UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMA, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

POLÍTICAS DE SEGURIDAD INFORMÁTICA Y VULNERABILIDADES EN EL SISTEMA PARA GENERAR CITAS Y PAGOS DE FACTURACIÓN DEL CONCESIONARIO AMBACAR

Trabajo de Titulacion, Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computaciones e Informáticos

LÍNEA DE INVESTIGACIÓN: sistemas administradores de recursos

AUTOR: Vanessa Michelle Sánchez Paredes

TUTOR: Ing. Dennis Chicaiza Castillo, Mg.

Ambato-Ecuador

marzo - 2022

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación con el tema: Políticas de Seguridad Informática y Vulnerabilidades en el Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Vanessa Michelle Sánchez Paredes, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2022

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Chicaiza Castillo, Mg.

TUTOR

AUTORÍA

El presente trabajo de investigación titulado: Políticas de Seguridad Informática y Vulnerabilidades en el Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR, es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2022

Vanessa Michelle Sánchez Paredes

CC: 1805340963

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señorita Vanessa Michelle Sanchez Paredes, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado Políticas de Seguridad Informática y Vulnerabilidades en el Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, juntamente con la señora presidenta del Tribunal.

Ambato, marzo 2022

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

Ing. Félix Fernández

PROFESOR CALIFICADOR

Firmado electrónicamente por:
CARLOS ISRAEL NUNEZ MIRANDA

Ing. Carlos Núñez

PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, marzo 2022

Vanessa Michelle Sánchez Paredes

CC: 1805340963

AUTOR

DEDICATORIA

El presente trabajo investigativo lo dedico primero a Dios, porque él me ha guiado y bendecido en este largo camino. Para mis padres en especial a mi madre Myrian quien ha sido mi pilar fundamental dentro de mi vida estudiantil y personal; a mi hermana quien con su amor y dedicación me ha enseñado a ser mejor persona.

Amo y respeto mucho a mi familia, especialmente a quienes ya no están a mi lado mis abuelitos, quienes con su experiencia me enseñaron muchas cosas en el transcurso de mi vida.

A los amigos y colegas que compartieron buenas y malas historias conmigo.

Vanessa Michelle Sánchez Paredes

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su guía y bendición llena siempre mi vida.

A toda mi familia quien me ha apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron a lo largo del camino.

También quiero agradecer a mis docentes por compartir su conocimiento, sabiduría, apoyo y experiencias laborales para ser un mejor profesional en la vida diaria.

Vanessa Michelle Sánchez Paredes

ÍNDICE DECONTENIDOS

INDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN EJECUTIVO

El foco de este trabajo investigativo es la necesidad de proponer un plan para mejorar la seguridad informática del sistema para generar citas y logística, para luego lograr crear y mejorar sistemas más robustos y seguros para los usuarios del concesionario AMBACAR, puesto que es una entidad que ha sido reconocida en el mercado automotriz y espera mejorar dicho software.

La distribución de la investigación sobre la propuesta del plan de mejora de la seguridad informática es la siguiente:

El Capítulo I, "Problemas", describe los problemas que deben investigarse e incluye justificaciones y declaraciones de objetivos.

El Capítulo II, "Marco teórico", contiene los antecedentes de la investigación que apoyará el proyecto de investigación y sugerencias de soluciones a los problemas planteados.

El Capítulo III, "Metodología", describe la implementación del proyecto y demuestra el uso y preparación de la metodología de investigación cualitativa-cuantitativa.

El Capítulo IV, "Formulación de Propuestas", utiliza los métodos descritos en el capítulo anterior para detallar cada paso a seguir en el proceso de investigación y desarrollo. Además, se elaborará un documento con los resultados obtenidos y un plan de mejora de la seguridad.

El capítulo V, "Conclusiones y recomendaciones", presenta las conclusiones de los resultados de la encuesta y las recomendaciones detalladas de un documento con un plan de seguridad informática mejorado elaborado en el capítulo anterior.

Palabras clave: Seguridad informática, Plan de mejora de Seguridad, AMBACAR.

ABSTRACT

The focus of this investigative work is the need to propose a plan to improve the computer security of the system to generate appointments and logistics, in order to later create and improve more robust and secure systems for the users of the AMBACAR dealership, since it is an entity that has been recognized in the automotive market and hopes to improve such software.

The distribution of the research on the proposed plan to improve computer security is as follows:

Chapter I, "Problems," describes the problems to be investigated and includes justifications and objective statements.

Chapter II, "Theoretical framework", contains the background of the research that will support the research project and suggestions for solutions to the problems raised.

Chapter III, "Methodology", describes the implementation of the project and demonstrates the use and preparation of the qualitative-quantitative research methodology.

Chapter IV, "Proposal Formulation", uses the methods described in the previous chapter to detail each step to be followed in the research and development process. In addition, a document with the results obtained and a security improvement plan will be prepared.

Chapter V, "Conclusions and Recommendations", presents the conclusions of the survey results and the detailed recommendations of a document with an enhanced IT security plan developed in the previous chapter.

Keywords: Computer security, Security improvement plan, AMBACAR.

INTRODUCCIÓN

Desde inicios de la historia, de una u otra manera siempre ha estado presente el concepto de seguridad, que ha evolucionado incomparablemente a través del tiempo para adaptarse a las nuevas circunstancias; en este ámbito ha existido la rivalidad entre quienes tienen el tesoro (datos e información) y quienes lo quieren adquirir. Los primeros colocan todo tipo de medidas de seguridad y los segundos intentan buscar debilidades y grietas que les permita burlar las medidas de seguridad y, de esta manera, ingresar al tesoro anhelado.

La irrupción de Internet y la consiguiente globalización permiten entrar a informaciones a las que las barreras que imponían el espacio o el tiempo para su obtención hacían desistir de obtenerla, sin embargo, la apertura de las empresas al mundo globalizado, comporta la necesidad de exposición de la información almacenada a un número ingente de probables candidatos a querer obtener dicha información por motivos bien diferentes ya sea, la evolución de la tecnología, de las comunicaciones, la movilidad de los individuos, etc.

El acceso a los servicios se ha convertido en algo habitual, esta cotidianidad y diversidad de dispositivos para acceder a estos servicios, han facilitado cada vez más la externalización de los sistemas de la información en las organizaciones, a lo cual, la nube es una propuesta de ofrecer servicios de forma ágil, flexible y de abajo costo.

El avance de los sistemas y la tecnología de la información ofrece un beneficio vital para las empresas. Sin embargo, también trae desafíos cada vez mayores debido a la existencia de piratas informáticos, malware, virus, delitos cibernéticos, etc. Por lo tanto, se requiere un seguimiento frecuente y sólido a través de la seguridad de los sistemas de información. Sin embargo, la escasez de profesionales y la falta de marcos adecuados en este dominio se citan con frecuencia como las principales barreras para el éxito.

Debido a la expansión de Internet y la aparición de técnicas de piratería informática más sofisticadas, las empresas se enfrentan hoy en día a una grave amenaza para la seguridad informática. Los incidentes de seguridad causados por ataques informáticos como la piratería informática, la denegación de servicio, los virus y el robo de información pueden tener un efecto negativo en la reputación de una empresa, como la pérdida de credibilidad, además de causar un gran daño financiero a la organización [1].

1 CÁPITULO I MARCO TEÓRICO

1.1 Tema de Investigación

Auditoría de seguridad informática al sistema para generar citas y pagos de Facturación del concesionario AMBACAR.

1.2 Antecedentes Investigativos

1.2.1 Estudio del arte

Hay una serie de investigaciones relacionadas con la seguridad de la información y las vulnerabilidades de los cuales se hacen tratamientos con la finalidad de comprender su importancia en el entorno actual de los sistemas informáticos.

Un estudio internacional desarrollado como revisión documental de Humayun y otros [2] detalla que ha habido un tremendo aumento en la investigación en el área de la seguridad cibernética para respaldar las aplicaciones cibernéticas y evitar las amenazas de seguridad clave que enfrentan estas aplicaciones. El objetivo de este estudio es identificar y analizar las vulnerabilidades comunes de ciberseguridad. Para lograr este objetivo, se realizó un estudio de mapeo sistemático y, en total, se identificaron y analizaron 78 estudios primarios. Los resultados muestran que los enfoques de seguridad mencionados hasta ahora solo se enfocan en la seguridad en general, y las soluciones proporcionadas en estos estudios necesitan más validación empírica e implementación real. Además, nuestros resultados muestran que la mayoría de los estudios seleccionados en esta revisión se enfocaron solo en algunas vulnerabilidades de seguridad comunes, como phishing, denegación de servicio y malware. Sin embargo, existe la necesidad, en futuras investigaciones, de identificar las vulnerabilidades clave de la seguridad cibernética, las aplicaciones dirigidas/victimizadas, las técnicas de mitigación y las infraestructuras, para que los investigadores y profesionales puedan obtener una mejor comprensión de esto.

Ninguna de las otras tres revisiones bibliográficas Flowerday y Tuyikeze [3] y Cram y otros [4] emplearon una perspectiva de herramienta computarizada en la investigación de gestión de PSI. En cambio, han contribuido a sintetizar el conocimiento existente sobre lo que debería influir en el diseño de los PSI, es decir, estas compilaciones pueden, hasta cierto punto, verse

como requisitos que las herramientas informáticas deben respaldar. Flowerday y Tuyikeze [3] revisaron 21 documentos, "elementos publicados citados y predominantes sobre el tema en Google Scholar", para comprender y sugerir un ciclo de vida de desarrollo de PSI. Los autores nunca abordaron explícitamente los requisitos detallados para el diseño de PSI. En cambio, su codificación de lo que las organizaciones deben tener en cuenta al desarrollar PSI resultó en tres áreas amplias: (1) impulsores de políticas de seguridad, (2) orientación de políticas de seguridad y (3) teorías existentes. Los impulsores de políticas de seguridad se refieren a lo que presiona a las organizaciones para diseñar PSI y, según los autores, dicha presión puede provenir tanto de fuentes externas como internas. La orientación de la política de seguridad se refiere al uso de estándares de seguridad de la información, como la serie ISO-27000, como apoyo al diseñar los PSI. Finalmente, las teorías existentes tratan sobre el uso de teorías para comprender el comportamiento de seguridad de la información de los empleados, argumentando que estas teorías deberían tener un impacto en el trabajo de diseño [5].

Cram y otros [4] sintetizó el conocimiento actual de 114 publicaciones de revistas influyentes relacionadas con PSI en forma de un marco de investigación. En total, su marco consta de 10 categorías y cinco relaciones entre estas categorías. Una de estas relaciones aborda influencias en el diseño e implementación de políticas de seguridad. Los autores identificaron tres categorías, que pueden verse como áreas de requisitos amplios: (1) estándares, pautas y regulaciones de seguridad, (2) formato y estructura deseados, y (3) consideraciones de gestión de riesgos internos y externos. La primera categoría se refiere a las opciones disponibles para guiar la gestión de PSI, como la serie ISO-27000, así como las pautas legales y reglamentarias requeridas. También se refieren a consejos paso a paso más tangibles para guiar el proceso- La segunda categoría se basa en investigaciones existentes que se enfocan en “los objetivos de crear una política que los empleados puedan leer y comprender”. Han ejemplificado con un conjunto de factores (brevedad, claridad y amplitud) que deberían afectar las decisiones de diseño de PSI. Finalmente, la tercera categoría aborda las consideraciones de gestión de riesgos. Significa que las características de las organizaciones, tanto internas como externas, deben influir en las decisiones de diseño del PSI.

Järveläinen [6] revisó 46 trabajos de investigación que abordan el desarrollo de PSI para comparar los métodos de desarrollo del diseño de PSI y la planificación de la continuidad del negocio y presentó un método integrado. Aunque no proporcionó ninguna categorización explícita de lo que debería influir en el diseño de los PSI, concluyó que: los PSI se supone que son un conjunto integral de principios duraderos, generales e independientes de la tecnología, (2) El principal objetivo de un PSI es garantizar la confidencialidad, integridad y disponibilidad de los datos de una organización, los PSI deben basarse en riesgos reconocidos, y las partes interesadas deben participar en el diseño de los PSI.

En AMBACAR existen elementos relacionados con las políticas de seguridad y vulnerabilidades utilizadas por sus diferentes usuarios. Por lo cual se presentan investigaciones nacionales hechas en el Ecuador, para considerar que tan arraigado se encuentra la seguridad de la información.

Escobar [7] en su trabajo de graduación “Sistema de Gestión de Seguridad de la Información aplicando las normas ISO/IEC 27001 en el DATACENTER de la empresa AMBACAR-Ambato”,2020; diseño el sistema de gestión para la entidad AMBACAR, para mejorar la seguridad de la información así también como mejorar los controles de los activos de información, sin embargo en sus recomendaciones manifiesta crear y analizar políticas de forma periódica en base a la necesidad de la empresa.

Cárdenas [8]en su proyecto "Diseño de una Estrategia de Seguridad de la Información para la Unidad Educativa Borja 3 Cavanis, Basada en Normas ISO / IEC (Organización Internacional de Normalización / Comisión Electrotécnica Internacional) 27002: 2013", 2020; mencionó que se pueden diseñar estrategias de seguridad de la información para proteger la integridad, confidencialidad y disponibilidad de la información.

Lino [9] en su tesis “Diseño de un plan de seguridad informática para la Cooperativa de Ahorro y Crédito “Por el Pan y el Agua” de la ciudad de Jipijapa”, en el 2019, sugirió que todos los niveles de la organización tienen una responsabilidad compartida dirigida por un plan y una adecuada coordinación.

Arias y otros [10] en su tesis de grado “Análisis y Solución de las vulnerabilidades de la seguridad informática y seguridad de la información de medio de comunicación Audio - Visual”, en el 2013, indica que la buena práctica de seguridad informática basado en la norma

ISO 27002:2005 ayuda en el aprendizaje de procesos seguros en el tratamiento de la información.

Según una investigación realizada por estudiantes de la Universidad Técnica de Babahoyo, Vega y Ramos [11] afirmaron en sus artículos científicos que no existe un software específico que pueda administrar las actividades de seguridad informática y manejar de manera efectiva las conexiones de los usuarios de la red y monitorear el acceso y el uso de Internet.

Debido al libre acceso a sitios inseguros en la intranet y a la falta de una gestión adecuada en la infraestructura técnica, esto restringe el trabajo al firewall de hardware, lo que a su vez conduce a una desconfianza total en los pasantes universitarios debido a una gran cantidad de vulnerabilidades.

Al final de su investigación Díaz [12], experta en seguridad de la información de la Universidad Pontificia Bolivariana seccional Bucaramanga, concluyó que las empresas de procesos de aseguramiento de la calidad deben buscar definir el rol del equipo de calidad del software, las responsabilidades de los desarrolladores y los siguientes aspectos de seguridad de la información requisitos de las actividades de la empresa, incluyendo estos aspectos en la prueba del software, no solo cuando el cliente lo requiera.

Las empresas dedicadas al desarrollo de software deben establecer sus políticas y procedimientos de aseguramiento de la calidad del software, definir los requisitos de seguridad basados en el análisis de riesgos y considerar el tiempo, los recursos (técnicos, humanos y económicos), las limitaciones del equipo y las ventajas competitivas (desarrollo y calidad) para invertir. por turnos Para capacitación; con el fin de brindar un alto nivel de integración en la prueba, mejorando así la calidad del software, esto se demostrará en la satisfacción de los clientes y usuarios finales y la reducción de costos por trabajo extra o incumplimiento con tiempo [12].

1.2.2 Planteamiento del problema

Actualmente, el uso de las tecnologías de la información (TI) por parte de organizaciones públicas y privadas de todo el mundo está aumentando de manera excesiva y muy importante porque hemos sido testigos de cambios sin precedentes en la economía mundial y el mundo del trabajo [13].

Hace diez años ocurrió un particular incidente de seguridad en una reconocida empresa del sur de Ecuador; quizás, este fue uno de los primeros casos de un ciberataque efectivo a una empresa en Ecuador. La víctima era un importador de equipos comprados regularmente en una fábrica china. En la comunicación por correo electrónico entre el jefe de la empresa local y el exportador asiático, un hacker se infiltró, defraudó al empresario ecuatoriano y lo impulsó a pagar a través de un banco internacional la Transferencia de dinero a una cuenta fraudulenta de Hong Kong por un valor aproximado de US $ 40.000; aquí está la importancia de la seguridad informática y las vulnerabilidades provocadas por múltiples sistemas informáticos, no solo en el departamento de producción de la empresa, sino también en los sistemas financieros, comerciales y de servicios de nuestro país [14].

El 11 de marzo, la Organización Mundial de la Salud (OMS) se refirió al brote del nuevo coronavirus como una pandemia e instó a los gobiernos de todo el mundo a tomar este problema en serio y prepararse para la primera ola de emergencias de salud pública. [15]. Con la implementación del encierro o medidas domiciliarias, gran parte de la fuerza laboral tiene que quedarse en casa para trabajar de forma remota, siempre que su función lo permita, por lo que se convierte en la principal herramienta de la tecnología para trabajar. De esta manera, se instalan nuevos métodos para simplificar cada uno de los procesos de la empresa AMBACAR, empresa con más de 50 años de trayectoria en el mercado automotriz, establecida en Ambato, hoy cuenta con una extensa red de distribuidores y talleres de servicio técnico y repuestos a través del país. La atención al cliente ha sido siempre un pilar importante dentro de la filosofía de la empresa, por esta razón suministra un gran servicio post venta, generador de citas y pagos de Facturación, logística entre otros servicios más, dentro de su página web con finalidad de hacer más fácil la accesibilidad a la empresa por parte de sus clientes y empleados, sin embargo, se requiere mejorar la eficiencia y fortalecer la seguridad informática existente con objeto de brindar confianza en sus clientes.

Es indiscutible que en la actualidad la seguridad en las aplicaciones web es el principal campo de batalla entre atacantes y aquellos que administran recursos y datos que se deben defender y es probable que siga así en el futuro mediato. Como parte de los mecanismos básicos de seguridad de las aplicaciones, los controles de acceso se encuentran construidos por encima de los mecanismos de autenticación y de gestión de sesión; la principal razón por la que una aplicación necesita incluir estas funcionalidades, al menos en términos de la seguridad, es la

necesidad de contar con algún mecanismo que le permita decidir si permite la ejecución de la acción indicada en una solicitud sobre los recursos indicados [16].

Muchas empresas actualmente no cuentan con planes de contingencia ante ataques de seguridad informática, y no es raro que aquellas dedicadas al desarrollo de software no vean la necesidad de implementar medidas para proteger la información, ya que, se suele tener la creencia de que su tarea se limita a crear un producto que es ajeno a ataques de seguridad informática, pues tiende a verse como un asunto de la infraestructura y redes de telecomunicaciones, y que no concierne al mundo de la programación.

En el periodo 2018- 2021 se ha detectado un incremento significativo del uso de la página web por parte de los clientes de AMBACAR, ya que, cuenta con un sistema en el cual posee varias herramientas que permite agilitar procesos al cliente, la mayor acogida que ha tenido este sistema radica en la herramienta de recepción de citas y logística, la misión de AMBACAR es proveer productos y servicios automotrices innovadores, tecnológicos, de calidad. Está hablando de artículos tecnológicos y ¿cómo no utilizar la tecnología para poder expandir el servicio a través de las redes?

Necesita fortalecer las condiciones de la seguridad informática existente, ya que, se limita a proteger los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no entre sí, es importante porque maneja información de facturación, maneja circulante y activos netos de nuestra empresa cualquier falla podría representar declives significativos para la economía y las finanzas de la misma, uno de las técnicas que fortifica de alguna manera la seguridad informática es el análisis y establecimiento de Políticas de seguridad informática y vulnerabilidades que permite tener un sistema productivo y eficiente tanto para el cliente como para la empresa.

1.2.3 Fundamentación Teórica

Auditoría de Seguridad de Sistemas de Información

Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en Tecnologías de la Información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones [17].

Una auditoría de seguridad de los sistemas de información (AISS) es una revisión y un examen independientes de los registros, actividades y documentos relacionados del sistema. Estas auditorías están destinadas a mejorar el nivel de seguridad de la información, evitar diseños de seguridad de la información inadecuados y optimizar la eficiencia de las medidas de seguridad y los procesos de seguridad. El término "marco de seguridad" se ha utilizado de diversas maneras en la literatura de seguridad durante el años, pero en 2006 pasó a utilizarse como un término agregado para los diversos documentos, algunas piezas de software y la variedad de fuentes que brindan asesoramiento sobre temas relacionados con la seguridad de los sistemas de información, en particular, con respecto a la planificación, gestión o auditoría de las prácticas generales de seguridad de la información para una institución dada [18]. Aunque la seguridad es un proceso interminable que requiere un seguimiento continuo, todavía está en pañales. Además, la auditoría de seguridad es un área inexplorada y requiere un marco simple para guiar el proceso. De ahí la necesidad de un estudio seguido de esta propuesta de marco genérico que describa la información principal para las tareas de auditoría de seguridad y las responsabilidades de los auditores desde el inicio de un proyecto [19].

Seguridad Informática

El entorno de gestión de riesgos de seguridad de la información está cambiando; por lo tanto, debe ser revisado y actualizado constantemente. Se entiende que la seguridad de la información se compone de todas las medidas preventivas y reactivas que permiten el resguardo y protección de la información para mantener la confidencialidad, disponibilidad e integridad [20].

Según ISO 27001, el objetivo de la seguridad de la información es "proteger la confidencialidad, integridad y disponibilidad de la información. Además, pueden estar involucrados otros atributos, como autenticidad, responsabilidad, no repudio y confiabilidad" [21]. El experto en seguridad informática Jorge Aguirre propuso un concepto en su libro, a saber, "la calidad de un sistema informático sin peligro" [22].

Por lo tanto, el concepto adecuado de seguridad informática es brindar confiabilidad e integridad al hardware y al software a través de diferentes procesos a seguir para garantizar la protección de los datos del usuario contra el acceso no autorizado [23].

La seguridad de la información tiene como propósito es salvaguardar los activos de información de una organización. Los controles para proteger la información se pueden clasificar en tres categorías principales: controles técnicos, controles formales y controles informales [24]. La implementación de controles técnicos, como firewalls, criptografía y redes privadas virtuales, es esencial para que las organizaciones se mantengan protegidas [25]. Sin embargo, las organizaciones no pueden depender únicamente de las soluciones técnicas. Las organizaciones también necesitan contar con controles formales, como rutinas administrativas, para prevenir incidentes de seguridad de la información y violaciones de la seguridad de la información. Finalmente, los controles informales se enfocan en aspectos sociales, como aumentar la conciencia de los empleados sobre temas de seguridad de la información mediante programas de educación y capacitación [24].

Entre los tipos de controles formales, la política de seguridad de la información (PSI) se considera una de las claves para tener una seguridad de la información efectiva [26]. La PSI son las reglas establecidas que brindan orientación en la protección de los activos de una organización [27].

Aun así, el concepto de PSI se usa con significados diferentes en diferentes contextos de uso [28]. Es común clasificar los PSI en tres niveles [4].

En el nivel más alto se encuentra el nivel estratégico, donde la alta dirección expresa la dirección estratégica y el alcance de los esfuerzos de seguridad de la información de la organización. Este tipo de políticas proporciona una guía general para el programa de seguridad de la información de la organización y asigna responsabilidades para diferentes áreas de seguridad de la información.

El siguiente nivel son los operativos, que brindan orientación al usuario para tareas de trabajo o tecnología específicas. Por lo tanto, estos PSI incluyen pautas y procedimientos de procedimientos aceptables que los usuarios de PSI, como empleados y actores externos que trabajan con activos de información del cliente, deben cumplir diariamente [4].

En el nivel más bajo son los PSI técnicos. Estos son la implementación de estándares, reglas y procedimientos en tecnología de la información [29].

Los PSI se promulgan y realizan a través de las acciones de los usuarios de PSI en función de su conocimiento local y situacional [28]. El incumplimiento de los PSI por parte de los

empleados se ha destacado como un problema perenne para muchas organizaciones, y estas fallas se caracterizan comúnmente como un "problema de personas". Por lo tanto, los investigadores han buscado y aumentado el conocimiento de los factores relacionados con el individuo que explican el bajo cumplimiento de los empleados. Además, los investigadores han explorado cómo los programas de educación, capacitación y concientización sobre seguridad pueden abordar este problema [30].

A pesar de los méritos de la investigación mencionada anteriormente, también se ha demostrado que aproximadamente la mitad de todas las brechas de seguridad de la información causadas por personas internas son accidentales. Karlson y otros [4], por lo tanto, han argumentado que también existe un aspecto de diseño de PSI relacionado con el problema de las personas. Las personas, o más específicamente los gerentes de seguridad de la información, diseñan los PSI y estas políticas pueden ser engorrosas de seguir, contradictorias y, a veces, incompatibles con las prácticas laborales existentes. En cuanto a esto último, los empleados deben priorizar entre la seguridad de la información y su práctica laboral. Cuando los empleados necesitan priorizar su práctica laboral sobre los PSI mal diseñados, con el tiempo puede disminuir la motivación de seguridad de la información de los empleados. Esto muestra la necesidad de PSI de alta calidad que puedan guiar los comportamientos de los empleados de manera útil [27].

El diseño de PSI no es una tarea trivial y, a menudo, se considera como una fase en todo el ciclo de vida de gestión de PSI [4]. La fase de diseño en sí contiene varias etapas y que es una tarea de varias capas que requiere mucho esfuerzo por parte de los gerentes de seguridad de la información. Por esa razón, los investigadores han propuesto diferentes tipos de soporte de diseño. En la literatura es posible, por ejemplo, encontrar factores y lineamientos que deben ser considerados al diseñar PSI como, así como marcos que muestran los procesos paso a paso del desarrollo [31]. Además, para aliviar la carga de los administradores de seguridad de la información, se han sugerido herramientas computarizadas [28].

La seguridad de la información incluye las amplias áreas de gestión de la seguridad de la información, seguridad informática y de datos, y seguridad de la red. Es el concepto de política. Las políticas, la concientización, la capacitación, la educación y la tecnología son

conceptos vitales para la protección de la información y para mantener los sistemas de información a salvo [10].

La seguridad de la información implica la protección de los activos de la organización contra la interrupción de las operaciones comerciales, la modificación de datos confidenciales o la divulgación de información patentada. La protección de estos datos generalmente se describe como el mantenimiento de la confidencialidad, integridad y disponibilidad de los activos, las operaciones y la información de la organización [32].

Elementos de la seguridad de la información

Un programa exitoso de seguridad de la información combina los siguientes elementos conceptuales para reducir el riesgo de sus activos de información:

Confidencialidad

La confidencialidad de la información asegura que solo aquellos con suficientes privilegios puedan acceder a cierta información. Cuando personas o sistemas no autorizados pueden acceder a la información, se viola la confidencialidad. Para proteger la confidencialidad de la información, se utilizan una serie de medidas:

- Clasificación de la información
- Almacenamiento seguro de documentos
- Aplicación de políticas generales de seguridad
- Educación de los custodios y usuarios finales de la información [10].

Integridad

La integridad es la cualidad o el estado de ser íntegro, completo e incorrupto. La integridad de la información se ve amenazada cuando se expone a corrupción, daño, destrucción u otra alteración de su estado auténtico. La corrupción puede ocurrir mientras se recopila, almacena o transmite información [33].

Disponibilidad

La disponibilidad es la característica de la información que permite al usuario acceder a la información sin interferencias u obstrucciones y en un formato requerido. Un usuario en esta definición puede ser una persona u otro sistema informático. La disponibilidad no implica

que la información sea accesible para cualquier usuario; sino que está disponible para usuarios autorizados [32].

Intimidad

La información recopilada, utilizada y almacenada por una organización se utilizará únicamente para los fines establecidos al propietario de los datos en el momento en que se recopiló. Esta definición de privacidad se centra en la libertad de observación (el significado generalmente asociado con la palabra), lo que significa que esta información se usará solo de la manera conocida por la persona que la proporciona.

Identificación

Un sistema de información posee la característica de identificación cuando es capaz de reconocer usuarios individuales. La identificación y la autenticación son esenciales para establecer el nivel de acceso o autorización que se otorga a un individuo.

Autenticación

La autenticación se produce cuando un control proporciona pruebas de que un usuario posee la identidad que afirma [34].

Autorización

Una vez que se autentica la identidad de un usuario, un proceso llamado autorización brinda la seguridad de que el usuario (ya sea una persona o una computadora) ha sido autorizado específica y explícitamente por la autoridad correspondiente para acceder, actualizar o eliminar el contenido de un activo de información [33].

Responsabilidad

La característica de rendición de cuentas existe cuando un control proporciona la seguridad de que todas las actividades realizadas se pueden atribuir a una persona nombrada o un proceso automatizado. Por ejemplo, los registros de auditoría que rastrean la actividad del usuario en un sistema de información brindan responsabilidad [33].

Análisis de Riesgos

El proceso de análisis de riesgos comprende la identificación de activos de información, sus 7 vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad

de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo [17].

Las organizaciones y las personas se han vuelto dependientes de la facilidad de acceso a los datos que brindan las tecnologías de la información y, al mismo tiempo, también se han vuelto más vulnerables a las violaciones de la seguridad de los sistemas de información. La gestión de riesgos es el proceso de descubrir el riesgo y determinar cómo se pueden controlar o mitigar esos riesgos. Las vulnerabilidades son debilidades explotables en el diseño, implementación y operación de los sistemas de protección de activos [32]. Una vez explotadas, las vulnerabilidades pueden provocar la interrupción de los servicios y el robo y destrucción de información y activos [32].

Mientras más redes informáticas se incorporen a las instituciones y mayor sea la facilidad de acceso a los datos a través de la tecnología, más sistemas de información serán vulnerables a las brechas de seguridad. Si bien es cierto que la posibilidad de interconexión a través de redes ha traído grandes mejoras en la productividad, lo cierto es que también ha traído más amenazas y riesgos [33].

La extensa lista de amenazas a la seguridad es grande y continúa creciendo y evolucionando. Entre los más conocidos se encuentran: la instalación de software malicioso, el acceso no autorizado al sistema de los datos, las interrupciones no deseadas, la denegación de servicio, el uso no autorizado de bases de datos y el cambio de hardware y firmware o software de los sistemas [35].

Vulnerabilidades

Las vulnerabilidades son debilidades en un sistema o su diseño que permiten a un intruso ejecutar comandos, acceder a datos no autorizados y/o realizar ataques de denegación de servicio. Las vulnerabilidades se pueden encontrar en una variedad de áreas. En particular, pueden ser debilidades en el hardware o software del sistema, debilidades en las políticas y procedimientos utilizados en los sistemas y debilidades de los propios usuarios del sistema [36]. Los errores de seguridad del software, también conocidos como vulnerabilidades, continúan siendo un problema importante y costoso. Ha habido un esfuerzo de investigación significativo para evitar que ocurran vulnerabilidades en primer lugar, así como para descubrir vulnerabilidades automáticamente, pero hasta ahora estos resultados siguen siendo

bastante limitados: la inteligencia humana a menudo se requiere para complementar las herramientas automatizadas y seguirá siendo necesaria en el futuro previsible [37].

Este incluye cualquier debilidad que pueda aprovecharse para causar pérdidas o daños al sistema. De esta manera, el punto de seguridad más débil del sistema está compuesto por el punto de seguridad más débil del sistema, que está compuesto por la mayor vulnerabilidad del sistema. Atacarla es cualquier medida para explotar la vulnerabilidad [38].

Una vulnerabilidad es una debilidad en un sistema de TI que un atacante puede explotar para lanzar un ataque exitoso. Pueden ocurrir a través de fallas, características o errores del usuario, y los atacantes buscarán explotar cualquiera de ellos, a menudo combinando uno o más, para lograr su objetivo final. Las vulnerabilidades son perseguidas y explotadas activamente por toda la gama de atacantes. En consecuencia, ha crecido un mercado de fallas de software, con vulnerabilidades de "día cero" (es decir, vulnerabilidades descubiertas recientemente que aún no se conocen públicamente) que alcanzan cientos de miles de dólares [39].

La evaluación de vulnerabilidades, también llamada análisis de vulnerabilidades, es un proceso que identifica, cuantifica y analiza las debilidades de seguridad en la infraestructura de TI. El objetivo principal es descubrir cualquier vulnerabilidad que pueda comprometer la seguridad y las operaciones generales de la organización. Como tal, puede ayudar a minimizar la probabilidad de amenazas.

Muchos profesionales de la seguridad usan los términos "evaluación de vulnerabilidad" y "prueba de penetración" indistintamente, aunque no significan lo mismo. Mientras el primero encuentra y mide la gravedad de las debilidades de un sistema, las pruebas de penetración son un ejercicio orientado a objetivos. En otras palabras, las pruebas de penetración se enfocan más en simular ataques de la vida real al trazar rutas que un atacante real puede tomar para violar las defensas de un sistema informático [40].

Sin auditoría, evaluación y supervisión de sus aplicaciones y sistemas, es posible vulnerabilidades de seguridad. Algunas áreas que necesitan políticas incluyen:

Parches y actualizaciones: esto es de vital importancia, demasiados ciberataques fácilmente evitables tienen éxito porque las organizaciones no parchean ni actualizan el software y las

aplicaciones. La política debe basarse en que la aplicación de parches y la actualización sean una parte obligatoria de las actividades de TI.

Software desactualizado, antiguo u obsoleto: los proveedores dejan de brindar soporte al software después de un período de tiempo específico. Una vez que desaparece el soporte, no se recibe parches, actualizaciones ni otro tipo de soporte. A veces, los ingenieros de TI pueden mantener este software sin el soporte oficial del proveedor. Sin embargo, con el tiempo, el software inevitablemente se ve plagado de fallas de seguridad. Se necesita una política para mantener el software actualizado y compatible.

Software no autorizado: lamentablemente, algunas organizaciones utilizan software no autorizado. Cuando no se paga por él y/o usa copias pirateadas, no obtiene parches ni actualizaciones aprobados por el proveedor. Esto deja expuesto a riesgos de seguridad.

Vulnerabilidades de código y base de datos: si el software o una aplicación está mal escrito, puede exponerse a vulnerabilidades de seguridad. La auditoría de su software y aplicaciones en busca de vulnerabilidades de seguridad a nivel de código ayudará a identificar los puntos donde los atacantes cibernéticos pueden atacar [41].

Hacking

Hacking Ético

Este ayuda a realizar pruebas de penetración para identificar vulnerabilidades y corregirlas [42]. Es un acto de intrusión/penetración en el sistema o las redes para descubrir amenazas, vulnerabilidades en esos sistemas que un atacante malicioso puede encontrar y explotar causando pérdida de datos, pérdidas financieras u otros daños importantes. El propósito es mejorar la seguridad de la red o los sistemas reparando las vulnerabilidades encontradas durante las pruebas [43].

El hacker ético es un profesional que tiene las habilidades para evaluar la seguridad de los sistemas informáticos de manera integral, poner en práctica una serie de pasos secuenciales y utilizar la "ética profesional" como criterio horizontal [38].

Políticas de seguridad informática

La política de seguridad es un documento que establece por escrito cómo una empresa planea proteger sus activos físicos y de tecnología de la información (TI). Las políticas de seguridad

son documentos vivos que se actualizan y cambian continuamente a medida que cambian las tecnologías, las vulnerabilidades y los requisitos de seguridad. La política de seguridad de una empresa puede incluir una política de uso aceptable. Estos describen cómo la empresa planea educar a sus empleados sobre la protección de los activos de la empresa. También incluyen una explicación de cómo se llevarán a cabo y se harán cumplir las medidas de seguridad, y un procedimiento para evaluar la efectividad de la política para garantizar que se realicen las correcciones necesarias [44].

Las políticas de seguridad de la información (PSI) son utilizadas por las organizaciones para comunicar reglas sobre el uso de los sistemas de información (SI). Los estudios de investigación muestran que el cumplimiento de los PSI no es un problema sencillo y que varios factores influyen en el comportamiento individual hacia el cumplimiento del PSI, como la conciencia de seguridad o la percepción individual de las amenazas de seguridad [43]. Las políticas de seguridad de la información están diseñadas para salvaguardar los recursos de la red de las infracciones de seguridad [45].

Las políticas de ciberseguridad también son fundamentales para la imagen pública y la credibilidad de una organización. Los clientes, socios, accionistas y posibles empleados quieren pruebas de que la organización puede proteger sus datos confidenciales. Sin una política de seguridad cibernética, es posible que una organización no pueda proporcionar dicha evidencia [46].

Las políticas de seguridad cibernética son importantes porque los ataques cibernéticos y las filtraciones de datos son potencialmente costosos. Al mismo tiempo, los empleados suelen ser los eslabones débiles de la seguridad de una organización. Los empleados comparten contraseñas, hacen clic en URL y archivos adjuntos maliciosos, usan aplicaciones en la nube no aprobadas y se olvidan de cifrar archivos confidenciales. Grand Theft Data, un informe de McAfee sobre exfiltración de datos, descubrió que las personas dentro de las organizaciones causaron el 43% de la pérdida de datos, la mitad de los cuales fue accidental. Las políticas de ciberseguridad mejoradas pueden ayudar a los empleados y consultores a comprender mejor cómo mantener la seguridad de los datos y las aplicaciones [47].

Las políticas de ciberseguridad también son fundamentales para la imagen pública y la credibilidad de una organización. Los clientes, socios, accionistas y posibles empleados

quieren pruebas de que la organización puede proteger sus datos confidenciales. Sin una política de seguridad cibernética, es posible que una organización no pueda proporcionar dicha evidencia.

Ciberseguridad

La ciberseguridad es un tema importante tanto para los departamentos de TI como para los ejecutivos de nivel C. Sin embargo, la seguridad debe ser una preocupación para todos los empleados de una organización, no solo para los profesionales de TI y los altos directivos. Una forma efectiva de educar a los empleados sobre la importancia de la seguridad es una política de seguridad cibernética que explique las responsabilidades de cada persona para proteger los sistemas y datos de TI [48]. Una política de ciberseguridad establece los estándares de comportamiento para actividades como el cifrado de archivos adjuntos de correo electrónico y restricciones en el uso de las redes sociales [49].

La red de información es una parte indispensable e importante de nuestras vidas, porque la mayoría de las entidades, ya sean financieras, educativas, medicas o de servicios, pasan por la red, por eso nació la ciberseguridad. El concepto de seguridad en la red se esfuerza por gestionar el proceso de obligaciones de protección a diferentes sistemas se promueven para prevean el uso no autorizado o no autorizado [50].

Tipos de ciberataques.

Malware: Tipo de ataque cibernético comúnmente llamado como software malicioso el cual incluye spyware, ransomware, virus y gusanos, se centra principalmente infringir redes mediante enlaces peligrosos o archivos adjuntos en los correos electrónicos, una vez dentro del sistema puede bloquear el exceso de componentes claves, obtener información furtivamente y alterar ciertos componentes del equipo [51].

Phishing: Método comúnmente utilizado por ciberatacantes, el cual consiste en el envío de mensajes fraudulentos usualmente a través de correos electrónicos que aparentemente proceden de fuentes confiables y seguras realizando suplantación de identidad; el objetivo principal es robar datos sensibles y personales como datos de tarjetas de crédito o contraseñas [52].

MitM: Comúnmente conocido como ataque de hombre en medio (Man in the Middle), es cuando un tercero consigue ingresar a la comunicación entre dos partes, sin que ninguna lo sepa, de esta forma acceder a la información e incluso manipularla [53].

Denegación de Servicio (DOS): Esto básicamente incluye cambiar servicios, dispositivos o aplicaciones para cancelar el acceso de usuarios legítimos. Los ciberdelincuentes que llevan a cabo estos ataques a menudo manipulan servidores con poco tráfico. Todo esto es para obligar al usuario víctima a pagar un rescate [54].

Inyección SQL: Esto sucede cuando un atacante utiliza el lenguaje de consulta del servidor (SQL) para insertar código malicioso en el servidor, lo que obliga al servidor a proporcionar información protegida. Este tipo de ataque suele implicar el envío de código malicioso a comentarios o cuadros de búsqueda en sitios web desprotegidos. Las prácticas de codificación seguras, como el uso de declaraciones preparadas con consultas parametrizadas, son formas efectivas de evitar la inyección de SQL [55].

Pruebas de Penetración

Las pruebas de penetración tienen varios marcos que se pueden usar, uno de los cuales es OWASP (Open Web Application Security Project) que se enfoca en la seguridad de las aplicaciones web [56]. Se define como un conjunto de técnicas y métodos utilizados para determinar el nivel de seguridad del sistema [42].

Las pruebas de penetración intentan aprovechar las debilidades o vulnerabilidades de los sistemas, las redes, los recursos humanos o los activos físicos para someter a prueba la eficacia de los controles de seguridad. Los diferentes tipos de pruebas de penetración incluyen servicios de red, aplicaciones, lado del cliente, inalámbrico, ingeniería social y física. Se puede realizar una prueba de penetración externa o internamente para simular diferentes vectores de ataque. Dependiendo de los objetivos de cada prueba, un probador de penetración puede o no tener conocimiento previo del entorno y los sistemas que intentan violar. Esto se clasifica como pruebas de penetración de caja negra, caja blanca y caja gris [57].

Clasificación de Pruebas de penetración

Caja negra: Se proporciona de antemano poca o ninguna información sobre los objetivos de la evaluación. Es más común en las pruebas de penetración de redes.

Caja de blanca: Suelen ser ejecutados por equipos internos, pero ahora es más común asignarlos a equipos externos. El equipo de pruebas suele ser parte del equipo de control de calidad y, por lo tanto, se convierte en parte del ciclo de vida del desarrollo de software. Puede acceder al código fuente para verlo e informar de las vulnerabilidades encontradas.

Caja gris: Este es el tipo de prueba más común. Se necesita más trabajo para obtener la información necesaria. La comunicación entre el equipo de prueba y la empresa evaluada es crucial [58].

OWASP

OWASP (Open web application security project) es un proyecto de seguridad en aplicaciones web de código abierto, se encarga de identificar y procesar las vulnerabilidades presentadas en los servidores web y evitar que usuarios malintencionados accedan a la información privada recopilada en el sistema de información web. La Fundación OWASP es una organización sin fines de lucro que apoya y administra los proyectos y la infraestructura de OWASP [59].

Los informes de estos proyectos incluyen un Manual de buenas prácticas de OWASP bien probado y autoevaluado para que las organizaciones lo utilicen como base para proteger los datos acoplados en el sistema de red. Los procedimientos de prueba para aplicaciones web se especifican en dos etapas: uso pasivo y activo de auditorías de caja negra [60].

OWASP es una organización sin fines de lucro que se enfoca en mejorar la seguridad del software. OWASP proporciona muchas herramientas, guías y metodologías de prueba para la seguridad cibernética bajo una licencia de código abierto, específicamente OWASP Testing Guide (OTG). El OTG se divide en tres partes principales, incluido el marco de prueba OWASP para el desarrollo de aplicaciones web, la metodología de prueba de aplicaciones web y los informes de evaluación del sistema. La metodología de prueba de aplicaciones web se puede usar de forma independiente o se puede usar como un marco de prueba. Un desarrollador de aplicaciones web puede usar el marco para crear aplicaciones web considerando los aspectos de protección y seguridad seguidos de pruebas de seguridad

con el método de prueba de penetración para probar la seguridad del sistema de la aplicación web desarrollada [61]. El marco de la guía de pruebas de OWASP tiene un fuerte enfoque en el nivel de seguridad de las aplicaciones web en todos los aspectos de los ciclos de vida de desarrollo de software que difieren de otros marcos de pruebas de seguridad de pruebas de penetración, como ISSAF y OSSTMM, que son ambos destinados a probar la seguridad. de la implementación. La Guía de prueba de OWASP está dirigida específicamente a un solo ámbito de dominio, que son las aplicaciones web [62]

Herramienta NESSUS

NESSUS es una herramienta de propósito general para calcular la respuesta probabilística o la confiabilidad e los sistemas de ingeniería, se puede usar para simular incertidumbres en carga, comportamiento y otras variables aleatorias definidas por el usuario para predecir la respuesta probabilística, la fiabilidad y las medidas de sensibilidad probabilística de los sistemas [63].

Nessus permite al usuario un análisis probabilístico con modelos analíticos, programas externos, como códigos comerciales de elementos finitos y combinaciones generales.

Herramienta Vega Scanner

Vega es un escáner de seguridad web gratuito y de código abierto y una plataforma de prueba de seguridad web para probar la seguridad de las aplicaciones web. Vega ayuda a encontrar y validar SQL Injection, Cross-Site Scripting (XSS), información confidencial divulgada inadvertidamente y otras vulnerabilidades. Está escrito en Java, basado en GUI y se ejecuta en Linux, OS X y Windows. Vega ayuda a encontrar vulnerabilidades tales como: secuencias de comandos entre sitios reflejadas, secuencias de comandos entre sitios almacenadas, inyección ciega de SQL, inclusión remota de archivos, inyección de shell y otras. Vega también investiga la configuración de seguridad de TLS/SSL e identifica oportunidades para mejorar la seguridad de sus servidores TLS. Vega incluye un escáner automatizado para pruebas rápidas y un proxy de interceptación para inspección táctica. El escáner Vega encuentra XSS (secuencias de comandos entre sitios), inyección de SQL y otras vulnerabilidades. Vega se puede ampliar mediante una potente API en el lenguaje de la web: Javascript [64].

OWASP ZAP

OWASP Zed Attack Proxy (ZAP) es una herramienta integrada dedicada a las pruebas de penetración que permite identificar vulnerabilidades en aplicaciones web y sitios web. Es una solución fácil y flexible que se puede usar independientemente del nivel de competencia: es adecuada para cualquier persona, desde un desarrollador que comienza con pentesting hasta profesionales en el campo. portada de owasp zap ZAP está compuesto por dos macro-secciones. El primero es un escáner de vulnerabilidades automatizado que puede identificar problemas y proporciona un informe para desarrolladores, administradores de sistemas y profesionales de la seguridad con todos los detalles de las vulnerabilidades descubiertas para solucionarlas. El segundo permite que ZAP funcione como un proxy e inspeccione el tráfico y todas las solicitudes y eventos HTTP/S; también existe la interesante capacidad de modificarlos para analizar comportamientos que se diferencien de la norma o analizar sus desencadenantes que pueden ser perjudiciales para el sistema. Dada su naturaleza riesgosa y al ser una herramienta muy poderosa, su uso debe limitarse a entornos en los que tenga el consentimiento para realizar la prueba y la seguridad de que no se pueden producir daños permanentes, ya que existe algún tipo de protección de la aplicación web [65].

1.3 Objetivos

1.3.1 General

Determinar el nivel de seguridad de información del sistema para generar citas y pagos de Facturación del concesionario AMBACAR mediante el análisis de vulnerabilidades.

1.3.2 Específicos

- Investigar sobre la tecnología y los procesos utilizados por AMBACAR para crear y administrar páginas web y sus repositorios.
- Determinar la metodología para el análisis de seguridad.
- Determinar las herramientas open source para el análisis de vulnerabilidades de acuerdo con la metodología seleccionada.
- Proponer soluciones para mejorar la seguridad del sistema para generar citas y pagos de Facturación de acuerdo con las vulnerabilidades y problemas de seguridad encontrados.

2 CÁPITULO II METODOLOGÍA

2.1 Materiales

En el presente trabajo investigativo se utilizó fuentes confiables de información, tales como repositorios académicos, revistas científicas, sitios web, trabajos de titulación en el área de informática. Además, en el siguiente tabal se detalló los elementos físicos, como los de software que fueron necesarios para la realización de este proyecto.

Tabla 1. Materiales

Fuente: Elaboración Propia

Material	**Figura**	**Descripción**
Laptop		Se utiliza para la instalación y aplicación de los diferentes softwares.
Zenmap		Software utilizado para análisis de vulnerabilidades del sitio web.
VEGA		Software utilizado para análisis de vulnerabilidades del sitio web.

OWAS ZAP		Software utilizado para análisis de vulnerabilidades del sitio web.
Microsoft Word		Software utilizado para la redacción del proyecto y almacenamiento de la entrevista realizada.
Microsoft Excel		Software utilizado para la realización de análisis de riesgos.

Tabla 2. Entrevista

Fuente: Elaboración Propia

Nº	**Preguntas**
1	¿Qué tipo de servidor utilizaron para crear el sistema para generar citas, pagos de Facturación y logística?
2	¿Cuál fue el lenguaje utilizado para el desarrollo del sistema para generar citas, pagos de Facturación y logística?
3	¿Qué tipo de base de datos utilizaron para crear el sistema para generar citas, pagos de Facturación y logística?
4	¿Cuál fue la arquitectura seleccionada para el desarrollo de dichos sistemas?
5	¿El sistema para generar citas, pagos de Facturación y logística se encuentra dividido en módulos, si es correcto cuántos y cuáles son?
6	¿Qué cantidad de usuarios se conectan en el sistema y cuántos son simultáneamente?

7	¿Existe un registro de errores del sistema de almacenamiento y en qué consiste?
8	¿El sistema contiene un certificado de seguridad?
9	¿Qué tipo de cifrado utiliza el sistema para proteger información vulnerable, como contraseñas?
10	¿Se elimino alguno de los sistemas?

2.2 Métodos

2.2.1 Modalidad de Investigación

Para recopilar, procesar y analizar la información para el presente proyecto se trabajaro en colaboración con el personal de TI (Tecnologías de la Información) de AMBACAR, el cual, entienden bien el funcionamiento del sistema y tienen la información suficiente para satisfacer las necesidades de seguridad de la información del negocio. Además, para obtener información precisa y completa, será de interés la información de revistas científicas, libros, documentos e Internet relacionados con el tema.

2.2.1.1 Modalidad de campo

La investigación fue de campo debido a que se requerido de la ayuda de los encargados en la administración del Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR para la recolección de información. La técnica utilizada fue una entrevista.

2.2.1.2 Modalidad bibliográfica

La investigación fue de tipo bibliográfica porque será de gran ayuda la indagación en libros, documentos técnicos, artículos y tesis del área informática para la elaboración y sustentación del marco teórico, posterior a ello será de fundamento en la realización de las políticas de seguridad.

2.2.1.3 Modalidad aplicada

La investigación fue de tipo aplicada, ya que con los conocimientos adquiridos durante los previos semestres aprobados se llevó a cabo la planificación, análisis y realización de nuevas

políticas de seguridad con respecto al Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR.

2.2.2 Población y Muestra

2.2.2.1 Población

Por la naturaleza del proyecto de investigación, se presentó a una población de empleados de AMBACAR - Corporación Ambato, donde trabajó en el proyecto de investigación.

2.2.2.2 Muestra

La muestra para el estudio en sí se obtendrá directamente de los empleados del departamento de TI, específicamente del desarrollador del Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR.

2.2.3 Recolección de Información

La información fue recolectada a través de una entrevista aplicada a la persona encargada del Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR, para lo cual se hará el uso de un cuestionario con preguntas cerradas con la finalidad de alcanzar los objetivos planteados en el trabajo de investigación.

Tabla 3: Recolección de Información

Fuente: Elaboración Propia

Preguntas básicas	**Explicación**
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Encargado del Sistema de citas y facturación del concesionario AMBACAR
¿Sobre qué aspectos?	Sistema de citas y facturación del concesionario AMBACAR
¿Quién, Quiénes?	Investigador
¿Cuándo?	En el periodo académico abril - septiembre 2021

¿Dónde?	AMBACAR
¿Cuántas veces?	1
¿Qué técnicas de recolección?	Entrevista
¿Con qué?	Cuestionario

2.2.4 Procesamiento y Análisis de Datos

Para la recolección de información se empleó una entrevista aplicada al personal encargado del Sistema de citas y facturación del concesionario AMBACAR correspondiendo a un total de 1 persona, donde se obtuvieron los siguientes resultados que se exponen posteriormente.

2.2.5 Desarrollo del Proyecto

Con el fin de cumplir los objetivos de la investigación se prevé la realización de las siguientes actividades:

1. Definir antecedentes
2. Describir las herramientas del Sistema para Generar citas y Pagos de Facturación del concesionario AMBACAR
3. Consensuar las vulnerabilidades con sus posibles soluciones, esto referente a cada herramienta de análisis previamente seleccionada.
4. Construir un plan de contingencia para prevenir ataques de seguridad informática.

3 CÁPITULO III RESULTADOS Y DISCUSIÓN

3.1 Análisis e Interpretación de Resultados

La entrevista aplicada al personal encargado del Sistema de citas y facturación del concesionario AMBACAR consta de un total de 10 preguntas de carácter abierta en su mayoría, todo esto con el fin de conocer la estructura, diseño, implantación del sistema dentro de la empresa.

3.1.1 Resultados de entrevista aplicada

Para el desarrollo de la investigación se inició con una entrevista en el departamento de Sistemas al Ing. Oscar Muñoz analista de sistemas encargado del Sistema de citas y facturación, esta entrevista fue con el fin de recolectar datos para tener en claro un punto de partida para la investigación.

Mediante esta entrevista se recolectó los datos pertinentes en cuanto a la creación y desarrollo del sistema, comprobando que la empresa creo un plan de gestión de riesgos de seguridad para el manejo y uso de la información, sin embargo, no se estaba cumpliendo a cabalidad.

Tabla de preguntas de la Entrevista

Tabla 4. Resultado de la entrevista

Fuente: Elaboración Propia

Preguntas	**Respuesta**
¿Qué tipo de servidor utilizaron para crear el sistema para generar citas, pagos de Facturación y logística?	Windows Server
¿Cuál fue el lenguaje utilizado para el desarrollo del sistema para generar citas, pagos de Facturación y logística?	Asp.net C# Javascript

¿Qué tipo de base de datos utilizaron para crear el sistema para generar citas, pagos de Facturación y logística?	MySQL
¿Cuál fue la arquitectura seleccionada para el desarrollo de dichos sistemas?	Programación en capas
¿El sistema para generar citas, pagos de Facturación y logística se encuentra dividido en módulos, si es correcto cuántos y cuáles son?	Si está dividido en módulos y son dos citas y pagos de facturación.
¿Qué cantidad de usuarios se conectan en el sistema y cuántos son simultáneamente?	Aproximadamente 2000 y 20 simultáneamente.
¿Existe un registro de errores del sistema de almacenamiento y en qué consiste?	Existe una bitácora con excepciones en Logística, los demás desarrollos no tienen esto.
¿El sistema contiene un certificado de seguridad?	Si
¿Qué tipo de cifrado utiliza el sistema para proteger información vulnerable, como contraseñas?	Encoding Unicode GetBytes
¿La empresa cuenta actualmente con una política de privacidad en cuanto al manejo de la información?	Si cuenta con políticas de seguridad de la información basados en la ISO 27001.
¿Los sistemas de TI administrados por la empresa monitorean continuamente los controles relevantes?	Si se monitorea de manera frecuentemente una vez al mes.

¿La empresa tiene un inventario de sus recursos de TI existentes y utilizados?	La entidad posee un inventario de sus recursos de Ti existentes y en uso.
¿Cuál es el proceso para creación de un sistema?	Primero realizamos un análisis organizativo, funcional y de control actual. Identificamos recursos y requisitos. Análisis de riesgos y criticidad. Cualificación de diseño, instalación, operación y proceso. Procedimientos normalizados de trabajo. Plan de seguimiento de validación.
¿Cuál es el proceso para creación de un repositorio?	Primero la compilación del proyecto creado. Preparar el servidor Windows de la nube. Subir la compilación al servidor. Asignar un subdominio de Ambacar. Publicar el proyecto.

3.1.2 Análisis e interpretación de resultados de la entrevista aplicada

La entrevista realizada al encargado del uso y manejo de la gestión de la información Ing. Oscar Muñoz afirma lo siguiente:

Fue posible identificar y conocer la tecnología con la que se desarrolló el sistema, a su vez se pudo identificar aspectos importantes que serán de gran ayuda en el análisis de vulnerabilidades del sitio web.

Entre los diferentes aspectos que se pudo identificar son: el servidor del sistema, base de datos, lenguajes de programación, arquitectura, modularidad, registro de errores, capacidad de usuarios, certificado de seguridad y cifrado utilizado en la protección de información

vulnerable, todo a favor de ser soporte en la generación de soluciones con respectos a las vulnerabilidades que posee el sistema.

3.2 Desarrollo de la Propuesta

3.2.1 Antecedentes de la propuesta

Los allanamientos de Internet y la posterior globalización han dado paso al acceso a la información, y se ha intentado frenar las barreras de espacio o tiempo previamente impuestas para el acceso a la información. Hay que añadir un nuevo elemento al proceso de globalización de los mercados, el concepto de liquidez, que significa la posibilidad o necesidad de obtener información en cualquier momento.

Establecer la seguridad de la información no es solo una cuestión técnica, sino también el personal, los procesos y las funciones de la naturaleza de los datos, así como la protección de todos los recursos lógicos y físicos de la organización.

Las aplicaciones web, deben cumplir con ciertos estándares de seguridad que permitan garantizar su adecuado funcionamiento, de manera que esté disponible cuando sea necesario, que existan garantías de que los datos de carácter sensible sean procesados correctamente y que solo puedan acceder a ellos las personas autorizadas.

Los usuarios de la aplicación web de facturación y reserva de concesionarios de AMBACAR expuesta son los principales interesados. Además de ellos, los desarrolladores, como aquellos que brindan soporte para sistemas web, están más preocupados por si la aplicación web tiene un nivel de seguridad suficiente y óptimo.

Con base en la situación anterior, se recomienda elaborar un informe que registre los resultados obtenidos anteriormente, señalando las posibles soluciones adecuadas para cada vulnerabilidad informática detectada en la aplicación para generar citas y pago de facturas para los concesionarios AMBACAR, para esta función se ha determinó que en la aplicación Web también se ha analizado la seguridad de su información a través de ataques informáticos. Finalmente, se presentará un documento final con una lista de posibles soluciones y sugerencias para mejorar la seguridad de la información del sistema Web.

3.2.2 Fundamentación teórica del Sistema Operativo y de las herramientas que usa su servidor.

Tabla 5.Descripción del sistema operativo

Fuente: Elaboración Propia

Sistema Operativo	**Versión empresarial**	**Versión ambiente de prueba**
Windows Server: Es un sistemas operativo diseñado por Microsoft que admite administración, almacenamiento de datos, aplicaciones y comunicaciones a nivel empresarial compatibilidad con la nube con funciones como direcciones IP mejoradas, Hyper-V actualizado y un nuevo sistema de archivos (ReFS) [66].	2012 R2	2012 R2

Tabla 6.Herramientas de almacenamiento y funcionamiento del aplicativo web.

Fuente: Elaboración Propia

Herramientas	**Versión Empresarial**	**Versión ambiente de prueba**
MySQL: Es un sistema de administración de bases de datos (SGBD, abreviado como DBMS en inglés), el cual es ampliamente conocido y ampliamente utilizado por su sencillez y excelente desempeño. Aunque le falta algo. Las funciones avanzadas que ofrecen otros DBMS del mercado, precisamente porque es fácil de usar y acorta el tiempo de inicio, es una opción atractiva para aplicaciones empresariales y de entretenimiento [67].	8.0	8.0

ASP.NET es una plataforma para el desarrollo de aplicaciones web compuesta por lenguajes, bibliotecas y herramientas, comercializado por Microsoft que permite a los desarrolladores crear sitios dinámicos usando un lenguaje de programación completo como C#, VB.NET, F# y Visual Basic [68].	6.0	6.0

3.2.3 Diagramas de proceso de creación y administración de páginas web y sus repositos.

Figura 1. Proceso de creación de sistemas de AMBACAR

Fuente: Elaboración Propia

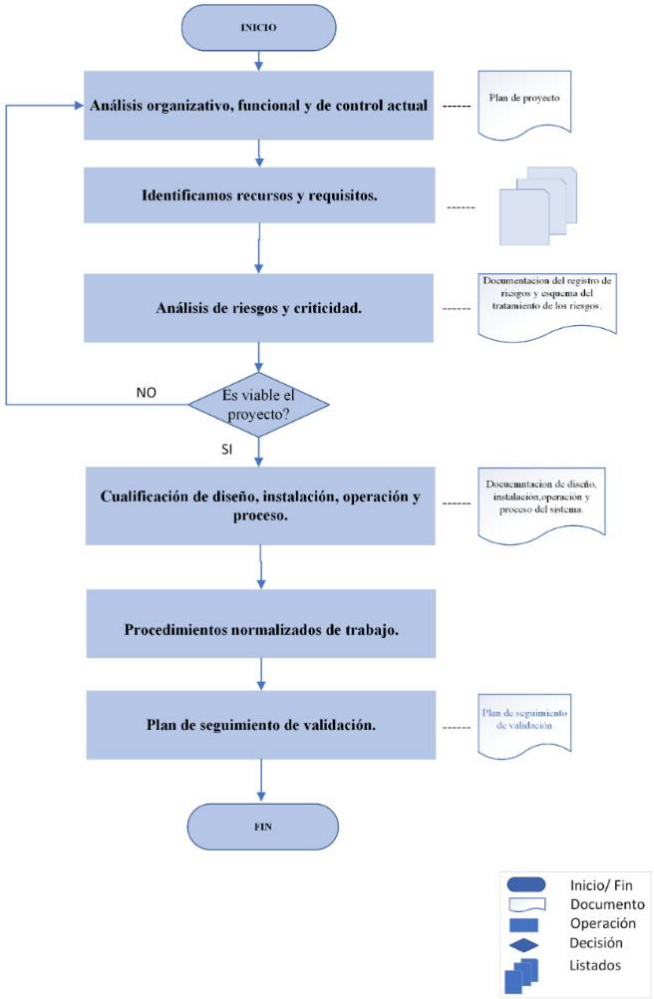
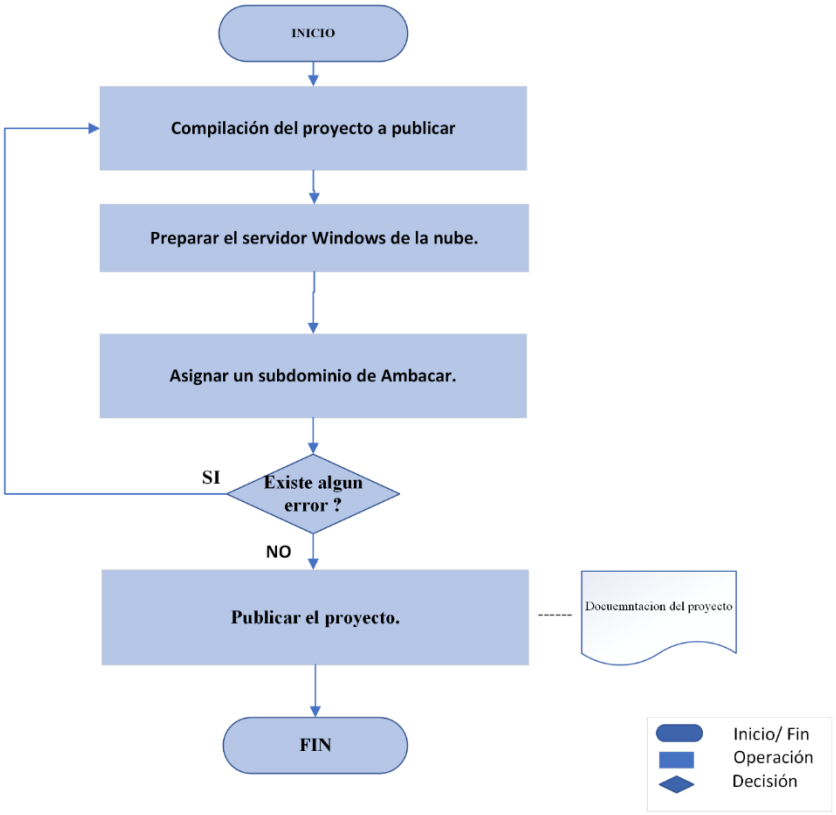


Figura 2.Proceso de creación de repositorios

Fuente: Elaboración Propia



3.2.4 Análisis Comparativo de Metodologías.

3.2.4.1 ISSAF

El ISSAF (Information Systems Security Assessment Framework) o el Marco de evaluación de la seguridad de los sistemas de información fue desarrollado por OISSG (Open Information Systems Security Group); es uno de los marcos más interesantes en el campo de los métodos de prueba. Realiza un análisis detallado de todos los aspectos que pueden afectar a las pruebas de seguridad [69].

La información de la ISSAF está organizada en torno a los llamados "criterios de evaluación", cada uno de los cuales está escrito y verificado por expertos en cada área de aplicación. El proceso de pruebas de penetración se divide en tres fases:

Fase I. Planificación y Preparación: Incluye comunicación inicial, planificación y preparación para las pruebas de seguridad.

Fase II. Evaluación: Pruebas de Seguridad de Penetración de la ISSAF.

Fase III. Informes, limpieza y destrucción de artefactos: los controles de seguridad eliminan toda la información creada y almacenada en el sistema.

Desde el punto de vista de las aplicaciones web, ciertamente proporciona pruebas y herramientas de seguridad efectivas, pero no permiten evaluar todos los aspectos requeridos actualmente.

3.2.4.2 NIST SP 800-115

Guía técnica para pruebas y evaluación de seguridad de la información NIST SP 800-115 (Technical guide for information security testing and evaluation) fue publicada por NIST en septiembre de 2008 [70].

Describe las pautas sobre cómo realizar una evaluación de seguridad de la información (ESI) y la conceptualiza como el proceso de determinar la eficacia de la evaluación de una entidad en relación con objetivos de seguridad específicos. Implica realizar pruebas de penetración y recomienda los siguientes pasos:

Fase de planificación: Definir las reglas a seguir durante las pruebas de penetración y crear las condiciones técnicas y organizativas necesarias.

Fase de descubrimiento: escanea y recopila información sobre la infraestructura informática de la entidad y detecta debilidades.

Fase de ejecución: comprueba las vulnerabilidades descubiertas previamente.

Fase de Documentación y Reporte: Genera un reporte sobre los problemas de seguridad detectados.

NIST SP 800-115 considera que la evaluación de seguridad a nivel de aplicación es un tema complejo y, por lo tanto, no se trata en esta metodología. Esto lo hace inadecuado para la autoevaluación de aplicaciones web.

3.2.4.3 OSSTMM

OSSTMM (Open-Source Security Testing Methodology Manual) 3ª edición fue publicada por ISECOM (Institute for Security and Open Methods) en 2010; esta metodología se ha convertido en un estándar de facto, sin duda, el primer acercamiento a la estructura global

del concepto de seguridad. Si bien las pruebas en él y las pruebas realizadas no son especialmente innovadoras, se han convertido en un verdadero referente para las organizaciones que buscan desarrollar pruebas de alta calidad, estructuradas y eficientes [71]. Incluye cuatro etapas:

Fase introductoria: Definir el alcance, los requisitos y las limitaciones de la auditoría.

Fase de interacción: se trata de explorar la relación entre el alcance, los objetivos y los recursos relacionados.

Fase de requerimientos: Validación de procesos, configuración, capacitación, propiedad intelectual, información pública, etc.

Fase de intervención: Se enfoca en penetrar en el target y su impacto.

En el caso de una aplicación web, no contiene etapas, canales o módulos específicos para ser evaluados.

3.2.4.4 OWASP

Lanzada en 2014, la cuarta edición de OWASP Testing Guide está muy enfocada a probar aplicaciones web y se está convirtiendo en uno de los proyectos de referencia en la materia. OWASP se ha convertido en el estándar común para cualquier desarrollador de seguridad [72]. Se divide en grupos de pruebas de seguridad para probar aspectos específicos de una aplicación web:

- Recopilación de Información.
- Pruebas de seguridad a la configuración y despliegue.
- Pruebas de seguridad a la gestión de la identidad.
- Pruebas de seguridad al proceso de autenticación.
- Pruebas de seguridad al proceso de autorización.
- Pruebas de seguridad al proceso de gestión de sesiones.
- Pruebas de seguridad a la validación de entradas.
- Pruebas de seguridad al manejo de errores.
- Pruebas de seguridad a los mecanismos criptográficos.
- Prueba de seguridad a la lógica de negocios.

- Pruebas de seguridad del lado del cliente.

Dado que los principios de prueba de OWASP son un enfoque específico del dominio, la fase de informes podría desarrollarse mejor. Duplica las pruebas de seguridad en varias etapas y, a menudo, descubre fuertes dependencias entre las fases de una prueba de seguridad sin abordar cómo se gestionan estas relaciones recíprocas para evitar la duplicación. Los esfuerzos conducen al mismo resultado.

3.2.4.5 Determinación de metodología a través de matriz

Tabla 7. Comparativa de metodologías

Fuente: Elaboración Propia

AMBACAR				
Metodología	**Definición**	**Ventajas**	**Desventajas**	**Pruebas de Penetración**
ISSAF	Marco de evaluación de la seguridad de los sistemas de la información, el cual, realiza un análisis detallado de todos los aspectos que pueden afectar a las pruebas de seguridad	Fase de evaluación conocidas. Largo recorrido en el campo de la auditoría. Facilita el informe en función de los pasos seguidos y resultados obtenidos.	Desactualizada desde 2006. No establece claramente los límites de las pruebas de penetración.	Fases de pruebas de penetración: Fase I: Planificación y reparación. Fase II: Evaluación. Fase III: Informes, limpieza y destrucción de artefactos.

NIST SP 800-115	Guía técnica para pruebas y evaluación de seguridad de la información, donde describe las pautas de como realizar una evaluación de seguridad de la información.	Soportada y mantenida por el gobierno de EEUU la hace una guía de confianza.	Difícil de comprender al auditor sin experiencia. Es poco usual conocer todas las recomendaciones y pruebas.	Fases de pruebas de penetración: Fase I: Planificación. Fase II: Descubrimiento. Fase III: Documentación y reporte.
OSSTMM	Metodología especializada en auditoria, con un alto nivel de exigencia en sus procesos y controles.	Comunidad Grande. Altamente documentada. Tiene un enfoque a base de estándares ISO de seguridad Informática.	El objetivo no es claro para el cumplimiento de cada prueba. El cambio de versiones es amplio. No recomienda ninguna herramienta.	Fases de pruebas de penetración: Fase I: Introductoria. Fase II: Interacción. Fase III: Requerimientos. Fase IV: Intervención.
OWASP	Metodología especializada en auditoria	Establece un TOP 10 de vulnerabilidades.	Presta solo para aplicativos webs.	Pruebas de seguridad a la

	web, con un alto nivel de exigencia en sus procesos y controles.	Ofrece pruebas necesarias para comprobar si un sitio web es vulnerable,		configuración y despliegue. Pruebas de seguridad a la gestión de la identidad. Pruebas de seguridad al proceso de autenticación. Pruebas de seguridad al proceso de autorización. Pruebas de seguridad al proceso de gestión de sesiones. Pruebas de seguridad a la validación de entradas.
ANALISIS	La guía de exámenes OWASP es la más completa, seguida del método ISSAF, OWASP se puede desarrollar un método de evaluación de red especializado, lo cual es muy deseable ya que todos sus procesos y controles pueden determinar con mucha precisión el grado de seguridad de la plataforma tal y como se utiliza globalmente. Una comparación con las vulnerabilidades más comunes en las aplicaciones web muestra la			

	necesidad de realizar pruebas de seguridad para evaluar la función de descifrado inseguro, así como el registro de la aplicación y el monitoreo del sitio web.

3.2.5 Determinación de herramientas a través de matriz

Los escáneres de vulnerabilidades de aplicaciones web son herramientas automatizadas que analizan aplicaciones web, normalmente desde el exterior, para buscar vulnerabilidades de seguridad como secuencias de comandos entre sitios, inyección SQL, inyección de comandos, ruta transversal y configuración de servidor insegura.

Dentro de Testing Guide 4.0 - OWASP Foundation menciona varias herramientas que se puede usar en cada una de las diferentes pruebas de seguridad, en las cuales consta software open source, comercial y gratis [72].

Tabla 8. Comparativa de herramientas [73].

Fuente: Elaboración Propia

AMBACAR				
Herramienta	**Definición**	**Ventajas**	**Desventajas**	**Características**
PortSwigger Burp Suite	Es una aplicación basada en la web que le permite utilizar la lógica de escaneo web de vanguardia de Burp Scanner para descubrir	Escaneo de cualquier número de aplicaciones y actualiza su base de datos. PortSwigger Burp Suite no obstaculiza el	La herramienta devuelve demasiados falsos positivos. Escases de documentación. Inconvenientes con su rendimiento y	Seguridad General. Herramientas de monitoreo. Licencia tipo Opens Source,

	docenas de diferentes tipos de vulnerabilidad [74].	nodo del servidor y no paga el servidor. La solucion tiene una configuración bastante simple,	generación de informes. Con el uso se ralentiza la herramienta.	
OWASP ZAP	Es una herramienta gratuita de prueba de penetración de código abierto que se mantiene bajo el paraguas del Proyecto de seguridad de aplicaciones web abiertas. OWASP ZAP está diseñado específicament e para probar aplicaciones web y es flexible y extensible [75].	Solucion escalable. Informa sobre la s vulnerabilidades de la aplicación. Interfaz fácil de usar. Ofrecen acceso gratuito a algunas otras herramientas. El escaneo automático es una característica valiosa y muy fácil de usar.	Requiere de muchos recursos. La implementación es compleja.	Seguridad General. Seguridad de aplicaciones web. Herramientas de monitoreo. Escáner de vulnerabilidades . Licencia tipo Open Source.
Vega	Subgrafo Vega | Escáner de	Rastreador de sitios web.	No realiza escaneo de	Seguridad General.

	seguridad y vulnerabilidad de aplicaciones web gratuito y de código abierto [76].	Observa e interactúa con la comunicación entre clientes y servidores. Multiplataforma.	puertos tan en profundidad. Vulnerabilidades en host pueden pasar desapercibidas por la herramienta en algunos casos.	Seguridad en aplicaciones web. Herramientas de monitoreo. Licencia tipo Open Source.
Nessus	Nessus Professional es una plataforma de seguridad diseñada para empresas que desean proteger su seguridad, la de sus clientes y la de sus clientes [77].	Fácil de instalar. Interfaz limpia, es agradable a la vista. Soporte por una única empresa.	Dependiendo de la versión tiene limitaciones. Problemas de plugin al usar en el navegador.	Seguridad General. Seguridad en aplicaciones web. Herramientas de monitoreo. Licencia tipo Open Source
Análisis	En este caso se ha seleccionado tres softwares open source según la necesidad Nessus para el análisis del servido y para el sistema web de citas y pagos de Facturación Vega, OWAS ZAP, debido a las características que brinda cada una de las herramientas se ha descartado PortSwigger Burp Suite por sus deficientes características y no estar tan apta para análisis de vulnerabilidades en sitios web.			

3.2.6 Documentación de los resultados obtenidos

3.2.6.1 Herramienta Zenmap

1. Utilización de la herramienta

1.1. Abrir el aplicativo e identificar las secciones que conforman la herramienta de análisis

1.1.1. El objetivo

1.1.2. El tipo de perfil a utilizar

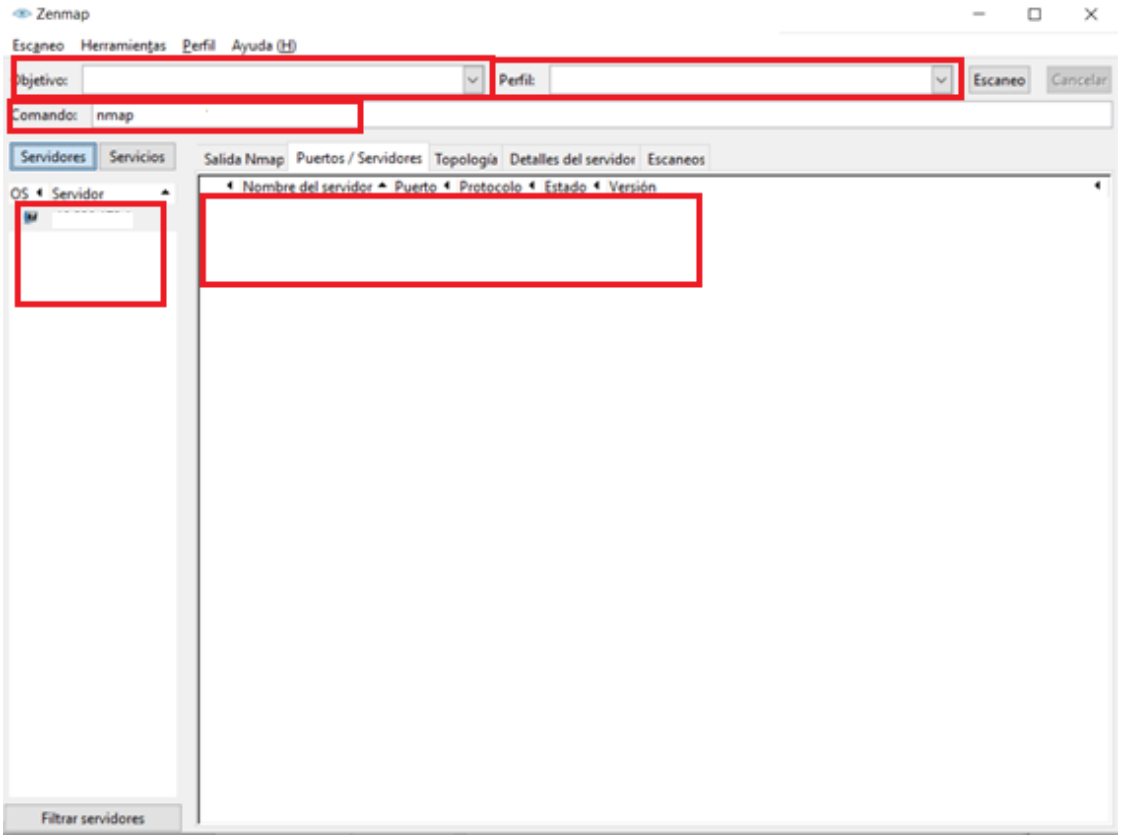
1.1.3. Comandos

1.1.4. Servidores que están en red

1.1.5. Área de salida

Figura 3. Interfaz de inicio de Zenmap

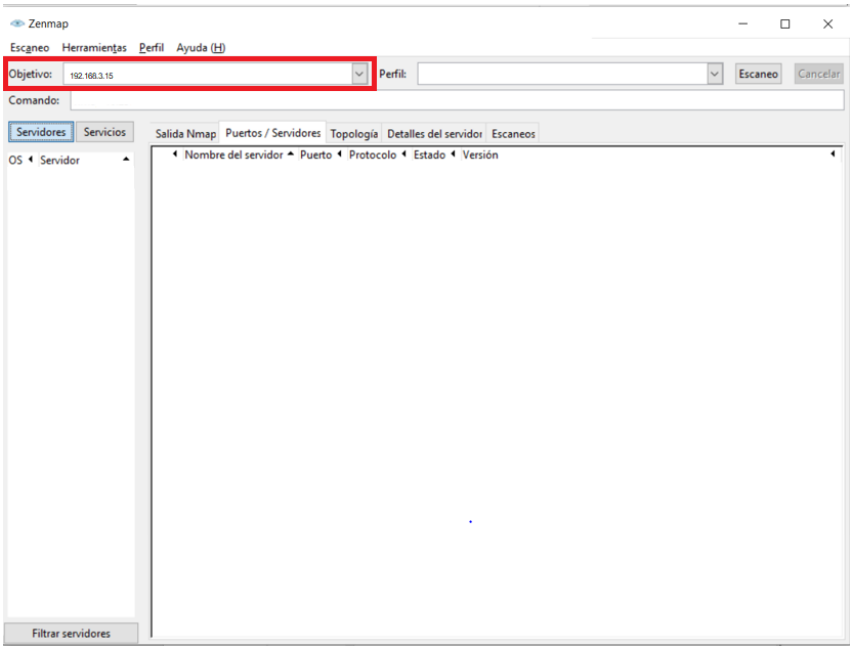
Fuente: Elaboración Propia



2. Colocar la IP de destino o rango de IP.

Figura 4. Interfaz de Zenmap, donde se está ingresando la dirección Ip

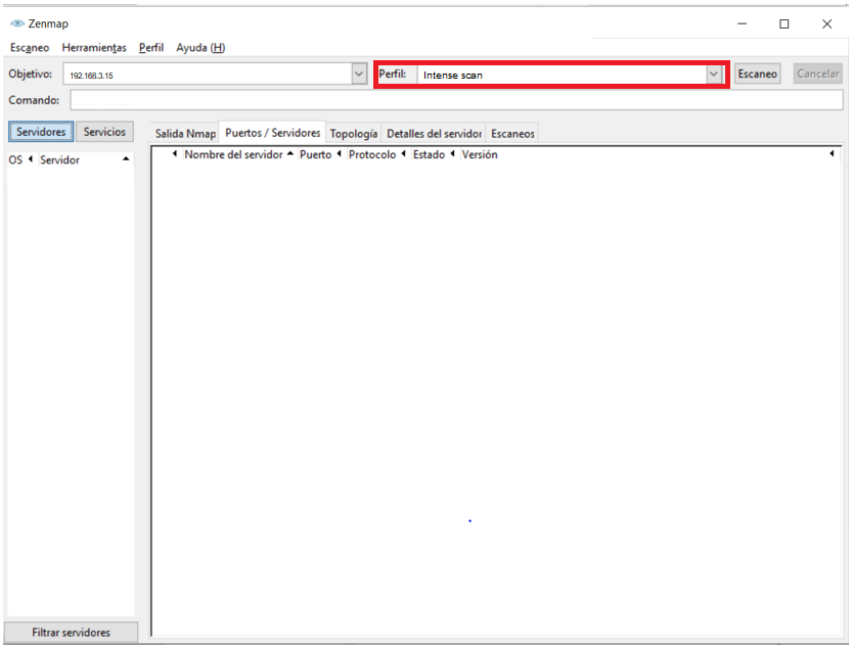
Fuente: Elaboración Propia



3. Seleccionamos una opción del menú desplegable de la sección de perfil.

Figura 5.Interfaz de Zenmap, Seleccionando el tipo de perfil

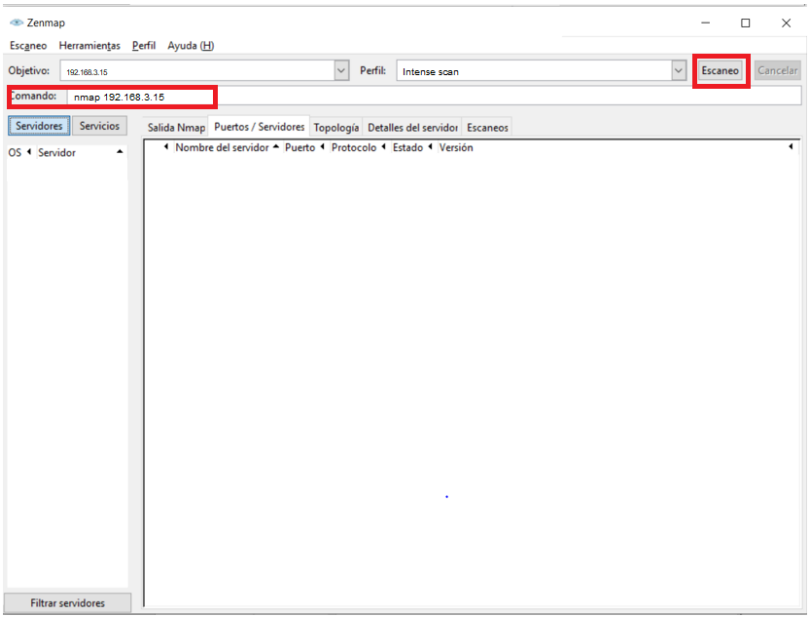
Fuente: Elaboración Propia



4. Colocar el comando NMAP para encontrar detalles adicionales para el escaneo.
5. Activar el proceso de escaneo para la dirección IP o link.

Figura 6.Interfaz de Zenmap, ingresando el comando y selección de Escaneo.

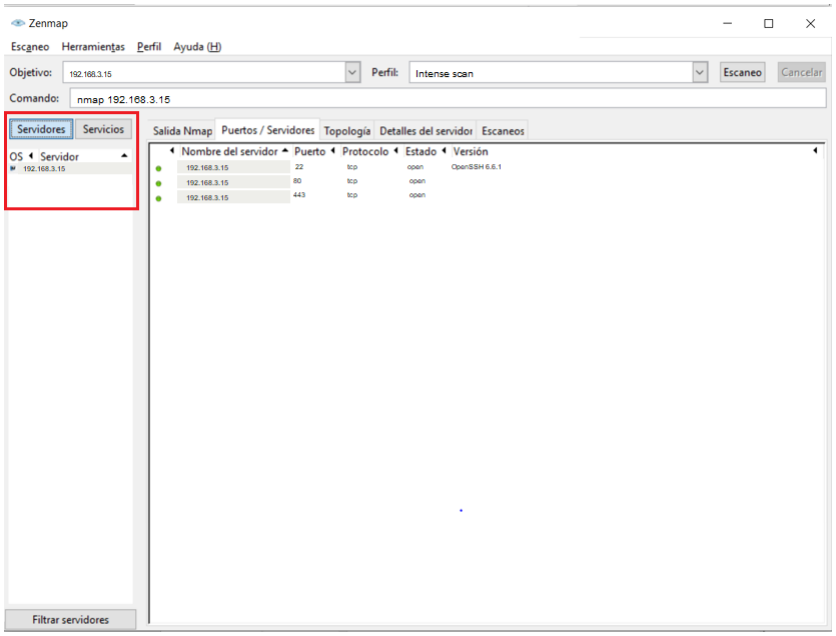
Fuente: Elaboración Propia



6. Terminado el escaneo podemos observar en la parte media izquierda los host y servidores.

Figura 7.Interfaz de Zenmap, donde se puede observar los servidores

Fuente: Elaboración Propia



7. En el área de salida podemos seleccionar entre Salida Nmap, Puertos/Servidores, Topología, Detalles del servidor, Escaneos.

Figura 8.Interfaz de Zenmap, donde se puede observar las Salidas

Fuente: Elaboración Propia

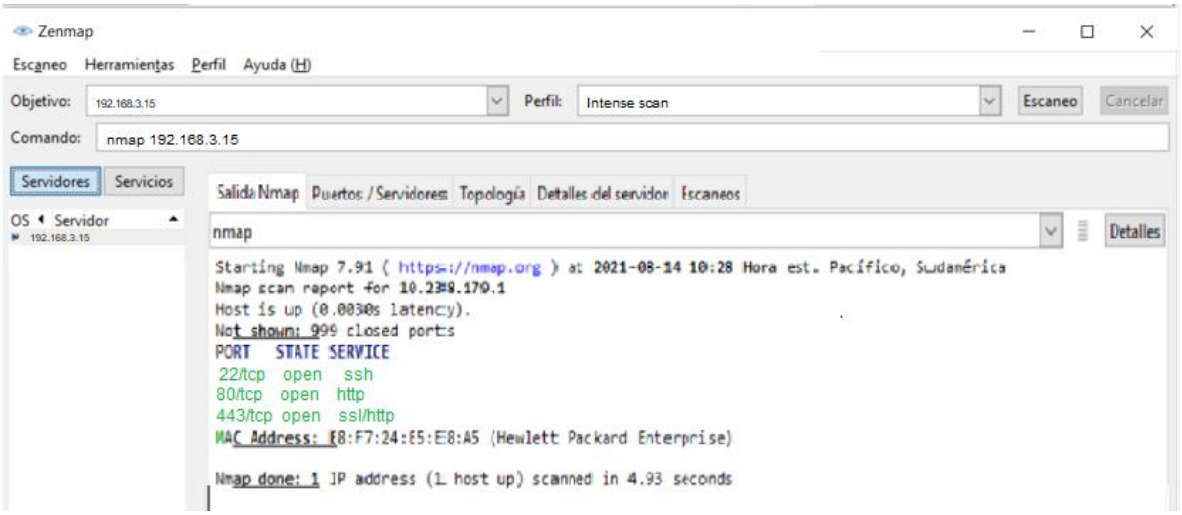
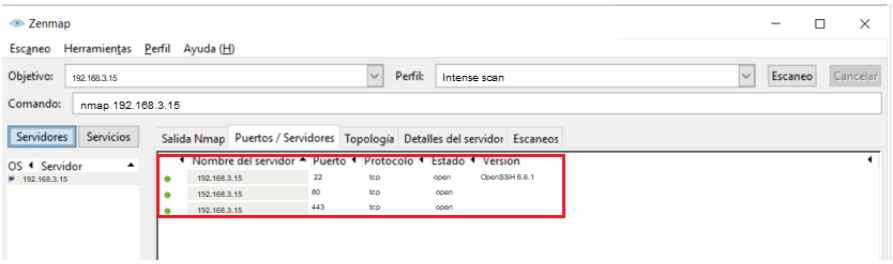


Figura 9.Interfaz de Zenmap, donde se puede observar las Puertos/ Servicios

Fuente: Elaboración Propia



3.2.6.2 Herramienta Vega Scanner

1. Utilización de la herramienta

1.1 Abrir el aplicativo e identificar las secciones que conforman la herramienta de análisis

A) Vista del sitio web

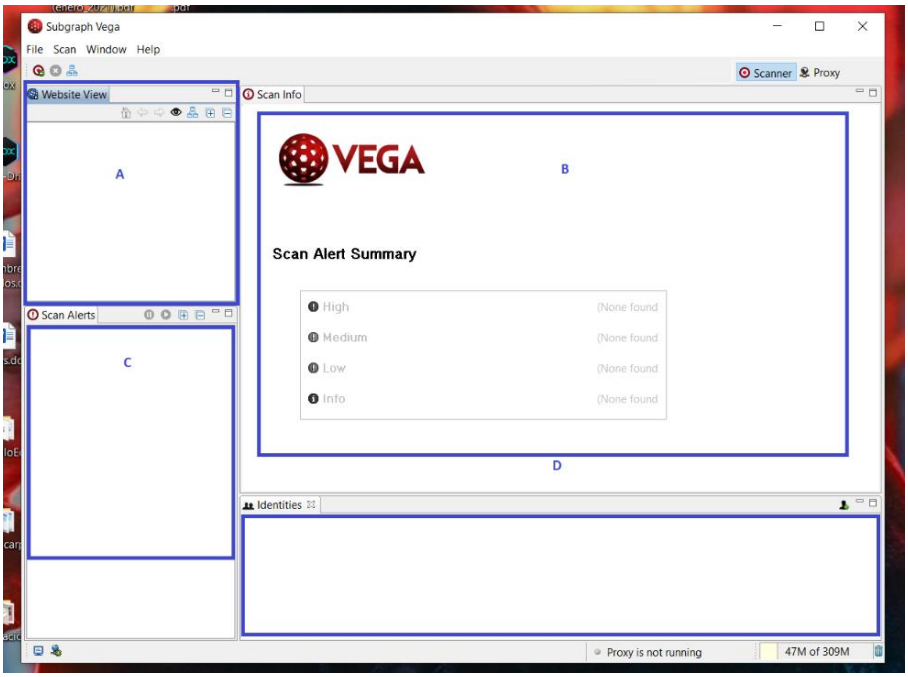
B) Información de escaneo

C) Alertas de escaneo

D) Identidades

Figura 10.Interfaz de inicio de Vega Scan

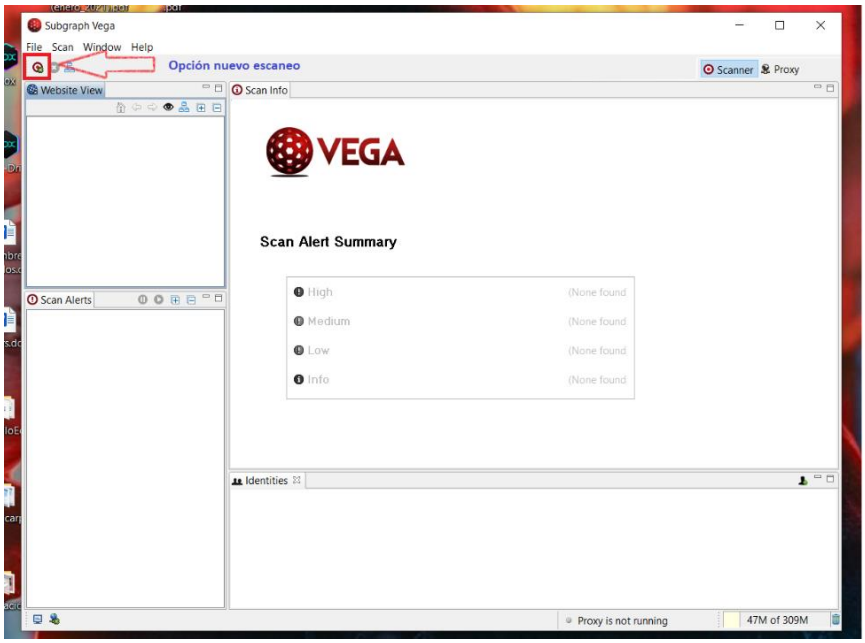
Fuente: Elaboración Propia



1.4 Presionar la opción empezar nuevo escaneo

Figura 11. Interfaz de Vega, seleccionar nuevo escaneo

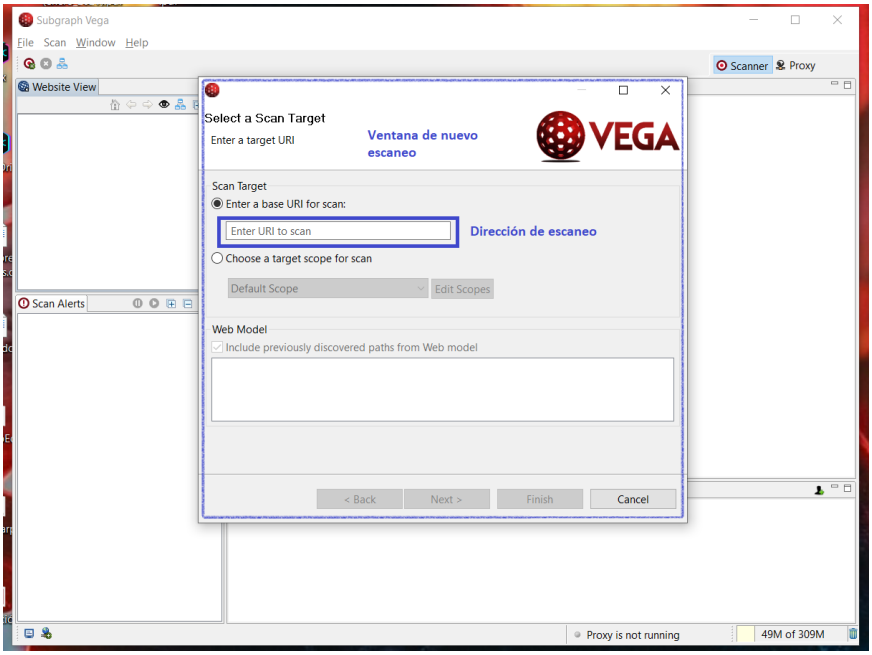
Fuente: Elaboración Propia



1.5 Identificar ventana de nuevo escaneo con sus respectivos elementos

Figura 12.Interfax de Vega de nuevo escaneo

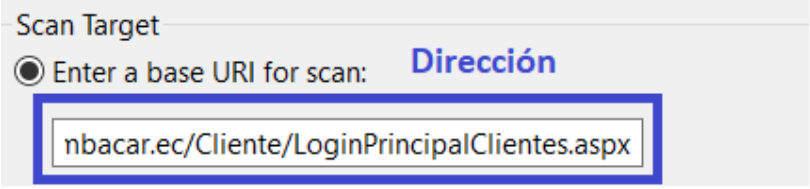
Fuente: Elaboración Propia



1.6 Ingresar dirección de análisis o la IP referencial al sitio web

Figura 13. Interfaz de ingreso de IP

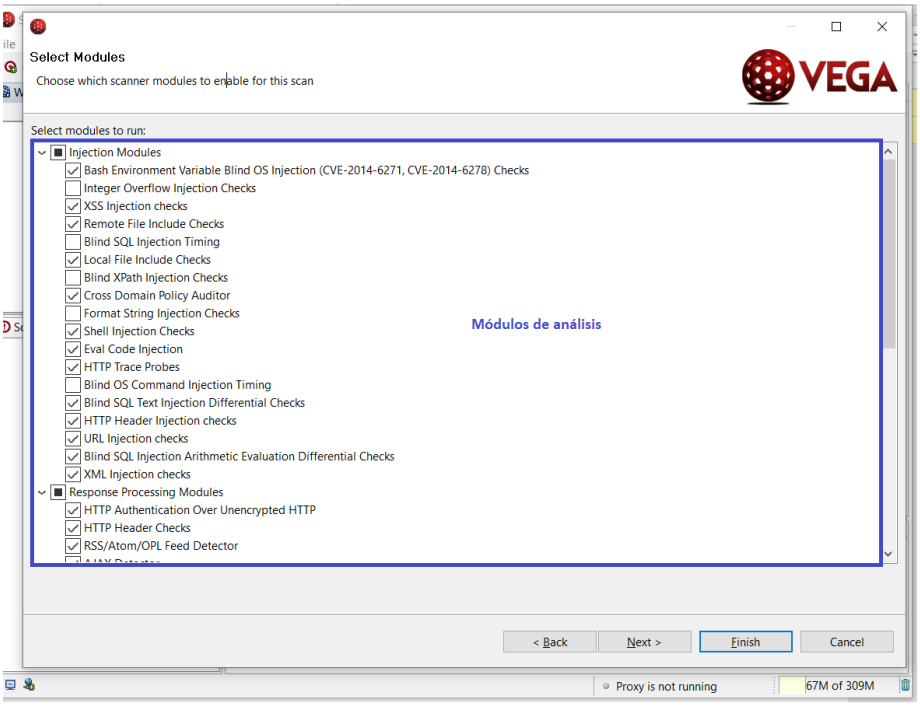
Fuente: Elaboración Propia



1.7 Seleccionar los módulos para el análisis

Figura 14. Interfaz de Vega, seleccionando módulos para el análisis

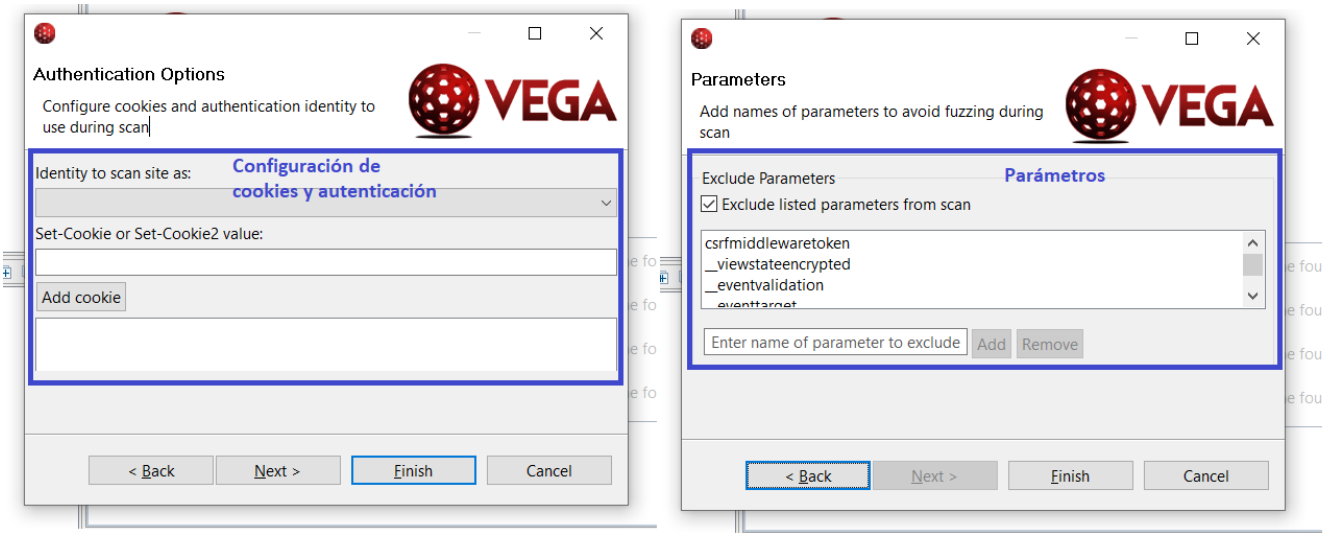
Fuente: Elaboración Propia



1.8 Configurar cookies e identidad de autenticación a usar durante el escaneo y agregar nombres de parámetros para evitar errores.

Figura 15. Interfaz de Vega, configurar cookies e identidad de autenticación

Fuente: Elaboración Propia

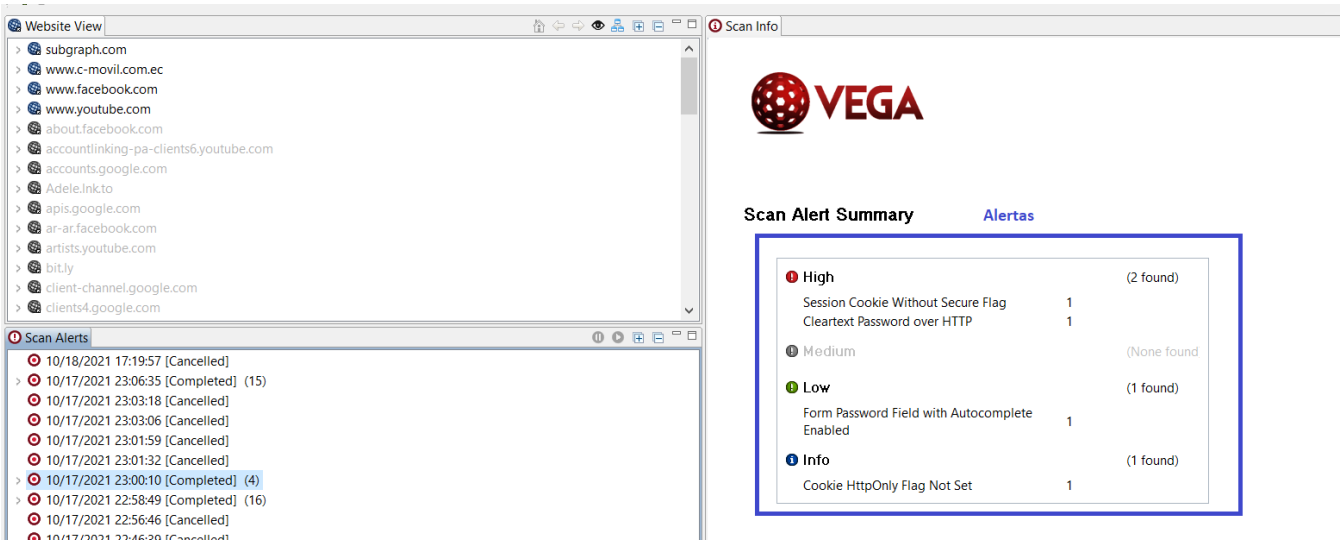


2. Resultados obtenidos

2.1 Visualizar las alertas encontradas en el escaneo, en ello se podrá visualizar el riesgo clasificándolos en alto, medio, bajo e informativo

Figura 16. Interfaz de Vega, visualizar las alertas encontradas

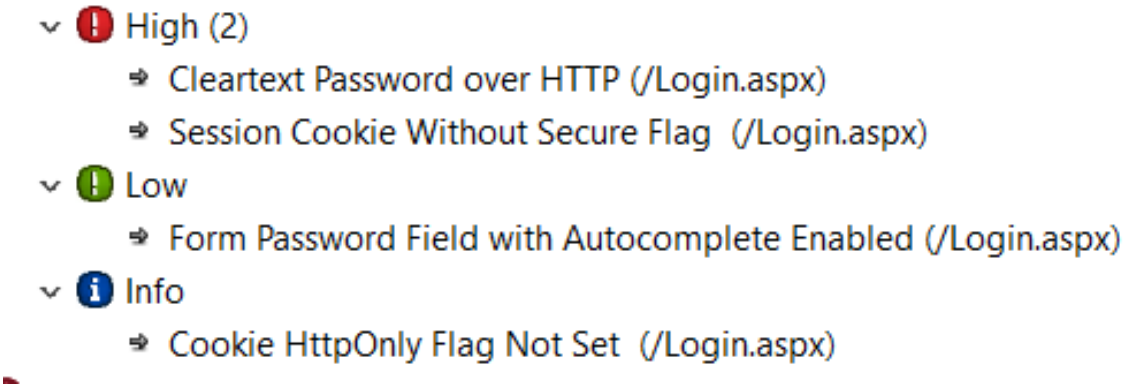
Fuente: Elaboración Propia



2.2 Identificar la descripción referente a cada riesgo

Figura 17.Interfaz de Vega, descripción referente a cada riesgo

Fuente: Elaboración Propia



2.3 Visualizar el detalle a cada riesgo identificando posible solución e impacto

Figura 18.Descripción de riesgo #1

Fuente: Elaboración Propia

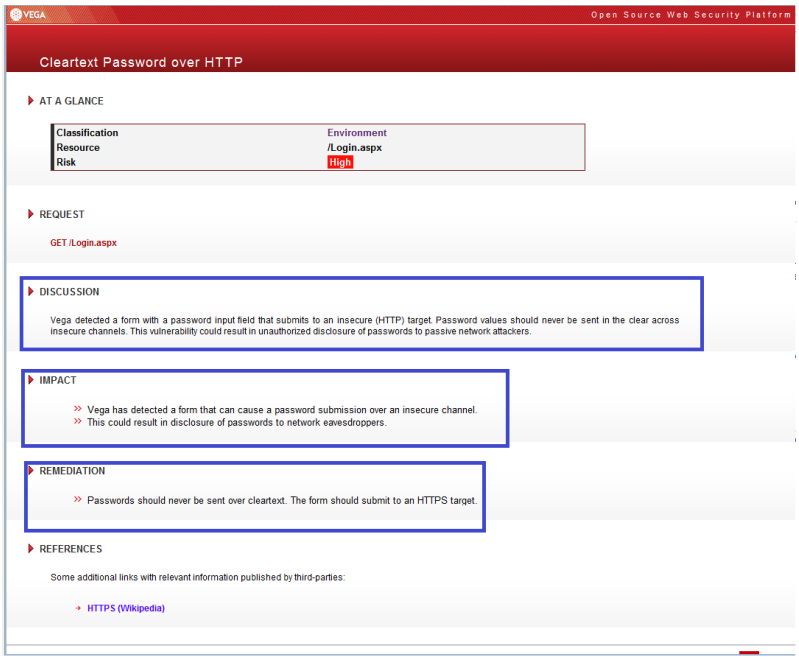


Figura 19.Descripción de riesgo #2

Fuente: Elaboración Propia

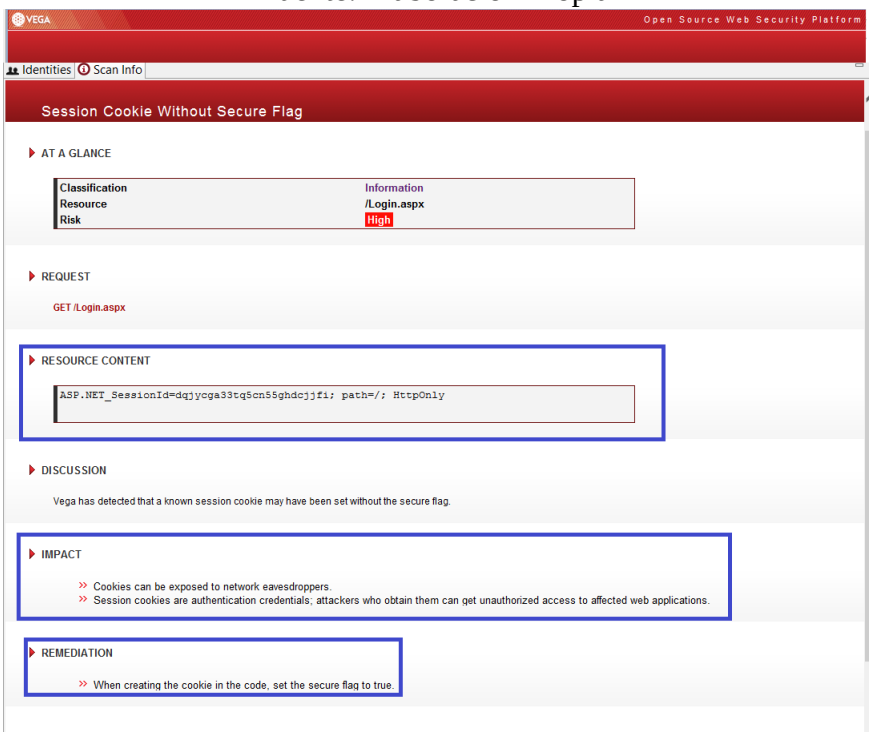


Figura 20.Descripción de riesgo #3

Fuente: Elaboración Propia

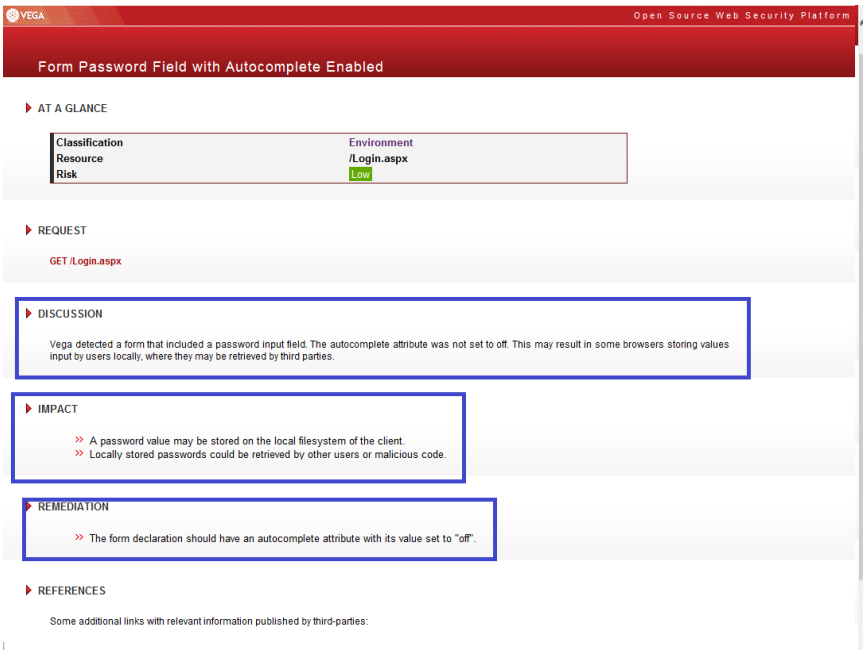
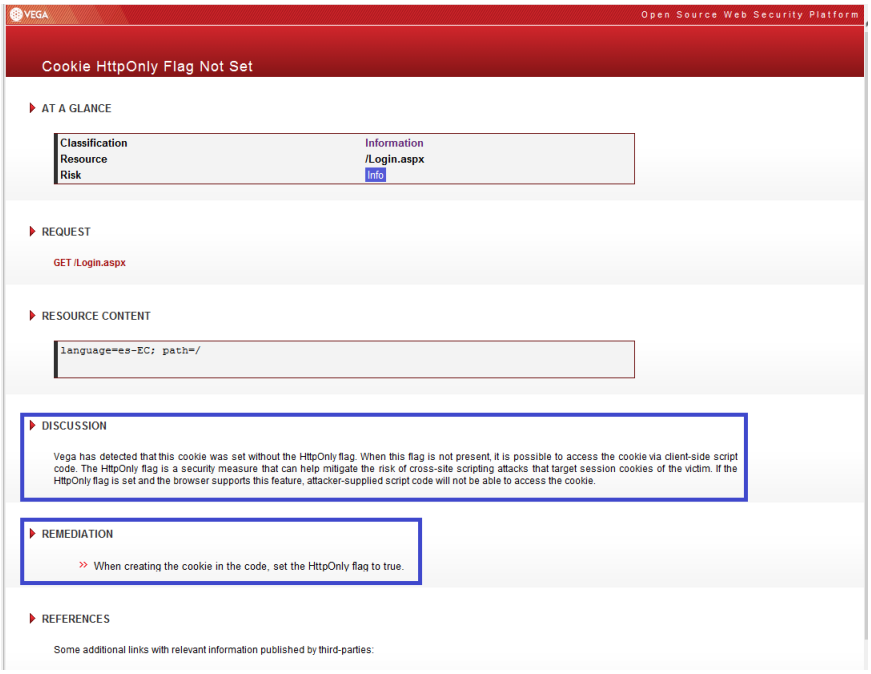


Figura 21.Descripción de riesgo #4

Fuente: Elaboración Propia



3.2.6.3 Herramienta Owasp Zap

1. Utilización de herramienta

1.1 Abrir el aplicativo e identificar las secciones que conforman la herramienta de análisis

A) Descripción de la herramienta de análisis

B) Sitios analizados

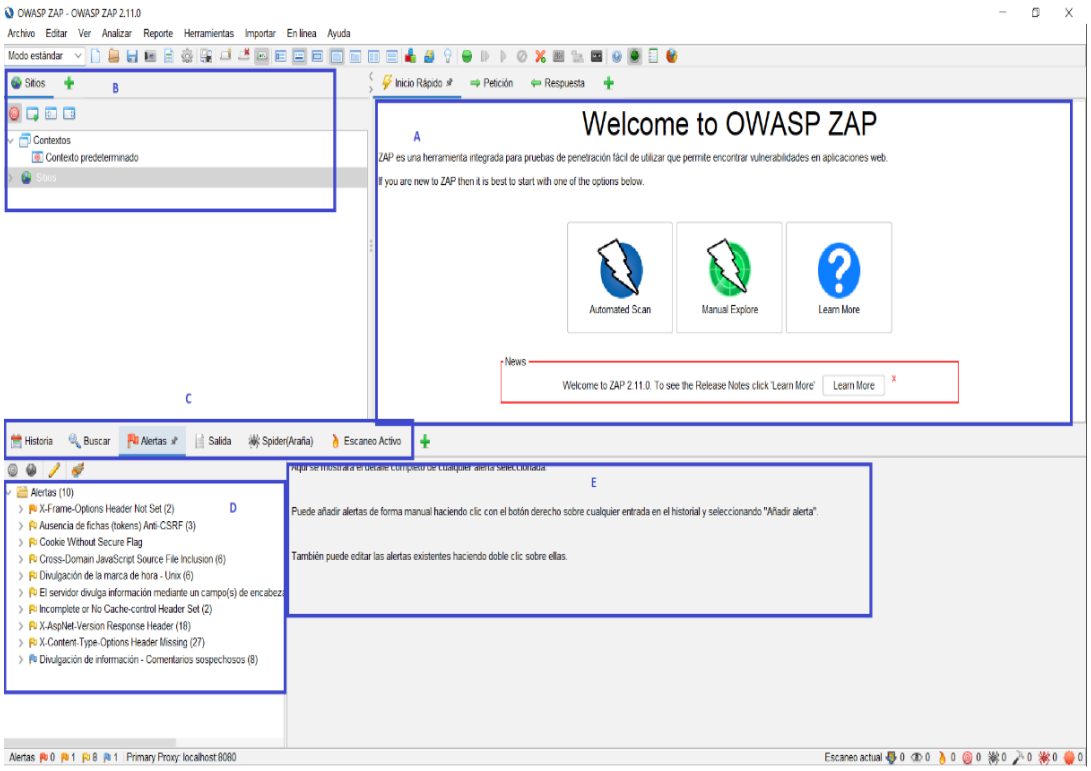
C) Opciones de salida

D) Vista de detalles de salidas

E) Descripción de cada alerta y soluciones a tomar

Figura 22. Interfaz de inicio de Owasp Zap

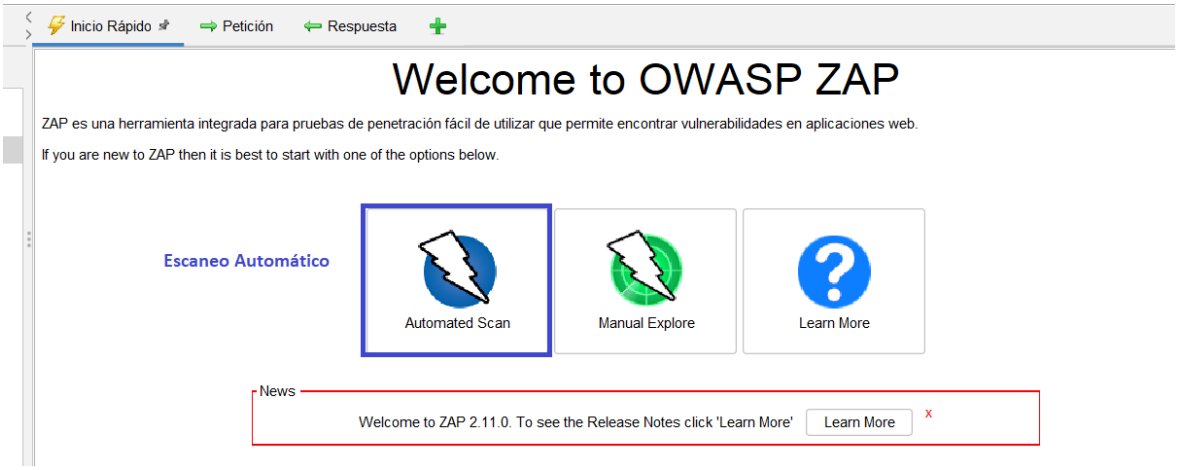
Fuente: Elaboración Propia



1.2 Seleccionar escaneo automático

Figura 23. Interfaz de Owasp Zap, seleccionar escaneo automático

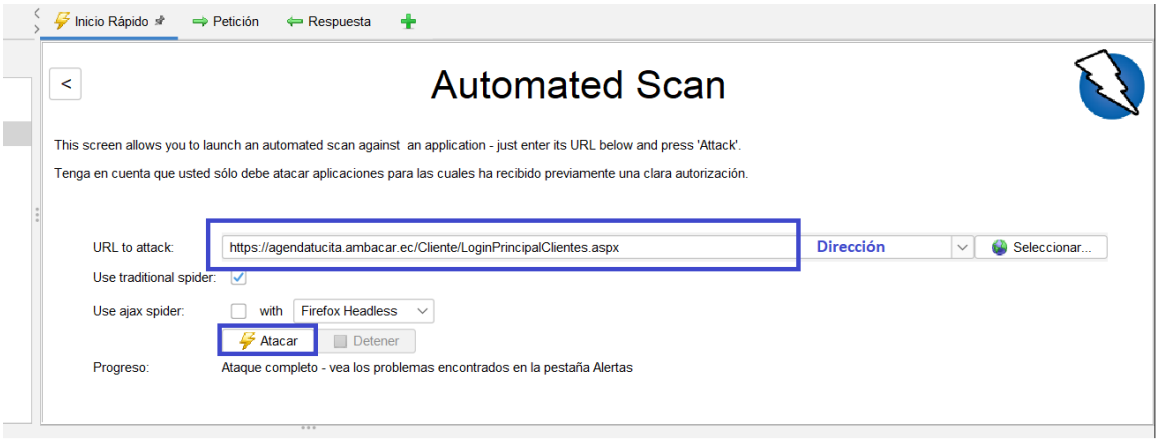
Fuente: Elaboración Propia



1.3 Ingresar la dirección a realizar el análisis y presionar en atacar para empezar con el escaneo

Figura 24.Interfaz de Owasp Zap, dirección a analizar.

Fuente: Elaboración Propia

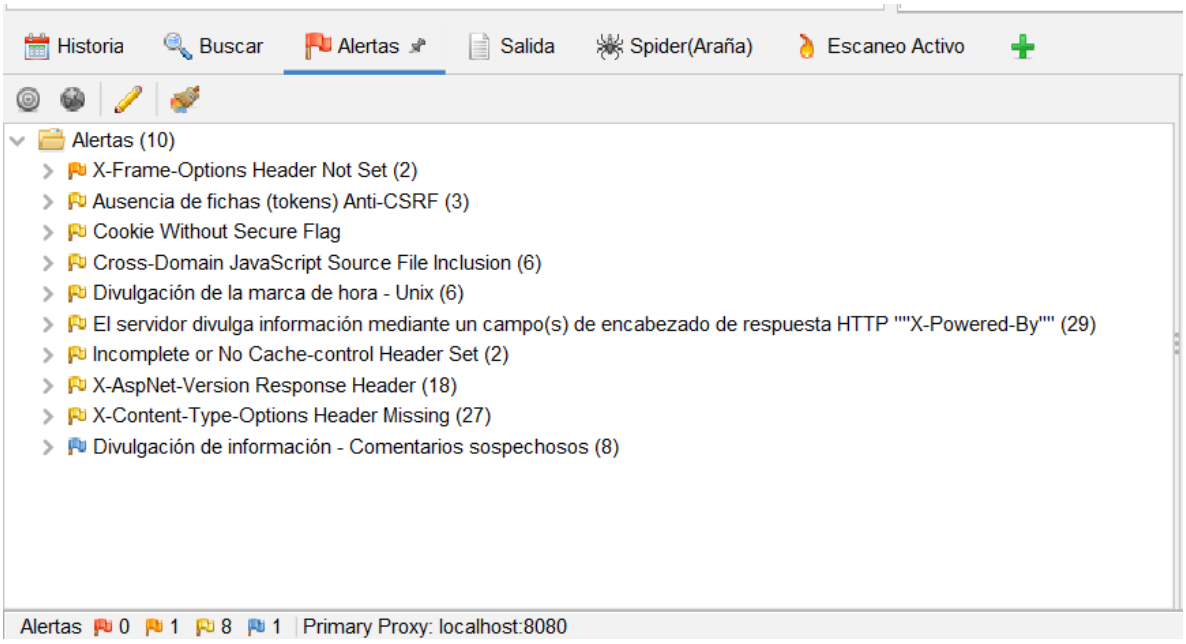


2. Resultados obtenidos

2.1 Identificar las salidas del escaneo realizado, en ello se visualizará todas las alertas de riesgo

Figura 25.Interfaz de Owasp Zap, Salidas de escaneo

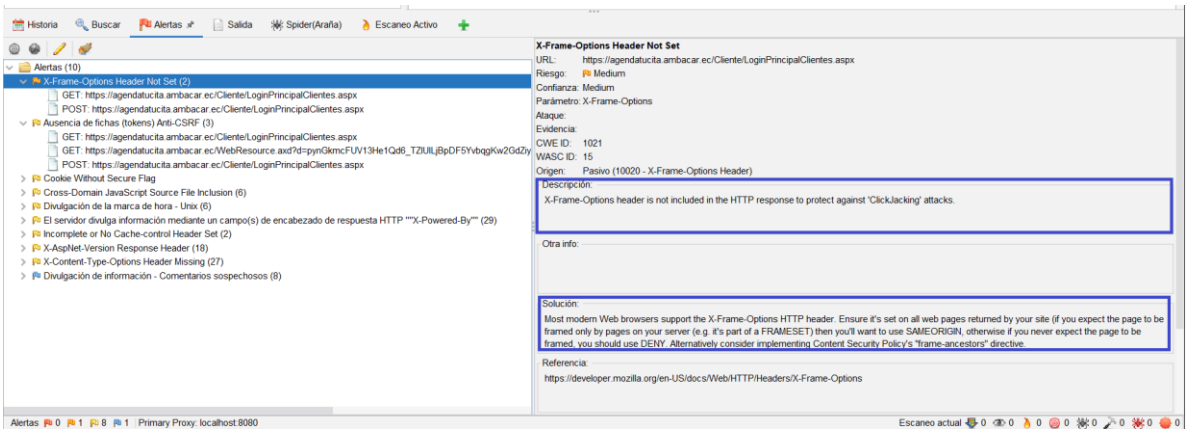
Fuente: Elaboración Propia



2.2 Visualizar la descripción detallada de cada alerta, identificando una breve información y la posible solución al problema encontrado

Figura 26.Interfaz de Owasp Zap, interfaz de alertas

Fuente: Elaboración Propia



Una vez visualizado el detalle referente a la alerta seleccionada se podrá visualizar la línea de codificación en donde se encuentra dicho problema.

Figura 27.Interfaz de Owasp Zap, Línea de codificación de la alerta seleccionada.

Fuente: Elaboración Propia

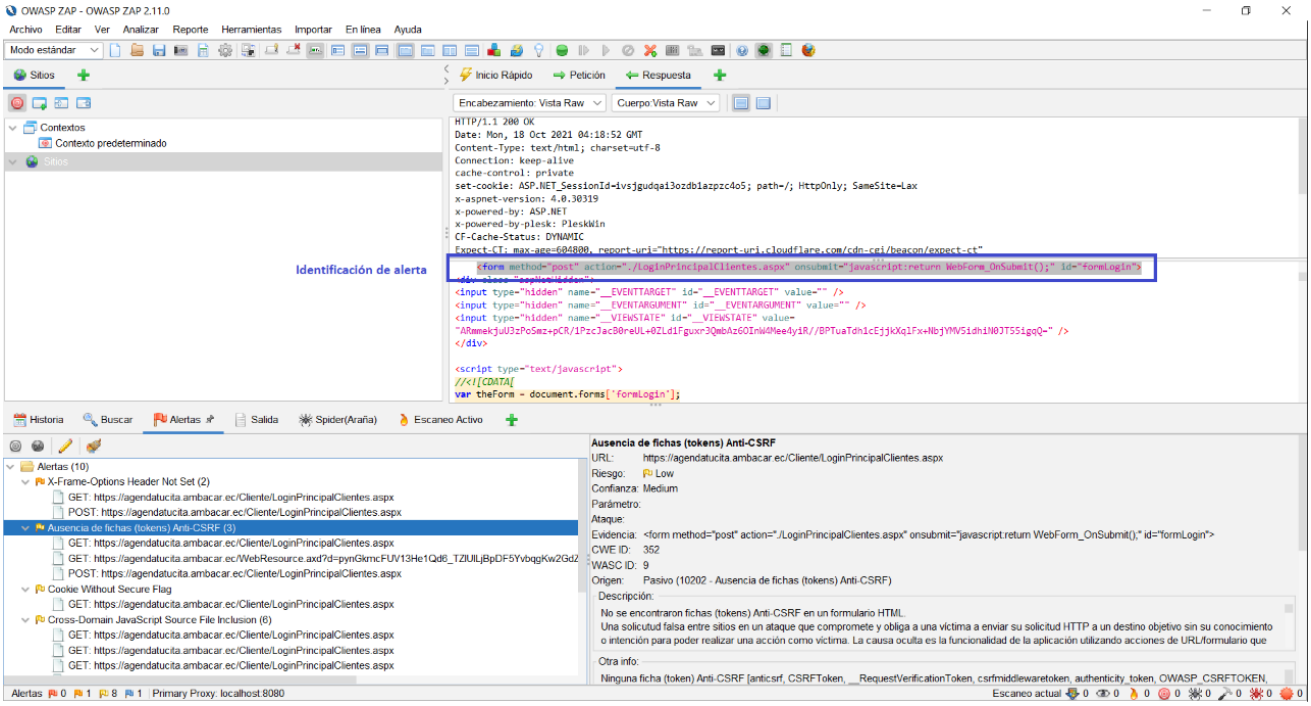


Figura 28.Descripción de la alerta #1 identificada

Fuente: Elaboración Propia

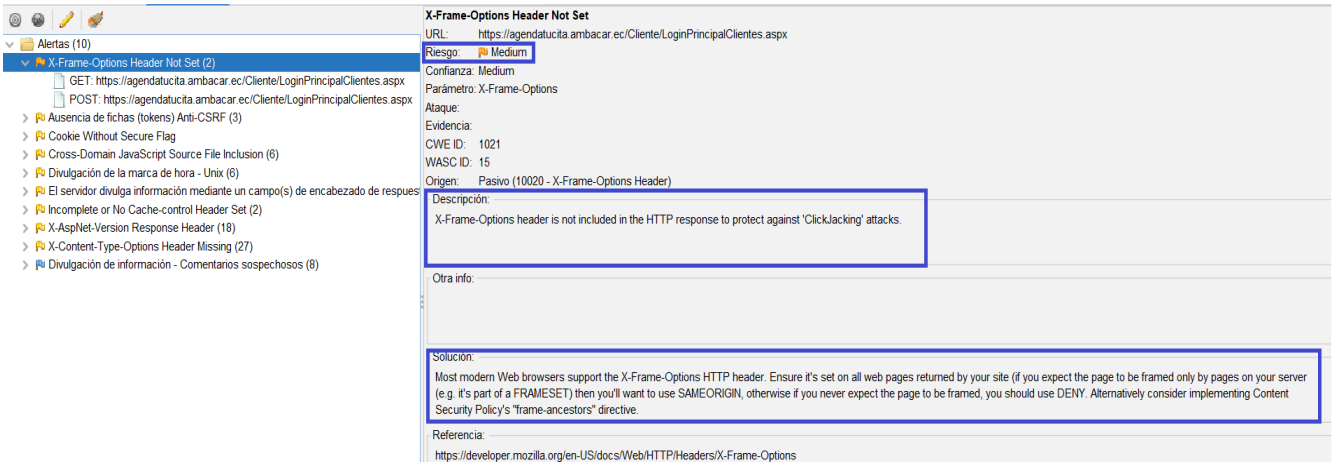


Figura 29.Descripción de la alerta #2 identificada

Fuente: Elaboración Propia

Figura 30.Descripción de la alerta #3 identificada

Fuente: Elaboración Propia

Figura 31.Descripción de la alerta #4 identificada

Fuente: Elaboración Propia

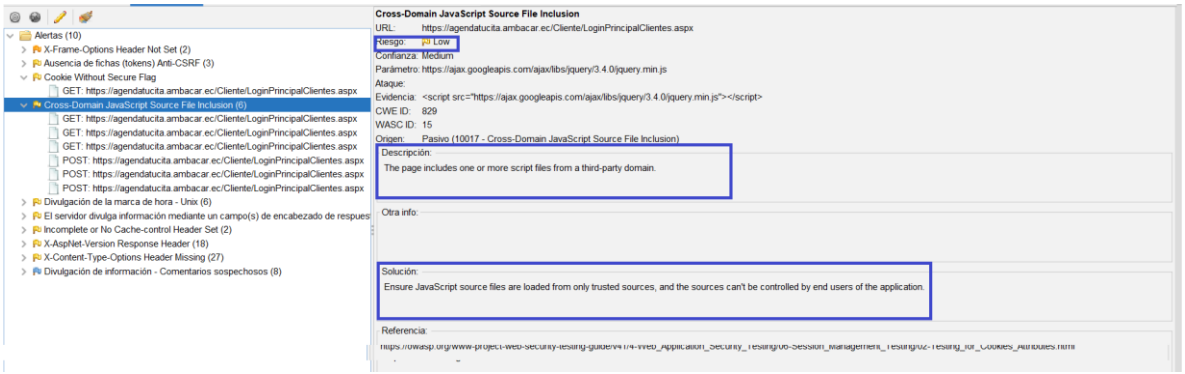


Figura 32.Descripción de la alerta #5 identificada

Fuente: Elaboración Propia

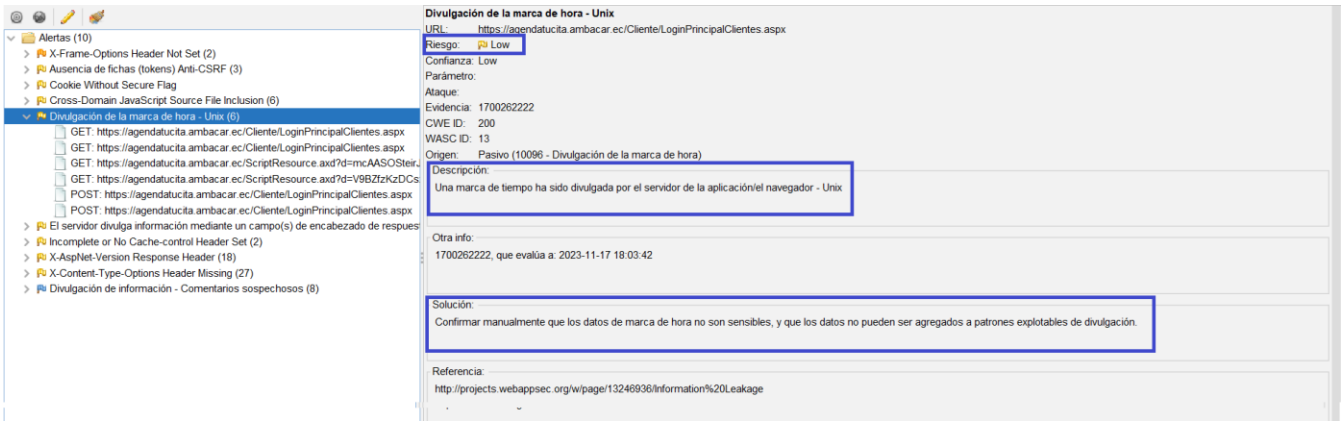


Figura 33.Descripción de la alerta #6 identificada

Fuente: Elaboración Propia

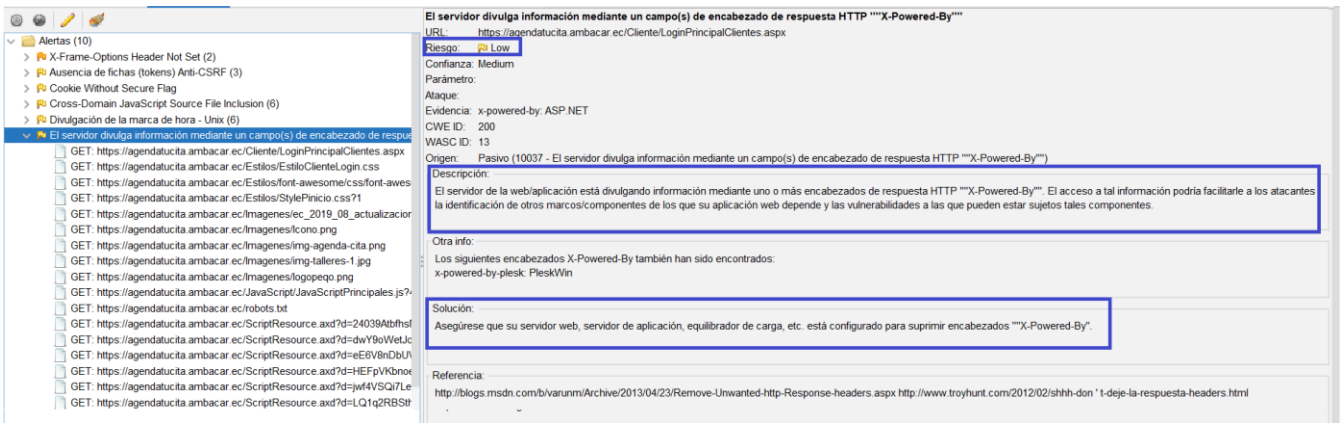


Figura 34. Descripción de la alerta #7 identificada

Fuente: Elaboración Propia

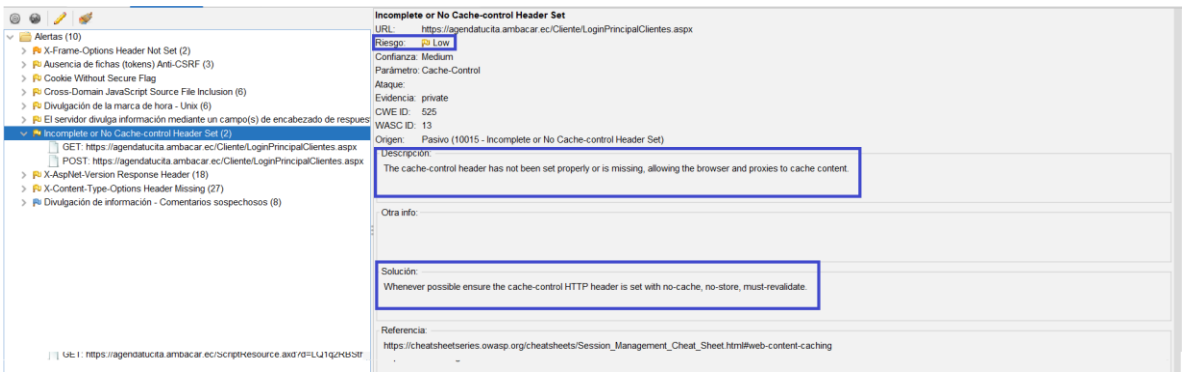


Figura 35. Descripción de la alerta #8 identificada

Fuente: Elaboración Propia

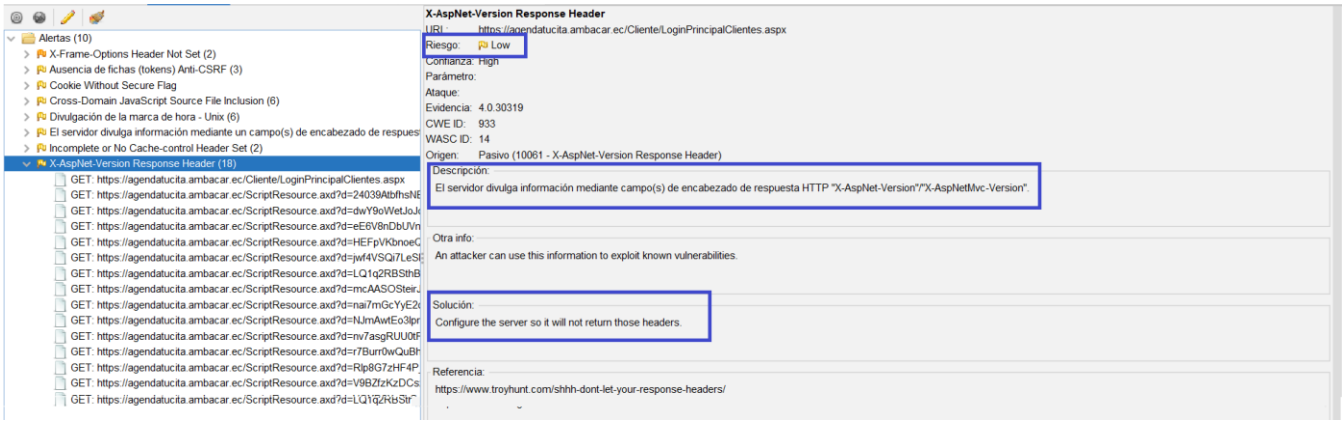


Figura 36. Descripción de la alerta #9 identificada

Fuente: Elaboración Propia

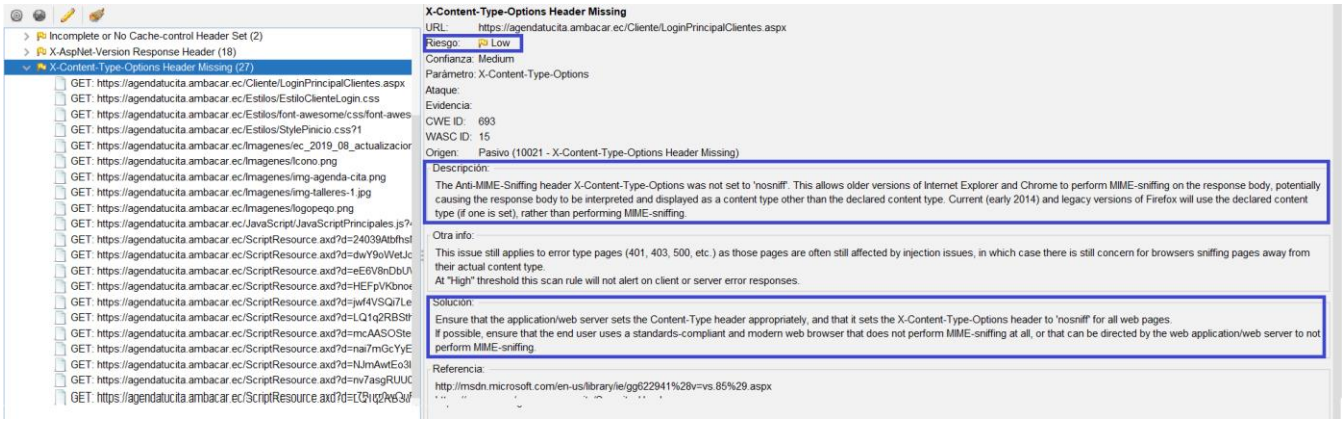
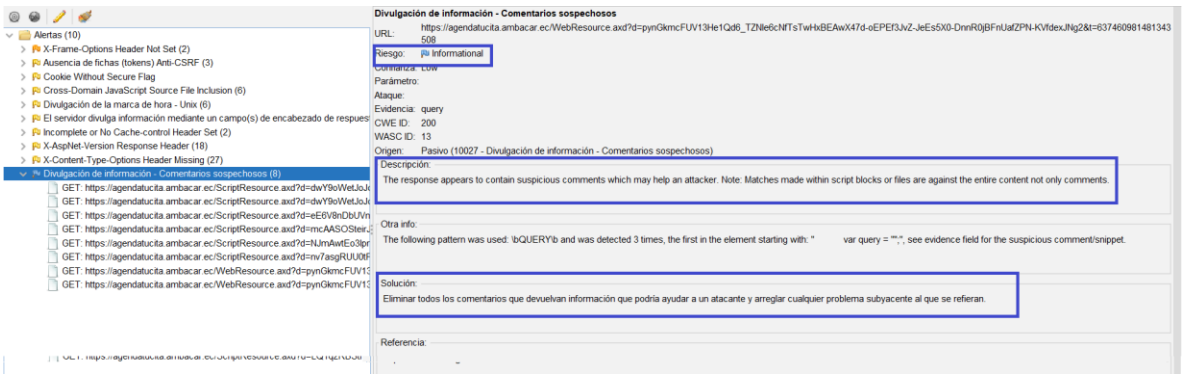


Figura 37. Descripción de la alerta #10 identificada

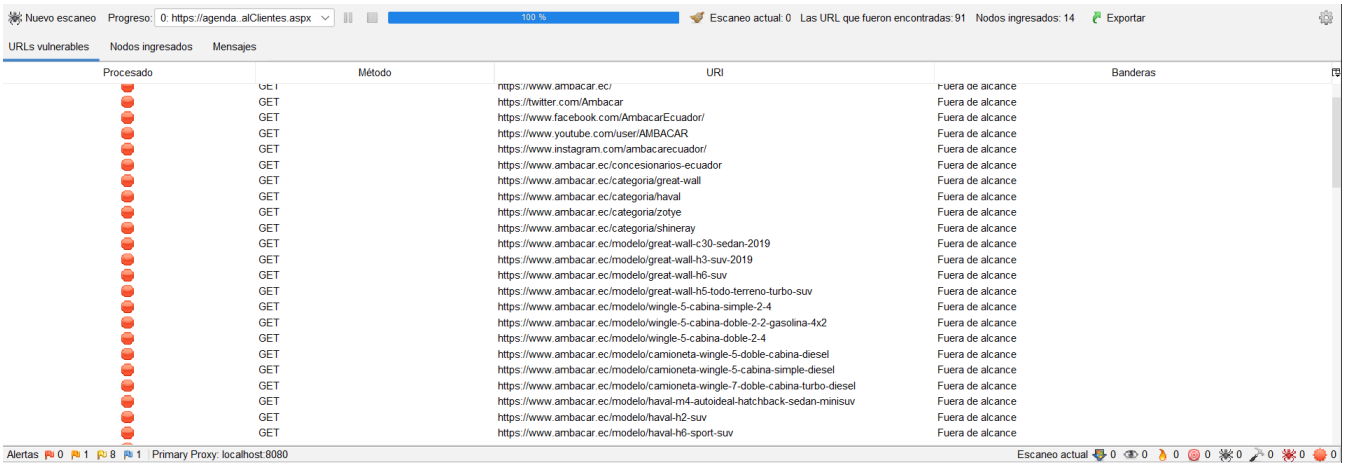
Fuente: Elaboración Propia



2.3 Visualizar las peticiones realizadas a las diferentes direcciones relacionadas con el url de análisis

Figura 38. Interfaz de peticiones

Fuente: Elaboración Propia



3.2.6.4 Herramienta Nessus

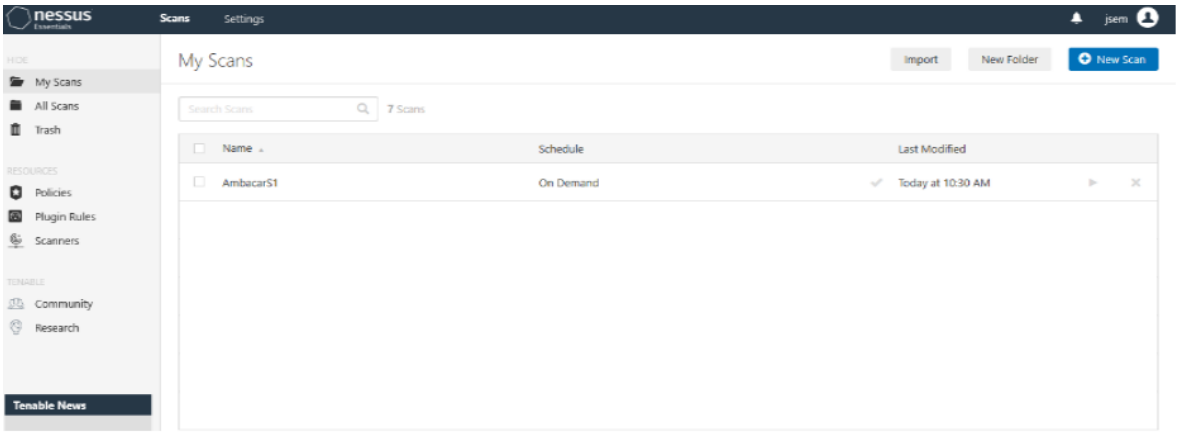
1. Utilización de herramienta

1.1 Abrir el aplicativo e identificar las secciones que conforman la herramienta de análisis

A. Sección de escanear
B. Ajustes
C. Importar
D. Nueva carpeta
E. Nuevo scan

Figura 39. Vista principal de Nessus

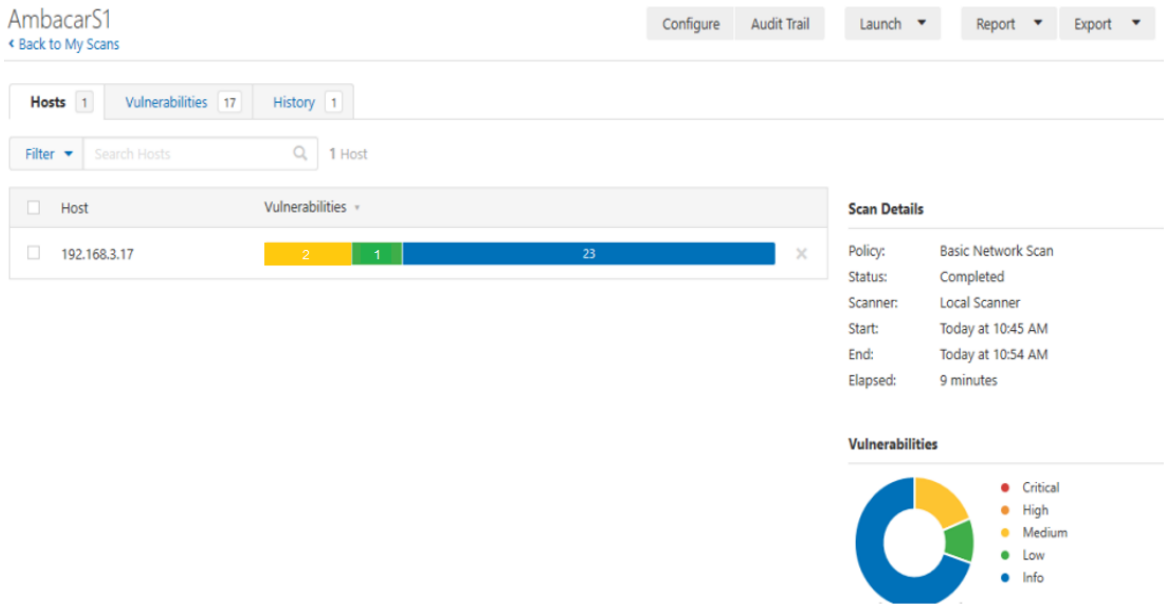
Fuente: Elaboración Propia



2. Análisis del servidor

Figura 40. Escaneo de vulnerabilidades con NESSUS

Fuente: Elaboración Propia



3.2.7 Análisis de las vulnerabilidades

Tabla 9. Listado de vulnerabilidades

Fuente: Elaboración Propia

Vulnerabilidad	Riesgo	Herramienta de análisis	Discusión	Solución
Cleartext Password over HTTP	Alto	VEGA	Se detectó un formulario con un campo de entrada de contraseña que se envía a un objetivo no seguro (HTTP). Los valores de contraseña nunca se deben enviar sin cifrar a través de canales no seguros. Esta vulnerabilidad podría resultar en la divulgación no autorizada de contraseñas a atacantes de red pasivos.	Diagrama de secuencia para él envió de datos. Revisar Anexo C.
Sessioni Cookie Without Secure Flag	Alto	VEGA	Vega ha detectado que es posible que se haya establecido una cookie de sesión conocida sin el indicador de seguridad.	Política de creación de cookies. Revisar Anexo C.

From Password Field with Autocomplete Enable	Baja	VEGA	Vega detectó un formulario que incluía un campo de entrada de contraseña. El atributo de autocompletar no estaba desactivado. Esto puede resultar en que algunos navegadores almacenen localmente los valores ingresados por los usuarios, donde pueden ser recuperados por terceros.	Política para la creación de campos. Revisar Anexo C.
Cookie HttpOnly Flag Not SeT	Informativa	VEGA	Vega ha notado que esta cookie se configuró sin el indicador HttpOnly. Cuando este indicador no está presente, es posible acceder a la cookie a través del código de secuencia de comandos del lado del cliente. El indicador Httponly es una medida de seguridad que puede ayudar a mitigar el riesgo de ataques de secuencias de comandos entre sitios que tienen como objetivo las cookies de sesión de la víctima.	Política de atributo HttpOnly de una cookie. Revisar Anexo C.
X-frame-Options Header Not Set	Media	OWASP ZAP	El encabezado X-FRAME-Options no está incluido en la respuesta HTTP para proteger contra los ataques de 'ClickJacking'.	Política de X-FRAME-Options en encabezados. Revisar Anexo C.

Ausencia de fichas Anti-CSRF	Baja	OWASP ZAP	No se encontraron tokens de fichas Anti-CSRF en el formulario HTML. Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible.	Política de fichas Anti-CSRF. Revisar Anexo C.
Cookie without Secury Flag	Baja	OWASP ZAP	Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.	Política de atributo HttpOnly de una cookie. Revisar Anexo C.
Cross-Domain JavaScript Source Files Inclusion	Baja	OWASP ZAP	La página incluye 1 o más archivos script de un dominio de terceros.	Política de fuente de archivos. Revisar Anexo C.

Divulgación de la marca de la hora – Unix	Baja	OWASP ZAP	Una marca de tiempo ha sido divulgada por el servidor de la aplicación/el navegador-Unix.	Política de divulgación. Revisar Anexo C.
El servidor divulga información mediante un campo de encabezado de respuesta HTTP X-Powered By	Baja	OWASP ZAP	El servidor de la web/aplicación está divulgando información mediante uno o más encabezados de respuesta HTTP "X-Powered-By". El acceso a tal información podría facilitarles a los atacantes la identificación de otros marcos/componentes de los que su aplicación web depende y las vulnerabilidades a las que pueden estar sujetos a tales componentes.	Política de encabezados de servidor. Revisar Anexo C.
Incomplete or No Cache-control Header Set	Baja	OWASP ZAP	El encabezado de control de caché no se ha configurado correctamente o falta, lo que permite que el navegador y los proxies almacenen en caché el contenido.	Políticas de directivas de control de cache. Revisar Anexo C.

X-AspNet-Version Response Header	Baja	OWASP ZAP	El servidor devuelve información mediante campos de encabezado de respuesta HTTP “X ASPNET VERSION”	Política preventiva de ataque tipo MIME. Revisar Anexo C.
X-Content-Type-Options Header Missing	Baja	OWASP ZAP	El encabezado Anti-MIME-Sniffing X-Content-Ttype-Options no se configuró en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un análisis MIME en el cuerpo de la respuesta, potencialmente haciendo que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido diferente al tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox usarán el contenido declarado type (si se establece uno), en lugar de realizar un rastreo de MIME.	Política de protocolos. Revisar Anexo C.
Divulgación de información	Informativa	OWASP ZAP	La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante.	Política de divulgación. Revisar Anexo C.

			Nota: Las coincidencias realizadas dentro de los bloques de secuencias de comandos o archivos son contra todo el contenido, no solo las comunicaciones.	
SSL Version 2 and 3 Protocol	Alto	NESSUS	El servicio remoto acepta conexiones encriptadas usando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, que incluyen: - Un esquema de relleno inseguro con cifrados CBC.	Política de uso de SSL. Revisar Anexo C.
SSL Certificate	Medio	NESSUS	No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir debido a que se puede romper la cadena de confianza. Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web.	Política de confiabilidad de certificado. Revisar Anexo C.
SSH Server CBC Ciphers	Bajo	NESSUS	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC).	Política de cifrado se servidor. Revisar Anexo C.

3.2.8 Plan de contingencia

Plan de contingencia de seguridad Informática

3.2.8.1 Introducción

La tecnología de la información (TI) y los sistemas de información automatizados son elementos vitales en la mayoría de los procesos comerciales. Debido a que estos recursos de TI son tan esenciales para el éxito de una organización, es fundamental que los servicios proporcionados por estos sistemas puedan operar de manera efectiva sin interrupciones excesivas. La planificación de contingencia respalda este requisito mediante el establecimiento de planes y procedimientos completos y medidas técnicas que pueden permitir que un sistema se recupere de manera rápida y eficaz después de una interrupción del servicio o un desastre.

Este documento brinda orientación a las personas responsables de preparar y mantener los planes de contingencia de TI. El documento analiza los elementos y procesos esenciales del plan de contingencia, destaca las consideraciones y preocupaciones específicas asociadas con la planificación de contingencia para varios tipos de sistemas de TI y proporciona ejemplos para ayudar a los lectores a desarrollar sus propios planes de contingencia de TI.

3.2.8.2 Objetivo

Esta guía de planificación de contingencia de TI identifica principios y prácticas de planificación fundamentales para ayudar al personal a desarrollar y mantener planes de contingencia de TI efectivos. Los principios satisfacen las necesidades organizacionales, sin embargo, se reconoce que puede aparecer nuevos tipos de ataques y falencias en la organización la cual, puede tener requisitos adicionales específicos. El documento brinda orientación para ayudar al personal a evaluar los sistemas de información y las operaciones para determinar los requisitos y prioridades de contingencia. Esta guía también proporciona un enfoque estructurado para ayudar a los planificadores a desarrollar soluciones rentables que reflejen con precisión sus requisitos de TI e integren los principios de planificación de contingencia en todos los aspectos de las operaciones de TI.

La orientación presentada debe considerarse durante cada etapa de la planificación de contingencia, comenzando con la conceptualización de los esfuerzos de planificación de contingencia hasta el mantenimiento del plan y la eliminación del plan de contingencia. Si se utiliza como una herramienta de gestión de la planificación durante todo el proceso de planificación de contingencias, este documento y sus apéndices deben brindar a los usuarios prácticas para ahorrar tiempo y costos.

3.2.8.3 Alcance

El documento presenta principios de planificación de contingencia para los siguientes sistemas comunes de procesamiento de TI:

- Computadoras de escritorio y sistemas portátiles (computadoras portátiles y de mano)
- sitios web
- Redes de área local (LAN)

La planificación de contingencia para supercomputadoras y redes inalámbricas no está cubierta en este documento, aunque muchos de los principios presentados aquí pueden aplicarse a estos sistemas.

Para ayudar al personal responsable de desarrollar planes de contingencia, este documento analiza las tecnologías comunes que pueden usarse para respaldar las capacidades de contingencia. Sin embargo, dada la amplia gama de diseños y configuraciones de TI, así como el rápido desarrollo y obsolescencia de productos y capacidades, el alcance de esta discusión no pretende ser exhaustivo. Más bien, el documento describe prácticas para aplicar tecnología para mejorar las capacidades de planificación de contingencia de TI de una organización.

El documento describe los principios de planificación que se pueden aplicar a una amplia variedad de incidentes que podrían afectar las operaciones del sistema de TI. El alcance incluye incidentes menores que causan daños a corto plazo interrupciones a desastres que afectan las operaciones normales durante un período prolongado. Debido a que los sistemas de TI varían en diseño y aplicación, los tipos de incidentes específicos y las medidas de contingencia asociadas no se proporcionan en este documento. En cambio, la guía de

planificación define un proceso que puede ser seguido por cualquier sistema de TI para identificar los requisitos de planificación y desarrollar un efectivo plan de contingencia para el desastre.

3.2.8.4 Requisitos legales

Para implementar una estrategia de seguridad de la información, el Concesionario Ambacar debe cumplir con regido dentro del acuerdo Ministerial 006-2021 del Ministerio de Telecomunicaciones y de la Sociedad de la Información publicado el 17 de mayo del 2021, además de utilizar la guía de pruebas de seguridad web de OWASP.

3.2.8.5 Definiciones

Acuerdo de Confidencialidad: Documento que todos los usuarios deben firmar para acceder a los recursos informáticos del concesionario Ambacar. Administrador: El usuario tiene encomendada la tarea de administrar los recursos informáticos y cuenta con una identidad que le permite tener derechos administrativos sobre los recursos informáticos de la entidad que estará bajo el control del coordinador del sistema.

Amenaza: Causa potencial de eventos inesperados que podrían dañar su sistema u organización. Copia de seguridad: copia de seguridad única de la información que se puede restaurar más tarde.

Contraseña: la clave para acceder a los recursos informáticos. Servicios de procesamiento de información: cualquier servicio de procesamiento de información, infraestructura o sistemas físicos o sitios web en los que están alojados.

Seguridad de la información: protege la confidencialidad, integridad y disponibilidad de la información y posiblemente otros atributos como la autenticidad, la responsabilidad, el no repudio y la confiabilidad.

Incidente de seguridad de la información: La existencia establecida de un sistema, servicio o estado de la red que indica una posible violación de la seguridad de la información, una falla de control o una situación previamente desconocida que puede estar involucrada en la seguridad. Cortafuegos: una colección de recursos de hardware y software que protegen los

recursos informáticos del acceso inapropiado. Incidente de seguridad de la información: indica un solo incidente o una serie de incidentes de seguridad de la información inesperado o inesperados que tienen una alta probabilidad de afectar las operaciones de la casa comercial Ambacar y afectar la seguridad de la información.

Información Confidencial: La información manejada por los Franquiciados de Ambacar de acuerdo con sus deberes y funciones debe ser conservada por razones legales y puesta a disposición únicamente con el consentimiento previo del titular.

Información Confidencial: La información generada por los Franquiciados Ambacar de acuerdo con sus deberes y funciones es conocida únicamente por un grupo de funcionarios autorizados por ellos. El acceso a dicha información debe ser limitado y basado en el principio de privilegio mínimo. La divulgación a terceros requiere el consentimiento del propietario de este acuerdo y el acuerdo de confidencialidad. Asimismo, la divulgación no autorizada de información puede causar un daño significativo a la entidad. Cualquier documento creado cuando se hace una copia de dicha información (como una mala calidad de impresión) debe destruirse.

Información Personal: La información generada por los franquiciados de Ambacar de acuerdo con sus responsabilidades y funciones no será puesta a disposición del público. Su divulgación no autorizada no causará daños significativos al sujeto y está disponible para todos los usuarios.

LAN: un grupo de computadoras y dispositivos relacionados que comparten un esquema de comunicación común y están ubicados en un área geográfica pequeña (edificio u oficina). Licencia de software: es una autorización o licencia otorgada por el propietario de un programa a un usuario para usar ese programa específicamente bajo los términos acordados. La licencia define los derechos (uso, modificación o redistribución) que se le otorgan y sus limitaciones, así como su duración y alcance.

Copyright: es un conjunto de derechos exclusivos utilizados por ley para regir el uso de ciertas expresiones, ideas o información. Más generalmente, se refiere a los derechos de autor de las obras (poemas, juegos, literatura, películas, obras musicales, grabaciones de sonido, pinturas, esculturas, fotografías, software, radio, televisión y otras formas de expresión de ideas o conceptos), independientemente de si se utiliza un medio auxiliar (impreso, digital),

y en muchos casos se asocia la protección asociada a un determinado período de tiempo. En muchos casos, los derechos de autor están directamente relacionados con la protección de los derechos patrimoniales sobre una obra. Salvapantallas: el programa se activa a voluntad o se inicia automáticamente después de un período de inactividad. Servidor proxy: un servidor que actúa como puerta de enlace a Internet. Recursos informáticos: Elementos de tecnología de la información tales como: servidores de datos y aplicaciones, computadoras de escritorio, portátiles, elementos multimedia, elementos del sistema visual, elementos de almacenamiento de información, programas y datos.

Riesgo: la combinación de la probabilidad de que ocurra un evento y sus consecuencias. Análisis de riesgo: el uso sistemático de información para identificar fuentes de riesgo y evaluar el riesgo. Evaluación de riesgos: Cualquier proceso de análisis y evaluación de riesgos. Evaluación de riesgos: El proceso de comparar el riesgo evaluado con los criterios de riesgo establecidos para determinar la gravedad del riesgo. Gestión de riesgos: Acciones coordinadas para dirigir y controlar la organización con respecto al riesgo. Enrutador: dispositivo que permite la comunicación entre dos o más redes informáticas. Sesión: Conexión establecida por el usuario al sistema de información. Sistema de control de acceso: un componente de hardware o software que concede o deniega el acceso a los recursos informáticos en función de políticas definidas. Sistema de Detección de Intrusos (IDS): Es un conjunto de hardware y software que ayuda a detectar intentos de acceso o intentos de acceso no autorizado a los recursos informáticos de Ambacar. Sistema de cifrado: una pieza de hardware o software que permite cifrar la información para evitar el acceso de usuarios no autorizados. Sistema multiusuario: una computadora y el software relacionado capaz de servir a múltiples usuarios simultáneamente a través de una red de comunicación. Propiedad Intelectual: Es la disciplina normativa que protege las creaciones intelectuales del esfuerzo, trabajo o habilidad humana y merece reconocimiento legal.

Open Source: Este es el término utilizado para entender el software desarrollado y distribuido libremente, donde una licencia define los usos que se le pueden otorgar al software. Software gratuito: una vez adquirido, el software se puede usar, copiar, modificar o redistribuir de forma gratuita, y tiene una licencia expresa para hacerlo. Software de piratería: copias ilegales de aplicaciones o programas utilizados sin una licencia según lo exige la ley. Software de Dominio Público: Un tipo de software que no requiere ninguna licencia, el

derecho de crear, usar y otras funciones está reservado para todos y su creador no se ve afectado ya que pertenece a todas las mismas personas. En general, el software de dominio público es software de uso completamente gratuito con propiedad intelectual.

Software Libre: Software informático que se distribuye gratuitamente sin código fuente. Shareware: una categoría de software o programas diseñados para ser evaluados durante un período de tiempo o para proporcionar alguna funcionalidad básica. Se requiere el pago en efectivo para la adquisición completa del software. Módem (Modulador): Es un componente de comunicación que permite transmitir información a través de líneas telefónicas. Monitoreo: Verificar la actividad de los usuarios en los recursos informáticos del franquiciado Ambacar. OTP (contraseña de un solo uso): Una contraseña proporcionada por el administrador del recurso informático que permite el acceso por primera vez a este recurso y obliga al usuario a cambiar la contraseña cuando se completa el acceso. Plan de Contingencia: Un plan que brinda flexibilidad de tiempo para restaurar los servicios relacionados con el sistema de información de franquicias de Ambacar en caso de un desastre y otras interrupciones de las operaciones normales. Política: Todas las intenciones y direcciones son formalmente expresadas por la gerencia.

Software de Dominio Público: Un tipo de software que no requiere ninguna licencia, el derecho de crear, usar y otras funciones está reservado para todos y su creador no se ve afectado ya que pertenece a todas las mismas personas. En general, el software de dominio público es software de uso completamente gratuito con propiedad intelectual.

Software Libre: Software informático que se distribuye gratuitamente sin código fuente. Shareware: una categoría de software o programas diseñados para ser evaluados durante un período de tiempo o para proporcionar alguna funcionalidad básica. Se requiere el pago en efectivo para la adquisición completa del software. Módem (Modulador): Es un componente de comunicación que permite transmitir información a través de líneas telefónicas. Monitoreo: Verificar la actividad de los usuarios en los recursos informáticos del franquiciado Ambacar. OTP (contraseña de un solo uso): Una contraseña proporcionada por el administrador del recurso informático que permite el acceso por primera vez a este recurso y obliga al usuario a cambiar la contraseña cuando se completa el acceso. Plan de Contingencia: Un plan que brinda flexibilidad de tiempo para restaurar los servicios

relacionados con el sistema de información de franquicias de Ambacar en caso de un desastre y otras interrupciones de las operaciones normales. Política: Todas las intenciones y direcciones son formalmente expresadas por la gerencia. Usuario: Cualquier persona con acceso a los recursos informáticos de la Sala. Usuarios de Web y Correo: Usuarios con los que la Concesionario Ambacar comparte un ID de Cliente para acceder a sus recursos informáticos.

Usuarios Externos: Clientes externos que utilizan los recursos informáticos del Departamento a través de Internet o de otro modo y tienen acceso únicamente a información clasificada. Usuarios externos contratados: Usuarios externos contratados con la Concesionario Ambacar y tienen acceso limitado a los recursos informáticos para uso interno.

3.2.8.6 Responsable

3.2.8.6.1 Compromiso de la dirección

La administración debe demostrar evidencia de su compromiso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los mecanismos para asegurar que la información:

Estableciendo una política de seguridad de la información. o Definir roles y responsabilidades para la seguridad de la información. o Informar a la organización sobre la importancia de cumplir con los parámetros de seguridad de la información, sus responsabilidades legales y la necesidad de mejora continua. o Velar por la realización de auditorías internas.

3.2.8.6.2 Gestión de recursos

Asegurar que las políticas de seguridad de la información apoyen la implementación de la misión y visión del Departamento. Identificar y tratar los requisitos legales y reglamentarios y las obligaciones contractuales de confidencialidad; mantener las salvaguardas apropiadas mediante la aplicación adecuada de todas las medidas de control implementadas; Asegúrese de que todos los empleados sean conscientes de la importancia de la seguridad de la información.

3.2.8.7 Procedimiento

Comunicación de políticas de privacidad:

Los responsables de Seguridad de la Información son conscientes de que las fuentes de información son utilizadas de forma continua por los usuarios que utilizan los distintos servicios objeto de este documento, proporcionándoles así unos códigos básicos de conducta cuando procede utilizar equipos informáticos y otros recursos de información y técnicos.

Aplicar política de privacidad:

Las políticas de seguridad informática están diseñadas para reducir el riesgo y minimizar el impacto de los incidentes de seguridad. Establecen los principios básicos por los cuales una organización debe operar sus recursos informáticos. Las reglas de seguridad informática están diseñadas para reducir y eliminar muchos de los principales factores de riesgo que existen.

3.2.8.6.1 Políticas generales de seguridad informática

Estos estándares se aplican a todos los usuarios de los recursos informáticos y se dividen en: Política de Cumplimiento y Sanciones, Política sobre el uso de los recursos informáticos, política de contraseñas, Política de uso de la información, Reglas para el uso de Internet y correo electrónico, Política del uso de Intranets y Sitios Web, Política general del Palacio Presidencial, Reglas para desarrolladores de software, Política para administradores de sistemas, Estrategia de respaldo, Política de uso de cortafuegos, Política para usuarios externos, Política de acceso físico, Reglas para el uso de computadoras portátiles.

3.2.8.6.2 Políticas de cumplimiento y sanciones

Cumplir con la seguridad de la información

Todos los empleados de la organización, así como los contratistas, deben cumplir y adherirse a las políticas y procedimientos relacionados con la protección y seguridad de la información. El presidente del Concesionario Ambacar y el Oficial de Seguridad de la Información son los responsables de velar por su estricto cumplimiento.

Medidas disciplinarias por incumplimiento de la política de privacidad

La violación de la Política de privacidad y cualquier estándar o procedimiento por parte de cualquier funcionario o contratista dará lugar a medidas disciplinarias y, según la gravedad, a la terminación del empleo por parte de los empleados o contratistas. Si la infracción proviene de la sede del Concesionario Ambacar, se podrá suspender la prestación de cualquier servicio de información.

3.2.8.6.3 Políticas de uso de recursos informáticos

Los recursos informáticos disponibles para Ambacar con fines operativos son únicamente para fines relacionados con el trabajo. Los productos que utilicen los recursos técnicos anteriores serán propiedad del Sujeto y se incluirán en el directorio de políticas del Sujeto. Todos los demás usos requieren aprobación previa del Palacio Presidencial.

3.2.8.6.4 Políticas de uso de las contraseñas

Confidencialidad de las contraseñas.

La contraseña asignada por cada usuario para acceder al sistema de información deberá ser personal, confidencial e intransferible. Cada usuario debe asegurarse de que su contraseña no sea vista por otros y saber

Uso de diferentes contraseñas para diferentes recursos informáticos.

Para evitar afectar múltiples recursos informáticos, cada usuario debe usar una contraseña diferente para cada recurso al que tenga acceso. Esto también se aplica a los dispositivos de comunicación (cortafuegos, enrutadores, servidores de control de acceso) y sus administradores.

Identificación única para cada usuario.

Cada usuario tendrá un ID único por sistema (usuario) al que tenga acceso, junto con un factor de autenticación personal y secreto (contraseña) para utilizar los recursos técnicos necesarios para mi trabajo. Esta política se aplica a las aplicaciones implementadas antes de la fecha de lanzamiento de este documento. Estos agentes tendrán una identidad personal única y una contraseña apropiada asignada por el coordinador del sistema del franquiciado Ambacar.

Cambios periódicos de contraseñas.

Todos los usuarios deben cambiar automáticamente sus contraseñas al menos cada 30 días.

Longitud mínima de contraseñas.

Todas las contraseñas deben tener al menos ocho (8) caracteres con alguna de las siguientes características: Contiene una combinación de números, letras mayúsculas y minúsculas y caracteres especiales.

Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña que sea esencialmente igual o similar a la contraseña que ha utilizado anteriormente. Esta política se complementa con la Política de circuito cerrado.

Almacenamiento de contraseñas.

Las contraseñas no se almacenan en forma legible en archivos por lotes, secuencias de comandos, macros, teclas de función de terminal, archivos de texto, en computadoras u otros lugares que puedan ser descubiertos por personas no autorizadas o que puedan utilizarlos. En ninguna circunstancia los usuarios deben usar su contraseña en ningún medio de impresión, excepto según lo dispuesto en la política "Almacenar contraseña de administrador".

Intrusión sospechosa deben forzar cambios de contraseña.

Cualquier contraseña debe cambiarse inmediatamente si se sospecha o se sabe que se ha perdido.

Revelación de contraseñas prohibida.

La divulgación de contraseñas a empleados o terceros está prohibida en ninguna circunstancia. Las contraseñas personales no deben introducirse en presencia de terceros, aunque sean personas físicas. Ningún usuario puede intentar obtener una contraseña de otro usuario.

3.2.8.6.5 Políticas de uso de la información

Divulgación de la información manejada por los usuarios de Ambacar

Los agentes de Ambacar pueden divulgar la información del usuario almacenada en el sistema con mi autorización firmada, solicitud legal, solicitud judicial o administrativa, sujeto a las excepciones establecidas en este documento y las leyes de protección de datos. individual.

Se hace constar expresamente que la información pública del registro sólo se gestiona para el registro público de conformidad con las normas legales y reglamentarias aplicables en la materia. La información para otras funciones de Ambacar es administrada y almacenada de conformidad con lo establecido en el sistema de protección de datos personales, garantizando la seguridad de la información previamente clasificada, salvo que el titular de la información consienta en tal divulgación.

Transferencia de datos solo a organizaciones con suficientes controles.

Los agentes de Ambacar sólo podrán proporcionar información personal a terceros que se hayan comprometido por escrito a someter la información a los controles de seguridad correspondientes.

Registro de las compañías que reciben información privada.

El personal del concesionario Ambacar que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

Transferencia de la custodia de información de un funcionario que deja el concesionario Ambacar

Cuando un empleado se retira el concesionario Ambacar, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar

quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

Transporte de datos sensibles en medios legibles.

Si la información confidencial se transfiere en medios legibles por computadora (disquetes, cintas, CD, pen drives), la información debe cifrarse si el destinatario acepta el intercambio de datos cifrados. En el caso de las computadoras portátiles, esta información está protegida por una aplicación de encriptación.

Datos sensibles enviados a través de redes externas deben estar encriptados.

Si se van a transmitir datos confidenciales a través de cualquier canal de comunicación externo, esos datos deben transmitirse de forma encriptada, siempre que el destinatario tenga los recursos necesarios y acepte un intercambio de datos encriptados.

3.2.8.6.6 Políticas de Intranet y sitios web

Reglas de uso de la Intranet.

Los concesionarios de Ambacar podrán utilizar la intranet como fuente para publicar documentos que gestionen su relación con los empleados o empleadas. Entonces, cuando está en uso, los empleados deben tener acceso constante a la intranet y a todos los documentos que se encuentran en ella.

Prohibición de publicitar la imagen del concesionario Ambacar en sitios diferentes a los institucionales.

La publicación en Internet de logotipos, marcas o cualquier otro tipo de información sobre Ambacar o sus operaciones sólo podrá realizarse a través de los sitios web de la organización y con el consentimiento previo del presidente o director de la entidad. Por tanto, queda terminantemente prohibido gestionar esta información en la página personal del empleado.

Prohibición establecer conexiones a los sitios Web el concesionario Ambacar

También se prohíbe a los empleados y sus sitios o sitios web privados crear enlaces o cualquier otro tipo de enlace a cualquier sitio web de Ambacar, a menos que se haya obtenido la aprobación previa del director ejecutivo en cada caso. En particular, no se permite la colocación de enlaces o marcos electrónicos y el uso del nombre comercial o marcas

registradas de una organización en páginas que no sean el sitio web de la organización o como etiquetas meta.

Prohibición de anuncios en sitios Web particulares.

La publicidad en un sitio web personal como agente de Ambacar o sus representantes está estrictamente prohibida, o la publicación de cualquier dibujo o diseño de producción que pueda inducir a los visitantes del sitio web a creer que existe algún enlace a Ambacar.

Sistemas de detección de intrusos (IDS)

Un componente importante de la arquitectura de seguridad del perímetro de una organización es un Sistema de detección de intrusos (IDS). Estos sistemas son capaces de detectar la presencia de cualquier señal, ataque o acción que pueda comprometer los sistemas de una organización o elementos de su infraestructura de red.

Funciones de los IDS.

Hay dos funciones principales de IDS, a saber, prevención y respuesta. La interceptación se realiza mediante el uso de herramientas que escuchan el tráfico de la red o de la computadora. Estos programas identifican los ataques utilizando modelos o métodos inteligentes.

Esta función permite a los identificadores realizar esfuerzos en ataques o actividades sospechosas inmediatamente dadas en la red de organizaciones. Estos dispositivos también permiten reaccionar con seguridad antes de realizar el ataque, que es lo que llamamos el método de respuesta. El método de respuesta utiliza el programa para analizar los archivos de registro (registros) en los sistemas, intente detectar muestras en enlaces de servicio de red o comportamiento del sistema. Modificar archivos compartidos, archivos del sistema y otros archivos también se considera un signo de invasión.

Las funciones de un IDS se pueden resumir de la siguiente forma:

• Analizar el comportamiento incorrectamente, por lo que, si detectan la conexión fuera del horario normal, el compuesto está roto, V.V. Muestra que esta es una invasión.

• En el sistema de detección de invasiones, es posible automatizar la búsqueda de nuevas plantillas de ataque con motores de búsqueda estándar y análisis de tráfico de red inusual.
• Sistemas para monitorear y analizar acciones de usuario. De esta manera, puede averiguar los servicios utilizados por muchos usuarios diferentes y analizar el contenido de tráfico en la búsqueda de elementos extranjeros.
• La auditoría de configuración de algunos sistemas y brechas también cae en identificadores.
• Puede automatizar tareas como actualizar reglas, recopilar y analizar registros, configurar firewalls y más.
• Puede detectar ataques en la red de una organización durante o poco después de un ataque.
• Mediante el análisis del tráfico de red y los logs generados (logs), pueden detectar sistemas que soportan servicios que no deberían estar habilitados.

3.2.8.6.7 Políticas de backup

Período de almacenamiento de registros de auditoría.

Los registros de aplicaciones que contengan eventos de seguridad significativos deben conservarse durante al menos tres (3) meses. Durante este tiempo, los registros deben estar protegidos contra modificaciones y solo deben ser vistos por personal autorizado. Estos registros son importantes para la depuración, las pruebas forenses, la investigación de infracciones u omisiones de seguridad y otros trabajos relacionados.

Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

Toda la información confidencial y el software de recursos informáticos importantes de un distribuidor de Ambacar deben respaldarse con la frecuencia necesaria y respaldarse con un programa de respaldo. Se deben realizar verificaciones periódicas para asegurar que la información almacenada esté en buenas condiciones.

Copias de información sensible.

Junto con el proceso de clonación de copias de seguridad, debe hacer una copia de cada copia de seguridad para minimizar el riesgo de dañar los discos y los medios de cinta.

3.2.8.6.8 Políticas de uso de firewall

Detección de intrusos.

Cada segmento de red accesible desde Internet debe estar equipado con un Sistema de detección de intrusos (IDS) para que se puedan tomar defensas oportunas contra los ataques.

Toda conexión externa debe estar protegida por el firewall.

Cualquier conexión desde el extranjero al servidor de un distribuidor de Ambacar, ya sea Internet, acceso telefónico o una red externa, primero debe pasar por alto el firewall. Esto es para restringir y controlar los derechos de acceso de la organización.

Toda conexión hacia Internet debe pasar por el Firewall.

El cortafuegos debe ser el único componente conectado directamente a Internet, por lo que cualquier conexión desde la intranet a Internet debe pasar por el cortafuegos.

Filtrado de contenido activo en el Proxy.

El coordinador del sistema del concesionario Ambacar debe asegurarse de que todo el contenido activo (como aplicaciones Java, reproductores Adobe flash, controles ActiveX) se filtre en la definición de la política del concesionario, debido al tipo de datos. Estos datos pueden afectar la seguridad de la información del concesionario Ambacar.

Firewall debe correr sobre un computador dedicado o servidor.

Para esto, cada firewall debe ejecutarse en una computadora o modelo de dispositivo dedicado. Por motivos de rendimiento y seguridad, no se recomienda ejecutar otros tipos de aplicaciones.

Inventario de conexiones.

Se deben mantener registros de conexiones a redes externas para que todos los puntos de entrada a la organización tengan una comprensión clara de lo que se logra con el diagrama de red.

El sistema interno de direccionamiento de red no debe ser público.

La dirección de la intranet y la configuración de la intranet deben estar restringidas de tal manera que los sistemas y los usuarios que no sean de la intranet no puedan acceder a esta información.

Revisión periódica y reautorización de privilegios de usuarios.

Los permisos otorgados a un usuario deben reevaluarse anualmente para analizar si los permisos existentes aún requieren las tareas normales del usuario o si se deben otorgar permisos adicionales. Esta política debe ser aplicada por el área de sistemas con la participación de cada gerente de TI.

3.2.8.6.9 Oficial de Seguridad de la Información

El Coordinador del Sistema es un Verificador de Seguridad de la Información y desempeñará las siguientes funciones:

- Identificar y dar respuesta a las necesidades de formación de los empleados certificados de la empresa en temas de seguridad de la información.
- Actualizar y monitorear periódicamente el mapa de riesgos de los franquiciados de Ambacar, verificar el impacto de cada mapa de riesgos de los proyectos implementados y utilizarlo siempre como base para la implementación de cada proyecto.
- Gestión de incidencias y planificación de seguimiento.
- Crear y establecer un método para categorizar la información en función de su relevancia e impacto en los concesionarios de Ambacar. También es necesario comunicarlo a la organización y verificar que se ha cumplido. El método debe especificar el nivel de acceso a la información.
- Crear y mantener un programa de concientización sobre la seguridad de la información.
- Evalúe continuamente el desempeño de seguridad de la información de su organización para identificar oportunidades de mejora y necesidades de capacitación.
- Revisar y evaluar las políticas de seguridad de la información.

- Informar al presidente sobre el estado de seguridad y protección de la información de la empresa y la necesidad de nuevos programas relacionados con la seguridad de la información
- Establecer y apoyar programas para aumentar la conciencia de seguridad y proteger la información corporativa
- Evaluar la idoneidad, coordinación e implementación de controles de seguridad específicos para nuevos sistemas o servicios de TI.
- Promover claramente el apoyo institucional para la seguridad de la información en toda la organización.
- Supervise y controle la exposición de sus activos de información a cambios importantes en amenazas clave.
- Ver y rastrear incidentes de seguridad de la información. Vigilar la aplicación de políticas, programas y programas que protegen los sistemas, recursos informáticos y servidores en la intranet y centros de cómputo de Ambacar Chartered Company.
- Participar activamente en la revisión, evaluación, mantenimiento, recomendación, mejora y actualización de esta Política por parte de los concesionarios Ambacar.

3.2.8.6.10 Política de uso de portátiles

- El software antivirus debe estar siempre actualizado
- No permita que extraños lo rastreen cuando esté trabajando en un dispositivo móvil, especialmente fuera de un concesionario Ambacar.
- Siga las reglas de acceso remoto
- Toda la información confidencial debe estar encriptada.
- Cuando sea necesario devolver el equipo a un distribuidor de Ambacar para su reparación, mantenimiento, etc.
- La información confidencial debe eliminarse y mantenerse separada para realizar copias de seguridad.
- Se deben crear copias de seguridad de la información del usuario de acuerdo con los requisitos del usuario para las áreas del sistema.
- Proteja su computadora portátil

- No deje las computadoras portátiles en lugares públicos
- Cuando viaje, las computadoras portátiles no deben dejarse en la cajuela de un automóvil y siempre deben llevarse con usted.
- Debe estar en el maletero cuando entres en el coche.
- No preste su computadora portátil a familiares y/o amigos.

3.2.8.6.11 Actualización, mantenimiento y divulgaciones las políticas de seguridad de la información.

Este documento debe revisarse periódicamente o cuando ocurran cambios significativos para garantizar que el dominio del sistema siga siendo relevante, completo y efectivo.

El oficial de seguridad de la información o la persona designada por el presidente ejecutivo debe aprobar el documento y es responsable de ponerlo a disposición y notificar a todos los empleados y partes externas apropiadas. Los mecanismos de notificación y divulgación de cambios a la política de privacidad de la información serán enviados vía correo electrónico.

4.5.7.12. Links de Normativas

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

https://owasp.org/www-project-web-security-testing-guide/

4 CÁPITULO IV CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- AMBACAR realizo en el año 2020 un sistema de gestión de seguridad, el cual, se califica como ineficiente porque no ha sido productivo y eficiente para el desarrollo de sistemas web.
- La protección de cookies de sesión de usuario no es efectiva, ya que, existe facilidad de secuestro de información lo que genera un alto riesgo para la empresa.
- Se elaboro un plan de contingencia con políticas generales de seguridad informática en aspectos como intranet, sitios web, uso de contraseñas, firewall, etc. En base la empresa el cual, reducirá posibles deficiencias en los futuros proyectos.
- El módulo de facturación se dio de baja, debido a que contenía vulnerabilidades significativas como perdida de la información, altos costos para la entidad y no aceptada por los usuarios, misma que desemboca en perdida de clientela y mal servicio al cliente.

4.2 Recomendaciones

- Revaluar periódicamente metas y objetivos del plan de contingencia en base al tiempo y el avance de la tecnología según la necesidad de la entidad y sus requerimientos.
- Capacitar en seguridad informática a los integrantes del departamento de TI de forma eventual para incrementar su conocimiento y aplicarlo en sus labores diarias.
- Aplicar el plan de contingencia de seguridad informática, la cual, contiene lineamientos en base al acuerdo Ministerial 006-2021 del Ministerio de Telecomunicaciones y de la Sociedad de la Información publicado el 17 de mayo del 2021, además de utilizar la guía de pruebas de seguridad web de OWASP.

Bibliografía

[1] H. C. a. I. B. B. Bulgurcu, «"Information Security Policy Complo¡iance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness",» MIS Q., 2010.

[2] M. N. N. Z. J. M. A. a. S. M. M. Humayun, «"Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study",» Arab. J. Sci. Eng., 2020.

[3] S. V. F. a. T. Tuyikeze, «“Information security policy development and implementation: The what, how and who,”,» Comput. Secur., 2016.

[4] J. G. P. a. J. D. W. A. Cram, «“Organizational information security policies: a review and research framework,”,» Eur. J. Inf. Syst., 2017.

[5] E. E. d. Excelencia, «“El papel del Director de Seguridad de la Información en ISO 27001,”,» 2019.

[6] J. Järveläinen, «“Integrated Business Continuity Planning and Information Security Policy Development Approach,”,» 2016.

[7] M. D. C. Escobar Meléndez Jhonatan Sebastián, «“SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO.”,» Ambato, 2020.

[8] I. A. Cárdenas, «“Diseño de una política de seguridad de la información para la Unidad Educativa Borja 3 cavanis, basado en Norma ISO 27002 (Máster en Tecnologias de la Informacióin con Mención en Seguridad en Redes y Comunicación),”,» 2016.

[9] C. Lino, « “Diseño de "Plan de Seguridad Informática para la Cooperativa de Ahorro ‘Por el Pan y el Agua’ de la ciudad de Jipijapa”,» 2019.

[10] N. M. A. a. N. N. G. G. Arias Buenaño, «“Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual,”,» 2013.

[11] G. V. V. a. R. A. R. Morocho, «Vulnerabilidades y amenazas a los servicios web de la intranet de la universidad técnica de babahoyo,» *3c Tecnología,* vol. 6, nº 1, pp. 53-66, 2017.

[12] S. M. D. Diaz, «Pruebas de seguridad en aplicaciones web como imperativo en la calidad de desarrollo del software,» [En línea]. Available: https://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo7_paper_13.pdf. [Último acceso: 5 10 2021].

[13] N. A.-R. ·. J. A. ·. M. Á. C. ·. A. C. ·. G. ·. F. G. ·. H. H. ·. J. K. ·. ANDRÉS, «El impacto de la tecnología en el crecimiento y el empleo,» de *La era de la perplejidad. Repensar el mundo que conocíamos*, 2018.

[14] S. Julio Navarrete, «"Ecuador en riesgo de ciberataques",» 2020.

[15] OMS, OMS, [En línea]. Available: https://www.paho.org/es/enfermedad-por-coronavirus-covid-19#:~:text=El%20Director%20General%20de%20la,puede%20caracterizarse%20como%20una%20pandemia.. [Último acceso: 02 11 2020].

[16] S. Romaniz, «"Seguridad de aplicaciones web: vulnerabilidades en los controles de acceso",» de *XIV Congreso Argentino de Ciencias de la Computación* , 2008.

[17] A. F. F. A. N. I. P. C. J. R. R. C. A. Avila Maldonado, "Módulo de educación presencial del sistema de información sobre ciberseguridad y plataforma educativa", B.S. thesis: Universidad Piloto de Colombia, 2013.

[18] R. M. Slade, «“Security frameworks,”,» Inf. Secur. Manag. Handbook, 2008.

[19] S. Gebremedhin, «“Feature. Information Systems Security Audit. An Ontological Framework”,» 2016.

[20] Instituto Nacional de Ciberseguridad, «Protección de la información,» 2010.

[21] Isotools, «“Sistemas de Gestión de Riesgos y Seguridad. ¿Qué es la ISO 27001?”,» 2022.

[22] M. I. Romero, «Introducción a la seguridad informática y el análisis de vulnerabilidades,» Editorial Área de Innovación y Desarrollo, Quedan, 2018.

[23] C. Tori, "Hacking Ético", Rosario Argentina: Carlos Tori, 2008.

[24] G. Dhillon, «Information Security,» he University of North Carolina at Greensboro, 2017.

[25] C. Easttom, «Computer Security Fundamentals,» Indianapolis, USA, 2016.

[26] N. F. D. a. H. Fulford, «“Aligning the information security policy with the strategic information systems plan”,» Comput. Secur, 2006.

[27] F. K. a. S. G. E. Rostami, «“Requirements for computerized tools to design information security policies”,» Comput. Secur., 2020.

[28] S. G. a. I. N. Chengalur-Smith, «“Metrics for characterizing the form of security policies”,» J. Strateg. Inf. Syst., 2010.

[29] F. K. a. K. H. E. Kolkowska, «“Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method”,» 2017.

[30] S. A. a. I. Chengalur-Smith, «“Evaluating the effectiveness of learner controlled information security training”,» 2019.

[31] K. H. a. G. G. F. Karlsson, «“Practice-based discourse analysis of information security policies”,» Comput. Secur., 2017.

[32] A. Caballero, «“Chapter 24 - Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems”,» de *Computer and Information Security Handbook (Third Edition)*, Boston, 2017.

[33] Departamento Administrativo de la Función Pública, «uía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital,» Bogotá, 2018.

[34] S. C.-G. a. J. G.-C. I. Candal-Vicente, «“Evaluation of Vulnerabilities in Computer Systems Users”,» J. Inf. Syst. Secur., 2017.

[35] OSRI, «“Metodología para la gestión de la seguridad informática”,» 2018.

[36] M. A. a. G. M. Køien, «“Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”,» J. Cyber Secur. Mobil., 2015.

[37] R. S. E. R. J. H. a. M. M. D. Votipka, «“Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes”,» 2018.

[38] H. B. M. B. a. G. A. M. E. Bernardis, «“Seguridad en servicios web”,» de *in XIX Workshop de Investigadores en Ciencias de la Computación*, WICC 2017, ITBA, Buenos Aires, 2017.

[39] National Cyber Security Centre, «“Understanding vulnerabilities”,» 2015.

[40] R. Fattakhov, «“What Is Vulnerability Assessment, and Why Is It Important?”,» Parallels RAS, 2020.

[41] V. Overview, «“5 Cybersecurity Vulnerabilities That Need Strong Policies”,» 2021.

[42] K. Beaver, «Hacking For Dummies,» Wiley Publishing, Inc, 2015.

[43] G. Campus, «“What is Ethical Hacking?”,» 2022.

[44] A. T. a. P. Holtkamp, «“Are users competent to comply with information security policies? An analysis of professional competence models”,» Inf. Technol. People, 2018.

[45] J. S. a. M. Muiru, «“Impact of Information Security Policies on Security Breach Incidences in Kenyan Public Universities: An Observational Approach,”,» Recent Adv. Math. Res. Comput. Sci, 2021.

[46] I. N. d. Cyberseguridad, «“Ciberseguridad en la identidad digital y la reputación online Una guía de aproximación para el empresario índice”,» p.25, 2016.

[47] McAfee Enterprise, «“How Cybersecurity Policies and Procedures Protect Against Cyberattacks”,» 2022.

[48] B. I. d. Desarrollo, «“CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en America Latina y El Caribe”».

[49] O. d. l. E. A. (OEA), «“Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”,» 2018.

[50] A. K. Lab, «¿Qué es la ciberseguridad?,» Resource Center, 2021.

[51] CISCO, «CISCO,» 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~tipos-de-ciberataques. [Último acceso: 8 10 2021].

[52] Iberdrola, «Ataques cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos?,» Innovación, 2022.

[53] R. Wilton, «Internet Society,» 2019.

[54] G. Rivas, «Estos son los 5 tipos de ciberataques más comunes,» 2020.

[55] Hostalia, «"Ataques de inyección SQL: qué son y cómo protegerse",» Pressroom, 2013.

[56] I. E. a. A. Wiradarma, «"Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company)",» Int. J. Comput. Netw. Inf. Secur., 2019.

[57] J. Firch, «"What Are The Different Types Of Penetration Testing?",» PurpleSec, 2021.

[58] A. M. O. Castillo, «Universidad Piloto de Colombia,» [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6863/Introducci%c3%b3n%20a%20las%20pruebas%20de%20penetraci%c3%b3n..pdf?sequence=1&isAllowed=y. [Último acceso: 14 10 2021].

[59] R. López, «"Pruebas De Penetración En Aplicaciones Web Usando Hackeo Ético",» *Tecnológica,* vol. 10, pp. 13-19, 2017.

[60] OWASP, «OWASP,» 2017. [En línea]. Available: https://owasp.org/www-project-top-ten/. [Último acceso: 21 10 2021].

[61] I. R. a. A. Y. W. Yunanri, «"Analisis Deteksi Vulnerability Pada Web Server Open Journal System Menggunakan OWASP Scanner",» Jurnal Rekayasa Teknologi Informasi (JURTI), 2018.

[62] A. L. a. A. Tarigan, «"Security Assessment of Web ApplicationThrough Penetration System Techniques",» *Int. J. Recent Trends Eng.*, vol. 3, nº 1, 2017.

[63] B. B. J. M. S. F. David Riha, «NESSUS Users' Manual,» Southwest Research Institute, 2015.

[64] Subgraph, *"Vega helps you find and fix cross-site scripting (XSS), SQL injection, and more",* 2014.

[65] G. Advisor, «"OWASP ZAP: a powerful tool to discover Websites vulnerabilities",» 2015.

[66] Microsoft, «Windows Server Evaluaciones».

[67] MySQL, «MySQL,» [En línea]. Available: https://misnovelasturcas.club/juego-del-destino/. [Último acceso: 25 10 2021].

[68] Microsoft, «Microsoft,» [En línea]. Available: https://dotnet.microsoft.com/en-us/learn/aspnet/what-is-aspnet. [Último acceso: 25 10 2021].

[69] B. M. B. M. D. O. H. RATHORE, «Information Systems Security Assessment Framework,» Colorado Spring: Open Information Systems Security Group, 2006.

[70] M. S. A. C. O. Karen Scarfone, «Technical Guide to Information Security Testing and Assessment,» Maryland: National Institute of Standards and Technology, 2008.

[71] P. Herzog, «OSSTMM: Open Source Security Testing Methodology Manual,» Barcelona: Institute for Security and Open Methodologies (ISECOM), 2010.

[72] M. A. A. M. MEUCCI, «OWASP Testing Guide 4.0,» OWASP Foundation, EEUU, 2014.

[73] OWASP, «Vulnerability Scanning Tools,» 2022.

[74] PortSwigger, «Burp Suite Enterprise Edition».

[75] OWASP, «OWASP ZAP».

[76] SBGRAPH, «Vega».

[77] TENABLE, «Nessus® Essentials».

[78] J. Petters, «"What is Metasploit? The Beginner's Guide",» *Inside Out Security,* vol. 1, nº 1, 2020.

[79] Zap, «Guía de inicio».

ANEXOS

Anexo A

Figura 41. Carta de compromiso empresarial

Fuente: Elaboración Propia

CARTA DE COMPROMISO

Ambato, 23 de junio de 2021

Ingeniero
Carlos Sánchez
Presidente
Unidad de titulación
Carrera de Ingeniería en Sistemas Computacionales e Informáticos
Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Ingeniero Jorge Parra en mi calidad de Coordinador del área de TI de la Empresa AMBACAR, me permito poner en su conocimiento la aceptación y respaldo para el desarrollo del Trabajo de Titulación bajo el Tema: "Auditoría de seguridad informática al sistema para generar citas y pagos de Facturación del concesionario AMBACAR." propuesto por la estudiante **VANESSA MICHELLE SÁNCHEZ PAREDES,** portadora de la Cédula de Ciudadanía 180534096-3, estudiante de la Carrera de **Ingeniería en Sistemas Computacionales e Informáticos** Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

A nombre de la Institución a la cual represento, me comprometo a apoyar en el desarrollo del proyecto.

Particular que comunico a usted para los fines pertinentes.

Atentamente.

ambacar ltda.

Ingeniero PARRA BARRERA JORGE MARCELO
Coordinador del área de TI de la Empresa AMBACAR
Cédula: 1802668614
Teléfono: 0995024984
Correo: jparra@ambacar.com

Anexo B

Figura 42. Certificado empresarial

Fuente: Elaboración Propia

CERTIFICADO

Ambato, 10 de febrero de 2022

Ingeniera
Pilar Urrutia
Presidenta
Consejo Directivo
Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Ingeniero Jorge Parra en mi calidad de Coordinador del área de TI de la Empresa AMBACAR, certifico que la Srta. **VANESSA MICHELLE SÁNCHEZ PAREDES,** portadora de la Cédula de Ciudadanía 180534096-3, realizo el Trabajo de Titulación bajo el Tema: "Políticas de seguridad informática y vulnerabilidades en el sistema para generar citas y pagos de Facturación del concesionario AMBACAR", ha sido concluido de conformidad a los intereses de la Empresa

Particular que comunico a usted para los fines pertinentes.

Atentamente.

ambacar ltda.

……

Ingeniero PARRA BARRERA JORGE MARCELO
Coordinador del área de TI de la Empresa AMBACAR
Cédula: 1802668614
Teléfono: 0995024984
Correo: jparra@ambacar.com

Anexo C

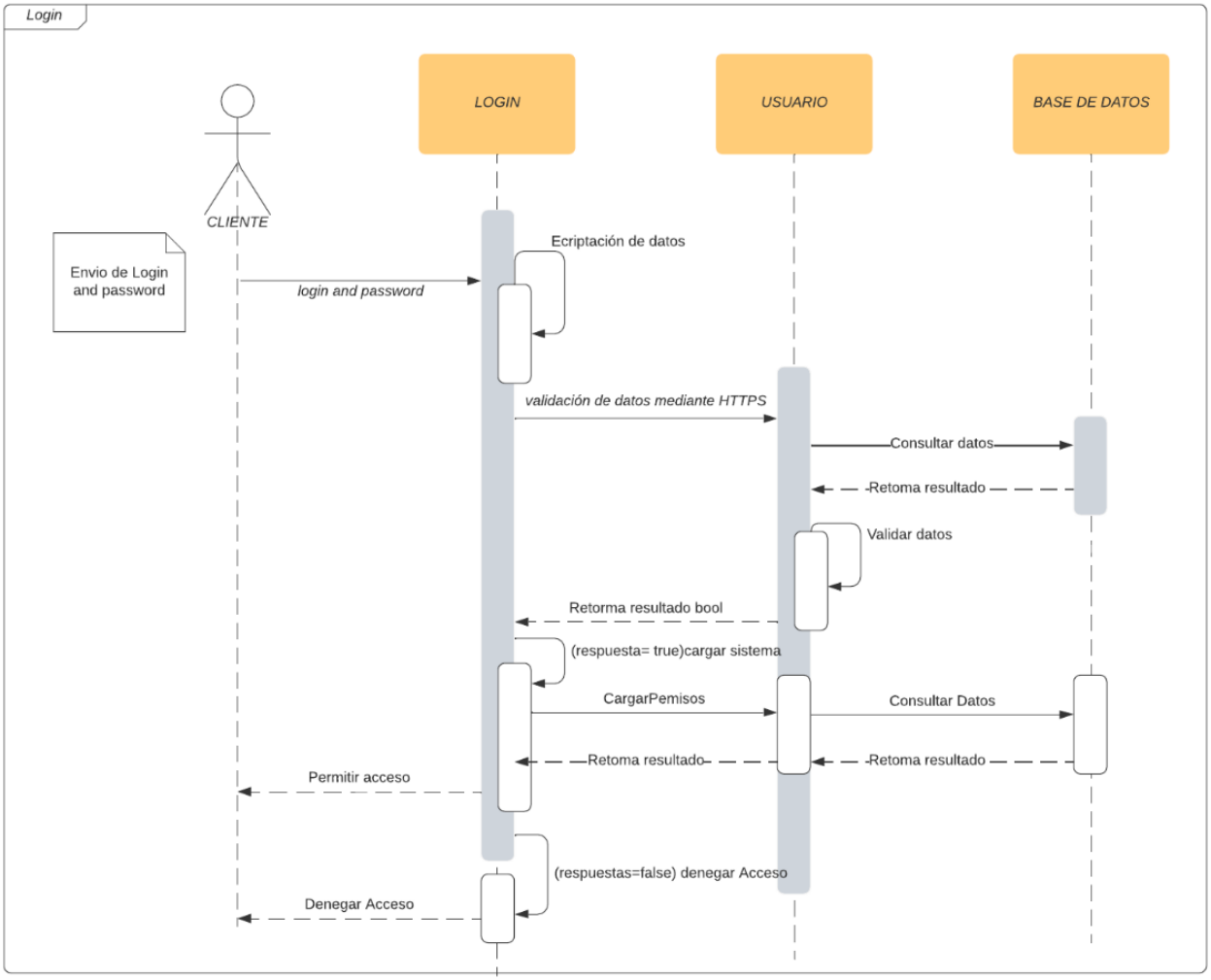
Soluciones a las diferentes vulnerabilidades encontradas, además de acotar que se puede observar técnicas de mejora en el plan de contingencia en el punto **3.2.5.6.6.**

1. Cleartex Password over HTTP

Cuando un formulario contiene un control de entrada de archivo, el atributo enctype siempre debe ser ""de varias partes/datos de formulario, lo que especifica que el formulario se enviará como un mensaje MIME de varias partes.

Figura 43. Diagrama de Secuencia del proceso de envió de datos.

Fuente: Elaboración Propia



2. Session Cookie Without Secure Flag

Riesgo detectado en la línea:

ASP.NET_SessionId=dqjycga33tq5cn55ghdcjjfi; path=/; HttpOnly

Política de atributo seguro de una cookie

Establecer el indicador seguro en verdadero, si este contiene un <forms> debe agregar el atributo requireSSL="true".

<httpCookies requireSSL="true" />

<forms requireSSL="true">

</forms>

3. From Password Field with Autocomplete Enable

Política para la creación de campos

Establecer el indicador de autocompletado en apagado “off”.

<form method="post" action="/form" **autocomplete="off"**>

[…]

</form>

4. Cookie HttpOnly Flag Not SeT

Política de atributo HttpOnly de una cookie

Establecer el indicador HttpOnly en verdadero.

HttpCookie myHttpOnlyCookie = new HttpCookie("LastVisit", DateTime.Now.ToString());

myHttpOnlyCookie.HttpOnly = true;

5. X-frame-Options Header Not Set

Política de X-FRAME-Options en encabezados

Configure el encabezado X-Frame-Options para todas las respuestas que contengan contenido HTML. Los valores posibles son "DENY", "SAMEORIGIN" o "ALLOW- FROM uri", según la necesidad.

X-Frame-Options: DENY

X-Frame-Options: SAMEORIGIN

6. Ausencia de fichas Anti-CSRF

Política de fichas Anti- CSRF

Usar una biblioteca o marco comprobado que no sea vulnerable CSRF o que proporcione construcciones que permitan que esta debilidad sea más sencilla de evitar, la cual se debe aplicar en la fase de arquitectura y diseño.

7. Cookie without Secury Flag

Política de atributo HttpOnly de una cookie

Establecer el indicador HttpOnly en verdadero.

HttpCookie myHttpOnlyCookie = new HttpCookie("LastVisit", DateTime.Now.ToString());

myHttpOnlyCookie.HttpOnly = true;

8. Cross-Domain JavaScript Source Files Inclusion

Política de Archivos de fuente

Analizar y determinar la confiabilidad de las fuentes de JavaScript a utilizar en las aplicaciones que se están desarrollando.

9. Divulgación de la marca de la hora – Unix

Política de divulgación

Borrar los comentarios de HTML/Script antes de enviar al entorno de producción, se puede producir una fuga de información confidencial y contextual.

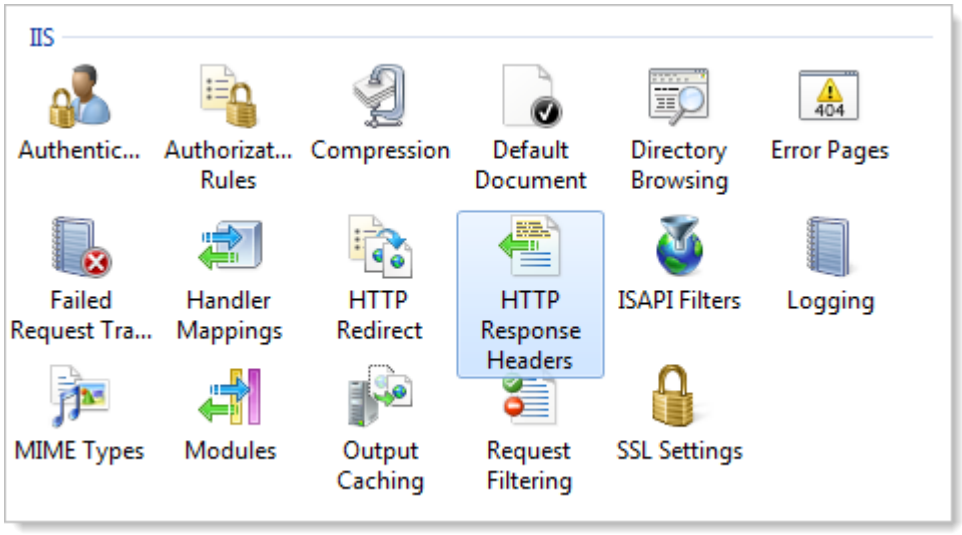
10. X-AspNet-Version Response Header

Política de Encabezados de servidor

Evaluar la necesidad de eliminar los encabezados de respuesta HTTP tanto de servidor, X-Powered-By y X-AspNet-Version, según la necesidad.

Figura 44. configuración de IIS del sitio web

Fuente: Elaboración Propia



11. Incomplete or No Cache-Control Header Set

Política de Directivas de control de cache

Siempre que sea posible, asegúrese de que el encabezado HTTP de control de caché esté configurado con "no-cache, no-store, must-revalidate". Si un activo debe almacenarse en caché, considere establecer las directivas 'public, max-age, inmutable'.

12. X ASPNET-Version Response Header

Política de Encabezados de servidor

Evaluar la necesidad de eliminar los encabezados de respuesta HTTP tanto de servidor, X-Powered-By y X-AspNet-Version, según la necesidad.

13. X-Content-Type-Options Header Missing

Política preventiva de ataques tipo MIME

Establecer el indicador X-Content-Type-Options en nosniff, de este modo se rechazará las respuestas con tipos MIME.

14. Divulgación de información

Usar la política de divulgación anteriormente mencionada.

15. SSL Version 2 and 3 Protocol

Política uso de protocolos de internet

Deshabilitar protocolos inseguros y obsoletos como: SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1.

16. SSL Certificate

Política de confiabilidad de certificados

Revisar periódicamente los avisos relacionados con el certificado SSL, analizar el tipo de aviso para mantener la entrada de los datos de acceso de manera segura.

17. SSH Server CBC Ciphers

Política de cifrado del servidor

Deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.

Anexo D

Tabla 10. Cumplimiento de objetivos.

Fuente: Elaboración Propia

Objetivo	**Medio de verificación**	**Cumplimiento**	
		SI	**NO**
Investigar sobre la tecnología y los procesos utilizados por AMBACAR para crear y administrar páginas web y sus repositorios.	3.1.1 Resultados de la entrevista aplicada. 3.2.2 Fundamentación teórica del Sistema Operativo y de las herramientas que usa su servidor. 3.2.3Diagramas de proceso de creación y administración de páginas web y sus repositos.	X	
Determinar la metodología para el análisis de seguridad.	3.2.4 Análisis Comparativo de Metodologías. 3.2.4.5 Determinación de metodología a través de matriz	X	
Determinar las herramientas open source para el análisis de vulnerabilidades de acuerdo con la metodología seleccionada.	3.2.5 Determinación de herramientas a través de matriz	X	
Proponer soluciones para mejorar la seguridad del sistema para generar citas y pagos	3.2.6 Análisis de las vulnerabilidades Anexo C	X	

de Facturación de acuerdo con las vulnerabilidades y problemas de seguridad encontrados.			