]. Available: https://observatoriociberseguridad.org/#/home.

[15] Ministerio de Telecomunicaciones y Sociedad de la Información, «ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR,» 2022. [En línea]. Available: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf.

[16] Y. T. Indio, «Trabajo de grado Universidad Politécnica Salesiana,» 06 2021. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf.

[17] Stackscale, «Modelo OSI: capas y ataques informáticos,» 27 04 2023. [En línea]. Available: https://www.stackscale.com/es/blog/modelo-osi/.

[18] OWASP, «Application Security Verification Standard 4.0.3 OWASP,» octubre 2021. [En línea]. Available:

https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-es.pdf.

[19] H. R. González Brito y R. P. Montesino , «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web,» vol. 12, nº 4, pp. 52-65, 08 octubre 2018.

[20] O. Foundation, «GUÍA DE PRUEBAS OWASP,» 2002-2008 . [En línea]. Available: https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf.

[21] M. d. H. y. A. Públicas, TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[22] C. S. d. A. E. d. G. d. España, «Magerit versión 3.0: Metodología de análisis y gestión de riesgo,» [En línea]. Available: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos.