REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

ANÁLISIS DE VULNERABILIDADES EN SERVIDORES DE APLICACIONES EMPRESARIALES MEDIANTE TÉCNICAS DE PENTESTING UTILIZANDO LA METODOLOGÍA OWASP Y PTES: ESTUDIO DE CASO EMPRESA CUBOSOFT

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en seguridad informática

AUTOR: Jefferson Stalin Yacelga Almeida

DIRECTOR: Ph.D. Cathy Pamela Guevara Vega

IBARRA - ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003770490		
APELLIDOS Y NOMBRES:	Yacelga Almeida Jefferson Stalin		
DIRECCIÓN:	Conjunto Laureles 5 casa #12, Luciano Andrade y Muñoz Vicuña, Ibarra, Ecuador		
EMAIL:	jeffersonyacelga@hotmail.com		
TELÉFONO FIJO:	0981438167	**TELÉFONO MÓVIL:**	0981438167

DATOS DE LA OBRA	
TÍTULO:	ANÁLISIS DE VULNERABILIDADES EN SERVIDORES DE APLICACIONES EMPRESARIALES MEDIANTE TÉCNICAS DE PENTESTING UTILIZANDO LA METODOLOGÍA OWASP Y PTES: ESTUDIO DE CASO EMPRESA CUBOSOFT
AUTOR (ES):	Yacelga Almeida Jefferson Stalin
FECHA:	05-06-2024
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en seguridad informática
ASESOR /DIRECTOR:	Msc. Mauricio Rea / Ph.D. Cathy Guevara

2. CONSTANCIAS

El autor Yacelga Almeida Jefferson Stalin, manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 05 días del mes de junio del 2024

EL AUTOR:

JEFFERSON STALIN YACELGA ALMEIDA

Firmado digitalmente por JEFFERSON STALIN YACELGA ALMEIDA
Fecha: 2024.06.05 16:12:23 -05'00'

Nombre: Jefferson Yacelga

APROBACIÓN DEL TUTOR

Yo Ph.D. Guevara Vega Cathy Pamela, en calidad de director de la tesis titulada: "ANÁLISIS DE VULNERABILIDADES EN SERVIDORES DE APLICACIONES EMPRESARIALES MEDIANTE TÉCNICAS DE PENTESTING UTILIZANDO LA METODOLOGÍA OWASP Y PTES: ESTUDIO DE CASO EMPRESA CUBOSOFT" de auditoría del Ing. Jefferson Stalin Yacelga Almeida, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 05 días del mes de junio de 2024

Lo certifico

1002334835
CATHY PAMELA
GUEVARA VEGA

Firmado digitalmente por 1002334835 CATHY PAMELA GUEVARA VEGA
Fecha: 2024.06.05 16:09:54 -05'00'

Ph.D. Guevara Vega Cathy Pamela
DIRECTOR DE TESIS

DEDICATORIA

Dedico todo el esfuerzo realizado principalmente a DIOS, que me ha acompañado durante estos años apoyándome en cada paso que doy y dándome fuerzas para afrontar los retos que se presentan a lo largo de mi camino.

A mi hermana Jessica Yacelga, le agradezco de corazón por estar a mi lado en cada momento, tanto en las alegrías como en las dificultades que nos ha tocado enfrentar juntos.

Asimismo, dedico este trabajo a mi pareja Samantha Mafla, quien ha sido mi fuente de amor, paciencia y apoyo incondicional en cada paso y decisión que he tomado.

Jefferson Yacelga

AGRADECIMIENTOS

En primer lugar, quiero expresar mi profundo agradecimiento a Dios por permitirme llegar a este momento en mi vida, brindándome la oportunidad de crecer profesionalmente, cuidando de mi salud y brindándome trabajo a pesar de las dificultades que se han presentado.

También deseo agradecer especialmente a mi hermana, quien siempre ha estado a mi lado, brindándome su apoyo y disposición para ayudarme en cualquier situación.

Agradezco a mi pareja actual por su incondicional apoyo y por acompañarme en mis decisiones, incluso en los momentos más difíciles.

Quiero expresar mi más sincero agradecimiento a Cubosoft por brindarme la oportunidad de realizar mi trabajo de grado en su empresa. El apoyo y la colaboración que recibí fueron fundamentales para el éxito de este proyecto, y la experiencia adquirida ha sido invaluable para mi desarrollo profesional y académico.

Asimismo, agradezco profundamente a mi tutora de tesis Ph.D. Cathy Guevara por su invaluable orientación y apoyo a lo largo de este emocionante viaje académico. Sus consejos expertos y su retroalimentación constructiva han sido una guía invaluable en cada paso del proceso de investigación. Estoy profundamente agradecido por su compromiso, inspiración y confianza en mi trabajo.

Por último, deseo expresar mi gratitud a la Universidad Técnica del Norte y a todos los docentes que han formado parte de este proceso de crecimiento profesional. Agradezco sinceramente los conocimientos compartidos y el apoyo brindado durante mi formación académica.

Jefferson Yacelga

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

ANÁLISIS DE VULNERABILIDADES EN SERVIDORES DE APLICACIONES EMPRESARIALES MEDIANTE TÉCNICAS DE PENTESTING UTILIZANDO LA METODOLOGÍA OWASP Y PTES: ESTUDIO DE CASO EMPRESA CUBOSOFT

Autor: Yacelga Almeida Jefferson Stalin
Tutor: Ph.D. Cathy Guevara
Año: 2024

RESUMEN

La presente investigación sobre vulnerabilidades en servidores de aplicaciones empresariales realizada para la empresa Cubosoft, utilizando las metodologías OWASP y PTES, revela un panorama crítico de amenazas cibernéticas. A través del pentesting, se descubrieron desde fallos de configuración hasta posibles inyecciones de código malicioso, destacando la importancia de aplicar una cultura de seguridad y comunicación efectiva en toda la organización. La validación de mitigaciones propuestas y el análisis detallado de datos del pentesting ofrecen recomendaciones concretas para fortalecer la seguridad, resaltando la necesidad de métodos estructurados y gestión proactiva de riesgos para salvaguardar los sistemas empresariales.

La investigación no solo se queda en la identificación de problemas, sino que también proporciona soluciones tangibles y prácticas. La validación de las medidas de mitigación propuestas, junto con un análisis detallado de los datos obtenidos durante el proceso de pentesting, culmina en una serie de recomendaciones sólidas y concretas para fortalecer la seguridad del sistema. Este análisis destaca la importancia de enfoques estructurados y proactivos en la gestión de riesgos cibernéticos, delineando un camino claro hacia la protección y la resiliencia en un mundo digital cada vez más complejo y desafiante.

Palabras clave: Análisis de vulnerabilidades, Pentesting, OWASP, PTES

ABSTRACT

Cubosoft's research into vulnerabilities in enterprise application servers, using OWASP and PTES methodologies, reveals a critical landscape of cyber threats. Through pentesting, everything from configuration errors to possible malicious code injections were discovered, highlighting the importance of applying a security culture and effective communication throughout the organization. Validation of proposed mitigations and detailed analysis of pentesting data provide concrete recommendations to strengthen security, highlighting the need for structured methods and proactive risk management to save enterprise systems.

Research not only identifies problems, but also provides tangible and practical solutions. The successful validation of the proposed mitigation measures, together with a detailed analysis of the data obtained during the pentesting process, culminates in a series of solid and concrete recommendations to strengthen the security of the system. This analysis highlights the importance of structured and proactive approaches in cyber risk management, outlining a clear path to protection and resilience in an increasingly complex and challenging digital world.

Palabras clave: Vulnerability analysis, Pentesting, OWASP, PTES

CAPITULO I
EL PROBLEMA

1.1. Problema de investigación

En el entorno tecnológico actual, caracterizado por la creciente complejidad y conexión de varios sistemas, el incremento exponencial de las amenazas cibernéticas plantea un desafío significativo. La defensa y protección en el ámbito cibernético adquiere un papel crucial para garantizar la seguridad y la adaptación de las infraestructuras críticas. La convergencia tecnológica, junto con la densidad digital y la presencia de productos y servicios digitalmente modificados, ha aumentado los niveles de riesgo cibernético (Realpe & M., 2020).

En la actualidad, los activos más valiosos para las organizaciones empresariales son los sistemas de información, los datos que contienen y la información en sí. Sin embargo, estos activos se encuentran expuestos a posibles intrusiones debido a las vulnerabilidades existentes en sus sistemas de seguridad. Es necesario brindarles una protección adecuada para mitigar estas amenazas (Solarte Solarte, Enriquez Rosero, & Benavides, 2015).

Una manera efectiva de descubrir y abordar estas vulnerabilidades y amenazas es a través de procesos diagnósticos que permitan evaluar el estado actual de la seguridad dentro de la organización. Esto implica tener en cuenta la normatividad vigente y utilizar procesos de análisis y evaluación de riesgos (Solarte Solarte, Enriquez Rosero, & Benavides, 2015).

El análisis y la evaluación de riesgos, junto con la verificación de la existencia de controles de seguridad, pruebas con software y el monitoreo de los sistemas de información, son elementos clave para establecer el estado actual de seguridad de la organización. Estos procesos permiten identificar las causas subyacentes de las vulnerabilidades y proponer soluciones de control que contribuyan a su mitigación (Solarte Solarte, Enriquez Rosero, & Benavides, 2015).

El análisis de las causas y consecuencias del problema de seguridad en los servidores de aplicaciones empresariales de Cubosoft muestra una serie de deficiencias preocupantes en materia de protección de datos. La falta de políticas de seguridad adecuadas, la ausencia de recursos humanos capacitados en pruebas de penetración (pentesting) y el desconocimiento de metodologías de evaluación de vulnerabilidades como OWASP y PTES son posibles causas identificadas. Estas vulnerabilidades pueden

dar lugar a graves consecuencias, como brechas de seguridad, pérdida de datos, daños a la reputación de la empresa y posibles sanciones legales.

Es importante destacar que Cubosoft es una empresa dedicada a la automatización de laboratorios clínicos, donde se lleva a cabo este estudio. La falta de medidas de seguridad en sus servidores de aplicaciones empresariales representa un riesgo significativo para la integridad de los datos de los clientes y la continuidad de sus operaciones.

Debido a la falta de análisis y evaluaciones de riesgos se concreta en la necesidad de generar conocimiento para resolver el problema específico de las vulnerabilidades en los servidores de aplicaciones empresariales de Cubosoft.

1.2. Interrogantes de la investigación

- ¿Cuáles son las técnicas de pentesting más efectivas para detectar las principales vulnerabilidades en los servidores de aplicaciones empresariales utilizados en la empresa Cubosoft?
- ¿Qué vulnerabilidades se pueden detectar en los servidores de aplicaciones empresariales de la empresa Cubosoft mediante pruebas de pentesting utilizando la metodología OWASP y PTES?
- ¿Cómo se puede desarrollar un proceso de seguridad basado en la metodología OWASP y PTES para su implementación en entornos empresariales?
- ¿Qué resultados se obtienen al aplicar una prueba de concepto del proceso de seguridad recomendado en el módulo de resultados web de los servidores de aplicaciones empresariales de la empresa Cubosoft?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Realizar un análisis de vulnerabilidades en servidores de aplicaciones empresariales mediante técnicas de pentesting utilizando la metodología OWASP y PTES, para desarrollar un proceso de seguridad recomendado para la implementación en entornos empresariales de la empresa Cubosoft.

1.3.2 Objetivos específicos

1. Identificar las técnicas de pentesting más efectivas para detectar las principales vulnerabilidades en los servidores de aplicaciones empresariales utilizados en la empresa Cubosoft.

2. Realizar pruebas de pentesting en los servidores de aplicaciones empresariales de la empresa Cubosoft mediante la metodología OWASP y PTES, para detectar vulnerabilidades.
3. Evaluar el informe técnico mediante una prueba de concepto aplicada al módulo de resultados web en los servidores de aplicaciones empresariales de la empresa Cubosoft.

1.4 Justificación

La seguridad de los servidores de aplicaciones empresariales es fundamental para proteger la información sensible y garantizar la confidencialidad, integridad y disponibilidad de los datos. En el caso de Cubosoft, una empresa especializada en la automatización de laboratorios clínicos (Cubososft, 2022), la seguridad de los servidores es crucial debido a la naturaleza de los datos de pacientes y procesos médicos que manejan.

Al asegurar la seguridad de los servidores de aplicaciones utilizados por Cubosoft, se protege la privacidad y confidencialidad de la información de los pacientes, lo que a su vez mejora la calidad de vida de la comunidad y genera confianza en los servicios de salud.

Los servidores de aplicaciones empresariales son objetivos frecuentes de ataques cibernéticos debido a la sensibilidad de la información que almacenan. Por ello, utilizar metodologías como OWASP (Open Web Application Security Project) y PTES (Penetration Testing Execution Standard) para realizar análisis de vulnerabilidades y pruebas de penetración es de vital importancia.

Este proyecto se encuentra alineado con el Plan de Creación de Oportunidades 2021-2025 aportando en sus 5 ejes (Secretaría Nacional de Planificación, 2021) mediante el desarrollo económico al fortalecer la seguridad de los datos y la infraestructura tecnológica, generando confianza en el entorno empresarial y atrayendo inversiones. Además, protege la información y promueve el bienestar digital de los usuarios y clientes, asegurando la privacidad y seguridad de los datos. Asimismo, el proyecto contribuye a garantizar la seguridad ciudadana y el orden público al abordar las vulnerabilidades en los servidores de aplicaciones empresariales. Aunque de manera indirecta, también se relaciona con la transición ecológica al prevenir posibles impactos negativos en el medio ambiente a través del fortalecimiento de la seguridad. Finalmente, el proyecto promueve

la transparencia, ética pública y cumplimiento de buenas prácticas, fomentando una cultura empresarial de integridad y lucha contra la corrupción.

En el marco del cambio de la matriz productiva en Ecuador, se destaca la importancia de garantizar estándares de calidad tanto en la producción nacional como en los servicios empresariales. La Secretaría Nacional de Planificación y Desarrollo 2017-2021 "Toda una Vida", a través de la Política 5.8, establece directrices para fomentar la producción con responsabilidad social y ambiental, lo que incluye el manejo eficiente de recursos y el uso de tecnologías limpias y duraderas (Guerra Guzmán, Guevara Vega, Imbaquingo Esparza, Guevara Vega, & Jácome León, 2019). En este contexto, la seguridad de los servidores de aplicaciones empresariales cobra relevancia, ya que garantiza la integridad y confidencialidad de la información, aspectos fundamentales para el desarrollo sostenible de las empresas en el ámbito nacional e internacional.

También se enmarca dentro de algunos de los Objetivos de Desarrollo Sostenible (ODS) los cuales son de carácter global dedicados a erradicar la pobreza, proteger el planeta y asegurar la prosperidad y la paz, orientados a la acción y universalmente aplicables, concisos y fáciles de comunicar (ODS Territorio Ecuador, s.f.).

Figura 1 Objetivos del desarrollo sostenible
Fuente: https://odsterritorioecuador.ec/ods/

- ODS 9: Industria, Innovación e Infraestructura: El análisis de vulnerabilidades y el fortalecimiento de la seguridad en servidores de aplicaciones empresariales contribuyen a promover infraestructuras resilientes, sostenibles y seguras. Esto es fundamental para garantizar la estabilidad y el funcionamiento adecuado de las

aplicaciones empresariales que respaldan las actividades económicas y la innovación tecnológica.

- ODS 16: Paz, Justicia e Instituciones Sólidas: Fortalecer la seguridad en los servidores de aplicaciones empresariales ayuda a prevenir posibles ataques cibernéticos, minimizando así los riesgos de pérdida de datos, interrupciones operativas y violaciones de privacidad. Esto contribuye a promover sociedades pacíficas, justas e inclusivas, al garantizar la protección de la información y la integridad de los sistemas empresariales.
- ODS 17: Alianzas para lograr los objetivos: La colaboración entre diferentes actores, como empresas, organismos gubernamentales y sociedad civil, es esencial para abordar los desafíos de seguridad en servidores de aplicaciones empresariales. El desarrollo de un proceso de seguridad recomendado basado en metodologías reconocidas, como OWASP y PTES, y la realización de pruebas de concepto para evaluar su eficacia, requieren alianzas estratégicas y cooperación entre diversas partes interesadas.

El proyecto de investigación se relaciona con la línea de investigación Nro. 10 vigente y aprobada por el Honorable Consejo Universitario de la Universidad Técnica del Norte el cual indica “Desarrollo, aplicación de software y cyber security (seguridad cibernética)” (UTN, 2023).

CAPITULO II
MARCO REFERENCIAL

2.1. Antecedentes

Durante el año 2022, se observaron diferentes incidentes y tendencias en el ámbito de la ciberseguridad, desde el surgimiento de ciberataques destructivos en el contexto del conflicto entre Rusia y Ucrania. Los ataques apuntaron a infraestructuras criticas empleando malware e incluso las grandes compañías se vieron afectadas infiltrando datos internos y confidenciales y exponiendo la vulnerabilidad incluso de empresas con gran envergadura resaltando la importancia de abordar adecuadamente la ingeniería social para proteger los sistemas (Harán, 2022).

En América Latina, los organismos públicos fueron objeto de numerosos ataques de ransomware y filtraciones de datos durante 2022. En Costa Rica, los grupos Conti y Hive afectaron a más de 25 entidades gubernamentales, ocasionando interrupciones en servicios críticos como el cobro de impuestos, el pago de salarios y el sistema de salud pública. Estos incidentes generaron preocupación a nivel nacional y evidenciaron la necesidad de fortalecer la seguridad en los entornos públicos (Harán, 2022).

Estos antecedentes subrayan la importancia de abordar de manera integral la seguridad de los servidores de aplicaciones empresariales, considerando tanto las técnicas de pentesting efectivas para detectar vulnerabilidades como el desarrollo de un proceso de seguridad basado en metodologías reconocidas, como OWASP y PTES. Asimismo, estos eventos resaltan la necesidad de estar alerta ante posibles ataques y la importancia de implementar medidas de protección adecuadas en entornos empresariales.

Además, se ha observado que la optimización y automatización de procesos de gestión de requisitos funcionales en el desarrollo de software juega un papel crucial en la prevención de vulnerabilidades y la mejora de la seguridad en los sistemas empresariales. Según investigaciones recientes (Guevara-Vega, Guzmán-Chamorro, Guevara-Vega, Andrade, & Quiña-Mera, 2019), la gestión inadecuada de requisitos funcionales puede conducir a problemas en el desarrollo de software, lo que a su vez puede exponer a la empresa a riesgos de seguridad. Por lo tanto, es fundamental implementar prácticas eficientes en la gestión de requisitos funcionales, no solo para mejorar la calidad del software, sino también para fortalecer la seguridad de los sistemas empresariales.

Según (Chilán González, Francisco Bolaños, & Navira Angulo, 2019) los ataques más frecuentes se dirigen a hospitales, donde los cibercriminales suelen exigir un rescate de entre $200 y $500 dólares para restaurar los archivos afectados. En el caso del

ransomware Samsam para Windows, el atacante aprovecha la red de la organización y se autentica en el servidor JBoss a través de SSH.

2.2. Marco teórico

2.2.1 Seguridad informática

2.2.1.1. Introducción a la Seguridad Informática.

Con el objetivo principal de garantizar la integridad y privacidad de los datos almacenados en los sistemas informáticos, la seguridad informática es una disciplina esencial en la era digital que se basa en políticas y regulaciones internas y externas de una organización. En un mundo cada vez más dependiente de la tecnología, esta disciplina es esencial para proteger la información confidencial en poder de una organización de una amplia gama de peligros, incluidos problemas lógicos y físicos (Urbina, 2016).

Las organizaciones ahora son vulnerables a una variedad de amenazas cibernéticas, que van desde el robo de datos hasta interrupciones en las operaciones corporativas, como resultado de la creciente interconexión de los dispositivos y la transferencia de datos en línea. Como resultado, la seguridad informática es crucial en la era digital y, para comprenderla completamente, es necesario investigar las propiedades de la información y las ideas principales detrás de este campo (Mayacela & Guerrero, 2023).

La seguridad informática es un conjunto de técnicas y herramientas que están centradas en la protección de la información, esto incluye también los activos tecnológicos y afines de la empresa los cuales pueden incluir equipos, impresoras, servidores, equipos de red para protección de intrusos (Erazo, 2017).

2.2.1.2 Características Fundamentales de la Información

Cuando se trata de seguridad informática, la información posee cualidades esenciales que garantizan tanto su seguridad como su utilidad:

- **Eficaz:** Significa que debe ser suficiente y apropiada para completar las tareas particulares que le asigna la organización. Debe contener sólo la cantidad adecuada de información.
- **Eficiente:** La información debe crearse y manejarse de manera que se maximicen los recursos de la organización, incluidas las personas y el tiempo.
- **Confidencialidad:** Los datos están protegidos contra accesos, manipulaciones y robos no deseados. Para mantener la privacidad de los datos, esto es esencial.

- **Precisa:** La información completa para los usos previstos y para cumplir con los estándares y valores de la organización, debe cumplir con estos requisitos.
- **Disponibilidad:** La información debe estar disponible para su procesamiento en todo momento y cuando sea necesario para las operaciones de la empresa.
- **Leyes y regulaciones:** La información que cumple con las leyes y regulaciones internas y externas que impactan a la empresa está garantizada por el cumplimiento de normas.
- **Confiabilidad:** La información no puede ser cambiada o modificada sin la autorización requerida, según confiabilidad.

Estas cualidades sirven como un pilar de la seguridad de la información y son necesarias para garantizar que los datos se gestionen de forma segura y eficiente dentro de una empresa (Urbina, 2016).

2.2.1.3 Importancia de la Seguridad Informática

La protección de la infraestructura de TI y los activos de información de una organización depende en gran medida de la ciberseguridad. Su importancia no ha hecho más que aumentar debido al continuo aumento de las ciberamenazas.

La autenticación y el control de acceso son dos temas importantes cubiertos por la seguridad de la información. Controlar quién está autorizado a acceder a datos confidenciales se conoce como control de acceso. Verificar la identificación de personas o entidades que interactúan con sistemas informáticos mediante técnicas como contraseñas, huellas dactilares o autenticación multifactor se conoce como autenticación.

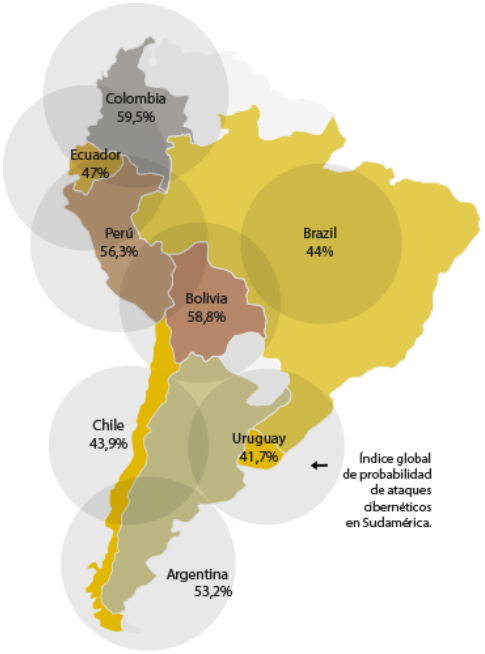
Encontrar posibles peligros y reducir los riesgos son los objetivos principales de la seguridad informática para mantener las operaciones corporativas. Será necesario el uso de varias tácticas para lograrlo. Para salvaguardar los sistemas de información se incluyen métodos técnicos como la instalación de cortafuegos y sistemas de detección y prevención de intrusos. También se recomienda el uso de redes privadas virtuales (VPN) para agregar un grado adicional de protección al conectarse a redes Wi-Fi inseguras.

Reducir la susceptibilidad de la organización a los ataques cibernéticos también requiere capacitación continua del personal sobre procedimientos de seguridad, incluida la creación de contraseñas seguras y la confirmación de la legitimidad de los correos electrónicos y sitios web (Mayacela & Guerrero, 2023).

2.2.1.4 Seguridad informática en Ecuador

La transacción digital ha llevado a la creación de una masiva cantidad de datos, lo que aumenta enormemente la posibilidad de ataques e infracciones de terceros. Ecuador ha tenido un gran impacto por este fenómeno, ya que las empresas están transfiriendo sus datos a la nube, aumentando su vulnerabilidad a los ciberataques. Además, el aumento de los ciberataques en todo el mundo plantea la cuestión de cómo las empresas pueden defenderse adecuadamente. Es fundamental mantenerse al día con los avances en ciberseguridad para adaptarse a las amenazas en constante cambio y preservar una postura defensiva sólida (Mayacela & Guerrero, 2023).

Según Mayacela & Guerrero (2023), "Ecuador en el 2022 se tuvo un índice de probabilidad de ataques cibernéticos de un 47% siendo el quinto más alto de Sudamérica y se ha tenido un incremento con respecto al 2021 de hasta un 66% en la industria minorista y mayorista a nivel global".



ÍNDICE GLOBAL DE ATAQUES CIBERNÉTICOS SEMANALES POR INDUSTRIA 2022 COMPARADO CON EL 2021

Industria	Número de ataques	Incremento % vs 2021
Educación / Investigación	2.314	+43%
Gobierno / Milicia	1.661	+46%
Salud	1.463	+74%
Comunicación	1.380	+27%
ISP / MSP	1.372	+28%
Finanzas / Banca	1.131	+52%
Servicios públicos	1.101	+48%
Seguros / Legal	957	+47%
Manufactura	950	+36%
Ocio / Hotelería	943	+60%
SI/VAR/ Distribuidores	904	+18%
Minoristas / Mayoristas	871	+66%
Transporte	750	+41%
Vendores de *Software*	747	+37%
Consultores	689	+19%
Vendedor de *Hardware*	448	+25%

Figura 2 Índice Global de ataques cibernéticos
Fuente: https://bit.ly/3U1HIzu

En Ecuador, se han identificado varios tipos de amenazas cibernéticas, desde Botnets hasta Ransomware. Estas amenazas requieren medidas proactivas y una mayor concienciación para reducir la vulnerabilidad de las empresas frente a posibles ataques. Para comprender estos tipos de amenazas es fundamental para fortalecer la seguridad informática en el entorno empresarial y para proteger los activos de información crítica (Mayacela & Guerrero, 2023).

Un componente esencial de la seguridad de la red de telecomunicaciones del Ecuador es el Ministerio de Telecomunicaciones y para la Sociedad de la Información "MINTEL". El MINTEL organiza trabajos técnicos a nivel nacional e internacional para garantizar un uso más seguro de estas redes a través del Centro de Respuesta a Incidentes Informáticos del Ecuador "EcuCERT", que forma parte de la Agencia de Regulación y Control de las Telecomunicaciones "ARCOTEL". Para salvaguardar a los usuarios de TIC del país, la cooperación entre los sectores público y comercial es crucial. La Ley Orgánica de Telecomunicaciones, la Ley de Comercio Electrónico, la Ley de Firmas Electrónicas y Mensajes de Datos, la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos conforman el sólido marco legal de ciberseguridad del Ecuador. Estas leyes sientan las bases para salvaguardar la privacidad y los datos de los ciudadanos y, al mismo tiempo, reiteran la importancia de la seguridad informática (Ministerio de Telecomunicaciones del Ecuador, 2017).

Con la implementación de la Ley de Comercio Electrónico, que tiene como objetivo proteger los derechos de los usuarios que realizan transacciones en línea. Esta ley establece normativas específicas para regular la publicidad en línea y fortalecer el derecho a la privacidad de los usuarios, aspectos fundamentales en un entorno digital en constante evolución.

Además, el Código Penal ecuatoriano ha incorporado disposiciones para sancionar los delitos informáticos, que abarcan desde el fraude electrónico hasta la intercepción de mensajes de datos y el acceso no autorizado a información privada. Estas medidas son cruciales para garantizar una seguridad básica en el ámbito empresarial y comercial (Basantes Andrade, y otros, 2017).

2.2.2 Gestión de riesgos

El análisis de riesgo es esencial para anticiparse a los riesgos futuros y estar preparados para enfrentarlos siendo esto un componente esencial para la protección de los activos críticos de una organización y en la anticipación de amenazas futuras. Esto implica la capacidad de identificar, evaluar y abordar las amenazas que podrían afectar a

los activos de la organización, priorizando las acciones necesarias (Maíllo Fernández, 2020).

2.2.2.1 Identificación de Amenazas

En esta fase, se analizan las posibles amenazas que pueden afectar a los activos identificados. Las amenazas pueden surgir de diversas fuentes, como:

- Amenazas ambientales (por ejemplo, desastres naturales).
- Amenazas humanas (acciones intencionadas o no intencionadas de individuos).
- Amenazas internas (provenientes de empleados o personal interno) o externas (como ataques de hackers).

Una evaluación de riesgos precisa requiere comprender que las vulnerabilidades y las malas configuraciones son la causa fundamental de muchas amenazas.

2.2.2.2 Análisis del Impacto

Una vez que se han identificado los activos y las amenazas, se procede al análisis del impacto el cual se centra en determinar las consecuencias que podrían resultar si una amenaza se materializa en el negocio. Esto incluye la evaluación de pérdidas económicas, pérdida de reputación y otros efectos tangibles e intangibles. Comprender el impacto de las amenazas es esencial para priorizar adecuadamente la gestión de riesgos.

2.2.2.3 Priorización de las Amenazas

La priorización de amenazas implica evaluar tanto el impacto como la probabilidad de ocurrencia (likelihood of occurrence) de cada amenaza. Esto ayuda a centrarse en las amenazas más críticas o aquellas con mayor probabilidad de impacto. Las métricas como CVSS (Common Vulnerability Scoring System) que pueden ser utilizadas para asignar valores a los riesgos identificados (Maíllo Fernández, 2020).

2.2.2.4 Identificación de Técnicas de Mitigación del Riesgo

Una vez priorizadas las amenazas, es necesario buscar soluciones para mitigar el riesgo. Esto implica la implementación de medidas y tecnologías de seguridad, como:

- Firewalls.
- Cifrado.
- Sistemas de control de acceso.
- Sistemas de prevención de intrusos (IPS).
- Actualizaciones de software y firmware.

- Auditorías de seguridad, entre otros.

La gestión de riesgos es esencial para salvaguardar la seguridad de la información y proteger los activos críticos de una organización. Al adoptar un enfoque sistemático, las organizaciones pueden reducir de manera efectiva las amenazas y los riesgos relacionados con la seguridad informática.

Estos procesos permiten no solo abordar las amenazas existentes sino también anticiparse a riesgos futuros y aprovechar oportunidades para la mejora continua. Se utilizan diversos marcos y estándares, como ISO 27001, ITIL, COBIT y NIST, para guiar y fortalecer estas iniciativas de seguridad de la información. En última instancia, garantizar la seguridad de la información es esencial en un entorno en el que los riesgos y las amenazas son una constante en el ámbito de los sistemas de información (Cuevas J. C., y otros, 2016).

2.2.2.5 Evaluación del Riesgo Residual

Después de aplicar medidas de mitigación, se realiza una reevaluación para asegurarse de que las amenazas se han reducido o eliminado. Cualquier amenaza que aún persista se considera riesgo residual y debe gestionarse de acuerdo con las políticas de seguridad. Esta fase es crítica para garantizar que no se pasen por alto riesgos que podrían tener un impacto significativo en la seguridad de la información de la organización.

2.2.3 Pruebas de Penetración (Pentesting)

El pentesting, también conocido como prueba de penetración, es un método utilizado por hackers éticos para evaluar y comprometer de manera controlada sistemas informáticos, equipos de computación, redes u otros dispositivos tecnológicos dentro de una organización. Su objetivo principal es identificar y corregir proactivamente las vulnerabilidades que se encuentren. Durante esta evaluación, se emplean técnicas y procedimientos similares a los que usaría un cibercriminal en un ataque real. Sin embargo, la diferencia clave radica en el propósito detrás de estos actos: mientras que un cibercriminal busca obtener beneficios económicos a través del robo, la destrucción o la modificación de información, el pentester busca revelar las vulnerabilidades existentes y ayudar a fortalecer los sistemas para prevenir futuros ataques (Erazo, 2017).

Es fundamental darse cuenta de que ningún sistema es 100% seguro. El hacker y el cracker son las dos funciones principales que se distinguen en este contexto. Ambos son personas muy hábiles y motivadas que saben cómo derribar un sistema, pero sus estándares morales y éticos para responder a las vulnerabilidades que han encontrado los

distinguen. Las acciones del cracker son malévolas, incluso cuando el hacker busca debilidades para fortalecer la seguridad del sistema (Cuevas J. C., y otros, 2016).

Las pruebas de penetración son una técnica útil para evaluar la seguridad en el contexto de aplicaciones web. Pero dado que las aplicaciones web suelen estar ampliamente personalizadas, estas pruebas se parecen más a una investigación pura. Es fundamental recordar que las pruebas de penetración de aplicaciones web no deberían ser el único ni el principal método de prueba, a pesar de que muchas personas lo utilizan como método principal para evaluar la seguridad. Pasar una prueba de penetración no garantiza que no haya problemas importantes; de hecho, fallar en uno puede exponer problemas graves. Para determinar si una vulnerabilidad particular realmente se ha reparado en el código fuente que se ha implementado en el sitio web, pueden ser útiles las pruebas de penetración concentradas, cuyo objetivo es explotar vulnerabilidades conocidas encontradas en revisiones anteriores (Owasp, 2014).

2.2.4 Tipos de Pentesting

Existen varios tipos de pruebas de penetración, cada uno con sus propios objetivos y enfoques:

1. **Network Pentesting:** Se centra en localizar sistemas y servicios en una red y buscar vulnerabilidades en los sistemas operativos y aplicaciones de servidor, así como malas configuraciones que puedan permitir a un atacante explotarlos de manera remota.
2. **Client-Side Pentesting:** Tiene como objetivo encontrar vulnerabilidades en el software instalado en equipos de usuario.
3. **Web Pentesting:** Su finalidad es encontrar vulnerabilidades en las aplicaciones web de una organización.
4. **Wireless Pentesting:** Consiste en evaluar la seguridad de las redes inalámbricas, generalmente Wi-Fi, en las instalaciones de una organización.
5. **Ingeniería Social:** Implica atacar a los usuarios para obtener información, ejecutar aplicaciones maliciosas, acceder a sitios web controlados por el atacante y realizar otras acciones que puedan permitir a un atacante obtener ventaja de sus acciones.
6. **Pentesting Físico:** Se enfoca en intentar acceder físicamente a las instalaciones del cliente para acceder a sus equipos, encontrar documentación, robar dispositivos de almacenamiento y realizar otras acciones que pudieran llevar a cabo un atacante.

Es fundamental recordar que un pentesting frecuentemente combina varios de estos tipos, ya que las empresas pueden necesitar evaluar varios sistemas y puntos de entrada diferentes (Pérez, 2022).

2.2.5 Fases de Pentesting

El proceso de un test de penetración consta de varias fases, que se pueden agrupar en tres bloques principales: preparación, ejecución y presentación de resultados (Pérez, 2022).

2.2.5.1 Fase de Preparación

Cada prueba de penetración (también conocida como pentesting) comienza con el paso preparatorio. En esta fase preliminar, se llevan a cabo una serie de procedimientos cruciales para definir los parámetros y objetivos del examen. Entre estos procedimientos se encuentran:

- Recolección de información inicial: Antes de iniciar cualquier acción, el equipo de pruebas de penetración debe obtener información básica sobre la organización. Esto incluye detalles como el tamaño de la red, las ubicaciones geográficas, los sistemas operativos utilizados y las aplicaciones críticas.
- Definición del alcance: Es fundamental establecer claramente qué sistemas, redes o aplicaciones se incluirán en la prueba y cuáles estarán fuera de ella. Esto garantiza que el equipo de pruebas se concentre en los objetivos específicos y no realice acciones no autorizadas.
- Acuerdo de confidencialidad (NDA): Se firma un acuerdo de confidencialidad entre el equipo de pruebas y la organización objetivo. El NDA protege la información sensible y asegura que todos los hallazgos y resultados se mantengan en estricta confidencialidad.
- Roles y responsabilidades: En esta fase, se definen los roles y responsabilidades tanto del equipo de pruebas como de la organización objetivo. Esto incluye el punto de contacto en la organización, la duración de la prueba y otros detalles logísticos (Pérez, 2022).

2.2.5.2 Fase de ejecución

El núcleo de las pruebas de penetración es la fase de ejecución, durante la cual se llevan a cabo operaciones técnicas para encontrar vulnerabilidades y evaluar la seguridad de la organización. Hay varias etapas en esta fase:

- **Escaneo y enumeración:** durante esta fase, los activos, sistemas y servicios de la infraestructura de la organización se ubican mediante software de escaneo de red. Esto implica determinar los sistemas operativos, los puertos abiertos y las aplicaciones activas.
- **Análisis de vulnerabilidades:** Tras la inclusión de la infraestructura, los sistemas y aplicaciones se someten a una investigación exhaustiva para buscar vulnerabilidades particulares. En esto se utilizan tanto procedimientos de revisión manual como herramientas de análisis de seguridad.
- **Explotación de vulnerabilidades:** Cuando se encuentran vulnerabilidades que pueden usarse para obtener acceso no autorizado a sistemas o datos, se hacen esfuerzos para aprovecharlas. Esto se lleva a cabo bajo estricta supervisión y con la aprobación de la organización objetivo.
- **Acceso:** en caso de que se adquiera acceso, se podrá conservar para un uso duradero o para investigaciones adicionales de la red. Esto ilustra el posible camino que podría tomar un atacante real a través de la red.
- **Limpieza y restauración:** una vez finalizadas las pruebas, se debe restaurar la red a su configuración inicial borrando cualquier acceso o huella digital no deseados. Al hacer esto, la empresa está protegida contra riesgos injustificados.

2.2.5.3 Fase de resultados

La fase de resultados es crucial para garantizar que los hallazgos se comuniquen de manera efectiva a la organización objetivo permitiendo tener un mejor enfoque de las vulnerabilidades encontradas. Esta fase incluye:

- **Informe y documentación detallada:** Se prepara un informe completo que incluye todas las vulnerabilidades identificadas, su nivel de criticidad, evidencia de explotación y recomendaciones de mitigación. Este informe es una herramienta invaluable para la toma de decisiones.
- **Reunión de presentación:** Se realiza una reunión con el cliente u organización objetivo para entregar el informe y discutir los resultados, las implicaciones y las acciones a seguir. Esta reunión permite aclarar cualquier pregunta y definir un plan de acción.
- **Seguimiento y revisión:** Después de la presentación, se realiza un seguimiento para garantizar que las recomendaciones se implementen y las vulnerabilidades se corrijan. Esto ayuda a mejorar la seguridad general de la organización (Pérez, 2022).

2.2.6 Metodologías de Pentesting

Hay un cierto proceso que se debe seguir al realizar una prueba de penetración. Aunque los pentesters experimentados son capaces de crear su propia metodología, es crucial estar familiarizado con algunos enfoques aceptados, como:

1. **Penetration Testing Framework:** se centra en el Pentesting de red y ofrece una explicación detallada de cada elemento que debe evaluarse junto con las herramientas e instrucciones necesarias.
2. **Penetration Testing Execution Standard (PTES):** Define describe las tareas que deben completarse durante un pentest para que las empresas puedan obtener un producto que sea valioso para ellas y para la empresa.
3. **Open Web Application Security Project (OWASP) Testing Guide:** Esta metodología se centra exclusivamente en la seguridad de aplicaciones web y describe en detalle las diferentes comprobaciones que se deben llevar a cabo, así como las herramientas que se pueden utilizar en todo el proceso (Pérez, 2022).

2.2.7 OWASP

El Open Web Application Security Project (OWASP), una organización sin fines de lucro trabaja para mejorar la seguridad del software de aplicaciones web fomentando la creación de instrumentos para evaluar su seguridad. Esta organización brinda a los usuarios acceso a una amplia gama de recursos, incluidas comunidades de desarrollo, materiales de capacitación y herramientas para la seguridad de aplicaciones web y móviles. También se encuentran disponibles recursos notables, como el modelo de madurez de Software Assurance y la colección de reglas Owasp Modsecurity para la detección de ataques a aplicaciones web. Es fundamental recordar que la seguridad en las aplicaciones web no es inherente; más bien, se logra mediante la administración y ejecución de políticas de seguridad en varias versiones y configuraciones. OWASP ha elaborado un manual completo sobre este tema (Sierra Huertas, 2023).

El estándar de verificación de seguridad de OWASP establece tres niveles de verificación, lo que permite una adaptación flexible según la criticidad de las aplicaciones.

- **Nivel 1: Requisitos Básicos de Seguridad**: está diseñado para aplicaciones con requerimientos de seguridad bajos. Los requisitos en este nivel son completamente comprobables a través de pruebas de

penetración. Aunque estos requisitos representan un nivel básico de seguridad, son esenciales como punto de partida para cualquier aplicación. Este nivel establece los cimientos necesarios para abordar preocupaciones de seguridad más complejas en aplicaciones empresariales.

- **Nivel 2: Protección de Datos Confidenciales**: se recomienda para la mayoría de las aplicaciones, especialmente aquellas que manejan datos confidenciales que requieren protección. En este nivel, los requisitos son más rigurosos que en el Nivel 1 y abordan preocupaciones de seguridad más avanzadas. Al considerar el análisis de vulnerabilidades en servidores de aplicaciones empresariales, este nivel adquiere una importancia significativa, ya que la mayoría de las aplicaciones empresariales gestionan información sensible que debe protegerse de manera efectiva.
- **Nivel 3: Aplicaciones Críticas y Máxima Confianza**: se aplica a aplicaciones críticas, es decir, aquellas que realizan transacciones de alto valor, almacenan datos médicos sensibles u operan en contextos que requieren el más alto nivel de confianza en términos de seguridad. Para el análisis de vulnerabilidades en servidores de aplicaciones empresariales, este nivel es de vital importancia cuando se trata de sistemas que manejan datos o procesos de alto valor, donde la seguridad y la confianza son prioritarias.

El estándar indica que no es necesario aplicar todos los requisitos de este para la seguridad en cada prueba, ya que sirve como una guía y puede adaptarse a casos de estudio específicos. Esto permite un enfoque selectivo en los requisitos de seguridad que son más pertinentes para proyectos y entornos particulares, lo que aumenta la eficiencia y la relevancia del análisis de vulnerabilidades en servidores de aplicaciones empresariales (Chancusig Chancusig, 2022).

Las aplicaciones web no son inherentemente seguras, sino que la seguridad se logra mediante la implementación y gestión de políticas de seguridad en sus diferentes versiones y configuraciones. OWASP ha elaborado una guía que aborda este tema en detalle (Sierra Huertas, 2023).

- Antes del desarrollo: Es importante establecer un ciclo de vida del desarrollo que incluya consideraciones de seguridad. Se deben definir estándares y documentación, así como métricas para medir el producto. La revisión de

requisitos de seguridad y la definición del diseño y arquitectura son fundamentales en esta etapa.

- Durante el desarrollo: Se codifica el diseño previamente definido, y se realiza una labor conjunta entre el equipo de seguridad y el de desarrollo. Se muestra el código al personal de seguridad para comprender la lógica y el flujo, y se realiza una revisión en busca de posibles fallos de seguridad.
- Durante la implementación: Se deben considerar aspectos de seguridad y se pueden realizar pruebas de penetración para encontrar vulnerabilidades en la aplicación y la infraestructura.
- Mantenimiento y operaciones: Se establece un procedimiento para evaluar periódicamente los sistemas y aplicaciones después de implementar cambios.
- Pruebas de seguridad de una aplicación web: Se dividen en pruebas pasivas y activas. Las pruebas pasivas implican interactuar con la aplicación para comprender su lógica, entradas y salidas. Las pruebas activas buscan vulnerar la aplicación y se basan en once categorías propuestas por OWASP, que abarcan aspectos como gestión de configuración, autenticación, autorización, criptografía, entre otros (Castro Vasquez, 2019).

2.2.8 PTES

El proyecto PTES (Penetration Testing Execution Standard) fue establecido en el año 2009 con el objetivo de unir a analistas y expertos en seguridad informática. Esta iniciativa ha desarrollado el estándar PTES versión 1.0, con el propósito de proporcionar a las empresas y proveedores de servicios un lenguaje y enfoque común para llevar a cabo pruebas de penetración (Torres Ortiz, 2019).

El estándar de ejecución de pruebas de penetración consta de siete secciones principales que abarcan todos los aspectos de una prueba de penetración. Estas secciones cubren desde la comunicación inicial y el propósito de la prueba de penetración, hasta las etapas de recopilación de inteligencia y modelado de amenazas, en las que los evaluadores trabajan en segundo plano para comprender mejor la organización que está siendo evaluada (PTES, 2014).

Las 7 fases o secciones de PTES son las siguientes:

Figura 3 Fases PTES.
Fuente: https://bit.ly/3Qd2JG9

- **Interacción previa (Pre-engagement Interactions):** En esta etapa se establecen las reglas y se define el alcance de las pruebas de penetración, incluyendo los objetivos, la infraestructura a evaluar, el tiempo y costo del servicio, la comunicación con el cliente y la recopilación de información sobre la empresa.
- **Recolección de información (Intelligence Gathering):** Se realizan diferentes niveles de recolección de información, desde automática hasta análisis profundo y conocimiento del negocio, con el fin de recopilar datos que serán utilizados en la evaluación de vulnerabilidades y la fase de explotación.
- **Modelamiento de amenazas (Threat Modeling):** Se enfoca en el análisis de las capacidades y representación de amenazas por parte del atacante, considerando el valor de los activos y el costo de adquisición. También se evalúa el impacto de las posibles amenazas en la organización.
- **Análisis de vulnerabilidades (Vulnerability Analysis):** Consiste en la detección de vulnerabilidades en sistemas y aplicaciones que pueden ser aprovechadas por un atacante para acceder. Se realiza una evaluación tanto activa como pasiva, interactuando directamente con los componentes y explorando los metadatos de los archivos expuestos.
- **Explotación (Exploitation):** El objetivo es obtener acceso al sistema identificando los puntos de entrada y reconociendo los activos de alto valor. Se

debe considerar las contramedidas implementadas por la organización y personalizar los ataques para adaptarse a la tecnología e infraestructura específica.

- **Post Explotación (Post Exploitation):** Se evalúa la máquina comprometida y se valora su utilidad, privilegios y acceso a otras máquinas o información en la red. Se establecen roles y responsabilidades, y se resalta la importancia de proteger a la organización durante esta fase.
- **Reporting o presentación de reporte:** Aunque la metodología PTES no especifica un formato de informe, se sugiere incluir el contexto de las pruebas, los lineamientos seguidos, los objetivos alcanzados, la clasificación de riesgos por su criticidad, los hallazgos encontrados y las recomendaciones para abordar los riesgos identificados (Castro Vasquez, 2019).

2.2.2.9 Ventajas de OWASP y PTES en el Pentesting

- **Amplia Cobertura:** PTES y OWASP abordan aspectos clave de la seguridad, desde pruebas de penetración y evaluación de vulnerabilidades hasta requisitos y pruebas de seguridad en aplicaciones web. Combinar estas metodologías permite una cobertura completa de la seguridad de aplicaciones y sistemas.
- **Marco de Referencia Común:** Ambas metodologías proporcionan un enfoque común y estructurado para abordar la seguridad. Esto facilita la comunicación entre equipos de seguridad, desarrolladores y partes interesadas.
- **Adaptabilidad:** PTES y OWASP son adaptables a situaciones específicas y pueden personalizarse para satisfacer las necesidades de proyectos individuales. Esto es esencial cuando se trata de servidores de aplicaciones empresariales, que pueden variar en complejidad y riesgos.
- **Complementariedad:** PTES se enfoca en pruebas de penetración y evaluación de seguridad desde una perspectiva de ataque, mientras que OWASP se centra en garantizar que las aplicaciones sean seguras desde el principio. Al combinar ambas metodologías, se obtiene un enfoque holístico que aborda tanto las vulnerabilidades existentes como la prevención de futuras.
- **Cumplimiento de Normativas:** Tanto PTES como OWASP están alineados con estándares y buenas prácticas reconocidas en la industria, como NIST y CWE. Esto facilita la demostración del cumplimiento de normativas de seguridad.
- **Evaluación Integral:** PTES permite evaluar la explotabilidad de las vulnerabilidades, mientras que OWASP se centra en garantizar que las

aplicaciones cumplan con los requisitos de seguridad. Combinar ambas evaluaciones proporciona una visión completa de la postura de seguridad de una aplicación o sistema.

2.3. Marco legal

El desarrollo del proyecto se tomará en cuenta los principios de LOPD (Ley organica de proteccion de datos personales, 2021) la cual establece los principios, derechos y deberes que rigen la protección de los datos personales en Ecuador. Algunos aspectos clave de la LOPD que deben considerarse son la definición de datos personales, la necesidad de obtener consentimiento informado para el tratamiento de datos, la implementación de medidas de seguridad adecuadas, el respeto a los derechos de los titulares de datos, los requisitos para la transferencia internacional de datos y la obligación de notificar brechas de seguridad. Cumplir con la LOPD garantiza la protección y privacidad de los datos personales durante el análisis de vulnerabilidades.

Según la constitución el artículo 66, numeral 19 de la Constitución de la República del Ecuador, establece el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección en donde entraría en vigor el LOPD.

También considerar normas y estándares reconocidos internacionalmente, como las directrices de la Open Web Application Security Project (OWASP) y el Penetration Testing Execution Standard (PTES). Estas metodologías proporcionan enfoques estructurados para realizar pruebas de penetración y análisis de vulnerabilidades.

Las políticas y reglamentos de Cubosoft también se tomará en cuenta en el proyecto con el fin de no incumplir las normas internas de la empresa se solicitará toda la materia y las pruebas de penetración con el consentimiento de la empresa

CAPITULO III
MARCO METODOLÓGICO

3.1. Descripción del área de estudio

Este proyecto se desarrollará en la ciudad de Ibarra en la empresa Cubosoft S.A. la cual se encarga de la automatización de laboratorios clínicos y desarrollo de sistemas para la mejora continua de los laboratorios. La matriz de esta empresa se encuentra situada en Portoviejo, pero el equipo de investigación y desarrollo se encuentra en Ibarra.

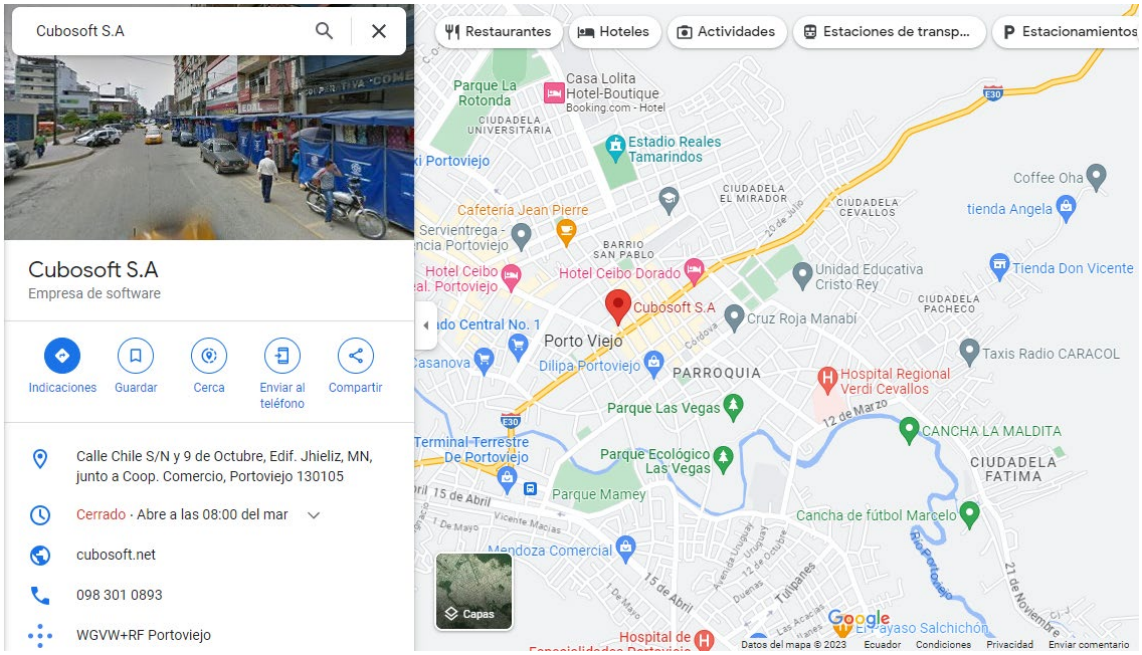


Figura 4 Ubicación de empresa Cubosoft.
Fuente: Google Maps

La población del equipo de investigación y desarrollo es de 6 personas. Para este estudio se considerará al equipo de sistemas que son 4 personas y 2 personas encargados del mantenimiento del sistema, Que cumplen los criterios de inclusión, así como un conjunto de individuos que son objetos de estudios o de los que se requiere información (Rivadeneira Flores, 2019) .

3.2. Enfoque y tipo de investigación

El desarrollo del proyecto se lo realizará con un enfoque cuantitativo que según Hernández, Fernández y Baptista (2014) indica que a diferencia del enfoque cualitativo el "Enfoque cuantitativo: Implica la recolección de datos para caracterizar una realidad o probar una hipótesis. Este enfoque conlleva la medición de variables (nominales ordinales, de intervalo o de razón) y el análisis estadístico".

Este enfoque se seleccionó ya que se realizará el análisis de vulnerabilidades mediante las metodologías OWASP y PTES con pruebas de pentesting donde mediante

indicadores se podrá seleccionar el nivel de riesgo y como se van a tratar cada uno de estos dentro de los servidores de aplicaciones.

Se especifica el enfoque asumido para abordar el problema de investigación: cuantitativo, cualitativo o mixto (se exponen las razones por las cuales el trabajo se enmarca en dicho enfoque).

3.3. Procedimiento de investigación

No hay un conjunto fijo y estandarizado de fases numeradas en OWASP, como lo hay en PTES. No obstante, OWASP ofrece recursos y guías para mejorar la seguridad en diversas áreas, y sus proyectos suelen abordar vulnerabilidades específicas. Por lo que las fases planteadas a continuación están basadas de la guía de implementación "OWASP Testing Guide v4" y las 7 fases de PTES basadas en el análisis de vulnerabilidades en el servidor de aplicaciones empresariales con las siguientes fases:

FASE 1. Recolectar información sobre el servidor de aplicaciones utilizado en Cubosoft y planificar el alcance del análisis de vulnerabilidades.

En esta fase, la recopilación de información incluye la identificación de activos, sistemas y servicios críticos para el servidor de aplicaciones empresariales. La planificación define claramente los objetivos del análisis, estableciendo el alcance y las áreas prioritarias para la evaluación de seguridad.

Proporciona una visión general de la arquitectura y la infraestructura, identificando áreas críticas que deben ser evaluadas en profundidad. Ayuda a definir los límites del servidor de aplicaciones utilizados por Cubosoft y las áreas específicas que requieren mayor atención en términos de seguridad basándose en el módulo de resultados.

FASE 2. Evaluar la configuración del servidor de aplicaciones empresariales de Cubosoft y gestionar las políticas utilizadas.

Esta fase se inspira en las recomendaciones de seguridad de OWASP y en la importancia de evaluar la configuración de seguridad y las políticas de gestión de identidades. La evaluación de configuraciones y políticas de identidad es fundamental para garantizar que las configuraciones del servidor estén alineadas con las mejores prácticas de seguridad. Esto incluye la revisión de configuraciones de red, permisos de acceso y políticas de autenticación y autorización.

Mejora la seguridad del servidor de aplicaciones al identificar y corregir configuraciones subóptimas o riesgosas. Además, garantiza que las políticas de identidad y acceso cumplan con los estándares de seguridad, mitigando posibles amenazas relacionadas con la gestión de identidades.

FASE 3. Identificación y preparación del entorno para la realización del pentesting en el servidor de aplicaciones empresariales.

Se recopila información adicional y se identificará el entorno donde se trabajará en el escaneo de vulnerabilidades tanto como la preparación de las herramientas a utilizar. Con esto se plantea tener una visión más completa de los posibles riesgos asociados al entorno y la preparación de las herramientas que no afecten al entorno donde se realiza el análisis.

FASE 4. Realizar pruebas de pentesting en los servidores de aplicaciones empresariales de Cubosoft mediante la metodología OWASP y PTES, para detectar vulnerabilidades.

La ejecución de pruebas de penetración y la evaluación de vulnerabilidades serán esenciales para validar la seguridad del servidor de aplicaciones. Esto incluye el escaneo de seguridad, pruebas activas y pasivas para identificar y clasificar vulnerabilidades. Esta fase se inspira en las prácticas de pruebas de penetración y evaluación de vulnerabilidades de OWASP y PTES. Con esto se obtiene una evaluación profunda de la seguridad del servidor de aplicaciones, identificando y clasificando vulnerabilidades específicas que podrían ser explotadas. Facilita la corrección proactiva de vulnerabilidades antes de que representen una amenaza seria para la seguridad.

FASE 5. Recopilar información de resultados y proporcionar recomendaciones de mitigación para el módulo de resultados en el servidor de aplicaciones empresariales.

Esta fase se deriva de la importancia de evaluar la persistencia de amenazas después de una explotación, una práctica destacada en las metodologías de pruebas de penetración. Se evalúa la persistencia de amenazas y documentara los resultados de las pruebas para comprender las posibles vulnerabilidades y proporcionar recomendaciones efectivas. También se aplica las recomendaciones del informe de resultados y evaluar el proceso de seguridad mediante una prueba de concepto aplicada al módulo de resultados web en los servidores de aplicaciones empresariales de Cubosoft. Los resultados de esta evaluación permitirán realizar ajustes y mejoras adicionales en el proceso de seguridad, de ser necesario.

3.4. Consideraciones bioéticas

En el marco de la investigación en la empresa Cubosoft, se priorizarán las consideraciones éticas y se obtendrá la autorización necesaria para llevar a cabo el

estudio. Se garantizará el cumplimiento de los principios éticos de beneficencia, no maleficencia y autonomía, así como la protección de los derechos de todos los involucrados.

Para ello, se solicitará y obtendrá la autorización explícita de las autoridades de Cubosoft, así como de los empleados y clientes que participen en la investigación. Se informará de manera oral y detallada a los participantes sobre los objetivos, los procedimientos involucrados, la importancia de su participación, la duración del estudio y las leyes, códigos y normas que salvaguardan sus derechos.

Se gestionarán todos los permisos y requisitos necesarios para acceder a la infraestructura de Cubosoft y se garantizará el anonimato y la confidencialidad de los participantes. El carácter voluntario de su participación será respetado en todo momento, y se destacarán los posibles beneficios derivados de la investigación.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. Evaluación inicial del módulo de resultados:

Este marco esta específicamente enfocado en el servidor de aplicaciones del módulo de resultados web denominado "Misanalisis" de la empresa Cubosoft.

Este módulo es esencial para el funcionamiento del sistema, ya que gestiona toda la parte postanalítica de un laboratorio clínico donde se encarga de:

- Procesamiento de los resultados.
- Validación de resultados.
- Generación de informes.
- Comunicación de resultados.

Tecnologías del módulo web:

- GraphQL: para las consultas, proporcionando flexibilidad y eficiencia en las interacciones con la base de datos.
- Spring: para publicación de web services Rest con herramientas como JWT para mantener los servicios protegidos.
- Ionic: creación de vista mediante componentes protegiendo el código ya que es compilado y cifrado.

Conexiones

- Comunicación con base de datos: El módulo no se conecta directamente a la base de datos, esto lo hace mediante microservicios.
- Servicios externos: Conexiones aparte de los datos del sistema se los realiza directamente desde la base de datos u otro aplicativo.

Infraestructura Técnica:

- El módulo de resultados está alojado en un servidor de aplicaciones empresariales Wildfly, desde donde se publica la página web correspondiente.
- Esta página web es utilizada por los laboratorios en el sistema "AVALAB" para acceder y revisar los resultados de los análisis realizados.
- Este servidor de aplicaciones es levantado en servidores Linux o Windows depende la solicitud del cliente.

Equipo de programación:

El equipo encargado del desarrollo y mantenimiento del módulo de resultados de "Misanálisis" de Cubosoft es fundamental para garantizar el funcionamiento eficiente y

confiable del sistema. Compuesto por tres miembros especializados, el equipo se adhiere a un proceso de desarrollo que prioriza la calidad del software y la satisfacción del cliente. El equipo sigue un proceso de desarrollo iterativo que permite adaptarse a las necesidades cambiantes del proyecto. Aunque no se sigue una metodología específica, se ha establecido un proceso interno que incluye:

Análisis de requisitos: Se recopilan y documentan los requisitos del cliente antes de comenzar cualquier desarrollo.

- Diseño: Se elabora un diseño detallado del sistema, teniendo en cuenta la arquitectura y la experiencia de usuario.
- Implementación: Se lleva a cabo la codificación del software siguiendo las mejores prácticas de programación y utilizando herramientas de control de versiones para mantener un código organizado y colaborativo.
- Pruebas: Se realizan pruebas exhaustivas para garantizar la calidad y fiabilidad del software, incluyendo pruebas unitarias, de integración y de aceptación.
- Despliegue: Se implementan las actualizaciones en producción bajo demanda del cliente, asegurando una transición sin problemas y minimizando el tiempo de inactividad.

Este enfoque al desarrollo del software se alinea con la filosofía ágil, priorizando la colaboración, la comunicación y la flexibilidad, aunque siempre manteniendo un enfoque disciplinado para garantizar la calidad y el cumplimiento de los objetivos del proyecto (Quiña-Mera, Andrade, Yugla, Angamarca, & Guevara-Vega, 2021).

Análisis previos

- Correcciones de seguridad por cliente hospitalario mediante la herramienta Acuanetic donde se encontraron varios puntos críticos por las configuraciones del certificado SSL que proporciono el cliente.
- Hasta la fecha no se tiene registros de ataques que se hayan producido por este módulo web.

Pruebas de configuración

Servidor de aplicaciones

- Archivo de configuración: standalone.xml.
- Interfaz de administración: Solo acceso localhost puerto privado.
- Puertos de salida: 80 y 443.
- Certificado SSL: Depende de cada laboratorio se configura con keystore.

Aplicación web módulo de resultados

- Archivo de configuración: config.json.
- Conexión con servidor: Web Service Rest y Graphql.
- Otras conexiones: ninguna.

4.2 Identificación y preparación del entorno de pruebas Pentesting

Datos del servidor objetivo

- Sistema Windows Server 2018.
- Memoria RAM 32.
- Disco Duro 1tb.
- Procesador Intel.

Servidor de aplicaciones empresariales

- Wildfly 26.1.2.
- Ubicación D://misanalisis/wildfly-26.1.2.Final
- 2gb RAM asignada.
- Certificado SSL.

Aplicación web

- Puerto del aplicativo 80 y 443 SSL.
- Acceso: resultados.autolab.com/preview.

A continuación, se proporcionará una descripción detallada de las herramientas empleadas en este proyecto las cuales son de Software Libre. Es importante destacar que se eligió obtener una réplica del código fuente utilizado por el sistema en producción para llevar a cabo la evaluación del código estático.

- **Nmap:** Para identificar los servicios y puertos abiertos en un servidor web. Ayudando a evaluar la exposición de la red y a detectar posibles puntos de vulnerabilidad al proporcionar información detallada sobre los servicios en ejecución.

- **OWASP ZAP**: Permite encontrar vulnerabilidades comunes en sitios web, como inyecciones de SQL, ataques de cross-site scripting (XSS), entre otros. Con este se identificará y brindará soluciones para corregir debilidades en el aplicativo.
- **SonarQube:** Escanea las aplicaciones web en busca de vulnerabilidades específicas, como fallos de configuración, debilidades en la gestión de sesiones, y otros problemas de seguridad.

Aspectos de evaluación

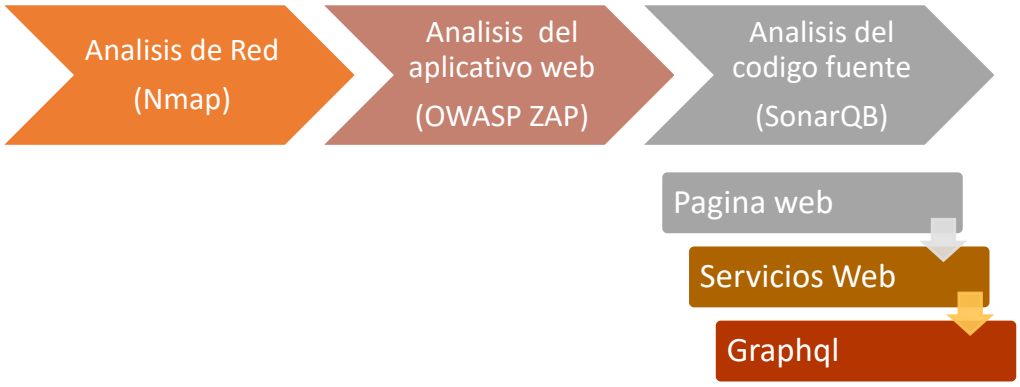


Figura 5 Aspectos de Evaluación Pentesting.
Fuente: Propia

4.3 Pruebas de penetración para el módulo de resultados

4.3.1 Escaneo de red del servidor de aplicaciones con NMAP

Información General

- Dirección IP Escaneada: 190.152.10.210.
- Nombre de Host Asociado: dipeibch.edu.ec.
- Versión de Nmap:7.94.
- Tiempo de actividad estimado 73.6 días.

Rastreo de Red y Resultados de NSE

- 8 saltos.
- Algunos scripts NSE fallaron debido a problemas de permisos de acceso a sockets.

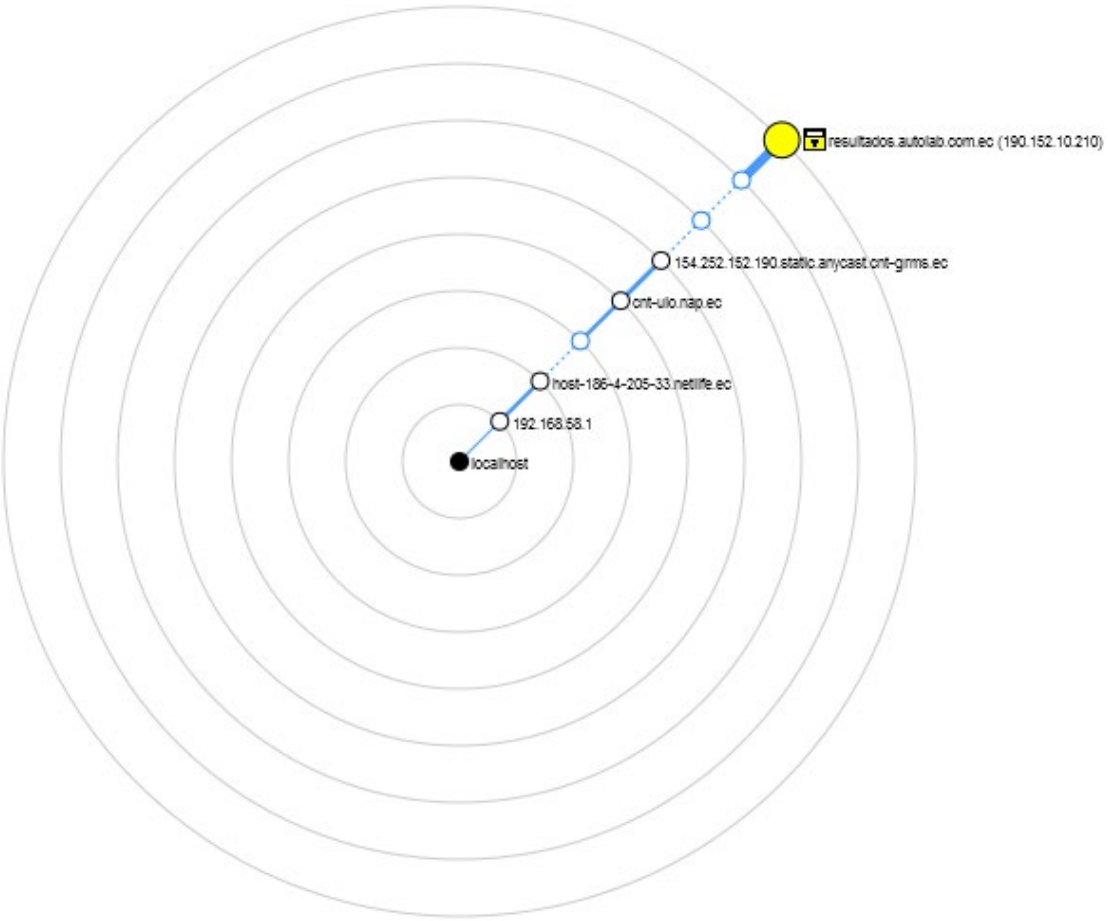


Figura 6 Topología del servidor.
Fuente: Zenmap

Información certificado SSL

- Nombre Común del Host: resultados.autolab.com.ec.
- Autoridad de certificación: Sectigo RSA Domain Validation Secure Server CA.
- Validez: 10 de enero de 2023 - 28 de enero de 2024.

Identificación de puertos y servicios

PUERTO	ESTADO	SERVICIO	VERSIÓN/IDENTIFICACIÓN
23/TCP	Filtrado	Telnet	
80/TCP	Abierto	HTTP	Servidor web
1723/TCP	Abierto	PPTP	Dispositivo de red MikroTik
443/TCP	Abierto	SSL/HTTPS	Servidor web seguro
8000/TCP	Abierto	IPCam	Servidor de control de cámara IP Hikvision
8001/TCP	Abierto	HTTP	Servidor HTTPAPI de Microsoft
2000/TCP	Abierto	Bandwidth-test	MikroTik bandwidth-test server

8081/TCP	Filtrado	Desconocido
8082/TCP	Filtrado	Desconocido
8083/TCP	Filtrado	Desconocido
8084/TCP	Filtrado	Desconocido
9080/TCP	Filtrado	Desconocido
9999/TCP	Filtrado	Desconocido
67/UDP	Abierto/Filt	DHCP
123/UDP	Abierto/Filt	NTP
500/UDP	Abierto/Filt	ISAKMP
520/UDP	Abierto/Filt	Route
4500/UDP	Abierto/Filt	NAT-T-IKE

Tabla 1 Escaneo de puertos
Fuente: NMAP

Riesgos y recomendaciones

Puerto	Servicio	Riesgo Potencial	Recomendación
80	HTTP	Medio	Mantener servicios web actualizados, aplicar firewalls y cifrado SSL/TLS.
443	HTTPS	Medio	Mantener servicios web actualizados, aplicar firewalls y cifrado SSL/TLS.
1723	PPTP	Alto (Desaconsejado)	Utilizar protocolos VPN más seguros como L2TP/IPsec o OpenVPN.
2000	MikroTik	Medio	Mantener firmware actualizado y configurar medidas de seguridad.
8000	IP Cam Control	Medio	Configurar cámaras IP de forma segura, con credenciales fuertes y firmware actualizado.
8001	Microsoft HTTPAPI	Medio	Configurar restricciones de acceso y mantener actualizado el servicio.
67, 123, 500, 520, 4500	Varios	Bajo	Configurar cortafuegos para limitar exposición y monitorear el tráfico.

Tabla 2 Análisis de puertos del servidor
Fuente: Propia

4.3.2 Escaneo del aplicativo web del servidor de aplicaciones

Mediante el escaneo con la herramienta OWASP ZAP hacia la página web resultados.autolab.com.ec se generaron varias alertas de seguridad las cuales se contabilizaron las veces que se reincidían y se detallan a continuación en la siguiente tabla.

TIPO DE ALERTA	RIESGO	INCIDENCIAS
Cabecera Content Security Policy (CSP) no configurada	Medio	5
Desconfiguración de Dominio cruzado	Medio	1
Falta de cabecera Anti-Clickjacking	Medio	2
Cookie No HttpOnly Flag	Bajo	2
Cookie Without Secure Flag	Bajo	2
Cookie sin el atributo SameSite	Bajo	2
Divulgación de la marca de hora - Unix	Bajo	2
Private IP Disclosure	Bajo	2
Strict-Transport-Security Header Not Set	Bajo	111
X-Content-Type-Options Header Missing	Bajo	108
Divulgación de información - Comentarios sospechosos	Informativo	35
Modern Web Application	Informativo	1
Re-examine Cache-control Directives	Informativo	6
Session Management Response Identified	Informativo	4
User Agent Fuzzer	Informativo	180
Total		15

Tabla 3 Alertas de seguridad del servidor encontradas con OWASP ZAP

Este escaneo destaca varias áreas de mejora en la seguridad del módulo de resultados en el servidor de aplicaciones, desde configuraciones de cabeceras hasta divulgación de información potencialmente sensible. Se recomienda abordar estas cuestiones para fortalecer la postura de seguridad del Sistema priorizando las de mayor riesgo.

El nivel de riesgo evaluado con esta herramienta indica que existe un nivel medio con tres incidencias.

		Risk			
		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)
Site	https://resultados.autolab.com.ec	0 (0)	3 (3)	7 (10)	5 (15)

Figura 7 Análisis de Riesgos del servidor
Fuente: OWASP ZAP

4.3.3 Escaneo del código fuente

El escaneo del código se realizó con la herramienta SonarQube, la cual permite encontrar fallas y vulnerabilidades en el código del módulo de resultados. Las calificaciones que ofrece esta herramienta están desde A hasta E donde las calificaciones con E son las más altas y en estas son las que se va a revisar y corregir el código.

Se realizo el análisis individual por cada una de las tecnologías utilizadas en el módulo de resultados:

- Página Web (Ionic).
- Servicios Web (Spring).
- GraphQL.

Este análisis permite reconocer fallas y vulnerabilidades de seguridad que tiene el sistema y su nivel de riesgo.

Resumen de análisis página web: En el resumen general se obtuvo un estado de aprobación de calidad según el software SonarQube, y en el apartado de revisiones de seguridad indica una calificación alta de “E” y 5 incidencias de este tipo, donde se revisa para localizar las que tengan un impacto alto.

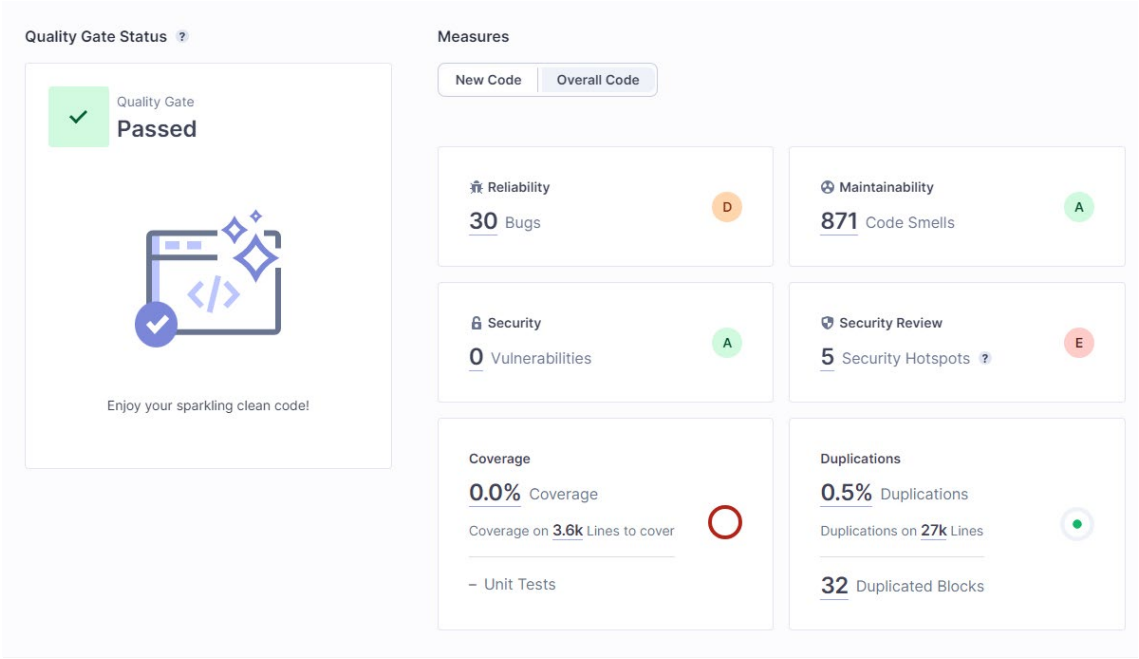


Figura 8 Resumen general del escaneo de código de la página web
Fuente: SonarQube

Resumen de escaneo de los servicios web: en el apartado de revisiones de seguridad indica una calificación alta de “E” y 95 incidencias de este tipo.

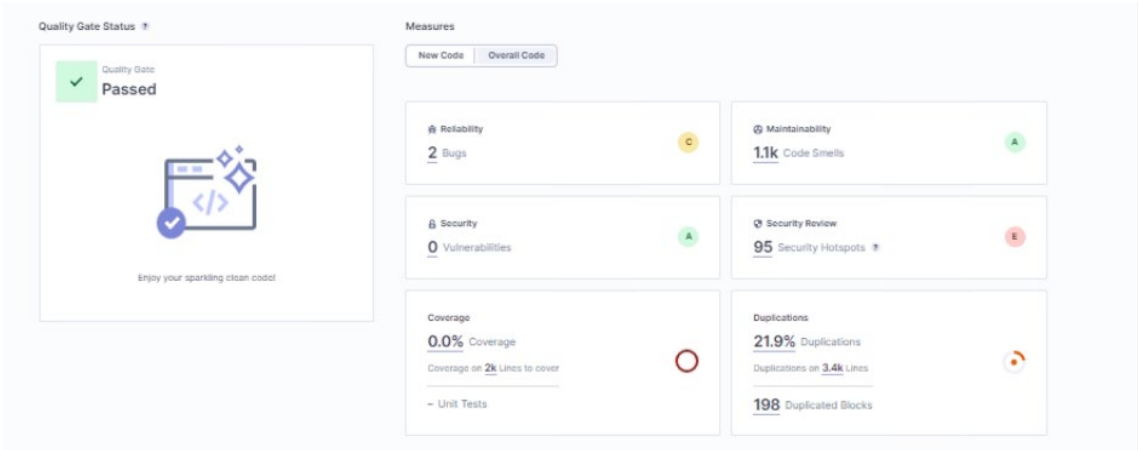


Figura 9 Resumen general del escaneo de código de servicios web
Fuente: SonarQube

Resumen de escaneo de GraphQL**:** en el apartado de revisiones de seguridad indica una calificación alta de “E” y 8 incidencias de este tipo.

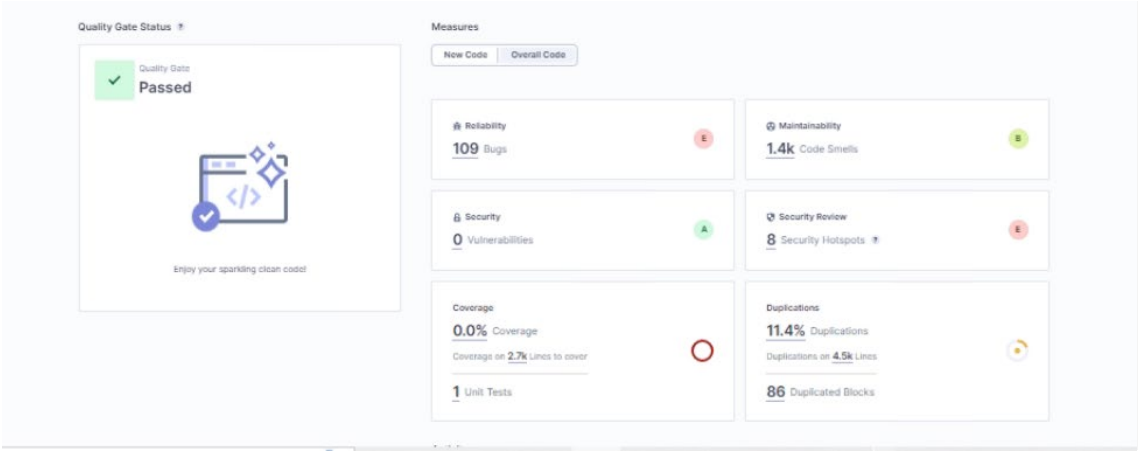


Figura 10 Resumen general del escaneo de código de GraphQL
Fuente: SonarQube

4.3.4 Alertas de seguridad

Las revisiones de seguridad que indica SonarQube tienen una calificación del riesgo encontrado donde el riesgo "alto" y "medio" es el que se da prioridad para el análisis de la vulnerabilidad ya que son los más críticos que deben corregirse.

TIPO DE ALERTA	RIESGO	INCIDENCIAS ENCONTRADAS
PAGINA WEB		
Secuencias de comandos entre sitios (XSS)	Alto	3
Criptografía débil	Medio	1
SERVICIOS WEB		
Cross-Site Request Forgery (CSRF)	Alto	1
GRAPHQL		
SQL Injection	Alto	3

Figura 11 Análisis de alertas de seguridad en Código
Fuente: Propia

4.4 Análisis de vulnerabilidades encontradas en las pruebas de penetración

A continuación, se detalla las alertas más relevantes o de riesgo más alto y su posible mitigación para la mejora del servidor de aplicaciones. No se toma en cuenta las de análisis de red ya que se especificó en la tabla las recomendaciones a los puertos abiertos.

4.4.1 Vulnerabilidades del aplicativo web

Cabecera Content Security Policy (CSP) no configurada	
Riesgo: Medio	**Incidencias**: 5
Descripción: La Política de Seguridad de Contenido (CSP) constituye una capa adicional de seguridad diseñada para identificar y mitigar ciertos ataques, como Cross Site Scripting (XSS) y ataques de inyección de datos, que pueden resultar en robo de datos, desfiguración del sitio o distribución de malware. CSP se basa en encabezados HTTP estándar que permiten a los propietarios de sitios web especificar las fuentes de contenido autorizadas para su carga en la página, abarcando JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.	
Solución: Asegurar de que el servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.	

Tabla 4: Cabecera Content Security Policy (CSP) no configurada
Fuente: Owasp Zap

Desconfiguración de Dominio cruzado	
Riesgo: Medio	**Incidencias**: 2
Descripción: Descargas de datos del navegador web podría ser posible, debido a una desconfiguración del intercambio de recursos cruzados de origen (CORS) en el servidor web.	
Solución: Asegurar que los datos sensibles no están disponibles de manera no autenticada (usando dirección IP listado-blanco, por ejemplo). Configurar el encabezado HTTP ""Access-Control-Allow-Origin" a un conjunto de dominios más restrictivo, o remover completamente todos los encabezados CORS, para permitir que el navegador web refuerce la política de mismo origen (SOP) en una manera más restrictiva.	

Tabla 5 Vulnerabilidad: Desconfiguración de Dominio cruzado
Fuente: Owasp Zap

4.4.2 Vulnerabilidades de código página web

Cross-Site Scripting (XSS)	
Riesgo: Alto	**Incidencias**: 3

Descripción: Angular previene vulnerabilidades XSS tratando todos los valores como no confiables de manera predeterminada. Los valores no confiables son sistemáticamente saneados por el marco de trabajo antes de ser insertados en el DOM. Sin embargo, los desarrolladores tienen la capacidad de marcar manualmente un valor como confiable si están seguros de que el valor ya está saneado. Confiar accidentalmente en datos maliciosos introducirá una vulnerabilidad XSS en la aplicación y permitirá una amplia gama de ataques graves, como acceder/modificar información sensible o hacerse pasar por otros usuarios.
Solución: Evita incluir código ejecutable dinámico y desactivar la sanitización incorporada de Angular a menos que sea absolutamente necesario. En su lugar, trata de depender tanto como sea posible de plantillas estáticas y de la sanitización incorporada de Angular para definir el contenido de la página web. Asegurar de entender cómo se construye el valor que se considera como confiable y nunca lo concatenes con datos controlados por el usuario. Asegurar de elegir el método de "bypass" correcto de DomSanitizer según el contexto. Por ejemplo, utiliza bypassSecurityTrustUrl solo para confiar en las URL en un contexto de atributo href.

Tabla 6 Vulnerabilidad: Cross-Site Scripting (XSS)
Fuente: SonarQube

Weak Cryptography	
Riesgo: Medio	**Incidencias**: 1
Descripción: El uso de generadores de números pseudoaleatorios (PRNG) es sensible desde el punto de vista de la seguridad. Por ejemplo, en el pasado ha dado lugar a las siguientes vulnerabilidades: • CVE-2013-6386: Vulnerabilidad relacionada con el uso de generadores de números pseudoaleatorios. • CVE-2006-3419: Otra vulnerabilidad asociada al uso de generadores de números pseudoaleatorios. • CVE-2008-4102: Una más, destacando la importancia de evitar debilidades en la generación de números aleatorios en aplicaciones de seguridad. Cuando el software genera valores predecibles en un contexto que requiere imprevisibilidad, es posible que un atacante pueda adivinar el próximo valor que se	

generará y utilizar esta suposición para hacerse pasar por otro usuario o acceder a información sensible.
Solución: Utiliza un generador de números pseudoaleatorios criptográficamente fuerte (CSPRNG) como crypto.getRandomValues(). Emplear los valores aleatorios generados solo una vez. No exponer el valor aleatorio generado. Si es necesario almacenarlo, asegúrate de que la base de datos o el archivo sean seguros.

Tabla 7 Vulnerabilidad: Weak Cryptography
Fuente: SonarQube

4.4.3 Vulnerabilidades de código de servicios web

Cross-Site Request Forgery (CSRF)	
Riesgo: Alto	**Incidencias**: 1
Descripción: Ataque de falsificación de solicitud entre sitios (CSRF): Este tipo de ataque sucede cuando un usuario de confianza en una aplicación web puede ser forzado por un atacante a realizar acciones sensibles que no tenía la intención de llevar a cabo, como actualizar su perfil o enviar un mensaje, en general, cualquier cosa que pueda cambiar el estado de la aplicación. El atacante puede engañar al usuario/víctima para que haga clic en un enlace que corresponde a la acción privilegiada o para que visite un sitio web malicioso que incrusta una solicitud web oculta, y dado que los navegadores web incluyen automáticamente las cookies, las acciones pueden autenticarse y volverse sensibles.	
Solución: Protección contra ataques CSRF se recomienda encarecidamente: • Activarla de forma predeterminada para todos los métodos HTTP no seguros. • Implementarla, por ejemplo, con un token CSRF difícil de adivinar. Por supuesto, todas las operaciones sensibles no deberían realizarse con métodos HTTP seguros, como GET, que están diseñados exclusivamente para la recuperación de información.	

Tabla 8 Vulnerabilidad: Cross-Site Request Forgery (CSRF)
Fuente: SonarQube

4.4.4 Vulnerabilidades de código de GraphQL

SQL Inyección	
Riesgo: Alto	**Incidencias**: 3

Descripción: Las consultas SQL formateadas pueden resultar difíciles de mantener, depurar y aumentar el riesgo de inyección SQL al concatenar valores no confiables en la consulta.
Solución: Utiliza consultas parametrizadas, declaraciones preparadas o procedimientos almacenados, y vincula variables a los parámetros de consulta SQL. Considera la posibilidad de utilizar marcos de trabajo de mapeo objeto-relacional (ORM) si es necesario contar con una capa abstracta para acceder a los datos.

Tabla 9 Vulnerabilidad: SQL Inyección
Fuente: SonarQube

4.4.5 Evaluación de Vulnerabilidades y análisis de riesgos

Se busca detectar vulnerabilidades, desde configuraciones inseguras hasta posibles riesgos en el código del servidor de aplicaciones, y analizar su nivel de riesgo proporcionando una visión detallada de las amenazas potenciales, evaluando su impacto y proponiendo medidas correctivas para fortalecer la seguridad y proteger la integridad del sistema de Cubosoft.

Para la metodología de clasificación del riesgo se utilizó la metodología de clasificación de riesgo de OWASP (Williams, s.f.) ya que PTES no cuenta con dicha clasificación ya que al ser más solo una metodología puramente de pentesting no cuenta con una clasificación en general.

El modelo estándar para clasificar el riesgo es:

Riesgo = Probabilidad * Impacto

Este modelo indica 6 pasos a seguir:

Paso 1 Identificar el riesgo:

El objetivo de este paso es la identificación de las amenazas las cuales fueron encontradas con las herramientas de análisis y las detallamos a continuación:

- Ausencia de Configuración de Política de Seguridad de Contenido (CSP).
- Desconfiguración de Cross-Origin Resource Sharing (CORS).
- Posibilidad de Inyección de Scripts Maliciosos (XSS).
- Uso de generadores de números pseudoaleatorios débiles.
- Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF).
- Riesgo de Inyección SQL.

- Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN.
- Riesgo asociado con firmware desactualizado en dispositivos MikroTik.
- Riesgo de seguridad en cámaras IP.
- Configuración de restricciones de acceso para evitar posibles vulnerabilidades.

Paso 2: Factores de probabilidad

El siguiente paso que indica la metodología de clasificación de riesgo de OWASP es la estimación de probabilidad la cual la metodología indica que existen dos conjuntos de factores los cuales se califican del 0-9 y se utilizaran para sacar la probabilidad asociada:

Factores del agente de amenaza:

- **Nivel de habilidad:** ¿Qué tan hábil es técnicamente este grupo de agentes de amenazas?
- **Motivo:** ¿Qué tan motivado está este grupo de agentes de amenazas para encontrar y explotar esta vulnerabilidad?
- **Oportunidad:** ¿Qué recursos y oportunidades se requieren para que este grupo de agentes de amenazas encuentre y aproveche esta vulnerabilidad?

Amenaza	**Nivel de habilidad**	**Motivo**	**Oportunidad**	**Tamaño**
Ausencia de Configuración de Política de Seguridad de Contenido (CSP)	**9**	**4**	**9**	**9**
Desconfiguración de Cross-Origin Resource Sharing (CORS)	**6**	**9**	**9**	**9**

Posibilidad de Inyección de Scripts Maliciosos (XSS)	**6**	**9**	**9**	**9**
Uso de generadores de números pseudoaleatorios débiles	**9**	**1**	**7**	**9**
Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	**9**	**4**	**7**	**9**
Riesgo de Inyección SQL	**6**	**9**	**9**	**9**
Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	**6**	**4**	**7**	**9**
Riesgo asociado con firmware desactualizado en dispositivos MikroTik	**9**	**4**	**7**	**9**
Riesgo de seguridad en cámaras IP	**9**	**4**	**7**	**9**
Configuración de restricciones de acceso para evitar posibles vulnerabilidades	**9**	**4**	**4**	**9**

Tabla 10 Factores de agente de amenaza
Fuente: Propia

Factores de vulnerabilidad:

- **Facilidad de descubrimiento**: ¿Qué tan fácil es para este grupo de agentes de amenazas descubrir esta vulnerabilidad?
- **Facilidad de explotación:** ¿Qué tan fácil es para este grupo de agentes de amenazas explotar esta vulnerabilidad?
- **Conciencia:** ¿Qué tan conocida es esta vulnerabilidad para este grupo de agentes de amenazas?
- **Detección de intrusiones:** ¿qué posibilidades hay de que se detecte un exploit?

Amenaza	**Facilidad de descubrimiento**	**Facilidad de explotación**	**Conciencia**	**Detección de intrusiones**
Ausencia de Configuración de Política de Seguridad de Contenido (CSP)	**9**	**5**	**4**	**8**
Desconfiguración de Cross-Origin Resource Sharing (CORS)	**9**	**5**	**6**	**8**
Posibilidad de Inyección de Scripts Maliciosos (XSS)	**9**	**5**	**4**	**8**
Uso de generadores de números pseudoaleatorios débiles	**9**	**5**	**4**	**8**

Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	**9**	**5**	**4**	**8**
Riesgo de Inyección SQL	**9**	**9**	**9**	**9**
Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	**9**	**3**	**1**	**3**
Riesgo asociado con firmware desactualizado en dispositivos MikroTik	**3**	**3**	**1**	**3**
Riesgo de seguridad en cámaras IP	**5**	**3**	**1**	**3**
Configuración de restricciones de acceso para evitar posibles vulnerabilidades	**3**	**3**	**1**	**3**

Tabla 11 Factores de vulnerabilidad
Fuente: Propia

Paso 3: Factores para estimar el impacto

Existen dos tipos de impactos que indica la metodología de clasificación de riesgo de OWASP : el técnico y el empresarial.

Impacto técnico:

- Pérdida de confidencialidad: ¿cuántos datos podrían divulgarse y qué tan sensibles son?

- Pérdida de integridad: ¿cuántos datos podrían corromperse y en qué medida están dañados?
- Pérdida de disponibilidad: ¿cuánto servicio se podría perder y qué importancia tiene?

Pérdida de responsabilidad: ¿Las acciones de los agentes amenazantes son rastreables hasta un individuo?

	Perdida			
Amenaza	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Responsabilidad**
Ausencia de Configuración de Política de Seguridad de Contenido (CSP)	**6**	**3**	**4**	**9**
Desconfiguración de Cross-Origin Resource Sharing (CORS)	**7**	**5**	**7**	**9**
Posibilidad de Inyección de Scripts Maliciosos (XSS)	**6**	**5**	**7**	**9**
Uso de generadores de números pseudoaleatorios débiles	**2**	**1**	**1**	**9**
Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	**2**	**5**	**5**	**9**
Riesgo de Inyección SQL	**9**	**9**	**7**	**7**

Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	**2**	**1**	**1**	**1**
Riesgo asociado con firmware desactualizado en dispositivos MikroTik	**2**	**1**	**5**	**7**
Riesgo de seguridad en cámaras IP	**6**	**3**	**1**	**7**
Configuración de restricciones de acceso para evitar posibles vulnerabilidades	**2**	**1**	**1**	**7**

Tabla 12 Factores para estimar impacto técnico
Fuente: Propia

Impacto empresarial

- Daño financiero: ¿cuánto daño financiero resultará de un exploit?
- Daño a la reputación: ¿un exploit provocaría un daño a la reputación que perjudicaría al negocio?
- Incumplimiento: ¿Cuánta exposición genera el incumplimiento?
- Violación de la privacidad: ¿cuánta información de identificación personal podría divulgarse?

	Perdida			
Amenaza	**Daño financiero**	**Daño reputación**	**Incumplimiento**	**Violación de la privacidad**
Ausencia de Configuración de	**3**	**3**	**2**	**7**

Política de Seguridad de Contenido (CSP)				
Desconfiguración de Cross-Origin Resource Sharing (CORS)	**3**	**7**	**2**	**7**
Posibilidad de Inyección de Scripts Maliciosos (XSS)	**3**	**3**	**2**	**5**
Uso de generadores de números pseudoaleatorios débiles	**1**	**1**	**2**	**3**
Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	**3**	**1**	**2**	**7**
Riesgo de Inyección SQL	**7**	**5**	**5**	**7**
Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	**1**	**1**	**2**	**1**
Riesgo asociado con firmware desactualizado en dispositivos MikroTik	**1**	**1**	**2**	**1**

Riesgo de seguridad en cámaras IP	**1**	**3**	**2**	**5**
Configuración de restricciones de acceso para evitar posibles vulnerabilidades	**1**	**1**	**2**	**1**

Tabla 13 Factores para estimar impacto empresarial
Fuente: Propia

Paso 4: Determinar la gravedad del riesgo

Según la metodología de clasificación de riesgo de OWASP se usa la probabilidad y la estimación de impacto para calcular la gravedad general de riego y luego se hace lo mismo con el impacto empresarial. La escala de 0 al 9 se dividen en:

NIVELES DE PROBABILIDAD E IMPACTO	
0 a <3	BAJO
3 a <6	MEDIO
6 a 9	ALTO

Tabla 14 Niveles de probabilidad e impacto
Fuente: OWASP

Según el método repetible de la metodología de estimación de OWASP sumamos los factores de probabilidad para sacar una probabilidad general y también sacamos un impacto técnico general y uno empresarial, por lo que con las amenazas obtenidas tenemos los siguientes resultados.

Amenaza	**Promedio probabilidad**	**Promedio impacto técnico general**	**Promedio impacto empresarial general**
Ausencia de Configuración de Política de Seguridad de Contenido (CSP)	**7.125 (ALTO)**	6.5 **(ALTO)**	5.5 **(MEDIO)**

Desconfiguración de Cross-Origin Resource Sharing (CORS)	**7.625 (ALTO)**	7 **(ALTO)**	7 **(ALTO)**
Posibilidad de Inyección de Scripts Maliciosos (XSS)	**7.375 (ALTO)**	6.5 **(ALTO)**	6.75 **(ALTO)**
Uso de generadores de números pseudoaleatorios débiles	**6.5 (ALTO)**	6.5 **(ALTO)**	3.25 **(MEDIO)**
Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	**6.875 (ALTO)**	6.5 **(ALTO)**	5.25 **(MEDIO)**
Riesgo de Inyección SQL	**8.625 (ALTO)**	9 **(ALTO)**	8 **(ALTO)**
Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	**5.25 (MEDIO)**	4 **(MEDIO)**	1.25 **(BAJO)**
Riesgo asociado con firmware desactualizado en dispositivos MikroTik	**4.875 (MEDIO)**	2.5 **(BAJO)**	3.75 **(MEDIO)**
Riesgo de seguridad en cámaras IP	**5.125 (MEDIO)**	3 **(MEDIO)**	4.25 **(MEDIO)**
Configuración de restricciones de acceso para evitar posibles vulnerabilidades	**4.5 (MEDIO)**	2.5 **(BAJO)**	2.75 **(BAJO)**

Tabla 15 Promedios de probabilidad e impacto
Fuente: Propia

Determinar la gravedad

Con la combinación de la probabilidad e impacto tenemos la calificación de gravedad final para cada riesgo. Con la información del impacto empresarial indica la metodología que debemos usarla en ves de la información técnica sobre el impacto, para guiarse en cada calificación se utiliza la siguiente tabla:

GRAVEDAD DEL RIESGO GENERAL				
IMPACTO	ALTO	Medio	Alto	Critico
	MEDIO	Bajo	Medio	Alto
	BAJO	Bajo	Bajo	Medio
		BAJO	MEDIO	ALTO
	PROBABILIDAD			

Tabla 16 Estimación gravedad de riesgo general
Fuente: OWASP

Con esto se aplica la formula del riesgo en cada ámbito tanto en el técnico como en el empresarial y se tiene la siguiente tabla:

Área de Análisis	Vulnerabilidad	Alerta	Gravedad técnica del riesgo	Gravedad empresarial del riego
Aplicativo web	Ausencia de Configuración de Política de Seguridad de Contenido (CSP)	Content Security Policy (CSP) no configurada	**CRITICO**	**ALTO**
Aplicativo web	Desconfiguración de Cross-Origin	Desconfiguración de Dominio cruzado	**CRITICO**	**CRITICO**

	Resource Sharing (CORS)			
Codigo Página Web	Posibilidad de Inyección de Scripts Maliciosos (XSS)	Cross-Site Scripting (XSS)	**CRITICO**	**CRITICO**
Codigo Página Web	Uso de generadores de números pseudoaleatorios débiles	Weak Cryptography	**CRITICO**	**ALTO**
Codigo Servicios Web	Vulnerabilidad de Falsificación de Solicitud entre Sitios (CSRF)	Cross-Site Request Forgery (CSRF)	**CRITICO**	**ALTO**
Codigo GraphQL	Riesgo de Inyección SQL	SQL Injection	**CRITICO**	**CRITICO**
Red	Uso de Protocolo PPTP, probabilidad de ataques por mala configuración VPN	Puerto abierto 1723 (PPTP)	**MEDIO**	**BAJO**
Red	Riesgo asociado con firmware desactualizado en dispositivos MikroTik	Puerto abierto 2000 (MikroTik)	**BAJO**	**MEDIO**
Red	Riesgo de seguridad en cámaras IP	Puerto abierto 8000 (IP Cam Control)	**MEDIO**	**MEDIO**
Red	Configuración de restricciones de acceso para evitar	Puerto abierto 8001 (Microsoft HTTPAPI)	**BAJO**	**BAJO**

	posibles vulnerabilidades			

Tabla 17 Evaluación de vulnerabilidades encontradas
Fuente: Propia

4.4.6 Mitigaciones y acciones correctivas

VULNERABILIDAD Ausencia de Configuración de Política de Seguridad de Contenido (CSP)			
Riesgo técnico:	Critico	**Riesgo empresarial:**	Alto
Acción: Configuración del archivo standalone.xml del servidor de aplicaciones para enviar el encabezado Content-Security-Policy con las directivas especificadas en cada respuesta HTTP.			
Respaldo: <filters> <response-header name="csp" header-name="Content-Security-Policy" header-value="default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline';"> </response-header> </filters>			

Tabla 18 Mitigación Ausencia de CSP
Fuente: Propia

VULNERABILIDAD Desconfiguración de Cross-Origin Resource Sharing (CORS)			
Riesgo técnico:	Critico	**Riesgo empresarial:**	Critico
Acción: Configuración del archivo standalone.xml del servidor de aplicaciones para forzar el encabezado Access-Control-Allow-Origin con la ip del servidor y el dominio de acceso.			

Respaldo:

```
<filters>
 <response-header name="allow-origin" header-
name="Access-Control-Allow-Origin" header-
value="http://192.168.100.190
https://resultados.autolab.com.ec">
 </response-header>
</filters>
```

Tabla 19 Mitigación desconfiguración CORS
Fuente: Propia

VULNERABILIDAD			
Posibilidad de Inyección de Scripts Maliciosos (XSS)			
Riesgo técnico:	Critico	**Riesgo empresarial:**	Critico
Acción: Creación de función para validar el origen del request.			

Respaldo:

```
private isSameOrigin(url: string): boolean {
const documentUrl = window.location.origin;
const targetUrl = new URL (url, document.baseURI). origin;
return documentUrl === targetUrl; }
this.http.request(request).subscribe(
(response: any) => {
const effectiveUrl = response.url;
if (this.isSameOrigin(effectiveUrl)) {
this.htmlContent =
this.sanitizer.bypassSecurityTrustHtml(response.body);
} else {
console.error('La URL no pertenece al mismo dominio:',
effectiveUrl);
}
```

Tabla 20 Mitigación inyección XSS
Fuente: Propia

VULNERABILIDAD			
Uso de generadores de números pseudoaleatorios débiles			
Riesgo técnico:	Critico	**Riesgo empresarial:**	Alto
Acción: Se cambio el Math.random() por un generador de números pseudoaleatorios criptográficamente fuerte (CSPRNG) como crypto.getRandomValues.			

Respaldo;

```
const crypto = window.crypto || window.msCrypto;
   var array = new Uint32Array(1);
   const random=crypto.getRandomValues(array)[0];
   var tabID = sessionStorage.tabID ?
     sessionStorage.tabID :
      sessionStorage.tabID =random;
```

Tabla 21 Mitigación números pseudoaleatorios débiles
Fuente: Propia

VULNERABILIDAD			
Falsificación de Solicitud entre Sitios (CSRF).			
Riesgo técnico:	Critico	**Riesgo empresarial:**	Alto
Acción: Se tiene configurado un token por cada servicio web exportado, existen algunos servicios Web que no utilizan el token y fue aceptado el riesgo porque son necesarios para la comunicación con otros aplicativos que usan los servicios que expone esta aplicación.			

Respaldo:

```
public Claims
validateToken(HttpServletRequest request){
                String jwtToken =
request.getHeader(HEADER).replace(PREFIX, "");
                try {
                        Jws<Claims>
claims=Jwts.parser().setSigningKey(secret.getBytes()).parseCla
imsJws(jwtToken);
                        return claims.getBody();

                } catch (SignatureException |
MalformedJwtException | UnsupportedJwtException |
IllegalArgumentException ex) {
                        throw new
BadCredentialsException("INVALID_CREDENTIALS", ex);
                } catch (ExpiredJwtException ex) {
                        throw ex;
                }
    }
```

Tabla 22 Mitigación falsificación de CSRF
Fuente: Propia

VULNERABILIDAD			
Riesgo de Inyección SQL			
Riesgo técnico:	Critico	**Riesgo empresarial:**	CRITICO

Acción: No se ejecuta el dato directamente desde el cliente ya que primero se lo realiza unas validaciones para construir la sintaxis, por lo que se está consciente del riesgo.

Respaldo:

```
String query="Select top 50 * from mob_pacientes";

 if(!nombre.equals("") || !apellido.equals("") ||
 !codigo.equals("") || !cedula.equals("")) {
                    query+=" where ";
                         }
                boolean flag_or=false;
                    int cont=0;
               if(!nombre.equals("")) {
                        if(cont>0) {
                          query+=" or ";
                                    }
                   nombre= "%"+nombre+"%";
                           cont++;
                 query+=" nom_pac like ? ";

}...
```

Las vulnerabilidades de red son competencia del servidor físico y la infraestructura de red de cada laboratorio por lo que se transfiere el riesgo al mismo. Se envía los detalles técnicos específicos de las vulnerabilidades identificadas en la red con enfoque particular en que se encuentran abiertos varios puertos en la red del laboratorio.

4.6 Prueba de concepto (POC)

La POC que se llevará a cabo para evaluar el pentesting de servidores de aplicaciones tiene como objetivo principal analizar la eficiencia de las mitigaciones implementadas. Enfocándose en la seguridad informática, la POC busca determinar la eficiencia de las mitigaciones ante posibles amenazas cibernéticas mediante la evaluación y análisis de las amenazas encontradas con su respectiva mitigación. Esta iniciativa se enmarca en la práctica común de validar las defensas antes de avanzar hacia pruebas más extensas y la implementación en producción. Durante la ejecución de la POC, se prestará especial al porcentaje de riesgo en total mediante las herramientas Owasp Zap y Sonar Qube asegurando que las mitigaciones son las adecuadas para cumplir con los requisitos críticos del cliente y del negocio.

Según la norma ISO 27003:2017, en la sección 9, habla de cómo seguir, medir, analizar y evaluar el Sistema de Gestión de Seguridad de la Información (SGSI), que usaremos como base. En lugar de centrarnos únicamente en el SGSI, buscaremos evaluar

la eficacia de las mitigaciones implementadas para que sea una guía adicional a la POC implementada.

La norma indica que para la evaluación necesitamos lo siguiente:

Para el seguimiento y medición:

a) qué monitorear y medir;

b) quién monitorea y mide, y cuándo; y

c) métodos que se utilizarán para producir resultados válidos (equiparables y reproducibles).

Para su análisis y evaluación:

d) quién analiza y evalúa los resultados del seguimiento y la medición, y cuándo;

e) métodos que se utilizarán para producir resultados válidos.

Hay dos aspectos de la evaluación:

f) evaluar el desempeño de la seguridad de la información, para determinar si la organización está hacer lo esperado, lo que incluye determinar qué tan bien los procesos y especificaciones.

g) evaluar la eficacia, para determinar si la organización está haciendo o no.

Existen dos tipos genéricos de medidas:

h) mediciones de desempeño, que expresan los resultados planificados en términos de las características de la actividad planificada, como el recuento de personas, el logro de hitos o el grado en que se implementan controles de seguridad de la información.

i) mediciones de efectividad, que expresan el efecto que tiene la realización de las actividades planificadas

4.6.1 Definición de la idea de la POC

La POC tiene como objetivo evaluar la eficiencia de las mitigaciones implementadas en el análisis de vulnerabilidades abordando así las amenazas identificadas mediante las herramientas de pentesting en el servidor de aplicaciones empresariales dentro del módulo de resultados.

4.6.2 Alcance del Proceso POC

La POC diseñada para evaluar el pentesting de servidores de aplicaciones se enfoca exclusivamente en los análisis que incorporaron las mitigaciones recomendadas para cada amenaza identificada en el servidor empresarial, particularmente en el módulo de resultados. Durante la ejecución de la POC, se implementarán estas acciones de manera exclusiva, utilizando las herramientas Owasp Zap y Sonar Qube.

4.6.3 Criterios para el Éxito

Con la POC realizada se piensa medir el riesgo de las amenazas después de haber aplicado las mitigaciones y su porcentaje de eficiencia de las mitigaciones aplicadas utilizando la misma metodología de estimación de riesgo de OWASP.

4.6.4 Duración del POC y Esfuerzos del Proyecto

El proceso de análisis de construcción de la POC fue de una semana una vez se aplicaron las mitigaciones a cada vulnerabilidad encontrada en el servidor de aplicaciones y el testing del servidor en horas donde no hay mucho tráfico de red para no afectar la disponibilidad del sistema.

4.6.5 Ejecución de la POC

Las vulnerabilidades y fallos identificados de las pruebas de pentesting en el servidor de aplicaciones han sido detectados y mitigados con éxito. Esta acción ha asegurado la integridad y seguridad del servidor, respaldada por la implementación de estrategias de pruebas de penetración, la adopción de buenas prácticas de seguridad y la aplicación de actualizaciones periódicas. Todo ello contribuye a reducir el riesgo de explotación del módulo de resultados.

4.6.5.1 Análisis del aplicativo web

A continuación, se presenta los resultados del nivel de riesgo del servidor de aplicaciones con la herramienta OWASP ZAP después de las correcciones.

		Risk			
		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)
Site	https://resultados.autolab.com.ec	0 (0)	0 (0)	7 (7)	5 (12)

Figura 12 Análisis de Riesgos después de mitigaciones

Fuente: Owasp Zap

Donde se puede observar que en el nivel medio se logró obtener un valor de 0 ya que se mitigó las alertas Content Security y Policy (CSP) no configurada.

4.6.5.2 Análisis del código fuente

Código de Pagina Web

Herramienta: SonarQube.

Calificación revisión de seguridad antes: E.

Calificación revisión de seguridad con mitigaciones: A.

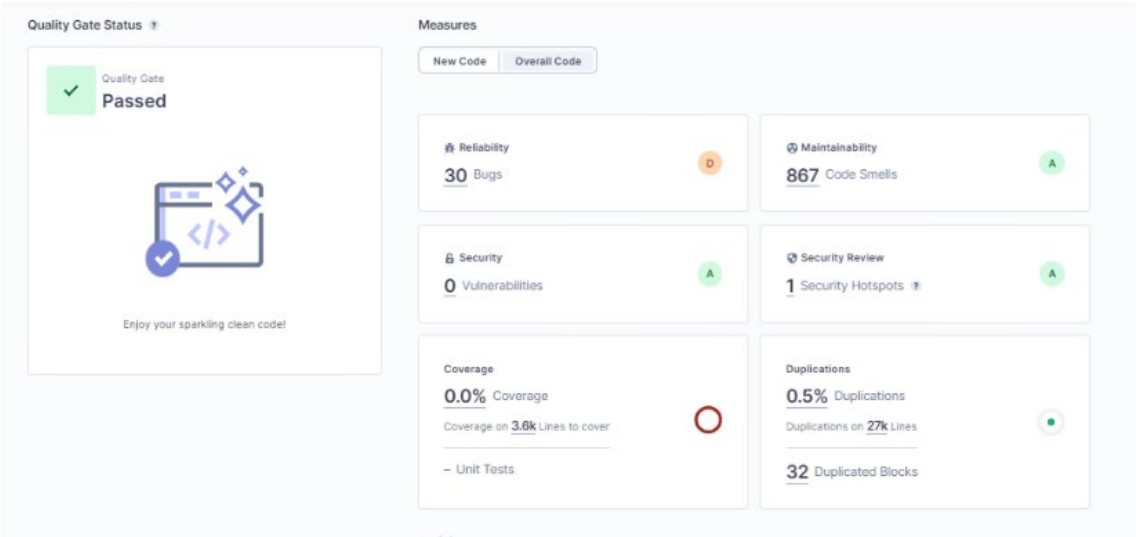


Figura 13 Resumen general del escaneo con mitigaciones de página web
Fuente: SonarQube

Código de Servicios Web

Herramienta: SonarQube.

Calificación revisión de seguridad antes: E.

Calificación revisión de seguridad con mitigaciones: E.

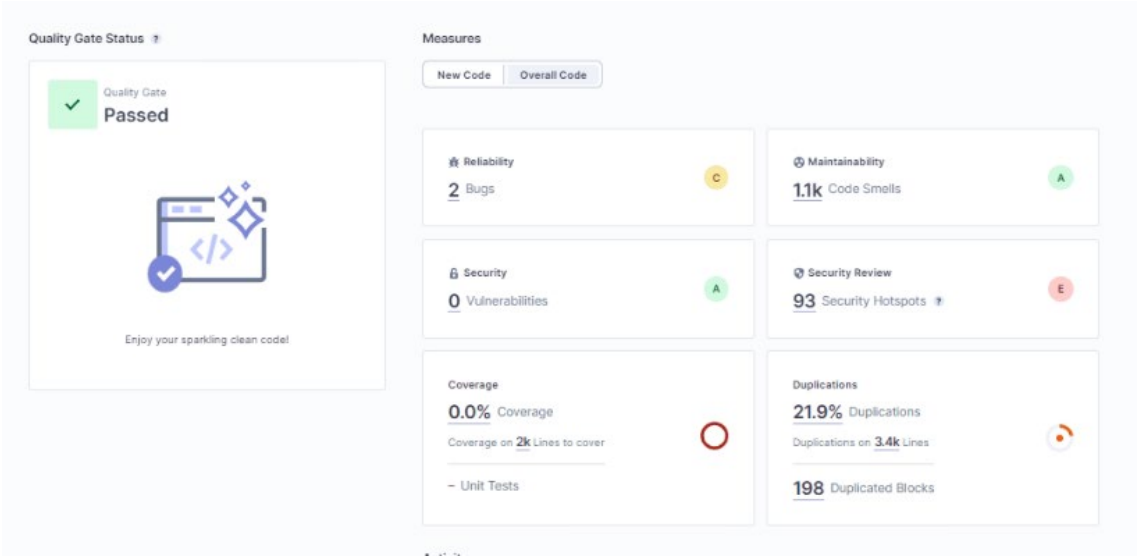


Figura 14 Resumen general del escaneo con mitigaciones de código de servicios web
Fuente: SonarQube

Observación: Esto se debe a que existen demasiadas alertas de vulnerabilidades calificadas como prioridad baja, la que tiene más reincidencia en la impresión de errores en consola con e.printStackTrace(); la cual, al no ser de un riesgo alto, el número de reincidencias afectan la calificación total.

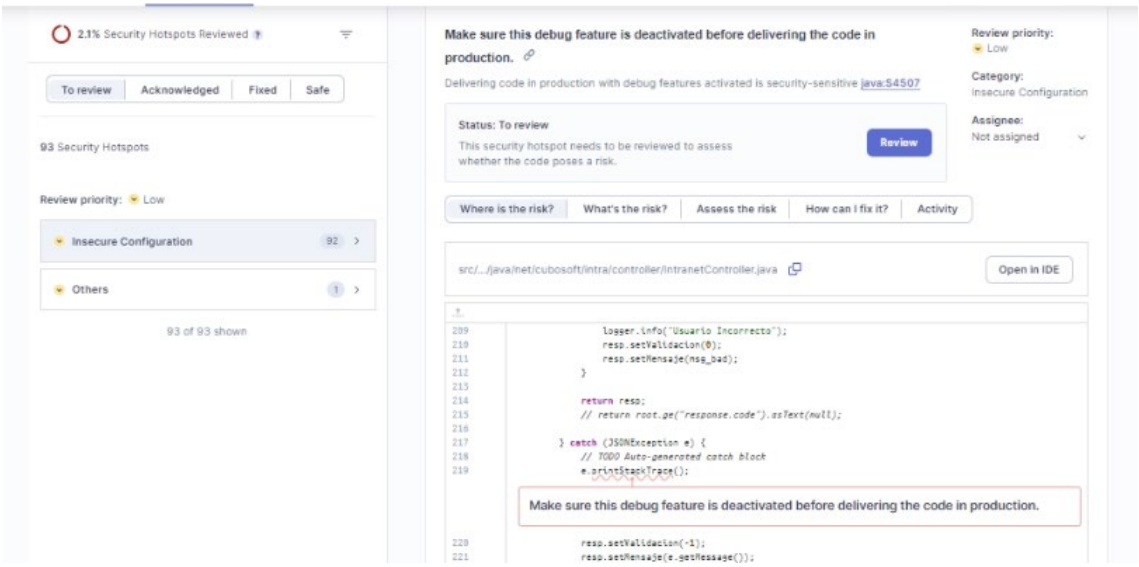


Figura 15 Revisiones de seguridad de código servicios web
Fuente: SonarQube

Código de GraphQL

Herramienta: SonarQube.

Calificación revisión de seguridad antes: E.

Calificación revisión de seguridad con mitigaciones: C.

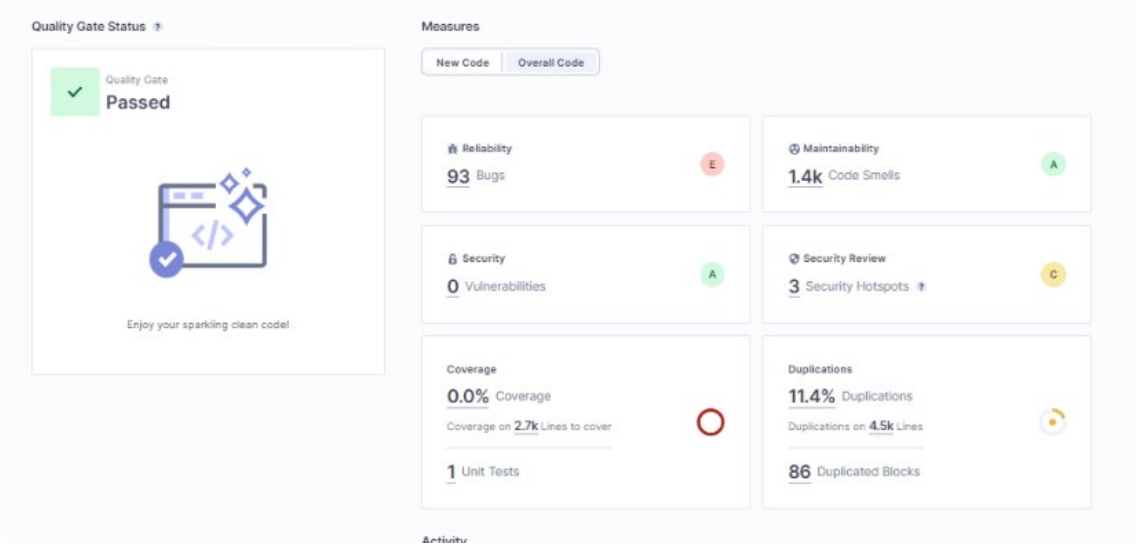


Figura 16 Resumen general del escaneo con mitigaciones GraphQL
Fuente: SonarQube

4.6.6 Análisis y Evaluación de la POC

Se ha completado con éxito la POC, logrando la mitigación efectiva de vulnerabilidades en el servidor de aplicaciones. Las estrategias de prueba de penetración, implementación de buenas prácticas de seguridad y actualizaciones periódicas redujeron significativamente el riesgo de explotación.

Para complementar el análisis de la POC y obtener una comprensión más amplia del panorama de seguridad, se realizó una encuesta dirigida a los 6 integrantes de la empresa responsables del desarrollo y mantenimiento de los servidores de aplicaciones empresariales. Se realizó esto con el fin de obtener una perspectiva directa de aquellos que trabajan en el tema y tienen un conocimiento práctico de las operaciones diarias y los desafíos relacionados con la seguridad de la aplicación dentro del servidor de aplicaciones.

Esta encuesta fue diseñada para recopilar información detallada sobre diversos aspectos, incluida la implementación de las mitigaciones a las vulnerabilidades identificadas durante la POC. Los resultados de la encuesta proporcionaron una comprensión más profunda de la experiencia, conocimientos y prácticas en materia de seguridad de los participantes, lo que permitió contextualizar mejor la eficacia de las medidas implementadas para abordar las amenazas detectadas.

A continuación, se presenta de manera detallada los resultados de la encuesta:

1. Área o rol dentro de la Empresa:

Este ítem identifica los diferentes roles que desempeñan los participantes dentro de la empresa, lo que es crucial para comprender la diversidad de perspectivas y responsabilidades relacionadas con la seguridad de los servidores de aplicaciones.

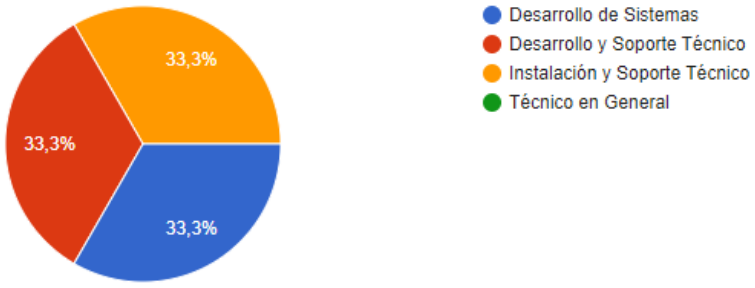


Figura 17 Encuesta: Roles personal involucrado
Fuente: Propia

2. Experiencia Profesional:

Aquí se evalúa la experiencia laboral de los participantes, lo que puede influir en su nivel de conocimiento y habilidades en seguridad. Una mezcla de experiencia moderada sugiere un equipo diverso, pero aún en desarrollo en términos de conocimientos de seguridad.

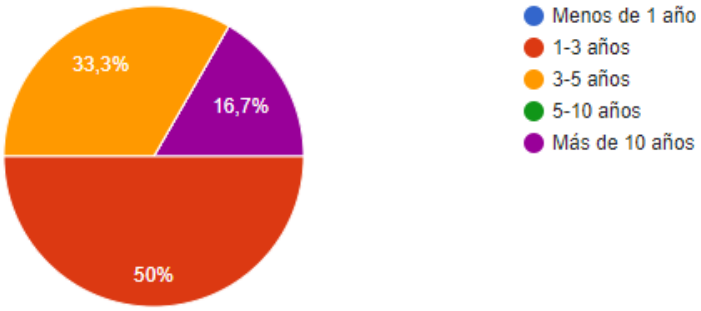


Figura 18 Encuesta: Experiencia personal involucrado
Fuente: Propia

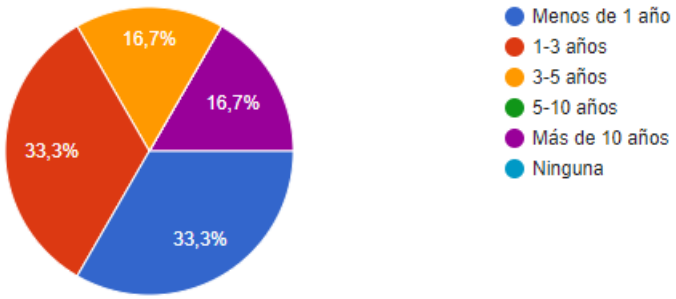


Figura 19 Encuesta: Experiencia en seguridad personal involucrado
Fuente: Propia

3. Conciencia y Conocimiento:

Este ítem aborda la familiaridad de los participantes con las amenazas de seguridad y su nivel de formación específica en seguridad. Destaca la necesidad de fortalecer la capacitación en seguridad para aquellos que no tienen formación específica.

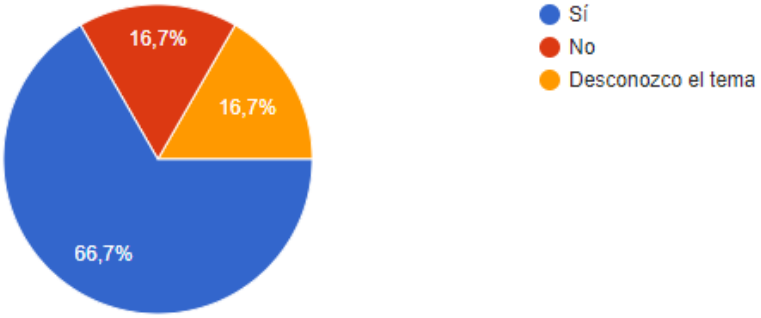


Figura 20 Encuesta: Familiaridad con amenazas
Fuente: Propia

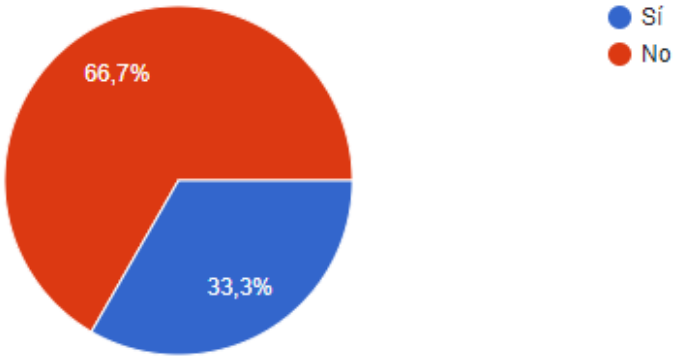


Figura 21 Encuesta: Formación en seguridad
Fuente: Propia

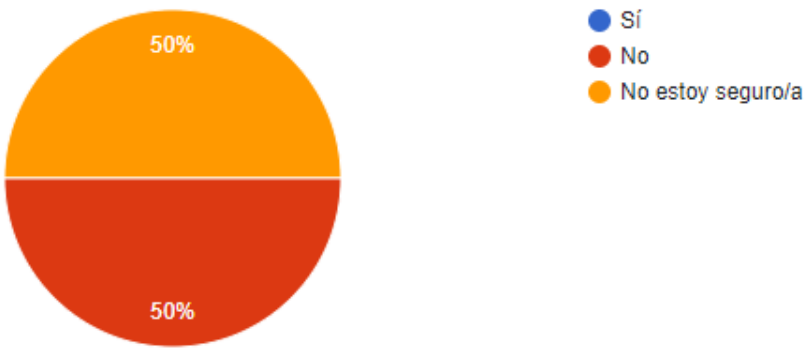


Figura 22 Encuesta: Incidentes en el modulo
Fuente: Propia

4. Uso de Metodologías de Seguridad:

Evalúa la familiaridad y la implementación de metodologías de seguridad reconocidas como OWASP y PTES. La falta de claridad sobre su implementación sugiere áreas potenciales de mejora en la aplicación práctica de estas metodologías.

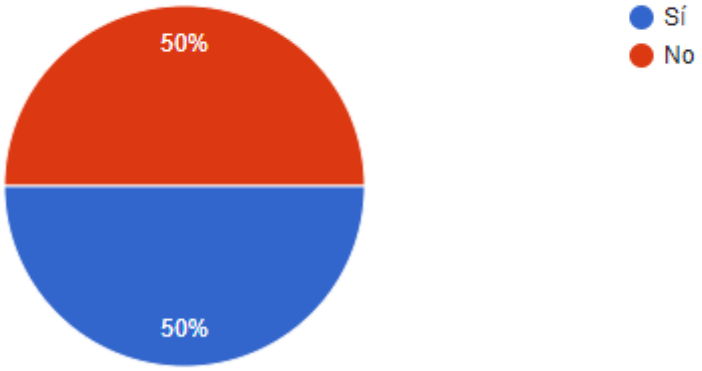


Figura 23 Encuesta: Familiaridad OWASP y PTES
Fuente: Propia

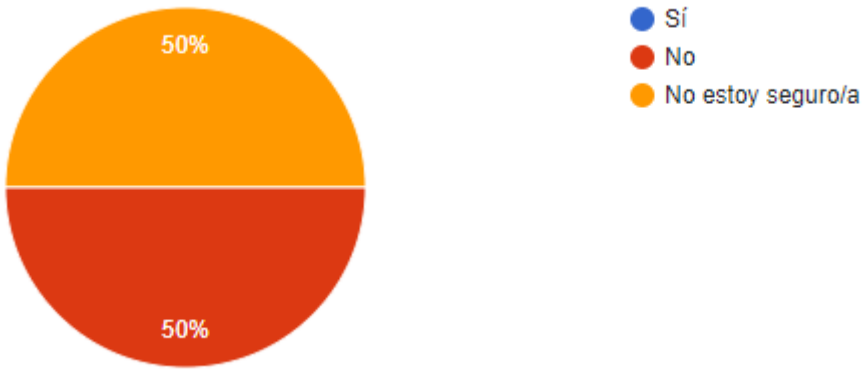


Figura 24 Encuesta: Implementación de OWASP y PTES
Fuente: Propia

Figura 25 Encuesta: Familiaridad actividades OWASP y PTES
Fuente: Propia

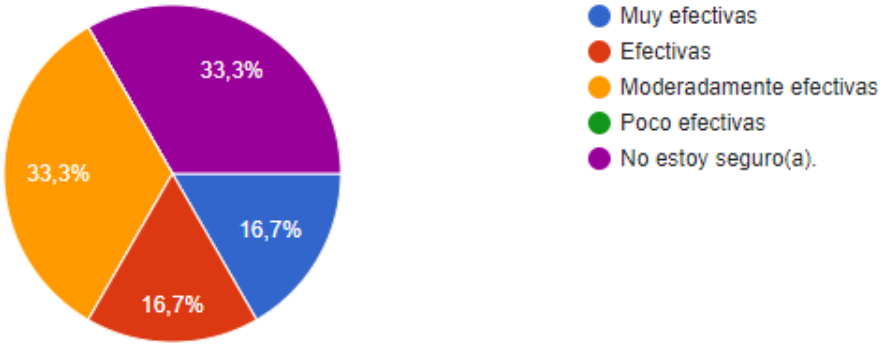


Figura 26 Encuesta: Efectividad percibida de las metodologías
Fuente: Propia

5. Prácticas de Seguridad Implementadas:

Se refiere a las medidas de seguridad que ya están en marcha y la percepción de su efectividad y robustez. Es importante evaluar la efectividad real de estas prácticas más allá de la percepción inicial.

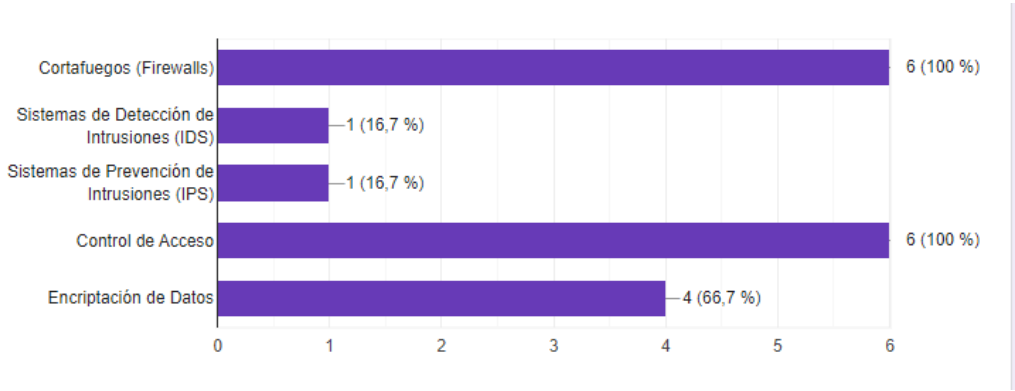


Figura 27 Encuesta: Practicas de seguridad implementadas
Fuente: Propia

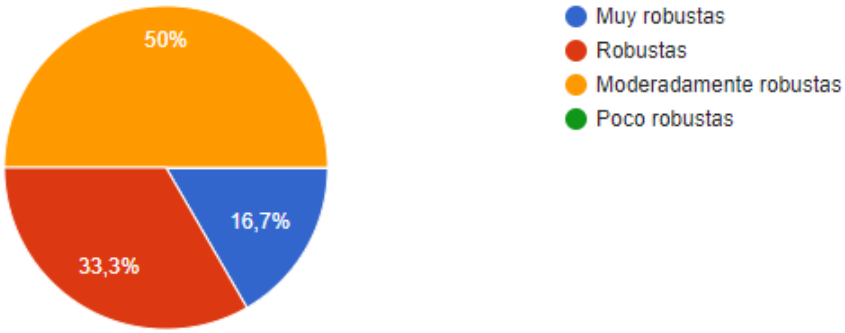


Figura 28 Encuesta: Robustez percibida de medidas
Fuente: Propia

6. Experiencia en pruebas pentesting:

Este ítem indica la experiencia previa de los participantes en pruebas de penetración, un área clave para el desarrollo de habilidades en seguridad.

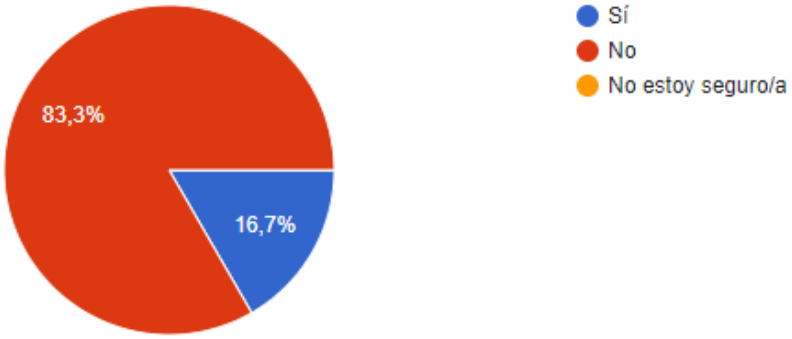


Figura 29 Encuesta: Participación en pruebas
Fuente: Propia

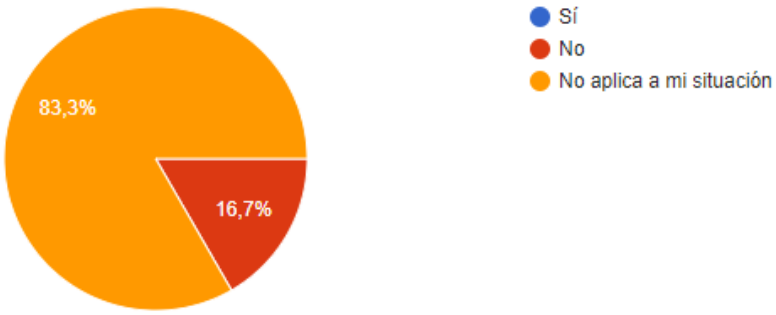


Figura 30 Encuesta: Experiencia en pruebas de seguridad
Fuente: Propia

7. Aplicativo Web - Configuración de Seguridad:

Evalúa el conocimiento y la certeza sobre las medidas de seguridad implementadas en el aplicativo web, subrayando la importancia de la comunicación clara y transparente sobre este aspecto.

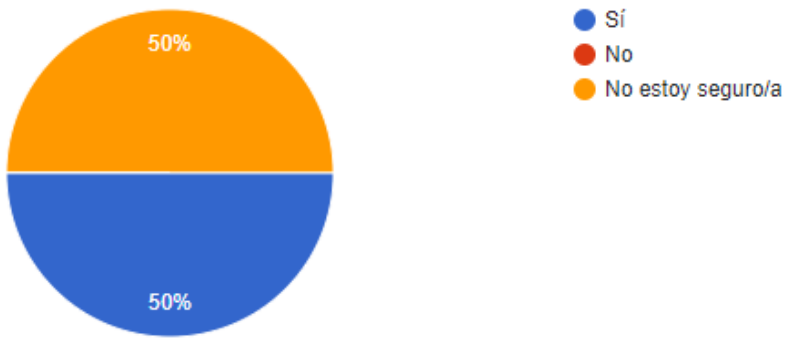


Figura 31 Encuesta: Conocimiento de medidas de seguridad
Fuente: Propia

- Interés en aprender seguridad del aplicativo se obtuvo 100%.

8. Código Página Web - Seguridad del Contenido:

Enfoca la prevención de la inserción de contenido malicioso en el código de la página web, destacando el interés en aprender y mejorar en este aspecto crítico de la seguridad web.

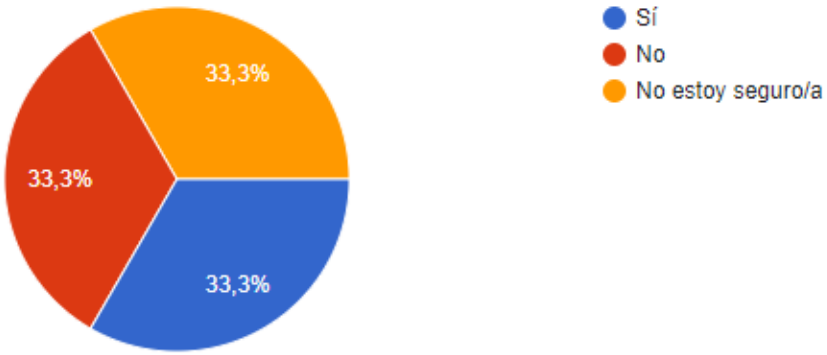


Figura 32 Encuesta: Prevención de inserción de contenido
Fuente: Propia

- Interés de aprender sobre la seguridad del contenido de la página web se obtuvo un 100%.

9. Red - Configuración de Redes:

Aborda el conocimiento y el interés en aprender sobre configuraciones de red que impacten la seguridad, aspecto fundamental en la protección de los sistemas.

- Conocimiento sobre configuraciones de red que afecten la seguridad e Interés de aprender sobre las configuraciones de red para mejorar seguridad se obtuvo un 100% en ambos casos.

10. Dispositivos y Firmware:

Se refiere a la conciencia sobre la importancia de las actualizaciones de dispositivos para mejorar la seguridad, un aspecto clave en la protección contra vulnerabilidades conocidas.

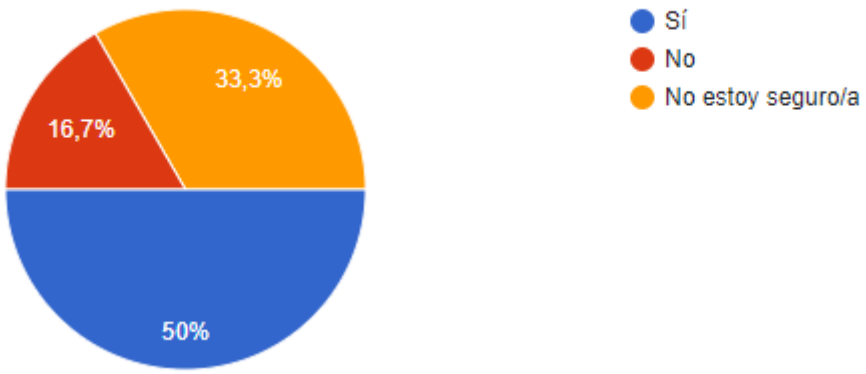


Figura 33 Encuesta: Actualizaciones de dispositivos
Fuente: Propia

- Interés de aprender sobre importancia de actualizaciones para mejorar seguridad se obtuvo un 100%.

11. Concientización en Seguridad:

Evalúa el nivel de conciencia y conocimiento sobre la seguridad de las aplicaciones empresariales, lo que es fundamental para una cultura de seguridad sólida dentro de la organización.

Figura 34 Encuesta: Seguridad de aplicaciones empresariales
Fuente: Propia

12. Colaboración entre Equipos:

Este ítem analiza la comunicación y colaboración entre equipos durante las pruebas de seguridad, destacando la importancia de una comunicación efectiva para abordar problemas de seguridad de manera coordinada.

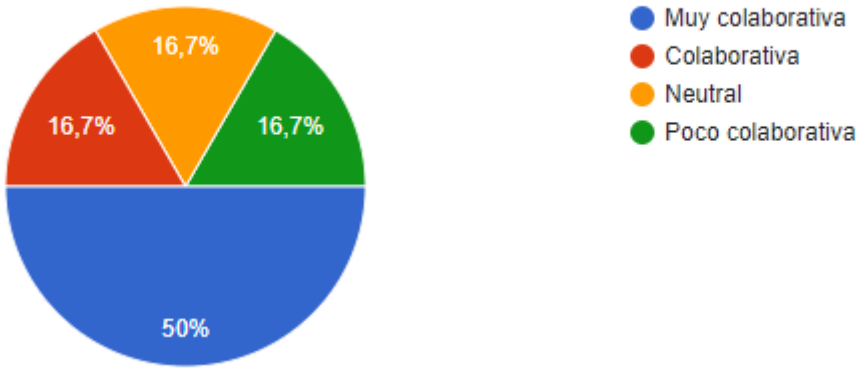


Figura 35 Encuesta: Colaboración entre equipos en pruebas
Fuente: Propia

- Comunicación de problemas de seguridad y soluciones.

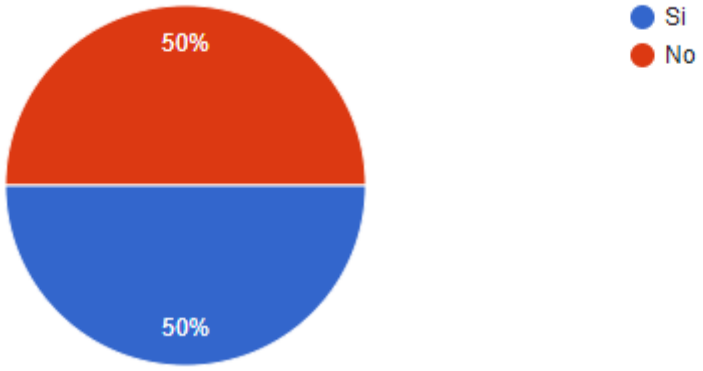


Figura 36 Encuesta: Comunicación de problemas de seguridad y soluciones
Fuente: Propia

4.6.6.1 Resultados Clave

Los resultados arrojaron información valiosa que respaldó nuestras observaciones durante la POC y proporcionó una visión más amplia del panorama de seguridad. A continuación, se presentan los hallazgos clave de la encuesta:

Área o rol dentro de la Empresa: La distribución de roles entre los participantes reflejó una variedad de funciones involucradas en el desarrollo y mantenimiento de los servidores de aplicaciones.

Experiencia Profesional: La mayoría de los participantes tuvo experiencia moderada en sus roles actuales, lo que indicó un equipo diverso, pero con conocimientos aún en desarrollo en materia de seguridad.

Conciencia y Conocimiento: Aunque la mayoría está familiarizada con las amenazas de seguridad, una proporción significativa no ha recibido formación específica en seguridad, lo que destaca la necesidad de fortalecer la capacitación en este aspecto.

Uso de Metodologías de Seguridad: A pesar de la familiaridad con metodologías como OWASP y PTES, hubo una falta de claridad sobre su implementación en la organización, lo que sugiere posibles brechas en la aplicación práctica de estas metodologías.

Prácticas de Seguridad Implementadas: Se observó una implementación sólida de medidas de seguridad, aunque se requiere una evaluación más detallada de su efectividad y robustez.

Experiencia en Pruebas de Penetración: La mayoría de los participantes no tuvo experiencia previa en pruebas de penetración, lo que indica un área potencial para el desarrollo de habilidades en seguridad.

Aplicativo Web - Configuración de Seguridad: Existió incertidumbre sobre las medidas de seguridad implementadas en el aplicativo web, lo que destaca la importancia de una comunicación clara y transparente sobre este aspecto.

Colaboración entre Equipos: Aunque la colaboración durante las pruebas de penetración se percibe como mayormente colaborativa, la falta de comunicación efectiva sobre problemas de seguridad identificados sugiere áreas de mejora en la coordinación entre equipos.

4.7 Discusión

En el estudio realizado por Padilla (2021) se indica la implementación de la metodología OWASP para la detección de vulnerabilidades en la página web de la Tienda DIGI, tales como problemas relacionados con la carga de archivos, inyección SQL y ejecución de código. En otro estudio realizado por Toala Paz (2018), se encontraron hallazgos similares con la implementación de la metodología OWASP y la detección de vulnerabilidades con un pentesting en un servidor de aplicaciones JBoss de un sistema de comisiones, incluyendo la obtención de credenciales y la exposición a ataques de denegación de servicio.

En discusión con el presente estudio, se indica que la investigación representa un avance en comparación con estos dos estudios mencionados, logrando identificar vulnerabilidades y aplicar medidas de mitigación en el servidor de aplicaciones Wildfly, basado en JBoss. Además de la adopción de las metodologías de OWASP y PTES, se implementaron medidas dirigidas a mitigar las vulnerabilidades con alto riesgo, y se llevó a cabo una POC para validar la efectividad de las soluciones propuestas. Este enfoque ampliado permitió una evaluación más completa de la seguridad en los servidores de aplicaciones empresariales, como Wildfly, al proporcionar soluciones específicas y demostrar su eficacia frente a un escaneo de validación de resultados.

Los resultados de la evaluación de amenazas y riesgos del servidor de aplicaciones empresariales de Cubosoft revelaron múltiples vulnerabilidades críticas. Se emplearon metodologías reconocidas en seguridad y privacidad, como OWASP y PETS, para identificar y evaluar estas vulnerabilidades, priorizando así las medidas correctivas necesarias.

Los resultados también resaltan la importancia de la dependencia crítica del código fuente y la configuración del servidor en la eficacia de la seguridad. Estos resultados promueven la eficiencia de incorporar mitigaciones de vulnerabilidades

encontradas con el análisis de pentesting y de esta manera proteger la integridad, confidencialidad y disponibilidad del servidor de aplicaciones.

La POC de mitigaciones realizada como parte de la investigación subraya la importancia de implementar medidas preventivas para evitar posibles ataques. Logrando una mejora sustancial en la seguridad del servidor, con una reducción del 100% en los riesgos de nivel medio y una calificación de seguridad mejorada para el componente de página web con la encuesta de los involucrados en el aplicativo.

Al lograr una mitigación efectiva de vulnerabilidades en el servidor de aplicaciones, se demuestra la eficacia de las estrategias de prueba de penetración, implementación de buenas prácticas de seguridad y actualizaciones periódicas.

Como recomendación para futuras investigaciones, se sugiere explorar el uso de más herramientas de pentesting para obtener un enfoque ampliado. Además, se destaca la importancia de comunicar de manera efectiva la realización de estas pruebas a los integrantes de la empresa, resaltando el impacto positivo en la seguridad del negocio. Este enfoque permite ayudar a generar confianza y conciencia sobre la importancia de mantener la seguridad en todos los aspectos de la empresa.

CONCLUSIONES

La evaluación de amenazas y riesgos del servidor de aplicaciones empresariales de Cubosoft, realizada con metodologías reconocidas en seguridad y privacidad como OWASP y PETS, reveló vulnerabilidades críticas que requieren atención inmediata. Desde la falta de configuraciones de seguridad hasta posibles fallos en dispositivos de red, estas vulnerabilidades representan un riesgo significativo para la integridad y seguridad del sistema. La evaluación del impacto y probabilidad de estas amenazas ha permitido priorizar la asignación de recursos y la implementación de medidas correctivas para fortalecer la seguridad del servidor de aplicaciones.

Esto representa una mejora sustancial en la seguridad del servidor de aplicaciones de Cubosoft, con una reducción significativa en los riesgos de nivel medio según OWASP ZAP y una mejora en la calificación de seguridad del componente de página web a una calificación A, indicando un progreso tangible en la mitigación de vulnerabilidades críticas. A pesar de la persistencia de algunos riesgos, como se refleja en las calificaciones de Sonar Qube, se ha logrado una reducción significativa en su gravedad, lo que demuestra la efectividad de las medidas correctivas implementadas.

Mediante la aplicación de mitigaciones a las amenazas encontradas con el pentesting realizado, se verificó que estas sean efectivas mejorando la seguridad del módulo de resultados web el servidor de aplicaciones empresariales de Cubosoft con una reducción significativa en los riesgos de nivel medio según OWASP ZAP y una mejora en la calificación de seguridad del componente de página web a una calificación A, indicando un progreso tangible en la mitigación de vulnerabilidades críticas. A pesar de la persistencia de algunos riesgos, como se refleja en las calificaciones de Sonar Qube, se ha logrado una reducción significativa en su gravedad, lo que demuestra la efectividad de las medidas correctivas implementadas.

Durante la validación de la POC, se consultó a los involucrados sobre la existencia de incidentes de seguridad, y se encontró que el 50% informó no haber experimentado incidentes, lo que refleja un cumplimiento parcial del objetivo de seguridad mientras que el otro 50% indicó que no estaba al tanto de la existencia de los incidentes, lo que sugiere que no existieron incidentes ya que el equipo no estaba al tanto. Además, se evaluó la robustez de las medidas de seguridad implementadas, con el 50% calificadas como moderadas, el 33% como robustas y el 16.7% como muy robustas, sin registros de calificaciones de "poco robustas". Estos resultados indican un avance significativo en la protección del sistema. La evaluación práctica de la POC aplicada al módulo de resultados

web ha proporcionado una confirmación tangible de la utilidad de las recomendaciones de seguridad propuestas, destacando la efectividad de las soluciones implementadas para abordar las vulnerabilidades identificadas durante el análisis de pentesting.

RECOMENDACIONES

Crear un plan de capacitación continuo en seguridad cibernética para el equipo involucrado en la gestión y el mantenimiento de los servidores de aplicaciones empresariales de Cubosoft, incluyendo sesiones de formación sobre las metodologías OWASP y PTES, así como también realizar ejercicios prácticos de pentesting para fomentar la seguridad del aplicativo.

Establecer procesos de auditoría y monitoreó periódico de los servidores de aplicaciones empresariales de Cubosoft. Incluyendo la realización de escaneos regulares, revisiones de configuraciones nuevas y registro de eventos. También hacer un seguimiento de las métricas de seguridad para evaluar el cumplimiento de las metodologías.

Desarrollar un plan de acción integral para abordar vulnerabilidades de bajo nivel o nuevas vulnerabilidades encontradas en los servidores de aplicaciones empresariales de Cubosoft. Este plan se lo puede realizar con las prácticas y técnicas recomendadas por OWAS o PTES, permitiendo estar preparado para responder de una manera rápida y eficiente ante cualquier incidente que afecte la seguridad del servidor de aplicaciones y asegurando la integridad del módulo de resultados.

Integrar la POC para evaluar mitigaciones de nuevas amenazas en actualizaciones del módulo de resultados, para validar de manera efectiva que las medidas implementadas sean efectivas y garantizar que el entorno de producción se encuentra protegido contra posibles incidentes de seguridad evaluados con la POC.

REFERENCIAS

Basantes Andrade, A. V., Gallegos Varela, M. C., Guevara Vega, C. P., Jácome Ortega, A. E., Posso Astudillo, Á. M., Quiña Mera, J. A., & Vaca Orellana, C. F. (2017). *Comercio electrónico.* Ibarra: Universidad Técnica del Norte. Facultad de Ingeniería en Cienias Aplicadas. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/6793

Castro Vasquez, C. A. (2019). Pruebas de penetración e intrusión. *Universidad Piloto de Colombia*.

Chancusig Chancusig, J. D. (25 de Enero de 2022). Analisis de seguridad en smarth home basado en la métodologia OWASP. Quito: EPN.

Chilán González, I., Francisco Bolaños, B., & Navira Angulo, M. (2019). ANALISIS DE ATAQUES RANSOMWARE EN SERVIDORES WEB, LINUX Y WINDOWS. *Revista Científica UNESUM Ciencias*, 12. doi:https://doi.org/10.47230/unesum-ciencias.v2.n3.2018.106

Cubosoft. (2022). *Cubososft*. Obtenido de https://www.cubosoft.net/

Cubosoft. (s.f.). *Cubososft.* Obtenido de https://www.cubosoft.net/

Cuevas, J. C., Muñoz, R. M., Di Gionantonio, M. A., Gastañaga, I., Gibellini, F., Parisi, G., . . . Zea Cárdenas, M. (2018). Análisis de vulnerabilidades de sistemas web en desarrollo y en producción. *RedUNCI*, 1033-1037. Obtenido de http://sedici.unlp.edu.ar/handle/10915/68347

Cuevas, J. C., Muñoz, R. M., Gibellini, F. A., Parisi, G., Zea Cárdenas, M., & Barrionuevo, D. (2016). Revisión del estado del arte y de las técnicas y herramientas orientadas al desarrollo de un sistema integrado de soporte para análisis de vulnerabilidades en sistemas web. *Universidad Católica de Salta*. Obtenido de http://bibliotecas.ucasal.edu.ar/opac_css/index.php?lvl=cmspage&pageid=24&id_notice=61714

Ecuador. (2021). Ley organica de proteccion de datos personales.

Ecuador, O. T. (s.f.). *¿Qué son los ODS?* Obtenido de https://odsterritorioecuador.ec/ods/

Erazo, C. (2017). *Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting.* Universidad Técnica del Norte, Ingeniería en Sistemas Computacionales, Ibarra. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/7396

Guerra Guzmán, J. G., Guevara Vega, C. P., Imbaquingo Esparza, D. E., Guevara Vega, V. A., & Jácome León, J. G. (2019). Estudio y automatizacióndel proceso

publicitariocon incidencia en negociosde baja productividad . *Ecos de la academia: Revista de la Facultad de Educación, Ciencia y Tecnología - FECYT Nro 10*. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/13607

Guevara-Vega, C. P., Guzmán-Chamorro, E. D., Guevara-Vega, V. A., Andrade, A. V., & Quiña-Mera, J. A. (2019). *Functional requirement management automation and the impact on software projects: case study in ecuador.* Ibarra: Springer International Publishing. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-11890-7_31

Harán, J. M. (23 de 12 de 2022). *5 hechos que resumen qué pasó durante 2022 en ciberseguridad*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2022/12/23/hechos-resumen-que-paso-2022-ciberseguridad/

Maíllo Fernández, J. A. (2020). *Hackers: técnicas y herramientas para atacar y defendernos: (1 ed.* Madrid: RA-MA Editorial. Obtenido de https://elibro.net/es/ereader/utnorte/222726

Mayacela, M., & Guerrero, M. (26 de Abril de 2023). *Ekos.* Obtenido de Los ciberataques incrementaron un 38% en 2022: https://ekosnegocios.com/articulo/los-ciberataques-incrementaron-un-38-en-2022

Ministerio de Telecomunicaciones del Ecuador. (Agosto de 2017). *Ministerio de Telecomunicaciones y de la Sociedad de la Información.* Obtenido de Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad

ODS Territorio Ecuador. (s.f.). Obtenido de ¿Qué son los ODS?: https://odsterritorioecuador.ec/ods/

Owasp. (2014). *Owasp Testing Guide v4.* Obtenido de https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

PADILLA, G. A. (2021). *ANÀLISIS DE TÈCNICAS PARA PRUEBAS DE ETHICAL HACKINGPENTESTING EN SITIOS WEB.* CAÑAR.

Pérez, L. H. (2022). *Hacking Ético.* Madrid: Ra-Ma.

PTES. (08 de 2014). *The Penetration Testing Execution Standard*. Obtenido de http://www.pentest-standard.org/index.php/Main_Page

Quiña-Mera, A., Andrade, L. C., Yugla, J. M., Angamarca, D. C., & Guevara-Vega, C. P. (2021). *Improving software project management by applying agile methodologies: a case study.* Quito: Springer International Publishing. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-71503-8_52

Realpe, M. E., & M., J. J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. doi:10.12804/si9789587844337.10

Rivadeneira Flores, J. O. (2019). *Marco de trabajo para los requerimientos no funcionales y su influencia en la calidad de construcción del software en la Universidad Técnica del Norte.* Universidad Técnica del Norte. Ibarra: Máster en Ingeniería de Software. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/9057

Secretaría Nacional de Planificación. (2021). *Plan de Creación de Oportunidades 2021-2025.* Quito.

Sevillano, F., & Beltrán, M. (2020). *Dirección de seguridad y gestión del ciberriesgo.* Madrid: RA-MA Editorial.

Sierra Huertas, T. (2023). La seguridad informática en el desarrollo de aplicaciones web mediante el uso de la metodología OWASP. *Universidad Nacional Abierta y a Distancia UNAD de Colombia*.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnologica ESPOL*.

Toala Paz, A. X. (2018). *Análisis de vulnerabilidades, pentesting y acciones correctivas sobre el sistema web de comisiones utilizado por instituciones financieras.* Guayaquil: Tesis de Postgrado de la la Facultad de Ingeniería Eléctrica y Computación.

Torres Ortiz, L. M. (2019). *Implementación de metodología PTES en auditorías de seguridad informática.* México: UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

Urbina, G. V. (2016). *Introducción a la seguridad Informática.* Mexico: Grupo Patria. Obtenido de https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=false

Williams, J. (s.f.). *OWASP*. Obtenido de OWASP Risk Rating Methodology: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology