ESCUELA DE INGENIERÍA EN SISTEMAS

Tema:

ANÁLISIS DE SEGURIDAD DE LA PLATAFORMA DE LIBRE COMERCIO ELECTRÓNICO DE LA EMPRESA CORPOAMBATO

Proyecto de investigación previo a la obtención del título de Ingeniero de Tecnologías de la Información y la Comunicación

Línea de Investigación:

Tecnologías de la Información y la Comunicación

Autor:

Alejandro Javier Valle Valle

Directora:

Ing. Mg. Liliana del Rocío Mena Hernández

Ambato – Ecuador

Enero 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

ANÁLISIS DE SEGURIDAD DE LA PLATAFORMA DE LIBRE COMERCIO ELECTRÓNICO DE LA EMPRESA CORPOAMBATO

Línea de Investigación:

Tecnologías de la Información y la Comunicación

Autor:

Alejandro Javier Valle Valle

Liliana del Rocío Mena Hernández, Ing. Mg. **f.**_____

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. **f.**_____

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. **f.**_____

CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. **f.**_____

DIRECTOR ESCUELA DE SISTEMAS

Hugo Rogelio Altamirano Villaroel, Dr. **f.**_____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Enero 2022

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ALEJANDRO JAVIER VALLE VALLE,** con **CC. 150089367-0,** autor del trabajo de graduación intitulado: “ANÁLISIS DE SEGURIDAD DE LA PLATAFORMA DE LIBRE COMERCIO ELECTRÓNICO DE LA EMPRESA CORPOAMBATO.”, previa a la obtención del título profesional de **INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN**, en la escuela de **Ingeniería en Sistemas**

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, Enero 2022

ALEJANDRO JAVIER VALLE VALLE

CC. 150089367-0

AGRADECIMIENTO

Agradezco enteramente a mis padres: Vilma y Nicacio quienes me incentivaron en mi decisión de seguir mis estudios en la universidad, por ellos nunca me rendí en la carrera.

DEDICATORIA

Dedico esta tesis a mi familia, por apoyarme en todo momento en el transcurso de la carrera.

RESUMEN

Las restricciones de la crisis del coronavirus han tenido un profundo impacto en el comportamiento del consumidor, y los servicios de compra electrónica en línea, que se han proporcionado en sitios web y aplicaciones, se han vuelto populares.
Este proyecto de investigación pretende identificar las vulnerabilidades de la plataforma libre comercio electrónico de CorpoAmbato, esto, con el fin de demostrar los riesgos de seguridad al que está expuesta la información privilegiada de los usuarios y a la vez precautelar la seguridad de los usuarios, allí se exponen los productos de pequeños empresarios asociados a la corporación. La plataforma es de reciente creación y para medir su nivel de seguridad, se aplicaron pruebas con diferentes herramientas de escaneo como: OWASP ZAP, Nmap, entre otras, para lo cual no se detectó amenazas relevantes, por lo que se decidió elegir riesgos que, a pesar del nivel bajo de amenaza, estas reciben tratamiento a través del método de reducción, dicha vulnerabilidad, se asocia a los ataques de fuerza bruta. Se utilizó la metodología OWASP pues, se enfoca en el desarrollo de auditorías *web* para el análisis de vulnerabilidades y correcciones de éstas. Además, se utilizaron escalas de valoración definidas por la metodología MAGERIT para que en base a los resultados obtenidos por las pruebas de OWASP, se establezcan puntajes cualitativos y cuantitativos a los riesgos encontrados a fin de centrarse en aquellos de mayor impacto. Así, se plantea un plan con políticas de seguridad y un conjunto de buenas prácticas aplicables a la plataforma.

Palabras clave: Comercio electrónico, seguridad informática, OWASP, MAGERIT

ABSTRACT

The restrictions of the coronavirus crisis have been causing a deep impact on the behavior of the customer, as well as the services of the electronic purchase online, which have been provided by the web sites and applications that have become popular. This research project aims to identify the vulnerabilities of the CorpoAmbato's free electronic commerce platform, in order to demonstrate the security risks to which the privileged information of the users is exposed and also to safeguard the security of the users; due to in this platform are shown the products of the small businesses associated to the CorpoAmbato. The platform is a recent creation; therefore, to review the security level of this, it was necessary to apply some tests with different scanning tools such as: OWASP AP, NMAP, among others; for which no relevant threats were detected, even though it was decided to confront some risks despite the low risks of the scanning tools, one example of this is the brute force attacks which are associated as a vulnerability that can be treated by the reduction method. The OWASP methodology was used because it focuses on the development of web audits for the analysis of vulnerabilities and their corrections. In addition, assessment scales defined by the MAGERIT methodology were used along with the results obtained from the OWASP tests, which establish scores to the risks found, in order to focus on those with the greatest impact. This is how a plan with security policies and a set of good practices applicable to the platform is proposed.

Keywords: E-commerce, IT security, OWASP, MAGERIT

ÍNDICE

PRELIMINARES

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto parte de los conceptos generales relacionados a la seguridad en plataformas de comercio electrónico, las bases principales, sus componentes, términos usados, definiciones, diferentes mecanismos de prevención y corrección en seguridad informática.

Para ello, se señala la importancia que posee tanto la seguridad informática como la seguridad de la información, si bien, se escriben de forma similar, tienen significados completamente distintos, no obstante, el objetivo principal que persiguen es el mismo, de precautelar la información mediante la gestión de riesgos (Romero Castro et al., 2018).

La seguridad informática, se define como el conjunto de normas, procedimientos, métodos y técnicas que forman la disciplina encargada de proveer un sistema de información confiable, por lo cual siempre está presente la gestión de riesgos, es decir, la forma de evitarlo o prevenirlo (López, 2010; Romero Castro et al., 2018). Esto afirma el hecho de que todo sistema está obligado a aplicar políticas de seguridad para controlar el nivel de riesgo que conlleva explotar las vulnerabilidades a las que estaría expuesto. Dichas políticas, no garantizan necesariamente que el sistema este fuera de peligro y sea un sistema seguro.

Como se ha expuesto, las políticas de seguridad son fundamentales en todos los sistemas informáticos, es así que las plataformas de comercio electrónico al gestionar información sensible de los usuarios, requieren de medidas de protección de la información así como buenas prácticas en la implementación de sus servicios;

En el contexto internacional, la Fundación Integra de Murcia, coordinadora del proyecto CECARM (Centro de Coordinación de Emergencias de la Región de Murcia), publica un guía de “Seguridad en el Comercio Electrónico”, la cual establece el estándar EDI (Intercambio Electrónico de Datos) para las transacciones, enfocado en una alta integridad y seguridad en el intercambio de los datos; brinda un esquema normalizado para los sistemas informáticos de quienes participan en transacciones comerciales, además, estructura y ofrecer un medio seguro para el intercambio de información. Sin embargo, esta tecnología está orientada a las grandes empresas que cuentan con el capital necesario para invertir en seguridad de la información, por lo que surge EDIWEB como una alternativa a implementar para pequeñas empresas que buscan establecer formas de

transacciones comerciales seguras (*Electronic Data Interchange*, 2020; Fundación Integra de Murcia, 2010)

Varios estudios (Pineda, 2017; Taque, 2011) demuestran los daños importantes que causan los ataques informáticos a las empresas al no contar con políticas o estándares de seguridad que permitan una respuesta inmediata ante ataques por parte de ciberdelincuentes. Los actos ilícitos suceden en gran mayoría por culpa de los mismos medios tecnológicos por los cuales la empresa, se comunica, lo que ocasiona como desenlace estafas, falsificaciones, sustracción de datos personales, entre otros. Es por ello que el estudio busca concientizar a las empresas y al país sobre la necesidad de reforzar la ciberseguridad no por medio de leyes penales sino mediante la implementación de tecnologías gratuitas de ciberseguridad.

En ese sentido la investigación de Sabillón & Cano M. (2019) señala la importancia del uso del CSAM (*Construction Safety Association of Manitoba*) para aplicar en empresas y naciones como método efectivo de dominios para evaluar controles y respuestas ante amenazas cibernéticas.

El CSAM ha sido diseñado para realizar auditorías de ciberseguridad parciales o completas para un dominio específico, varios dominios o para la auditoría integral de todos los dominios. Según datos proporcionados por CSAM en cuanto al porcentaje de acciones requeridas para fortalecer las medidas de seguridad están: la identificación de vulnerabilidades con un 30%, riesgos cibernéticos con un 60%, activos cibernéticos con un 60%, en recuperación ante desastres 30% y una diversidad de conjuntos de datos estadísticos que dan una idea general del nivel de importancia que tomaría en cada caso ya mencionado (Sabillón & Cano M., 2019).

En el contexto nacional, el Gobierno de la Republica del Ecuador a través Ministerio de Telecomunicaciones (2020), promulga la “Estrategia Nacional de Comercio Electrónico”, que aborda diversos componentes referentes al marco legal, sistemas de pago electrónico, a la logística en los procesos que intervienen y establece líneas de acción que definen buenas prácticas en las que intervienen tanto las empresas, como las áreas encargadas de la implementación de los servicios del comercio electrónico. No obstante, surgen cuestiones de credibilidad en cuanto a establecer un nivel de confianza para los usuarios en los sistemas de transacciones comerciales seguros implementados en plataformas de comercio

electrónico del Ecuador. En ese sentido, en vista de la problemática dada a raíz de la pandemia mundial, los negocios han optado por una forma de comercio moderna y provechosa mediante las ventajas que proporciona el uso de las tarjetas de crédito como un método aceptado para adquirir bienes y servicios desde cualquier lugar establecido para retirar el pedido.

Investigaciones pasadas revelan que el Banco Pichincha contaba con uno de los métodos de transferencia más confiables en su tiempo, usaba un sistema seguro apoyado por la herramienta TCS BaNCS (*Tata Consultancy Services*) considerada por varios expertos como una de las mejores implementaciones bancarias (Telégrafo, 2012). Sin embargo, los sistemas de seguridad han ido en evolución constante al pasar los años hasta llegar a implementar un sistema altamente confiable en los bancos del Ecuador, lo que ha resultado en el cambio del modus operandi de los ciberdelincuentes al centrarse en ataques que aprovechan el descuido del usuario al desconocer los peligros que enfrentan en cuanto a: correos falsos, links de páginas falsas, premios engañosos, entre otros, lo que conllevan al engaño, fraude, robo extorción u otro tipo de delito informático (Saltos Salgado et al., 2021). En conclusión, a pesar de los esfuerzos enfocados en la seguridad informática y campañas de prevención de varias entidades bancarias, no excluye totalmente a los usuarios de sufrir estafas en cuanto a pérdida y difusión de datos personales por motivos mencionados anteriormente.

En lo que concierne a la protección de información en el área del comercio electrónico está el estudio de Becerril (2019), el cual afirma que tanto gobiernos o empresas de cada país son responsables de elaborar estrategias de implementación de ciberseguridad que permitan establecer una posición en el mercado del comercio electrónico de tal forma que de paso a la inversión extranjera. Así mismo, el comercio electrónico estaría sujeto a un marco normativo que no represente un impedimento en lograr un desarrollo y crecimiento económico, sino proporcionar la seguridad jurídica para personas que deseen emplear medios electrónicos y no convencionales como forma de comercio. Con eso en mente, la ciberseguridad es implementada con objetivos específicos con la capacidad de solucionar aspectos asociados a la gestión de riesgos, con respeto a los derechos humanos y orientada al enfoque *multistakeholder.*

La investigación de Escalante & Molina (2018), de igual manera establece estrategias para responder a incidentes de inseguridad ambientado a la legalidad ecuatoriana. Las estrategias estan basadas en el estándar internacional de tal modo que, a raíz de un incidente informático, se otorguen los permisos necesarios para actuar en función de cumplir la legalidad ecuatoriana. Dichos permisos, responden los motivos por los cuales realizan las pruebas de identificación que actúan conforme a las políticas internas establecidas. El estudio muestra de resultado como, cuando, donde y quien manipulo tanto los indicios digitales como los dispositivos digitales.

En Ecuador la problemática de los delitos informáticos, desde el año 2014, han ido en aumento; hasta el mes de agosto del 2020, se han registrado más de cinco mil delitos informáticos (Ramos, 2020a), esto debido a que actualmente convive con un manejo masivo de información privilegiada por parte de los usuarios, que cada día, se interconectan a todos los niveles productivos, financieros y de salud en la sociedad (Ramos, 2020b; Muro & Ramírez, 2000). Al respecto, se señala que este manejo de información masiva en la web requiere un mayor nivel de control de seguridad contra los ciberdelincuentes; estas son personas mal intencionadas, que mediante la explotación de vulnerabilidades situadas en plataformas *Web*, buscan comprometer los datos de los usuarios (Ramos, 2020a). Dicha información está asociada principalmente a las transacciones comerciales en línea, pues éstas sufren transgresiones como: suplantación de identidad, robo de números de cuenta y tarjetas de crédito, entre otros; y posterior a eso, ser utilizados de manera fraudulenta (Ramos, 2020b; Chiriguayo-Lozano, 2015; Monsalve-Pulido et al., 2014)

El comercio electrónico a nivel mundial es tan amplio y, debido al confinamiento, en Ecuador durante los meses febrero a marzo, se incrementó en un 1500% el uso de plataformas web para fines comerciales, (Ramos, 2020a) así como las probabilidades de recibir ataques que perjudiquen virtualmente la información.

A pesar de estos inconvenientes descritos, el comercio electrónico es una realidad que las empresas y organizaciones nacionales y locales tienen la obligación de implementar las mejores prácticas y herramientas que brinde un servicio seguro a sus clientes. CorpoAmbato, es una organización que acoge a pequeños emprendedores y consciente de que el mecanismo para mantener los negocios

activos era el comercio electrónico, implementó un portal de libre comercio electrónico actualmente habilitado y en crecimiento, al servicio de la ciudad de Ambato y del país. Dentro del proceso de implementación del portal, no se incorporaron estándares de seguridad, por lo que la información sensible de los usuarios posiblemente se encuentra en riesgo con los servicios que actualmente están implementados.

Con estos antecedentes, se plantea para la investigación el siguiente problema científico: el nivel de seguridad implementado actualmente en la plataforma de libre comercio electrónico de la empresa CorpoAmbato no permite cubrir las necesidades de protección de información privilegiada de sus usuarios frente a amenazas internas y externas, lo que desemboca en delitos informáticos.

A partir del problema antes descrito, parte de la investigación, se enfoca en utilizar una metodología adecuada para que, mediante la experimentación, se demuestre la siguiente hipótesis científica: el sistema de seguridad implementado actualmente en la plataforma de libre comercio electrónico de la empresa CorpoAmbato, no protege íntegramente la información privilegiada de sus usuarios frente amenazas internas y externas.

Tras una breve explicación sobre los rasgos más notables de la problemática planteada, la investigación, se enfoca en incrementar el nivel de seguridad en plataformas de comercio electrónico, a través del siguiente objetivo general: Analizar la seguridad de la plataforma de libre comercio electrónico de la empresa CorpoAmbato, por medio de la identificación de vulnerabilidades sobre la gestión de la información privilegiada de los usuarios CorpoAmbato, lo que, a su vez, exige cumplir con los siguientes objetivos específicos:

1. Fundamentar teóricamente aspectos de seguridad de las plataformas de libre comercio electrónico que son sensibles de considerar para mantener sitios seguros.
2. Identificar las vulnerabilidades en la plataforma de comercio electrónico con el fin de medir el nivel de riesgo existente y los posibles ataques.
3. Analizar los resultados para determinar los niveles de seguridad requeridos.
4. Proponer un plan de seguridad y buenas prácticas aplicable a la plataforma de comercio electrónico de la empresa CorpoAmbato.

Para establecer un orden lógico a lo largo del desarrollo del proyecto es necesario trabajar en base a una metodología que permita delimitar reglas, permisos y estándares necesarios para realizar buenas prácticas de seguridad. Este proceso incrementa el nivel de confianza en las organizaciones que analizan sus sistemas de seguridad para alcanzar los mejores resultados en lo que corresponde resguardar la información privilegiada.

Para tal efecto, existen varias formas de experimentación en relación a la seguridad de la información por medio de varias metodologías que permiten la ejecución de auditorías de código, pruebas de penetración, programación segura y aplicación de cualquier tipo de ataque a lo largo de la trayectoria de pruebas de penetración (Wagner, 2016). Esto aclara la idea de que para mantener un sitio seguro no basta con implementar políticas o estándares de seguridad, pues resultaría necesario una serie de pruebas por medio de la identificación de vulnerabilidades e identificar como es aprovechado por los ciberdelincuentes.

En base a lo mencionado, la metodología OWASP es la guía principal del desarrollo del proyecto, pues, se enfoca en la utilización de auditorías web para el análisis de vulnerabilidades y correcciones de éstos lo que, a su vez, refleja en la elaboración de un plan que contenga políticas de seguridad y un conjunto de buenas prácticas. OWASP (Proyecto de Código Abierto), es una fundación sin ánimo de generar ingresos económicos que busca, mediante su enorme comunidad, brindar de proyectos de investigación de seguridad *web*, para que, los usuarios hagan uso de la información proporcionada, detecten y eviten riesgos relacionados a la seguridad de información en sistemas de *software* de aplicaciones. Su repertorio cuenta con cientos de trabajos documentados en ensayos, guías, informes y proyectos elaborados por miembros de la fundación expertos en el área de seguridad (*OWASP Fundation*, 2020). Con esto en mente, se define a OWASP como una metodología de revisión transparente y participativa sobre la seguridad en torno a las auditorías *web* y encaminada al análisis de seguridad de aplicaciones *Web*, y usada como referente en distintas actividades de auditorías *web.*

En relación con lo indicado, OWASP posee dos modalidades de revisión de seguridad, los cuales son: OWASP TOP 10 y OWASP completa, para el proyecto, se trabaja con la guía de pruebas OWASP como principal enfoque de auditoría, es

la recomendada si se da por primera vez una situación que requiera estudiar la seguridad o si la seguridad de este entorno no es crítica para la empresa.

El uso de una metodología como OWASP, se justifica por cuanto consta de un marco de pruebas encaminadas a una serie de actividades para detectar y evitar riesgos de seguridad *web* tales como fallas de inyección, que ocurren si se envían datos que no son de confianza a un intérprete como parte de un comando o consulta; perdida de autentificación de usuario debido a una incorrecta implementación de sesiones como principal causa de pérdidas de contraseñas por acciones de usuarios mal intencionados; y el riesgo de sufrir difusión de datos que terminan con resultados desfavorables al usuario como: fraude con tarjetas de crédito, robo de identidad u otros delitos (OWASP, 2020).

Como se observa, es fundamental mitigar los riesgos a los que están expuestos los portales de comercio electrónico, más aún en el caso de CorpoAmbato que tiene como objetivo a futuro añadir más de mil emprendimientos en su plataforma, por lo que la cantidad de información en el servidor aumentaría en a un punto que obligaría a la empresa a tener un control masivo de información privilegiada.

De ahí, se desprende el compromiso de la empresa de integrar políticas de seguridad y un conjunto de buenas prácticas para que los administradores de la plataforma resguarden la información de sus usuarios y mediante el seguimiento de guías de auditoría de seguridad, detectar y reducir la probabilidad de sufrir ataques que giran en torno a la vulneración de la información sensible de los usuarios que en su mayoría surgen por personas mal intencionados o ciberdelincuentes.

A pesar de que la empresa, no se encuentra en una situación urgente que dependa de un análisis extenso de seguridad de información, por lo que no está en su obligación invertir en los aplicativos de políticas y estándares de seguridad, que se definan en el proyecto, sigue en constancia el hecho de poseer como opción a emplear los resultados del proyecto acerca de la identificación de vulnerabilidades, riesgos y pruebas de auditorías, que se utilizan como referencia cuando la empresa tenga la motivación de desarrollarse en el comercio electrónico y posicionarse en el mercado a través de la implementación de módulos afines al control y posesión de información sensible tales como métodos de pago, publicidad, transporte, entre otros.

CAPITULO I. ESTADO DEL ARTE Y LA PRACTICA

1.1 Comercio electrónico

Para iniciar con la temática de investigación, es importante conceptualizar al comercio electrónico, con base en el criterio de varios autores citados a continuación:

Tabla 1. Concepto de Comercio electrónico

Autor	Concepto
(González, 2020)	El comercio electrónico, se contempla como una moderna forma de conseguir bienes y servicios que han alterado las transacciones comerciales de los compradores tanto de familias como en empresas.
(Sigmond, 2018)	Es un servicio exclusivo de los usuarios que aprovechan los beneficios que ofrecen los canales electrónicos (internet) para comprar y vender productos o servicios.
(Álamo, 2016)	El comercio electrónico, se define como toda actividad de comercialización propia de los mercados tradicionales mediante el uso de publicidad, búsquedas de información sobre productos, servicios y proveedores aplicación del pago electrónico y servicios post-venta.

Fuente: elaboración propia

A partir de los resultados antes mencionado, se distingue al comercio electrónico como el conjunto de actividades comerciales dentro de una empresa, organización, negocio o familia ya sean encauzados a la compra o venta y todo esto realizado a través de herramientas tecnológicas que empleen como medio principal de transporte de información, el internet.

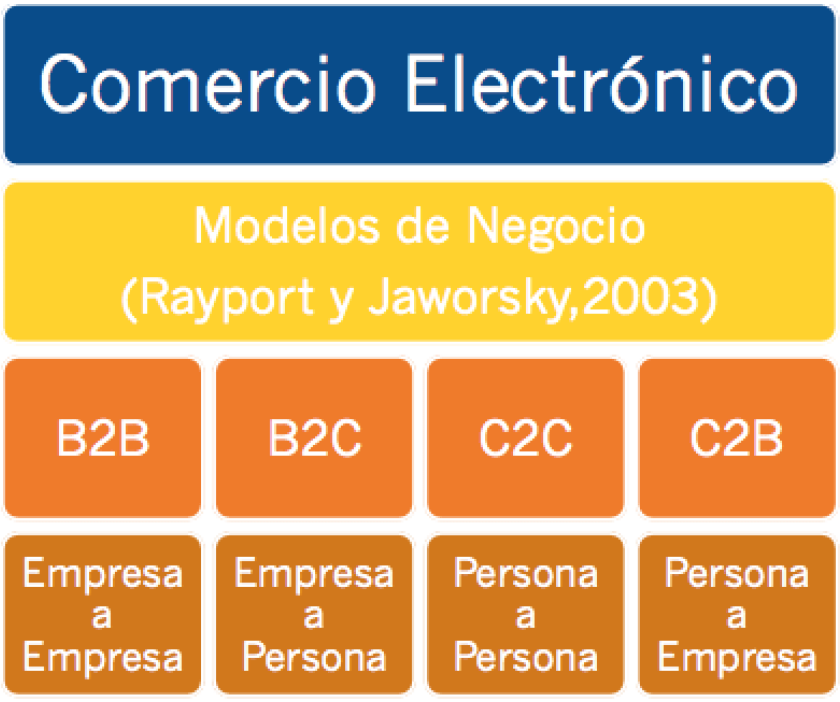
Es necesario incidir en el acelerado crecimiento que ha tenido el comercio electrónico a partir de los inicios de la pandemia en el año 2019, pues, ha tenido un impacto profundo en las personas principalmente en los comerciantes locales, lo que los deja en condiciones vulnerables de grandes pérdidas económicas al no contar con un medio de comercio por internet, no obstante, ha dado paso a considerar como obligatorio el uso del comercio electrónico como una opción viable

para adaptarse a la situación urgente. Por ello, es correcto decir que el comercio electrónico ha sustituido los modos habituales en las que las empresas y negocios realizaban transacciones comerciales de bienes y servicios por herramientas tecnológicas como plataformas web o aplicaciones móviles.

Tipos de comercio electrónico

Existen estudios sobre los tipos de comercio electrónico existentes en el área del comercio electrónico(RockContent, 2018; Murillo, 2009) que son aplicados según el modelo de negocio que requiera:

Figura 1. Tipos de Comercio electrónico



Fuente: tomado de Andoni Villarreal (2018)

El autor da a conocer los tipos de comercio electrónico, que se tienen a disposición para implementar de acuerdo a las actividades que el negocio se dedica, por ejemplo, investigar a quien, o qué tipo de personas van a vender los productos o servicios constituye una forma de comprobar el tipo de *e-commerce* que demanda el negocio.

Seguidamente, los modelos de negocio *online* poseen características que los diferencian unos con otros, cada uno de ellos están destinados a emplearse en diferentes entornos de trabajo. En ese sentido, como primer punto, está el modelo B2B *(business to business)* el cual, significa en español “negocio a negocio”, se

enfocan en aquellas empresas, que se dedican exclusivamente al comercio electrónico (internet) e igualmente mantienen relaciones comerciales sin más que para empresas de la misma categoría de negocio. Por otro lado, el modelo B2C (*business to customer*), busca establecer una relación comercial con el cliente en general, es decir, no distingue entre pequeñas, medianas y grandes empresas. Luego están los negocios C2C (*customer to customer)*, orientadas a personas que buscan vender un producto por el mismo motivo por el cual ya no lo necesitan o buscan sacar utilidad de ello, por ejemplo, la compra de un producto por parte del consumidor final para posterior a eso venderlo a un cliente de otro mercado, lo que da origen al término C2C. Del mismo modo el modelo C2B *(consumer to business)* establece como objetivo principal ubicar a la empresa como el demandante y al cliente como el que realiza la oferta del producto, o sea, la operación de compra venta del producto o servicio empieza por los estándares que el cliente disponga (Golan, 2020; Murillo, 2009).

Conviene explicar que el comercio electrónico no es solo vender o comprar bienes y servicios por internet, sino que abarca situaciones más complejas como en el caso de ayudar a determinar del modelo de negocio en la que una empresa funcionaría en base a los procesos internos ejecutados en su entorno de trabajo.

Elementos de un *eCommerce*

Según la Escuela de Administración, Liderazgo, Dirección y Emprendimiento (2017), una plataforma de comercio electrónico es considerada como tal si tiene los siguientes elementos:

- La página de inicio es lo primero que el usuario observa al entrar a sitio web. Cuenta con buscadores de productos o servicios.

- El Catálogo muestra al usuario los productos disponibles en el sitio, cada producto tiene los rasgos que buscan los consumidores como: precio, tipo, características, valoración de los usuarios, vendedor y disponibilidad, entre otros.
- Al decir fichas de producto, se describen como funcionalidades de la plataforma al disponer con descripciones de búsqueda fácil, fotografías ampliables, características de producto, coste final, gastos de envío, disponibilidad, tiempo previsto de entrega, enlaces de información de garantía del producto y un botón siempre visible para iniciar la compra.
- El carrito de compra por lo general, se encuentra ubicado en la parte superior izquierda de la plataforma y, se encarga de guardar las compras que el cliente registra antes de realizar el pago.
- Preguntas frecuentes o FAQs una ventana que proporciona las normas y políticas de compras, envíos, reembolsos, ofertas, facturas y garantías que ofrece la plataforma

Con respecto a lo mencionado, cada elemento cumple con una función esencial en el funcionamiento de una plataforma de comercio electrónico como lo es la interacción entre la interfaz y el usuario, todo esto tiene como fin el retener al usuario en función de establecer recurrencia y recompra en la plataforma.

Tipos de plataformas de comercio electrónico

Actualmente en el basto espacio de la red existen una diversidad de plataformas de tiendas *online,* por lo que resulta difícil elegir entre una de ellas, puesto que cuentan con funcionalidades que el otro no posee y viceversa. En ese sentido, la empresa *Diligent Team* (2017), dedicada al desarrollo de sitios *web* personalizados, menciona que, es necesario establecer una comparativa sobre las plataformas más utilizadas en la red que permitan una análisis previo sobre las características como: tecnología, seguridad, flexibilidad, localidad e integración.

Tabla 2. Cuadro Comparativo de Plataformas de comercio electrónico

	Tecnología	Seguridad	Flexibilidad	Localidad	Integración
MAGENTO	-PHP + MySQL -Mature -Zend Framework -Expensive to run	-High secure	-Very powerful -Fully customization -Custom statuses -Complex to create themes	-Multishop -Multilanguage -Multicurrency	-Old API -Lots of plugins avvailable
PRESTASHOP	-PHP + MySQL Requirements are not so big	-High secure	-Very powerful -Fully customization -Custom statuses -Compex to create themes	-Multishop -Multilanguage -Multicurrency	-Plugins available -Quite Old API -Quite Old Source Code
WOOCOMERCE	-PHP + MySQL -Wordpress -Runs on smaller machines	-Wordpress is very unsecure but is updated frequently	-Not as flexible as other platforms but much simple to use	-One single shop -Multilanguage via plugin -Single currency	-Lots of Wordpress plugins -Good API
SHOPIFY	-Proprietary software as a Service -Themes using Liquid	-Very secure	-Not flexible -Not hierachycal categories	-Single shop -Single language -Single currency	-Lots of apps available -Very good API -Apps use too much JavaScript which impacts in performance

Fuente: tomado de Diligent Team (2017)

En referencia a lo expuesto la empresa *Diligent Team* (2017) no busca categorizar entre rangos de bueno y malo a las plataformas ya mencionadas sino dar a conocer sus ventajas en cuanto a recomendar o descartar el uso de una plataforma implementar en el negocio por medio de caracterizar sus funcionalidades.

Al observar el cuadro comparativo acerca de las plataformas de comercio electrónico mostrado con anterioridad coincidiría que todas son muy buenas opciones para implementar, una plataforma, no se elige por la cantidad máxima de funcionalidades que posea sino en función de las características y requerimientos que exija la empresa o negocio. No obstante, hay que recalcar que la mayoría las plataformas son de código abierto (*Open Source*) a excepción *Shopify,* por lo que resulta desfavorable para aquellas personas que no posean los recursos económicos necesarios.

Componentes de plataformas de comercio electrónico

Una plataforma para funcionar de manera óptima utiliza distintos elementos de sistemas de información, algunos funcionan de forma invisible al ojo humano y otros por lo general, se presentan en todo momento al usuario, sin embargo, esto no cambia la importancia de su labor al encargarse de todas las gestiones de actividades que mantienen en funcionamiento a la plataforma.

Front End

Según Somalo (2017), es básicamente la *web* que el usuario observa al ingresar al sitio, es decir, la herramienta principal para establecer comunicación entre la plataforma y el cliente o usuario. En resumidas cuentas, es el apartado con el que el usuario va a interactuar de forma intuitiva la mayor parte del tiempo, por lo que no necesita comprender como funciona en realidad el proceso de ejecución de código por cada acción que realiza, por ejemplo, presionar un botón o enviar un mensaje.

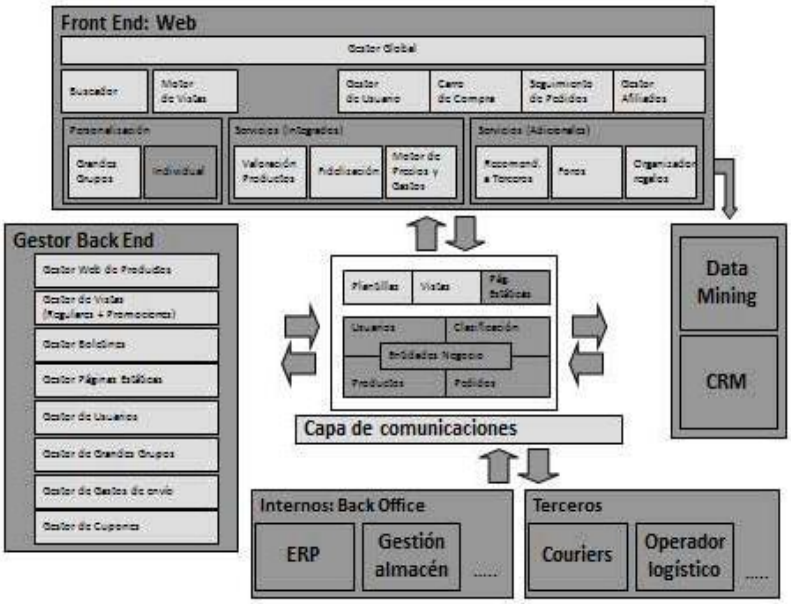
Back End

Es todo complemento o funcionalidad de las herramientas de la plataforma que no son perceptibles al usuario o cliente, o sea, está asociado a la gestión del catálogo

de productos, espacios comerciales y contenidos, ventana de pedidos, gestión de ofertas, facturación, gestor de usuarios, entre otros (Somalo, 2017).

Un ejemplo claro y conciso acerca de los componentes que posee una plataforma y como están estructurados, se exhibe a continuación:

Figura 2. Esquema de sistemas comercio electrónico y sus correlaciones



Fuente: tomado de Somalo (2017)

Esto en resumidas instancias constituye la categorización de todas las herramientas que funcionan y relacionan tanto interna como externamente en la plataforma, algunas de las cuales se mencionamos a continuación: ERPs, Sistemas de Gestión Almacenamiento o Logísticos, sistemas de atención al cliente, proveedores, EPLs, transportistas entre otros.

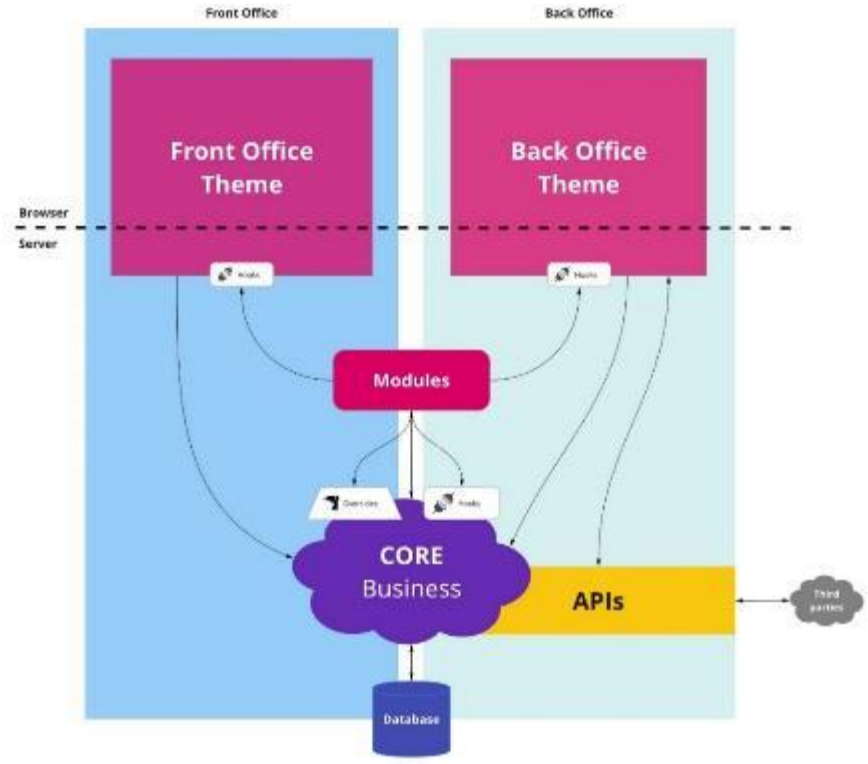
Arquitectura de plataformas de comercio electrónico

Varias investigaciones sostienen que, la arquitectura de un sistema abarca todos los componentes básicos y conceptos significativos, que se establecen en una plataforma de modo que los creadores de contenido y los administradores interactúen con la misma, ya sea encaminada al comercio electrónico o cualquier tipo, todo depende de la naturaleza del negocio (Winkels, 2019; Zuñiga, 1999). A la vez, la empresa FourWebs (2019) especializada en diseños *web,* afirma que la

mayoría de arquitecturas de plataformas web, se basan en el SEO (*Search Engine Optimization*), es una fuente principal de aplicación y clave del éxito para desarrollos de plataformas *web* en general, el cual, cuenta con cuatro tipos de arquitecturas funcionales tales como arquitectura vertical, plana, de silos, *all link structure* y a medida. Por otro lado, varias investigaciones (García, 2017; Torres R. et al., 2015), coinciden en que el uso MVC (Modelo Vista Controlador) constituye una fuente principal de guía en el desarrollo de plataformas de cualquier tipo que requieran, pero orientadas a instaurarse en PYMES (Pequeñas Y Medianas Empresas). En definitiva, existen variedad de arquitecturas aplicables en plataformas de comercio electrónico, que son adaptadas en función de las características del negocio, no obstante, existen plataformas comerciales, las cuales no se moldean o adaptan al gusto del negocio, pues cuentan con un formato preestablecido y, por lo tanto, no requiere seguir los pasos que giran en torno al desarrollo de plataformas desde un inicio, basta con instalar en el servidor de la empresa y configurar los módulos disponibles.

En referencia a lo mencionado, aparecen los sistemas CMS (*Content Management System*) como una herramienta de *software* fácil de crear, administrar y gestionar orientado mayormente a tiendas online cuya característica principal recae en la separación de la GUI (Graphical User Interface) del contenido (Base de datos), lo que permite que usuarios sin conocimientos básicos de informática configuren y ensamblen una plataforma web (Alonso, 2018; Bojorque, 2008). En otras palabras, todos los sistemas gestores de contenido poseen una arquitectura que permite gestionar el contenido de forma independiente al diseño como es el caso de Prestashop:

Figura 3. Descripción básica de la arquitectura de *PrestaShop* 1.7



Fuente: tomado a partir de guías de *Prestashop* (2019)

Como se observa, *Prestashop* asume una característica principal que diferencia al resto de gestores de contenido como es la utilización de módulos para soluciones personalizadas de control y manejo de información tanto de la tienda como de los usuarios. Por esta razón, como se evidencia en la tabla 2, destaca la ventaja que la plataforma de *Prestashop* al ser gratuita y poseer varios módulos, los cuales permiten agregar funcionalidades adicionales que mejoran el servicio en cuanto a la gestión de contenido enfocado al negocio *ecommerce.*

Seguridad en plataformas de comercio electrónico

Con respecto a la seguridad orientada al comercio electrónico, se considera aspectos y conceptos importantes, por ejemplo, requisitos, normas, estándares, protocolos, detallados a continuación:

Requisitos la seguridad

Varias instituciones (Instituto Nacional de Ciberseguridad de España, 2020a; Fundación Integra de Murcia, 2010) a través de estudios consideran las siguientes características básicas para que la seguridad en el comercio electrónico esté presente en todo momento.

- Autenticación en todos los medios de acceso a través del uso de claves de autenticación que permitan verificar la identidad de los usuarios y a la vez proteger sus datos confidenciales.
- Confidencialidad por medio de técnica de encriptación y de codificación de datos para mantener de incógnito la información sensible de usuarios en la red.
- Integridad de la información de los usuarios, pues evitaría la modificación y cambio de información que por lo general acaba en la suplantación de identidad u otras transgresiones, por lo que resulta beneficioso el uso de firmas digitales.
- No repudio, se refiere evitar casos en los que los usuarios sin su consentimiento estén en participación con la transmisión de información de información privilegiada.

Con lo anterior expuesto, se define a los requisitos de seguridad como los estados en los que el sistema del comercio electrónico se encuentra y mantiene en todo momento para establecer confianza en los usuarios en cuanto a protección de datos en medios de comunicación empleados principalmente para transacciones electrónicas.

Normas y estándares de seguridad

Los estándares de seguridad orientados al comercio electrónico por lo general están relacionadas a los sistemas de pago disponibles en internet, los cuales atienden al resguardo de la confidencialidad, integridad y disponibilidad de la información que la empresa o negocio figura en la plataforma para brindar una forma segura y rápida de pago en línea (Basantes Andrade et al., 2016). Algunos de los estándares, que se encuentran operativos en la actualidad, se detallan a continuación:

Estándar ISO

Las normas ISO *(International Organization for Standardization)* constituyen una serie de documentos que son utilizados como guías en una organización para garantizar que los servicios o productos ofrecidos por dicha organización, se lleven a cabo con las especificaciones correspondientes. En ese sentido el autor, Arriola (2018) hace mención a la familia de estándares de la categoría ISO 27000, en ella, se exponen guías, requisitos, directrices y técnicas de seguridad para emplear y mantener segura la información de la empresa. A la vez, la Organización Internacional de Normalización (2020) define a dicha familia de estándares como el conjunto de requisitos necesarios para que la gestión activos de información tales como información financiera, datos de empleados o información sensible de terceros, se mantenga segura. Por otro lado, la investigación de Díaz et al (2020) confirma la importancia del empleo de estándares, protocolos, métodos, reglas y herramientas como procedimiento principal para reducir los riesgos y amenazas dentro del entorno de la información tales como software, programas plataformas, bases de datos, archivos entre, otros.

De acuerdo con lo mencionado en lo anterior, la certificación ISO ofrece fuentes confiables de información sobre estrategias que buscan cómo mantener segura la información, representa el activo más importante y por ende intangible de la organización o empresa que decida confiar en utilizar el estándar ya mencionado.

Estándar IEEE

El estándar IEEE *(Institute of Electrical and Electronics Engineers)* es la organización encargada de estandarizar y registrar el avance e innovación de la tecnológica en beneficio de la humanidad a través del apoyo de más de miles de ingenieros, científicos, tecnólogos y profesionales capacitados en el área (Instituto de Ingenieros Eléctricos y Electrónicos, 2018).

Instituto Ecuatoriano de normalización

Según el gobierno nacional del Ecuador está contemplado por la sociedad como la organización encargada de ofrecer procesos establecidos en el Sistema ecuatoriano de la calidad para satisfacer la demanda nacional en los campos de normalización. Con eso en mente, dicha organización establece normas, controles,

requisitos, estrategias y técnicas basadas en el estándar ISO para aplicar en aquellas instituciones nacionales que, a raíz de un análisis y evaluación profundo del sistema, necesiten mantener segura la información.

Hosting

Para la empresa Neubox (2020), es un espacio, donde se guardan datos informativos de un sitio en Internet como son: paginas HTML, imágenes, documentos, videos, correos, entre otros. Por otro lado, el autor Cabello (2015), define al *Hosting* como un servidor externo, donde se alojan paginas o documentos web para que los clientes gestionen y consulten con ellas para obtener resultados. Simultáneamente, el autor Martinez Rolan (2019) concuerda que, el *hosting* es, donde se depositan todos los archivos de formato multimedia, es decir, imágenes, videos, documentos para mostrarse en la página web.

Con respecto a lo expuesto, el alojamiento o *hosting* en gran mayoría, se la utiliza para publicar en la red una página *web* de cualquier tipo y la información publicada depende de cuanto almacenamiento haya contratado el cliente para trabajar en función del tráfico de usuarios que naveguen dentro de la misma.

Certificados de seguridad

Para la empresa Nerion (2020), los certificados de seguridad sirven para que la información viaje de forma cifrada por medio del mecanismo criptografía asimétrica, es decir, claves publicas entre el navegador del cliente y el servidor, por lo que el nivel de seguridad depende del algoritmo del certificado. A la vez, el autor Soriano (2014) menciona que un certificado es un documento electrónico almacena una firma digital para asociar a una clave publica con una identidad, el nombre de una persona o una organización. En ese sentido, estudios en el área (Organización SSL.com, 2020), mencionan que, existen varios certificados clasificados a través de la autoridad de certificación como: validación de dominio (DV), de organización (OV), individual (IV) y extendida (EV).

Como se expuso en el anterior párrafo, los certificados son una pieza esencial para que cualquier sitio web tenga visitas de forma segura para los usuarios, se evidencia que la información que viaja por el sitio web está cifrada por la empresa encargada de alojar la página.

Protocolo HTTP

El protocolo HTTP *(Hypertext Transfer Protocol)* según los estudios de Avellaneda et al. (2014) son notaciones de los elementos de comunicación *web* gestionados por el protocolo antes mencionado para transmitir todo tipo de contenido. Por otro lado, los autores JULIO et al. (2020), coinciden en que, es el protocolo más utilizado en la internet para transferir páginas *web* entre el navegador y el cliente a través del reconocimiento y la ejecución de una URL *(Universal Resourcer Locator).* Por otro lado, estudios similares (Heredia, 2015) afirman que, es un proceso gestionada por la WWW *(World Wide Web)* para el intercambio de información a través de varias plataformas, en el cual el cliente solicita información al servidor HTTP.

Una vez mencionadas las anteriores definiciones, se entendería al protocolo HTTP como el conjunto de normas y especificaciones únicas ubicadas en la capa de aplicación para el reconocimiento de métodos o solicitudes enviadas entre el servidor y el cliente.

Luego del análisis bibliográfico, se encuentran evidencias sobre la inseguridad respecto a plataformas de comercio electrónico, los cuales se refieren a la gran cantidad de casos de estafas vía internet que son compartidos día a día por las redes sociales como *Facebook,* muchos suceden por no realizar las preguntas necesarias para comprobar la validez del comerciante. Es así, como el caso de una persona en Ecuador, el cual perdió cuatrocientos dólares al querer comprar una laptop en un sitio *web* que a simple vista parecía una plataforma confiable (Rosero, 2020). El mismo sitio *web* o plataforma de comercio electrónico, se borró al instante de concretar la compra y en consecuencia desprestigia y perjudica a las plataformas de comercio electrónico similares que si funcionan de forma legal. En ese sentido, Amazon una plataforma de gran escala de comercio electrónico, para prevenir este tipo de situaciones y establecer confianza en sus usuarios, hace uso de sus servicios de seguridad ya implementados en *Amazon Web Services* (AWS) servicio en la nube que brinda cifrado de información, administración de claves y detección de amenazas, además, cuenta con su propio sistema de pago, que

garantiza , si una persona no está satisfecha con la compra, reciba su merecido reembolso o retener sus fondos en garantía. Al respecto, muchas entidades bancarias para reducir los niveles de riesgos en sus plataformas establecieron niveles de seguridad adicionales al usuario y contraseña tales como tarjetas de coordenadas, certificados digitales y mecanismos de generación claves de único uso (OTP).

1.2 Gestión y seguridad de la información

Para entender mejor la extensión de la materia acerca de la seguridad en comercio electrónico es necesario desglosar su significado, lo que conlleva a conceptualizar el término seguridad de la información.

Estudios realizados en varias empresas (Tecon, 2019; Melo & Hernando, 2008) que ofrecen soluciones informáticas , define la seguridad de la información como el conjunto de reglas y medidas preventivas aplicadas en orden físico y lógico a los sistemas encargados de la gestión de información de tal modo que permitan resguardar la misma, por lo que resulta un compromiso exclusivo del área de informática de la empresa u organización. En tal sentido, los autores Blanca & Morales (2016), están de acuerdo en que la seguridad de la información es la razón de ser de la empresa u organización, es lo que asegura la supervivencia de la misma, pues la mayoría de la información y activos esenciales de la empresa están distribuidos y almacenados en la red con un formato virtual. En concordancia, otros estudios (Ingertec, 2019; Tarazona, 2007), definen a la seguridad de la información como el objetivo principal de una organización, en la actualidad la información, se ha convertido en un requisito imprescindible para un correcto funcionamiento de la misma, así que las empresas tienen la obligación de estar al tanto de los problemas relacionados al control de datos en los computadores tales como la protección de la confidencialidad, integridad y disponibilidad de la información.

De las definiciones antes indicadas, se concluye que, la seguridad de la información es un elemento de suma importancia, si llegara a vulnerarse afectaría a todos los usuarios o miembros relacionados con la empresa u organización, en ella, se guarda información sensible, por ejemplo, acuerdos de confidencialidad, registros de transacciones de compraventa, entre otros.

Con estos antecedentes, se entiende que la información es uno de los activos más importantes hoy en día para las organizaciones, por esta razón es fundamental comprender cómo está concebida:

Información

Para el Instituto Nacional de Ciberseguridad de España (2020a), la información adquiere una relevancia relativa, pues su importancia varía en función del sector de negocio que la necesite como en el caso del sector sanitario o financiero, suelen tener en su posesión gran cantidad de datos de información privilegiada tales como información de pacientes u operaciones financieras de compra y venta, lo que constituye el activos que son protegidos en la empresa. No obstante, existe información tanto de acceso público como privado por eso para profundizar en esta temática hay que diferenciar los conceptos de los términos de información pública y privada, los cuales se detallan a continuación.

Información pública

Según Muñoz (2016), la define como toda información disponible de forma pública y gratuita, es decir, cualquier ciudadano o empresa tiene acceso a dicha información para que sea analizada, reutilizada y redistribuida, lo que genera nuevos servicios. Por otro lado, en el contexto internacional, a través de la ley dispuesta y vigente hasta hoy en la actualidad, se comprende a la información pública como al conjunto de datos que permiten a los ciudadanos adquirir cualquier tipo de información generada por el estado para el pueblo (Organización de los Estados Americanos, 2013). Seguidamente otros estudios afirman que, la información pública significa colocar contenidos o documentos a disposición de los consumidores para la toma de decisiones en todos los aspectos, además, en esos que son interesantes para la recompra y circulación del comercio (Tatiana, 2016; Cuzcano, 2004;).

Como se ha expuesto, se conceptualiza a la información pública como el acceso gratuito a toda información y datos dentro del marco legal suministrado

principalmente por el ámbito de trabajo de los sectores públicos disponibles en distintas formas para mostrar un documento tales como casos, expedientes, registros u otro material que evidencie la información pública.

Información confidencial

La información confidencial dentro del contexto de los medios digitales, abarca toda el área que tenga que ver con los datos personales de un usuario que no desea que su información sea divulgada, de tal manera que su manejo y almacenamiento necesita contar con la certeza legal de confiar en el administrador de la empresa o institución respecto a la seguridad y resguardo de la misma (Meraz, 2018). Así mismo, estudios afirman que, es aquella información personal que no es manipulada o divulgada, es decir, solo el usuario dueño de la información tiene autorización para realizar dichas acciones, lo que otorga protección frente a amenazas tales como destrucción, perdida, alteración o difusión, accesos no autorizados, entre otros (Instituto Nacional de Ciberseguridad de España, 2021; Chen Mok, 2010). Por otra parte, la Organización de los Estados Americanos, (2019b), clasifica a la información privada con un nivel de riesgo alto, si se llegara a divulgar por usuarios no autorizados, pues causaría daños a la seguridad nacional.

En base a lo antes expuesto, se define a la información privada como un recurso inamovible de las personas o usuarios que tengan registros de ella en la red de distribución de datos, es decir, la única persona capaz de manipular los datos es el dueño y el administrador autorizado.

Información Privada

Es aquella que contiene información exclusiva, o sea, es la información de uso individual y acceso restringido para quien no posea autorización (TechTarget, 2020; INFOAGRO, 2005). Por otro lado, el autor Badia (2015), en el ámbito de la confidencialidad define a la información privada a aquellos datos personales, que

se ha facilitado para el acceso a una determinada persona para que los use con la finalidad concreta, a la que se ha justificado la revelación. En ese sentido, según la firma de abogados Pérez Bustamante & Ponce (2016), contempla a la información privada como toda información no pública de la persona que permita identificarla, contactarla o localizarla o que este referida a sus características físicas, morales o emocionales, a su vida afectiva y familiar, entre otros.

Se determina en base a las definiciones antes expuestas, que los términos confidencialidad y privacidad están relacionados, pero no significan lo mismo, por un lado, la privacidad de la información hace referencia a los datos personales de un individuo o un sujeto y, por otro lado, la confidencialidad son las acciones del investigador sobre la seguridad informática.

Triada de la Seguridad de la información

Constituyen tres términos distinguidos como los pilares de la seguridad de la información, establecen un solo objetivo, el cual es proteger la información mediante herramientas, técnicas o medidas de seguridad. A continuación, se exponen más detalles al respecto:

Disponibilidad

El Instituto Nacional de Ciberseguridad de España (2020a), hace referencia al término como toda información accesible y a disposición en todo momento, se establece prioridades en cuanto a mantener disponible a un conjunto determinado de información. Por otro lado, diversas fuentes sostienen que la disponibilidad, es mantener la información accesible en el momento adecuado para las personas u organismos con los que trabaja y están autorizados o legítimos (Apser Cloud Services, 2015; Gasco, 2013a). Simultáneamente los autores Tejerina Rodriguez & Pinar Manas (2014), argumentan que la disponibilidad busca asegurarse de que los usuarios accedan al servicio con normalidad dentro de un horario establecido. Por ello, se emplean de herramientas necesarias que resistan de trabajar sin descanso para mantener disponible la información.

De lo previamente expuesto, se afirmaría que la disponibilidad es el acceso que por derecho tienen los usuarios a los sistemas o aplicaciones para utilizar sin la posibilidad de que ocurra una interrupción imprevista. Para ello, se cuenta con los implementos necesarios para mantener la información disponible en todo momento y en cualquier lugar.

Integridad

Para los autores Tejerina & Pinar (2014) la integridad constituye la forma en que los datos, se guardan tal y como quería el usuario y no sean alterados sin su consentimiento. Así mismo, el autor Gasco (2013) contempla a la integridad como un principio básico que busca garantizar la exclusividad de los usuarios autorizados a acceder y alterar a la información. Seguidamente para el autor Costas-Santos (2015), menciona que la integridad es una peculiaridad que posee la información al demostrar que no ha sido alterada y a la vez que el documento original no ha sido manipulado por terceros. En ese sentido, la integridad forma parte de uno de los elementos a tomar en cuenta para mantener segura la información, pues la manipulación o vulneración de esta resultaría en pérdidas permanentes o temporales dentro de la empresa.

Finalmente, se conceptualiza a la integridad como un estado inalterable en que la información, se encuentra para que exista confianza y seguridad entre los usuarios y la administración (dueños de la información). La manipulación solo ocurriría en casos especiales que obliguen a la empresa manipular los datos confidenciales, pero esto, no con fines que busquen vulnerar los datos.

Confidencialidad

La confidencialidad para el autor Costas-Santos (2015), es un estado que permanece tanto en los documentos como los archivos establecidos para que este solo sea de uso exclusivo de los usuarios que hayan tenido la autorización para leer o manipular la información. En ese sentido el autor Gasco, (2013) argumenta que la confidencialidad forma parte de los principios básicos de la seguridad informática, se encarga de dar acceso a la información solo a personas o sistemas

autorizados. Es por ello que, es obligación del administrador de la información mantener el estado de confidencialidad de los datos informativos de los usuarios, poseen datos sensibles a ser expuestos.

Dicho esto, la confidencialidad, se define como la forma en que la empresa administra y controla a sus usuarios para que tengan acceso solo a la información pertinente y no a información a la cual no están autorizados, lo que es perjudicial para otros usuarios.

Vulnerabilidades

Las vulnerabilidades según el Instituto Nacional de Ciberseguridad de España (2017), representa una debilidad o fallo dentro de un sistema de información que pone en riesgo la seguridad en la empresa, abre a la posibilidad de que un atacante comprometa la integridad, disponibilidad o confidencialidad, lo que implica priorizar el encontrarlas y mitigarlas. Así mismo, la empresa *Ambit building Solutions Together S.a (2020),* está de acuerdo en que la vulnerabilidad es un hueco en el sistema originado por un error de configuración, una carencia de procedimientos o un fallo de diseño, las mismas son aprovechadas por ciberdelincuentes para robo de información sensible o paralización de funcionamiento. Seguidamente, la autora Woodbury (2021), argumenta que, las vulnerabilidades son huecos que son utilizados como medio de ataque de un programa maligno para omitir medidas de seguridad del equipo e infectar el dispositivo.

De las definiciones indicadas en el párrafo anterior, se conceptualiza a las vulnerabilidades como errores o fallos ubicados en puntos críticos del sistema que son causados tanto por factores humanos, pues la falta de concientización sobre la seguridad es algo común dentro de una empresa y errores del sistema, un sistema puede y tiene la capacidad de funcionar de forma defectuosa.

Amenazas

Para el autor Gomez Vieites (2015), una amenaza es cualquier evento que ocasionado por la naturaleza o por agentes internos o externos dentro de la organización resulta en algún daño en el sistema informático y resulta en

situaciones perjudiciales tales como pérdidas materiales, financieras o de cualquier tipo dentro de la organización. A sí mismo, estudios similares, afirman que, las amenazas ocurren debido al moldeo del sistema, lo que altera el flujo de información hacia una fuente desconocida, es decir, cambiar de destino los archivos, mensajes, documentos de la empresa (Universidad Internacional de Valencia, 2021; Alvarez Maranon, 2004). Simultáneamente, fuentes similares, mencionan que las amenazas dentro de un sistema informático que daña los procedimientos o recursos se clasifican de la siguiente forma: amenazas de software, físicas y humanas. Un sistema nunca está cien por ciento seguro, los seres humanos no son perfectos, cometen errores, lo que los convierte en una vulnerabilidad (Romero Castro et al., 2018; Pilar & Alfonso, 2011)

En base a las definiciones expuestas, se argumenta que una amenaza es una situación, que se presentaría en cualquier momento dentro de un sistema debido a la ausencia de actividades de seguridad como la implementación de medidas, protocolos, políticas de seguridad y principalmente falta de capacitación de personal para actuar ante este tipo de sucesos.

Ataques

Los ataques a los sistemas informáticos según estudios en el área (Medina Rojas & Rivas Montalvo, 2020; Mieres, 2009), afirman que es la actividad realizada por un individuo mal intencionado que aprovecha alguna debilidad o vulnerabilidad en el *software, hardware* o incluso, en el descuido de algunas personas que forman parte de un ambiente tecnológico, esto con el fin de obtener control y por ende beneficio por lo general económico, lo que posteriormente repercute principalmente en los activos de la empresa. Por otra parte, para la compañía de seguros y servicios Caser (2019), un ataque es un atentado que pone en riesgo la seguridad informática de uno o varios equipos, esto, con el fin de causar daños deliberados que afecten el funcionamiento de la misma. En ese sentido, varios estudios, sostienen que los ataques suceden, por un lado, de forma física, es decir, ajeno a lo que es la utilización de las TICs, por ejemplo, golpes al ordenador, exposición a

líquidos, cortocircuito de los componentes, introducción de cuchillas en la CPU, entre otros; y por otro lado de forma lógica dividido en dos formas de ataque (pasiva y activa), o sea, vinculados a la manipulación de las TICs como, por ejemplo, introducción de virus, troyanos, gusanos, entre otros. Así pues, ambos casos afectan significativamente el funcionamiento del sistema y dan como resultado la perdida y vulneración de la información (Romero Castro et al., 2018; Barranco & Hernández, 2012;).

Tipos de ataques

Para que un ataque al sistema informático ocurra antes el usuario mal intencionado sigue una serie de pasos para detectar la vulnerabilidad del sistema y en base a eso, aprovecharla mediante la elección y aplicación adecuadas a las siguientes formas de ataques que se detallan a continuación

Pishing

Este tipo de ataque consiste en establecer comunicación con la usuario mediante él envió de un correo electrónico que simula los correos que por lo general el usuario suele recibir por parte de la empresa o banco al que está relacionado, es decir, está estrechamente relacionado con técnicas de ingeniería social y subterfugio, para después convencer a la usuario que ingrese al enlace e inicie sesión como habitualmente lo hace y en ese instante ya es un perjudicado más de este tipo de ataque (Dominguez, 2018; Roa Buendia, 2013).

Spoofing

Sucede cuando el atacante hace una suplantación de la dirección IP de otra persona miembro de la empresa para esconder su identidad, lo que brinda los permisos asignados en dicha IP, lo cual conlleva a que el atacante reciba todos los mensajes, documentos, archivos y registros guardados dentro del sistema de la empresa (Baca Urbina, 2016).

Ingeniería Social

Es la forma de ataque que por lo general, se realizan a través de llamadas telefónicas a números aleatorios que están vinculados con bancos o empresas para después el atacante mediante un estudio previo sobre el escenario, se hace pasar por una entidad importante dentro de la empresa (administrador), lo que influye en el usuario para confiar en el atacante al solicitar que comparta sus datos personales, por ejemplo, número de tarjetas de crédito, contraseñas, claves, entre otros (Romero Castro et al., 2018).

Fuerza bruta

Consiste en comparar mediante el uso de aplicación *malware* las combinaciones disponibles de contraseñas de inicio de sesión, es decir, automatizar el intento de accesos a una cuenta por medio de verificar las posibles combinaciones tanto de usuario y de contraseña (Romero Castro et al., 2018; Alvarez Maranon, 2004).

Análisis de riesgos

Para el autor Urbina (2016), se define como la probabilidad de recibir ataques externos o internos a los sistemas de información de una empresa, lo cual varía en función de la cantidad de puntos débiles o vulnerabilidades que tengan los sistemas. Por otro lado, para el autor Gómez (2015), el análisis riesgos al formar parte de una serie de estimaciones previas para la detección de riesgos del sistema informático y tienen que ser realizadas con la importancia pertinente, de modo que asegure cumplir con los objetivos que garantizan la seguridad. En ese sentido, varias fuentes en el área (Romero Castro et al., 2018; Alvarez Maranon, 2004), afirman que el análisis de riesgos tiene como finalidad detectar los riesgos que generen un gran impacto no solo en los equipos tecnológicos sino en los objetivos de la organización, para después evaluar los costos que requieran para prevenir o si llegase a ocurrir la amenaza, para mitigarlos.

Se define al análisis de riesgos como, la prevención o mitigación de la ocurrencia de un ataque o amenaza mediante la búsqueda y detección de riesgos que afecten y vulneren la información sensible de un sistema dentro de una empresa, lo que conlleva a que la misma empresa deba poseer en su dominio los controles, procedimientos y medidas necesarias para combatir dichos riesgos.

Metodologías de análisis de riesgos

Las metodologías de análisis de riesgos funcionan mediante el empleo de técnicas y procedimientos que siguen un orden lógico para realizar estudios sobre cómo reducir el riesgo presente en un sistema. En tal sentido, existen diversas propuestas metodológicas a implementar para realizar el análisis correspondiente, entre algunas de ellas, se destacan a continuación:

CRAMM (*CCTA Risk Analysis and Management Method*)

Su origen data del año 1985 cuando el gobierno de Reino Unido decidió a través de la agencia CCTA (*Central Computer and telecommunications Agency*) desarrollar una metodología para evaluación de riesgos informáticos y que hasta la fecha, se ha caracterizado por proveer de escalas para la valoración del impacto en la organización o empresa (Gomez Vieites, 2015).

Margarita

Esta metodología fue desarrollada por España en el año 1997 y su posterior revisión data del año 2005 y posee características propias de análisis de riesgos tales como métodos, medidas, planes de contingencia, pero además de eso, otorga contenidos de concientización de personal responsable de los sistemas de información por medio de evidenciar los riesgos y necesidades a implementar para mitigar el impacto (Gomez Vieites, 2015).

Citus One

Es una herramienta de software comercial desarrollado por la empresa privada Citicus, el cual emplea un método innovador llamado FIRM (*Fundamental International Risk Manager*), que mide y gestiona el riesgo en empresas de cualquier tipo de tamaño (Baca Urbina, 2016; Citicus, 2020).

OWASP

Es una metodología de análisis de seguridad, que posee en sus documentos una serie de guías de implementación de modelos para estimar y clasificar el riesgo de

acuerdo al impacto del negocio, lo que ayuda a reducir el tiempo en la toma de decisiones (OWASP *Fundation*, 2020).

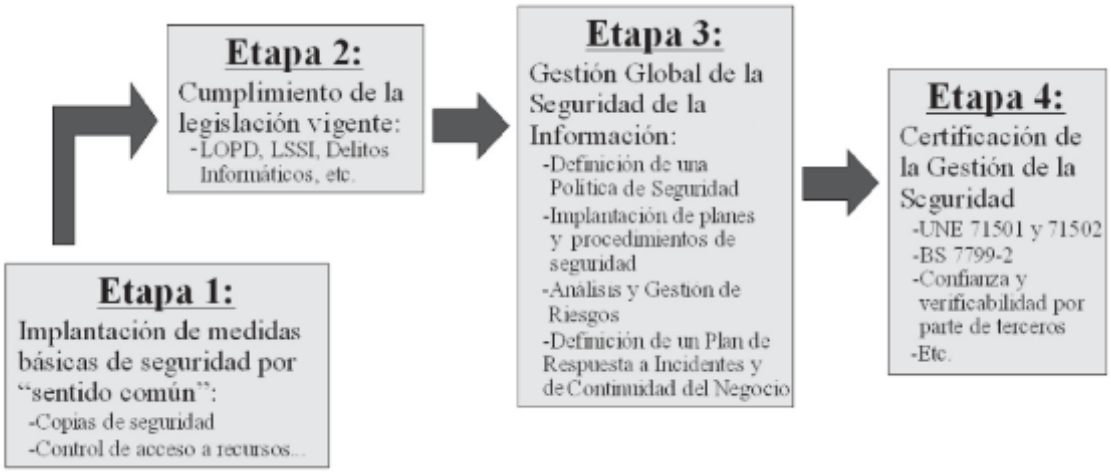
Modelos de madurez

Un modelo de madurez es aquel que posee objetivos y prácticas definidas para determinar el porcentaje de cumplimiento de los procesos de trabajo a dependencia del nivel de madurez o capacidad asignada (Pérez et al., 2014). Por otro lado, los autores Galarza & Uriona (2012), argumentan que, los modelos de madurez sirven para mejorar los procesos de las organizaciones que son responsables de mantener todo el funcionamiento, es decir, se concentran en el refinamiento de la gestión del objeto o disciplina, en la cual trabajan. Así mismo, el modelo de madurez orientado al desarrollo de proyectos tiene como objetivo medir el grado de efectividad de administración y alineación de los procesos continuos con la estrategia general de la empresa (Castellanos et al., 2014).

Como se expuso anteriormente, se definiría a los modelos de madurez como una escala de medición para determinar el nivel de desempeño o alcance de éxito de los procesos de trabajo, que se ejecutan internamente en una organización, empresa o institución.

La siguiente figura es uno de los modelos desarrollado por CMMI (*Capacity and Maturity Model Integrated*), el cual expone las prácticas y competencias de seguridad implementadas en base al seguimiento de cuatro etapas para mantener segura de información,

Figura 4. Niveles de madurez



Fuente: tomado de Gomez Vieites (2015)

Cada uno de los pasos expuestos en la figura son considerados y gestionados a conciencia por la misma organización, cada uno representa una inversión en tiempo y economía, pues resulta difícil encontrar y contratar al personal adecuado para realizar dichas actividades. Es por ello que muchas empresas debido a la falta de preocupación terminan estancadas en la etapa uno, esto por el simple hecho de ahorrase el capital en implementar herramientas, políticas o medidas de seguridad para mantener de segura la información.

Controles y Medidas de Seguridad

Casi todas las actividades de una empresa u organización se registran en formas de documentos tales como facturas, órdenes de compra, orden de pagos y nominas entre otros. En consecuencia, la empresa tiene el compromiso de asegurar dicha información por medio de la implementación de medidas y controles de seguridad informática.

Políticas de seguridad corporativa

Es la principal medida que una empresa prioriza, que se cumplan, pues representa las normas y controles que siguen los administradores para gestionar la información (Escriva Gasco, 2013).

Copias de seguridad

Para el autor Costas-Santos (2015) la copia de seguridad son réplicas de datos que a raíz de un ataque o daño a la información de forma permanente de la empresa, permiten establecer un estado anterior mediante la recuperación de toda la información original.

Concienciación e información

El empleado representa un activo importante dentro de la seguridad en las empresas. La seguridad es importante, pero no siempre es suficiente para proteger los sistemas de información. La implicación y participación de todos los empleados, incluidos los de más nivel en la jerarquía de la empresa, es esencial para llevar una gestión adecuada de la ciberseguridad en la empresa. Por este motivo concienciar y formar a los miembros de la organización, se convierte en una pieza clave para asegurar los sistemas de la empresa (Instituto Nacional de Ciberseguridad, 2020).

Después de las descripciones previamente expuestas, se encuentran evidencias sobre la implementación de seguridad de la información en una empresa como el trabajo de Molina (2015), el cual realiza un análisis de seguridad para una empresa de servicios financieros mediante el uso de la norma ISO/IEC 27001 con el objetivo de conocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad. Así mismo, la investigación de Cárdenas et al. (2016), establece mediante un estudio bibliográfico basado en una metodología de recolección de información un marco de trabajo de seguridad de la información, que contiene buenas prácticas, políticas, gestión de riesgos, recursos humanos, entre otros. Por otro lado, el estudio internacional de Microsoft (2018), sobre la seguridad en plataformas de comercio electrónico ha resaltado que las pequeñas y grandes empresas carecen de protección básica contra los ataques comunes, por lo que ofrecen una solución viable, que consiste en instaurar y configurar Microsoft 365, ofrece mediante un conjunto de programas, la protección frente a ciber amenazas, protección de la información confidencial y varias características avanzadas de seguridad que cada día mediante actualizaciones constantes van en aumento.

1.3 Metodología OWASP

El Proyecto Abierto de Seguridad en Aplicaciones *Web* (OWASP), está conformado por una comunidad abierta dedicada a brindar oportunidades a las organizaciones para que independientemente desarrollen, adquieran y mantengan aplicaciones y APIs de forma segura. La mayoría de los miembros asociados a OWASP son voluntarios, es decir, cuenta con una comunidad unida que buscan como objetivo esencial el apoyar en las investigaciones a través de innovar en el uso de la seguridad. En ese sentido, OWASP nace como una entidad sin fines de lucro, o sea, que sus proyectos en su mayoría están desarrollados en código abierto, lo que brinda la posibilidad de aprovechar sus metodologías para el desarrollo y éxito a largo plazo de un proyecto de seguridad. Así mismo, OWASP define e implementa guía sobre controles o revisiones de seguridad que verifican de una forma u otra que la evaluación de seguridad en una plataforma, se lleve a cabo de forma correcta y en función del objetivo independientemente del estado en el que se encuentre la organización o empresa.

No obstante, OWASP mantiene constantes actualizaciones y extensiones sobre sus guías, por lo que es factible elegir y adecuar la metodología correcta, lo que, en este caso, el proyecto está relacionado al control de seguridad en el área de comercio electrónico.

A continuación, se listan las principales fases a seguir en el siguiente capítulo para realizar las pruebas en base al seguimiento de la metodología OWASP:

- Recopilación de información
- Pruebas de gestión de configuración y desarrollo
- Pruebas de manejo de identidad
- Pruebas de autentificación y autorización
- Pruebas de manejo de sesiones
- Pruebas de validación de entradas
- Pruebas de manejo de errores
- Pruebas de criptografía débil

Cada una de las fases mostradas proceden en base las pruebas propuestas por la guía, por ejemplo, en la fase de recopilación de información, se determinan las herramientas apropiadas para la finalidad de esta, que es recopilar la mayor cantidad de información sobre vulnerabilidades de información expuesta presentes

en la plataforma. En ese sentido, la fase de gestión de configuración y desarrollo se encarga de detectar potenciales errores de configuración fáciles de aprovecgar por usuarios mal intencionados para ingresos no autorizados al servidor. Por otro lado, la fase de manejo de identidad tiene como finalidad exponer los roles, que se emplean para el control y manejo tanto de la plataforma como del servidor o base de datos. Así mismo, las pruebas dentro de la fase de autentificación y autorización tienen como objetivo verificar la seguridad en los mecanismos de registro e inicio de sesión de la plataforma, lo que convoca a la siguiente prueba. El Manejo de sesiones es la siguiente fase de validación de seguridad, pero en el entorno de gestión de sesiones de usuario y la aplicación para encontrar vulnerabilidades asociadas. Por otra parte, las pruebas de validación de entrada verifican si no existen fallas en cuanto a la ausencia del mecanismo de validación. De igual manera las pruebas de manejo de errores buscan fallas en sitios web inexistentes dentro de la plataforma. Por último, las pruebas de criptografía débil se encargan de comprobar si la información enviada entre el usuario y el servidor se encuentra segura.

A continuación, en la tabla 3, se muestra una comparativa sobre las metodologías relacionadas conservar la integridad de la seguridad en la información para justificar el motivo del empleo de la metodología OWASP en el desarrollo de la investigación.

Tabla 3. Pros y Contras de Metodologías

Metodología	Descripción	Pros	Contras
SANS	Es una metodología enfocada al análisis forense de seguridad contra delitos informáticos (Pinto, 2014).	-Metodología que cubre todas las etapas para hacer un análisis forense -Toma en cuenta el cuidado de la cadena de custodia	-No propone métodos de análisis para volúmenes grandes de datos -Es específica para dispositivos que cuenten sistemas operativos Windows o Linux
OSSTMM	El OSSTMM (*Open Source Security Testing Methodology Manual*) para el autor Valdez Alvarado (2013), es una guía para realizar una verificación a fondo sobre el estado operativo y de seguridad actual de una organización que poseen conexión a internet.	-Posee métricas, lo que permite medir de forma global si la organización es atacada -Se utiliza tanto en el ámbito digital como el físico y humano.	-Se requiere de una gran cantidad de información para logar obtener métricas. -Al ser muy extensa resulta un poco tediosa de implementar
OWASP	Esta metodología define una serie de requerimientos a través de un estándar de verificación de seguridad en aplicaciones, lo cual se utiliza como pruebas para determinar qué tan segura es una aplicación (OWASP, 2017).	-Se aplica a una variedad de situaciones -Su procedimiento es rápido -Se enfoca directamente en comprobar la seguridad de páginas o aplicaciones *web.*	-Algunas pruebas, se realizan manualmente, por lo que llevaría mucho tiempo. -Pruebas como revisión de código fuente requieren desarrolladores de seguridad altamente calificados. -Resulta difícil detectar vulnerabilidades en el código fuente.

Fuente: elaboración propia

En relación con lo expuesto, se entiende que la metodología SANS (*SysAdmin Audit, Networking and Security Institute)* no es utilizada en la investigación debido a que emplea el análisis y descubrimiento del causante de los ataques informáticos ya ejecutados, es decir, la investigación trata de buscar al ciberdelincuente a través de la detección de la vulnerabilidad causante por medio de conservar evidencias físicas o digitales que estén relacionados con el ataque informático. Por otro lado, la metodología OSSTMM tiene posibilidades de ser empleada en la investigación, en su guía menciona que tiene la capacidad de abarcar la seguridad de todas las localizaciones físicas enlazadas a la red, interacciones humanas y todas las formas de comunicación existentes, lo que incluye aplicaciones y páginas *web*. No obstante, al ser una metodología completa requiere de un exhaustivo proceso de obtención de información y requere invertir mucho tiempo en la investigación, así que no aplica en este proyecto debido a que la investigación, se centra únicamente en el entorno digital a la plataforma CorpoAmbato. En conclusión, existen varias metodologías y estándares para realizar evaluaciones y auditorias de seguridad, sin embargo, OWASP destaca por encima de las demás, posee una característica esencial necesaria para el tema de investigación. Dicho rasgo, se lo denomina como: “Metodología enfocada al elemento a auditar”, en definitiva, OWASP con los años ha adquirido documentos y proyectos otorgados por la comunidad de profesionales en el área para brindarlos como guías de evaluación independiente de seguridad de aplicaciones móviles, páginas *web* o dispositivos IoT.

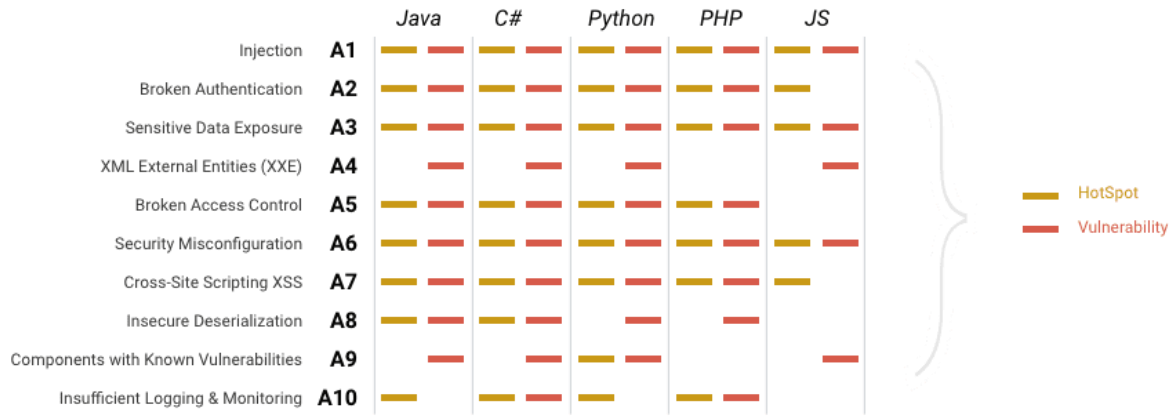
OWASP top 10

Como su nombre lo indica es un ranking de los diez riesgos más peligrosos para aplicaciones *web* y plataformas, determinado por su comunidad conformado por expertos en la industria. Por cada punto de la clasificación, se calcula el riesgo en base a la metodología de calificación de riesgos OWASP, lo cual incluye una serie de evaluaciones de detección de vulnerabilidades mediante la explotación de debilidades, así como la medición del impacto si llegase a suceder.

A continuación, se presenta las principales vulnerabilidades determinadas en base al análisis y comparación de publicaciones de usuarios, discusiones abiertas, firmas de consultoría, entre otros; todos ellos situados en una base de datos general que

ha encontrado y almacenado más de quinientos mil tipos de vulnerabilidades dentro de organizaciones, aplicaciones y plataformas.

Figura 5. OWASP Top 10



Fuente: tomado de SonarQube (2018)

En referencia a la figura expuesta, se contempla que las vulnerabilidades mantienen dos enfoques: *HotSpot* o punto de acceso, se refiere a aquellos códigos que son sensibles a la seguridad, aquellos que a simple vista están bien pero que requiere revisión humana para saberlo con certeza. Luego, están las propias vulnerabilidades de seguridad, que requieren una acción inmediata para evitar riesgos.

Luego de un análisis realizado, se encuentran evidencias sobre el uso de metodología OWASP en el ámbito de seguridad, por ejemplo, el estudio de Chicaiza et al. (2020), el cual establece un medio investigativo para detectar vulnerabilidades a través de la metodología OWASP en función de la ejecución del ataque de inyección SQL. Dicho estudio, realizó varios análisis a distintos sitios *web,* lo que en su proceso detectó más de dos vulnerabilidades por cada sitio analizado vinculados en permitir ataques *SQL injection.* No obstante, en el desarrollo de la investigación, se establecieron escenarios para simular un ataque de *SQL injection* para posterior a eso, establecer las medidas necesarias para mitigarlo en base a la metodología empleada. Al finalizar la investigación, se determinaron medidas y recomendaciones a seguir para mitigar los riesgos en base a técnicas otorgadas por OWASP, las mismas que se usaron como referencia para realizar ataques.

CAPÍTULO II. DISEÑO METODOLÓGICO

En el siguiente capitulo, se describe la metodología a emplear para realizar la investigación conforme a las actividades a ejecutar para el desarrollo de las pruebas. También, se presenta a la organización en la cual se desarrolla la investigación su misión, visión, estructura, entre otros.

2.1 Caracterización de la organización

CorpoAmbato aparece como una organización sin fines de lucro cuya fundación tuvo lugar en el año 1999, por medio de un programa del Banco Interamericano de Desarrollo, para el fortalecimiento de capacidades locales. Sus miembros fundadores son: el H. Gobierno Provincial de Tungurahua, el GAD Municipalidad de Ambato, la Cámara de Comercio de Ambato, la Cámara de Industrias de Tungurahua, la Universidad Técnica de Ambato y la Pontificia Universidad Católica del Ecuador Sede Ambato (PUCESA). Dicha organización adquiere validez, confianza y credibilidad al estar correctamente inscrita en el Ministerio de Industrias y Productividad y legitimada ante la Secretaría de Gestión de la Política con certificado ROUS (CorpoAmbato, 2018).

Misión

La organización, se enfoca en incentivar el comercio por medio de proyectos de desarrollo económico en zonas urbanas dentro de la provincia esto, mediante la percepción de las necesidades a resolver de todos los actores sociales beneficiarios del proyecto y la colaboración de los gobiernos locales, empresarios, universidades, líderes comunitarios y políticos (CorpoAmbato, 2018).

Visión

CorpoAmbato como proyección a futuro busca fortalecerse entre los organismos de ayuda social para dar paso a más proyectos de desarrollo innovadores en función de ayudar en el sector económico para mejorar la calidad de vida de los ciudadanos y a raíz de esto, adquirir cada día, mayor experiencia en procesos de desarrollo sostenible (CorpoAmbato, 2018).

La empresa cuenta con varios miembros encargados de vincular y establecer relaciones correspondientes para el desarrollo de proyectos que requieran de la colaboración y comunicación de instituciones específicas para su debido desempeño. Por ello, la empresa cuenta con un organigrama para determinar las

acciones encargadas a cada uno de los miembros, como se observa a continuación.

Figura 6. Organigrama de CorpoAmbato

Fuente: CorpoAmbato (2018)

La organización lleva años en labor con la provincia, por lo que ya cuenta con proyectos ejecutados en distintas localidades, lo cual, en este caso de ejemplo, se instauro una plataforma de comercio electrónico en colaboración con la PUCESA para dar a conocer los productos de sus pequeños empresarios asociados a CorpoAmbato. Dicho proyecto, actualmente, se encuentra en funcionamiento y disponible en la red y está abierto a propuestas de proyectos para mejorar continuamente la calidad de comercialización electrónica. Por ello, el presente proyecto, se centra en establecer un punto de partida enfocado a la seguridad en los equipos informáticos, sistemas de información que al estar en funcionamiento son susceptibles a vulnerabilidades tales como *pishing*, *spoofing*, ataques de fuerza bruta, que ponen en peligro la permanencia de una organización. Al respecto, Estruga (2020) menciona la rama de estudio de seguridad de la información

adquiere relevancia en las empresas u organizaciones, está directamente ligada a la gestión de riesgos empresariales.

2.2 Metodología de la investigación

Son aquellos procesos que siguen un camino y técnicas ordenadas con la finalidad de cumplir los objetivos tales como, la construcción de leyes, teorías y modelos a través de sistematizar los datos obtenidos en la investigación (Eugenia, 2014). Es decir, cumple un proceso lógico metodológico a seguir en un solo sentido a través de establecer fases ordenadas, los cuales se realizan de forma rigurosa y responsable para obtener resultados confiables, por lo que la presente investigación cuenta con un enfoque cuantitativo para establecer mediciones y niveles sistemáticos de seguridad al momento de realizar el análisis respectivo. Además, permite realizar entrevistas estandarizadas a los miembros asociados a la organización, así como el gerente o el administrador de la plataforma.

Para el sustento documental, se aplica el método de análisis documental y de información debido que permite interpretar el contenido de varios documentos referentes a la seguridad de la información y prevención de la misma, esto con el fin de adecuar a los propósitos y objetivos de la investigación. Además, es una forma de investigación que define operaciones apropiadas, permiten describir, identificar y representar el contenido extraído en un documento de forma sistemática para su análisis respectivo (Dulzaides & Molina, 2004;Hernández et al., 2014). Así mismo, el proyecto, se apoya en la investigación bibliográfica, pues otorga una forma de entregar información de los elementos asociados al problema en cuestión y así dar a conocer de forma previa un amplio panorama sobre lo que va a tratar la investigación. Al respecto, el autor Ayala (2020), coincide en que la información encontrada es admitida únicamente de fuentes confiables tales como libros, revistas académicas, artículos, documentos, entre otros, relacionados a la materia de investigación para después del análisis y extracción de la misma presentarla de forma simplificada al usuario.

Se emplea, también, el método analítico-sintético, se analizan distintas amenazas relacionadas a la seguridad, por lo que, para optimizar el proceso, se extrae los

elementos más importantes, tal como lo menciona Rodríguez & Pérez (2017), sobre el apartado de análisis, el cual establece un procedimiento ordenado para descomponer o estudiar en partes un componente y después realizar la operación a la inversa (síntesis), es decir, agrupar los componentes previamente analizados para descubrir características adicionales. En ese sentido, al término del proceso de análisis de todas las amenazas la información obtenida, se ajusta para su respectiva clasificación grado de riesgo, por ejemplo, vector de ataque, debilidades, explotabilidad e impacto; para después determinar medidas o estrategias de prevención adecuadas a emplear en los casos mencionados.

Se apoya en la investigación cuali- cuantitativa, puesto que se efectúan diferentes pruebas para obtener mediciones de los niveles de seguridad y en base al puntaje, determinar el riesgo y su correspondiente valor cualitativo, a través del registro de las vulnerabilidades y amenazas presentes en la plataforma, de modo que permita llevar a cabo un análisis previo a la aplicación de estrategias de prevención.

Debido a factores que limitan el estudio de la población en la empresa CorpoAmbato, como el hecho de poseer pocos miembros en su infraestructura, no se define un área en específico que permita determinar una muestra a estudiar en la investigación. Por esta razón en el proyecto, se toma como población de estudio a dos personas: Gerente General y un Gerente Técnico, como fuente principal de información, mediante la técnica de la entrevista.

Para el proyecto, se aplica la técnica de entrevista como una forma de recopilar información de sujetos asociados a la investigación como lo menciona el autor Bravo et al. (2013), que resulta de gran utilidad, si se requiere entablar una conversación con el medio estudiado, esto, con el propósito de conseguir datos relevantes de respuestas verbales a las interrogantes planteadas. En tal sentido, se elaboró como instrumento dos cuestionarios en los constan las preguntas adecuadas asociadas al tema del proyecto para mantener comunicación con un miembro asociado a CorpoAmbato quien tiene la capacidad de responder de forma técnica a las preguntas relacionadas a la seguridad de la plataforma. En parte, esto

es debido al hecho de que la plataforma fue desarrollada por actores externos a la organización y no cuenta con un miembro experto en el tema.

Mas adelante, se presenta un modelo de entrevista aplicado al Gerente Técnico en seguridad de aplicaciones asociado a la organización, con la finalidad de recabar información sobre las estrategias empleadas como medidas para proteger la información de sus usuarios y conservar la integridad (ver anexo 1).

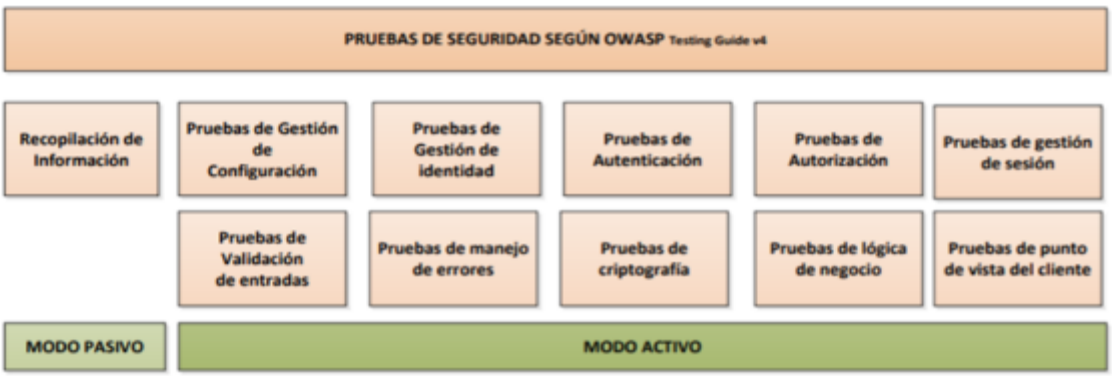
El otro cuestionario, se aplica a la gerente de CorpoAmbato para tener conocimiento sobre los proyectos desarrollados en el área de TIC o en temas de mejoras aplicables a la plataforma de comercio electrónico CorpoAmbato.

El formato de entrevista aplicado a la persona que actualmente ocupa el cargo de Gerente General de CorpoAmbato para responder las preguntas relacionadas a los proyectos realizados en el área de TI y planes futuros sobre la plataforma de comercio electrónico, se evidencia en el anexo 2.

2.3 Metodología OWASP

En base a la metodología OWASP, que se contextualizó en el capítulo uno, en lo que respecta a las pruebas de seguridad, Salazar (2018), establece una serie de fases observadas en la figura 7 necesarias para cumplir el objetivo de la investigación, por lo que se procede en el presente apartado a su desarrollo y documentación.

Figura 7. Fases de la metodología OWASP



Fuente: Salazar Edgar (2018)

Si bien OWASP define para cada fase un gran conjunto determinado de pruebas a ejecutar ya sea de caja negra o caja blanca, no es empleada en su totalidad para evitar realizar daños a la plataforma de la organización, el objetivo de esta investigación no es más que detectar y analizar las vulnerabilidades encontradas en la misma. Es decir, no realizar pruebas perjudiciales para la integridad o confidencialidad de la información de los usuarios de la plataforma y a su vez evitar realizar pruebas de tipo fuerza bruta causantes de caídas de páginas, lo que limita el alcance de ejecución las pruebas de escaneo. En resumidas instancias, las pruebas, se limitan a efectuar distintos tipos de escaneo y detección que dependen de las vulnerabilidades requeridas a encontrar dentro de la plataforma para su posterior propuesta de mitigación o reducción de riesgo ante ataques.

La URL y la dirección, en la cual se realizan las pruebas es la siguiente:

https://corpoambatoemprende.com/

70.X.X.23

Como se observa, la dirección IP permanece oculta para evitar problema a futuro relacionado con la vulnerabilidad de la integridad de la plataforma CorpoAmbato, no obstante, si de alguna forma la dirección IP fuera descubierta, esta no representaría un peligro, pues al estar alojado servidor privado, está protegida por usuarios de terceros.

Si bien la metodología OWASP define una amplia gama de pruebas a ejecutar, lo que incluye información de descripciones, objetivos, herramientas de escaneo y amenazas, estas no fueron empleadas en su totalidad, puesto que se determinó que ponen en peligro la integridad de los datos de los usuarios de la organización. Así mismo, debido a que muchas herramientas propuestas en la metodología revelan cantidades variables de información, en algunos casos, se utilizaron varias herramientas para una sola prueba o una herramienta para una sola prueba a fin de encontrar y comparar la mayor cantidad de información posible para el posterior análisis del riesgo.

2.3.8 Fase l – Recopilación de información

En esta fase, se va a emplear herramientas de recopilación de información definidas en las fases de la metodología tales como *Spiders, Robots, Crawlers*, motores de búsqueda, análisis de códigos de error, entre otros que permitan establecer un punto de partida necesario, antes de realizar las pruebas de intrusión. En relación con lo mencionado, la empresa Cloudflare (2019), afirma que dichas herramientas de búsqueda, se los conoce como rastreadores *web* para de encontrar información, descargar e indexarla mediante el software utilizado. Por ello, en el presente proyecto utiliza como primera herramienta de búsqueda de información al navegador Google Hacking como lo menciona la metodología OWASP en la guía para realizar pruebas de seguridad en aplicaciones y plataformas. Adicionalmente, se emplean los resultados de las entrevistas como punto de partida para determinar el ecosistema a trabajar dentro de la plataforma de manera que permita establecer cuántas pruebas de intrusión y detección de vulnerabilidades son necesarias realizar para establecer un nivel de seguridad en la misma.

- **Recopilación de información por parte de los entrevistados**

Ahora las siguientes preguntas fueron escritas y dirigidas hacia la gerente general de CorpoAmbato sobre cuestiones relacionadas con proyectos desarrollados en torno al área de Tecnologías de la información y la comunicación, cómo han resultado en beneficio de sectores vulnerables que requieran de actividad comercial presencial (ver anexo 2).

Pregunta 1: ¿Cómo están organizados para apoyar el desarrollo de proyectos de emprendimiento?

-Tenemos un programa de apoyo y acompañamiento al emprendedor, se llama “Aprendiendo a Emprender”, es un proceso especializado de capacitación con fuerte enfoque de asistencia técnica. Brindamos servicios a emprendedores con potencial de escalabilidad. Adjunto, se encuentra un *brochure* de nuestro programa.

Pregunta 2: ¿Qué tipo de proyectos han realizado relacionados con las tecnologías de la información?

- Estamos en el inicio de un proceso en conjunto con su universidad para poner en funcionamientos dos plataformas *ecommerce.* Por otro lado, la corporación cuenta con una plataforma educativa y de *networking* para emprendedores llamada INSPIRA DIGITAL SPACE. Tiene 8 módulos para la preincubación de emprendimientos y esta funcional para iniciar procesos de *networking* entre emprendedores.

Pregunta 3: ¿Qué los impulsa a ayudar a otros sin obtener beneficio alguno?
- La razón de ser de la corporación es el apoyo al desarrollo económico sostenible de la provincia de Tungurahua, está dentro de nuestros estatutos y justamente este objetivo es lo que nos mueve.

Pregunta 4: ¿Actualmente qué proyectos se llevan a cabo en la provincia dentro del área de TI?
- Al momento desarrollamos capacitación de la mano con PUCE en cursos de la academia CISCO. Estamos en presentación de macroproyectos a la cooperación que involucra las TI para lograr objetivos de desarrollo sostenible.

Pregunta 5: ¿Cuál es su criterio en cuanto al proyecto de seguridad en la plataforma de comercio electrónico CorpoAmbato?
- Para que la plataforma de *ecommerce* funcione es imperativo que todos sus usuarios sientan confianza en usar sus funcionalidades, por tanto, es imperativo blindar la plataforma de manera que brindemos un servicio de excelencia a todos nuestros *stakeholders*.

Pregunta 6: ¿Qué planea hacer para mejorar en un futuro la plataforma de comercio electrónico de CorpoAmbato?
- Estamos en el desarrollo de un proyecto en conjunto con el HGPT y MPCEIP para generar espacios de comercialización y networking que estimulen la actividad comercial en Tungurahua, este proyecto incluye el uso de las dos plataformas de comercialización que tenemos al momento. La idea siempre es fortalecer este proceso.

En base a las respuestas aportadas por parte de la gerente General de CorpoAmbato, se permite remitir un análisis general sobre las preguntas y respuestas expedidas por la misma. En tal sentido, la organización CorpoAmbato tiene la posibilidad de llevar a cabo varios proyectos de sostenibilidad económica enfocada a los sectores vulnerables y con el menor costo posible a través del uso de las tecnologías de telecomunicación que actualmente predominan en el mercado debido al confinamiento de la pandemia. Una de las mayores ventajas que posee la organización es el de estar asociado con otras instituciones para el apoyo de desarrollo de proyectos conjuntos que buscan ayudar de alguna u otra forma en el desarrollo económico independiente mediante la adaptabilidad del comercio en el entorno virtual o de plataformas. Así mismo, la organización menciona que tienen planeado desarrollar más proyectos de espacios de comercialización para estimular la actividad comercial, lo que incluye la implementación y adaptación de plataformas comerciales para distintos emprendimientos. Todo esto es realizado sin necesidad de remuneración económica, es uno de los principios de la organización el no tener motivaciones de lucro para ayudar a otros a mejorar su diligencia comercial y económica.

A continuación, este cuestionario ha sido desarrollado para el técnico Gerente de seguridad de la organización para abordar requisitos aplicables a la seguridad de los usuarios que frecuentan la plataforma de comercio electrónico CorpoAmbato, por lo que las preguntas constan de respuestas acordes al tema y que son esenciales para determinar un ecosistema seguro en la plataforma (ver anexo 1).

Pregunta 1: ¿Qué mecanismo considera es el mejor para mantener segura la información de una plataforma de comercio electrónico?

La persona entrevistada manifiesta los siguientes puntos a tener en cuenta en los mecanismos de seguridad:

- Actualmente disponemos de servidores propios de alta potencia y confiables, los cuales se encuentran monitoreados 24/7/365, lo que garantiza que la información como páginas web y archivos están alojados de forma segura y monitoreados en todo momento

- Todos nuestros sitios disponen de protocolo HTTPS que incrementa el nivel de seguridad para los pagos online, el cual se actualiza de forma trimestral, lo que garantiza la integridad de información.
- Para garantizar la disponibilidad o integridad de información, se mantiene copias de seguridad diarias, de los cuales el usuario dispondría de los últimos 30 días de respaldo.

Análisis: Las plataformas de comercio electrónico que son altamente frecuentadas disponen de pruebas necesarias para verificar el uso de protocolos de seguridad y disponibilidad de los servidores *web* donde esta alojada.

En la siguiente pregunta, se realiza una consulta sobre los niveles de seguridad que normalmente posee una plataforma de comercio electrónico, es esencial preservar la información de esta, así que, se detallan a continuación, las respuestas aportadas.

Pregunta 2: ¿Qué niveles de seguridad emplearía en una plataforma de comercio electrónico para garantiza la información tratada?

La persona entrevistada manifiesta los siguientes puntos en cuanto a niveles de seguridad:

- Implementar forma de pago o cobro seguras como vincular a plataformas de pago externas como PayPal o mantener un convenio directo con la entidad bancaria para garantizar que el pago lo realice de forma segura.
- Disponer varias alternativas de cobro que permitan al proveedor confirmar la recepción de este antes de gestionar el despacho de mercadería.
- Validación de datos al momento de crear las cuentas, utilización de herramientas como Google recaptcha para confirmar que el registro es una persona y no un robot, almacenamiento de contraseñas encriptadas cuyo periodo de caducidad sea recurrente
- Evitar el uso de las últimas 10 contraseñas registradas, las cuales estan encriptadas en la base de datos.
- Uso de software antifraude con geolocalización para determinar procesos o acciones fallidas al momento de gestionar un pago.

Análisis: Añadir métodos de pago en una plataforma web resulta un de los procesos más sensibles dentro de cualquier operación de comercio electrónico, se maneja información de tarjetas de crédito y cuentas bancarias, por lo que, de forma obligatoria, la seguridad tiene que estar establecida y verificada a través de pruebas.

Para esta pregunta, se analizan que aspectos observan de primera un usuario o cliente al entrar a una plataforma web de comercio electrónico y que hace que se quede para que exista recurrencia y recompra.

Pregunta 3: ¿Qué indicadores le evidencian que una plataforma de comercio electrónico se encuentra segura?

La persona entrevistada manifiesta los siguientes puntos acerca de la seguridad del comercio electrónico:

- Utilización de protocolos de seguridad HTTPS, certificados de seguridad SSL con nivel de encriptación superior a los 256-bit
- Apoyarse en plataformas de pago y cobro como PayPal o PayPhone que disponen de un nivel de seguridad certificado para garantizar una transacción segura
- Uso de mensajes de confirmación o validación de doble factor generado en el sitio web que garantice que el proceso es seguro
- Uso de token de seguridad antes de realizar el pago, lo que permite conocer o certificar el proceso de pago dentro del sitio.
- Bloque de acceso a IP tras 3 intentos fallidos a la plataforma.

Análisis: El primer indicador en el que un usuario se enfoca para asegurarse de que la plataforma es segura, es que las políticas de privacidad implementadas en dicha plataforma estén claras y visibles para el análisis de los clientes. Además, mostrar toda la información relevante sobre la empresa que gestiona la plataforma para generar confianza en los clientes tales como contacto, teléfono y modalidades de pago. En resumen, manifestar toda la información necesaria aumenta las posibilidades de que un cliente permanezca dentro de la plataforma.

En la pregunta 4, se consulta sobre las medidas aplicadas para prevenir o en caso de que la información de sus usuarios sea vulnerada haya respuesta de recuperación y esté nuevamente preservada en el servidor.

Pregunta 4: ¿Qué medidas aplicaría para responder, si se llegase a vulnerar la información de sus clientes

La persona entrevistada manifiesta los siguientes puntos en cuanto a medidas de prevención:

- Para evitar esto es recomendable que las aplicaciones mantengan actualizada su plataforma tanto en plugin como en componentes y que no almacenen datos de tarjetas de crédito y en el caso de que se llegara a obtener información que esta sea la menos comprometedora posible
- Es recomendable que la información crítica, no se guarde en una sola base de datos o en un solo servidor y que esta esté distribuida de forma redundante que permita la reactivación del servicio cuando suceda algún ataque.
- Si se utiliza herramientas web gratuitas es recomendable conocer las vulnerabilidades que tiene la misma y como corregirlas para evitar disponer de un punto de acceso a la plataforma
- En el lado del servidor, si se detecta un intruso es necesario determinar cuál es el punto que accedió, si este fue por una aplicación de un sitio web, pues se notifica al cliente y su cuenta queda elimina automáticamente, si el acceso es por un puerto de acceso libre, se bloquea el servidor y como se dispone de enlaces redundantes el servicio, se mantiene activo para el usuario mientras bloquea los puntos débiles del servidor en el caso de que existiera.
- Si el sitio web presenta un punto débil ya sea por componente o plugin, se notifica al responsable de la cuenta para su corrección, en el caso de que no se realicen acciones y esta sea un punto de acceso indebido y este se materialice, la cuenta se elimina

Análisis: Es necesario realizar todas las pruebas de intrusión necesarias o ataques más recurrentes para determinar las acciones a ejecutar y responder ante los ataques mencionados para luego establecer medidas de control y prevención de los riesgos asociados a la vulneración de los datos que recopilen en dichas pruebas.

En la pregunta 5, se examina los controles utilizados para para garantizar la seguridad de la información dentro de sitios web para de este modo conocer si alguna es aplicada en la plataforma de comercio electrónico CorpoAmbato una vez realizadas las pruebas de detección de vulnerabilidades.

Pregunta 5: ¿Qué controles implementaría para garantizar la seguridad en la información en las plataformas de comercio electrónico?

La persona entrevistada manifiesta los siguientes puntos en cuanto a garantizar la seguridad de la información:

- Validación de usuarios por doble factor, o envío de mensajes de confirmación.
- Control de verificación de procesos automatizados.
- Herramientas de control de fallas al momento de desarrollar una aplicación como Coss Site Scripting (XSS).
- Inyección de código o ejecución de código malicioso para validad la efectividad de la seguridad o firewall.

Análisis: Una vez realizada las pruebas en todos los niveles de seguridad de la plataforma resulta necesario analizar los posibles controles a implementar en la plataforma para asegurar la información pertinente a la misma.

La pregunta 6 hace referencia a la pregunta 5, al igual que las respuestas sobre controles, también, se utilizan herramientas de pago o de código libre para mantener la información segura.

Pregunta 6: ¿Qué herramientas y técnicas utiliza para prevenir ataques?

La persona entrevistada manifiesta los siguientes puntos en cuanto a herramientas y técnicas de prevención:

- Nuestros servidores trabajan con sistemas operativos Linux para ello una herramienta que permite el análisis de vulnerabilidades es Nessus de arquitectura cliente-servidor que dispone de una base de datos con patrones para simular el ataque a un servidor y como resultado obtener las vulnerabilidades de la misma.
- También, se utiliza Conan, encargado de analizar la configuración del sistema y se lo utiliza como apoyo a un software antivirus

- Software antivirus que evita que el usuario suba un archivo infectado al servidor, por lo que es eliminado automáticamente.

Análisis: Las mismas herramientas, con las que se analiza la seguridad permiten a la plataforma determinar la mejor forma de actuar o prevenir los ataques o vulnerabilidades encontradas al realizar las pruebas.

La pregunta 7 se refiere a la necesidad de conocer que tipos de ataques que son frecuentes dentro de una página web, pues da una idea sobre el panorama en el que trabajan los ciberdelincuentes o personas mal intencionadas, lo que permite establecer las medidas necesarias para controlar dicho riesgo de impacto si llegase a suceder un ataque de vulneración de datos.

Pregunta 7: ¿Qué tipos de ataques son comunes dentro de la organización?

La persona entrevistada manifiesta los siguientes puntos en cuanto a tipos de ataques:

- Ataques SQLI orientado a modificar una cadena de consulta ya sea para modificar información de una base de datos o redirigir sitios web
- Ataques DoS, pue se orienta a inundar el sitio con solicitudes externas, lo que provoca la caída o no disponibilidad de este.
- Ataques XSS mediante la inserción de script maliciosos causan la saturación de la cuenta y posterior suspensión de la misma hasta que el usuario corrija el problema.

Análisis: Algunos de los ataques mencionados están vigentes en las pruebas de la metodología *OWASP* top 10, por lo que cuenta con las medidas aplicables para prevenir o responder ante las mismas.

- **Prueba 1: descubrimiento de información por motores de búsqueda**

Objetivo de la prueba

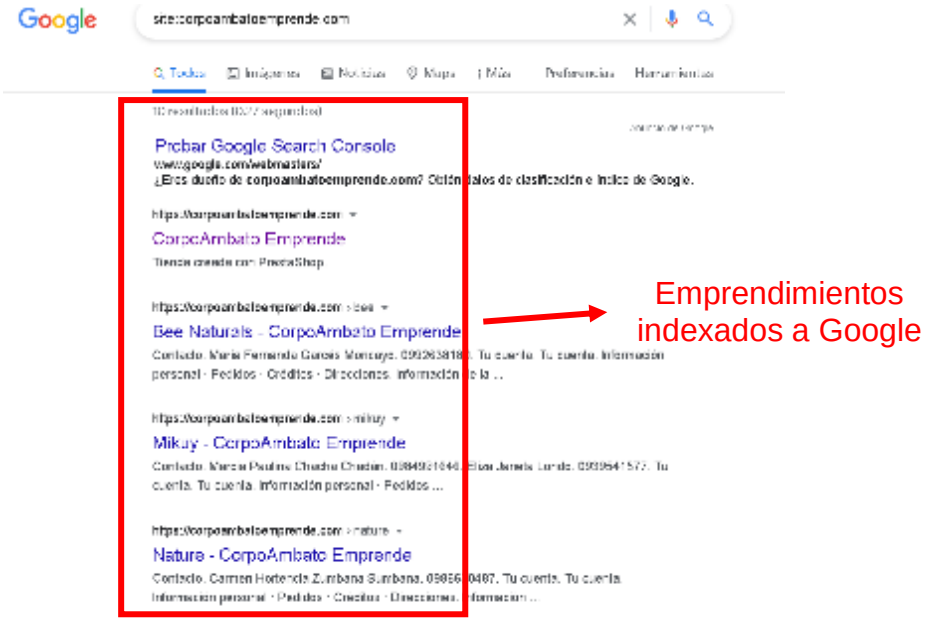
La presente prueba tiene como objetivo recopilar la mayor cantidad de información de la *url* de la plataforma de CorpoAmbato y encontrar si existe información que no estaría expuesta como *cpanel* o *webmail*.

Ejecución de la prueba

Para la ejecución de la prueba, se hace uso de la herramienta *Google* para encontrar información indexada a la misma.

A continuación, en la figura 8, se muestran los resultados de la recopilación de información a través de Google

Figura 8. Búsqueda de información pública en Google - URL

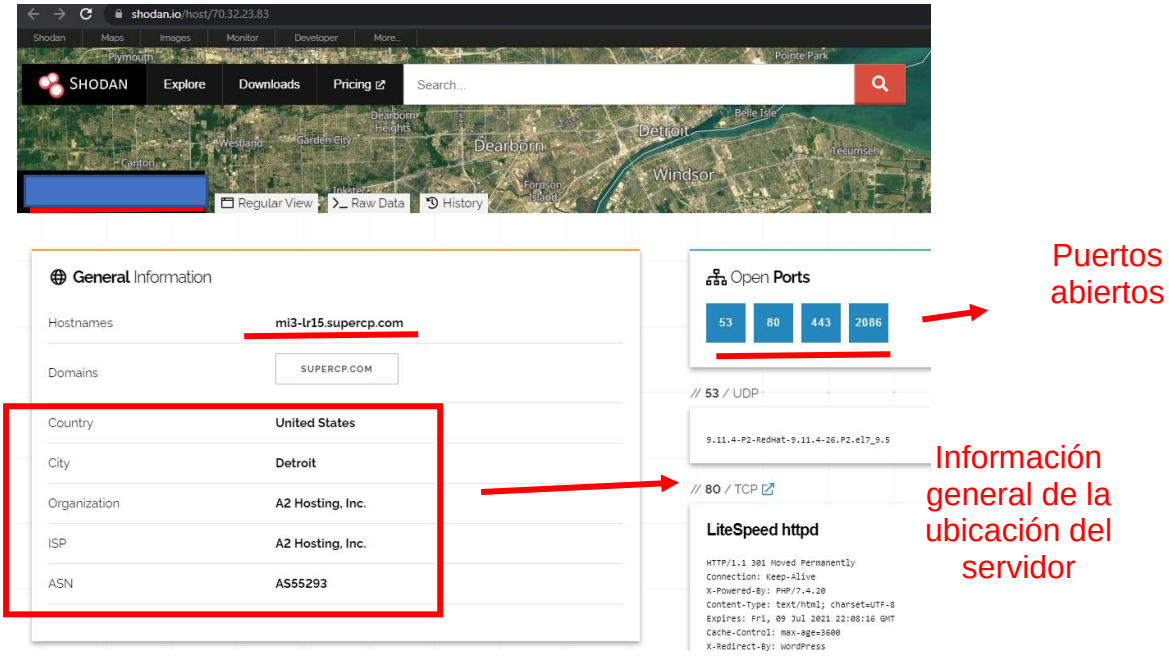


Fuente: elaboración propia

Como se observa en la imagen, el comando *site* permite observar toda la información que corresponda estar a la vista del público, ya sean documentos, videos o accesos a otros sitios administrativos, entre otros. Pero en este caso, solo se encontraron los emprendimientos anclados a la plataforma, por lo que no se hace uso de otros comandos que ofrece *Google* para filtrar información publicada.

A continuación, en la siguiente figura, se utiliza la herramienta *shodan* para determinar si existen dispositivos anclados a dicha dirección IP

Figura 9. Recopilación de información – *Shodan* - IP

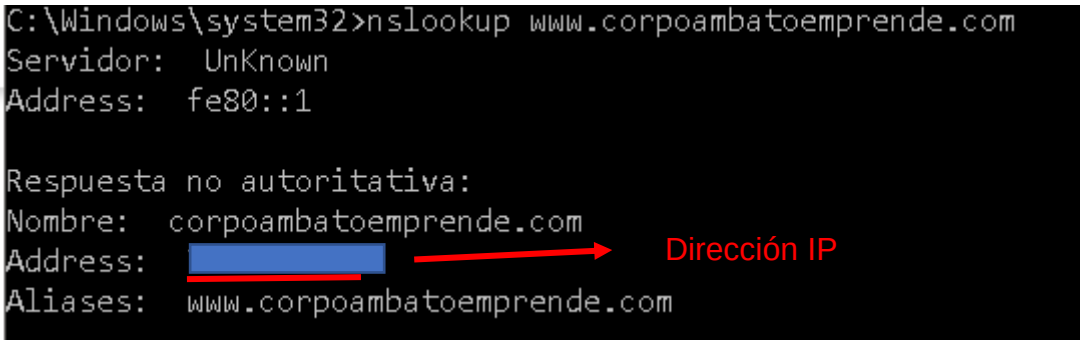


Fuente: elaboración propia

Se observa que, no se encontraron dispositivos anclados a dicha dirección IP solamente información aproximada del servidor donde funciona la plataforma como: el tipo de servidor, ubicación, servicios, puertos, entre otros.

Ahora, la siguiente prueba, se utiliza el comando *nslookup* para comprobar cuál es la dirección IP al que está asignado al dominio “corpoambatoemprende.com” y buscar si a través de comandos para filtrar la información existen otros dominios anclados a dicha IP.

Figura 10. Aplicación nslookup a la url del sitio

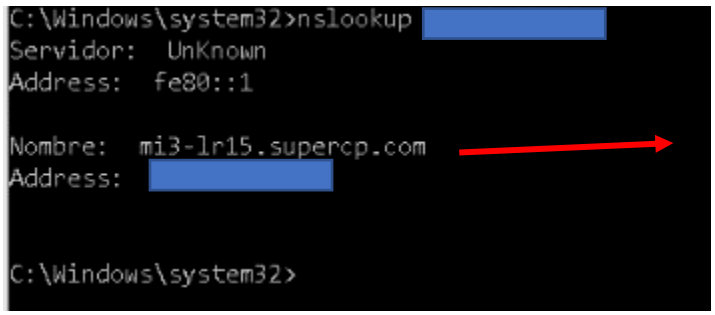


Fuente: elaboración propia

Como se observa, la herramienta nslookup permite identificar información sobre el dominio y dirección del servidor *web,* en el cual funciona la aplicación o plataforma.

A continuación, se realiza la misma prueba, pero con la dirección IP encontrada para comprobar si resuelve la dirección y muestra el dominio corpoambatoemprende.com y a su vez analizar si existen otros dominios anclados a la misma IP.

Figura 11. Aplicación *nslookup* a la dirección ip del sitio

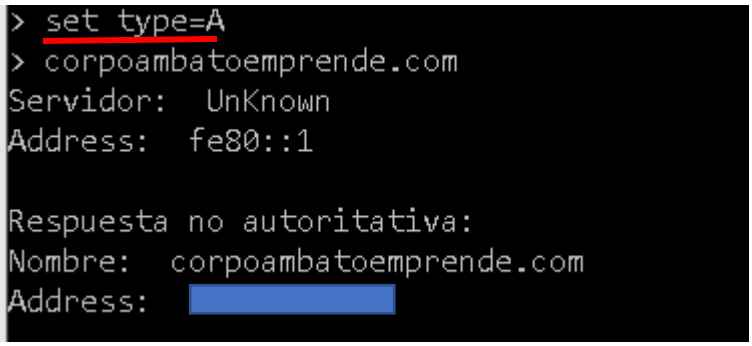


Fuente: elaboración propia

El resultado obtenido confirma que el dominio no cuenta con dirección IP propia, no muestra el dominio de corpoambato como tal, sino que otorga el dominio del acceso al hosting o al cpanel. No obstante, si se trata de ingresar esa dirección no da resultado debido a que no se sabe en qué puerto esta alojada y solo arroja un error de ingreso al CPanel.

Adicionalmente, se realiza una búsqueda con una configuración de comandos extra, como el que se muestra a continuación. La inclusión del comando *"set type=A",* el cual identifica direcciones IP alternas a las que ya se identificaron.

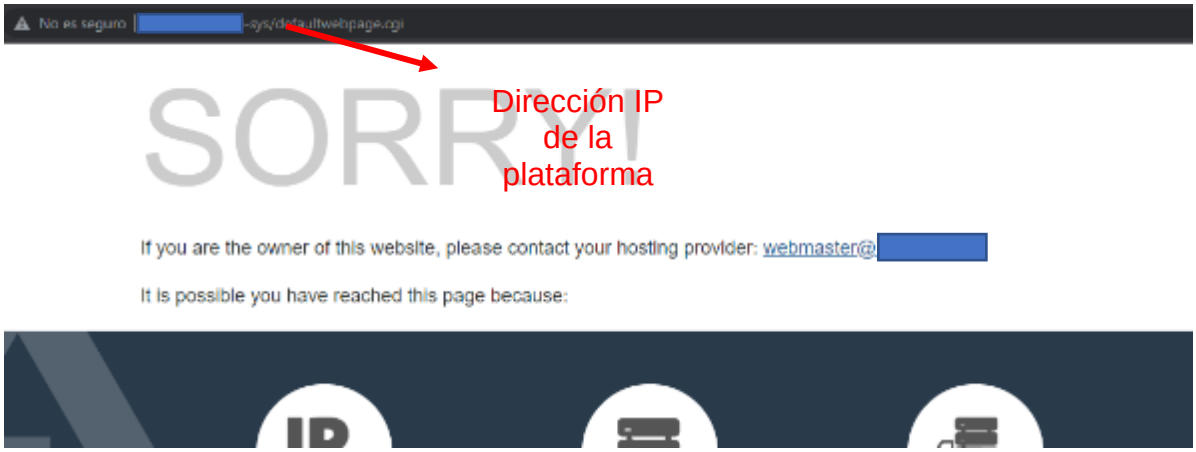
Figura 12. Aplicación nslookup a la url del sitio 2



Fuente: elaboración propia

Se observa la dirección IP del servidor alojado, por lo que se procede a ingresar a la misma para verificar el acceso al servidor

Figura 13. Ventana de Base de datos



Fuente: elaboración propia

Se observa que, si buscamos la dirección IP de la plataforma, solo se ingresa a la base de datos del servidor, el sitio no posee una dirección IP que redirija a la plataforma.

- **Prueba 2: Use huellas digitales en el servidor web**

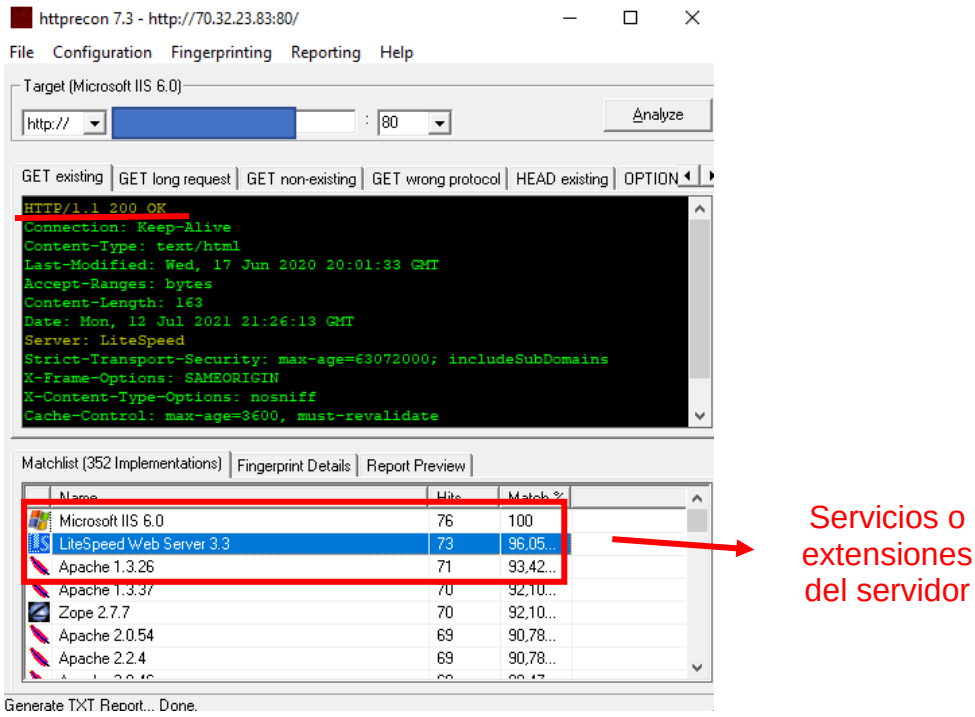
Objetivo de la prueba

El objetivo de esta prueba es encontrar el tipo de servidor alojado en la plataforma para encontrar y analizar vulnerabilidades conocidas por versiones antiguas o desactualizadas para determinar el nivel de riesgo.

Ejecución de la prueba

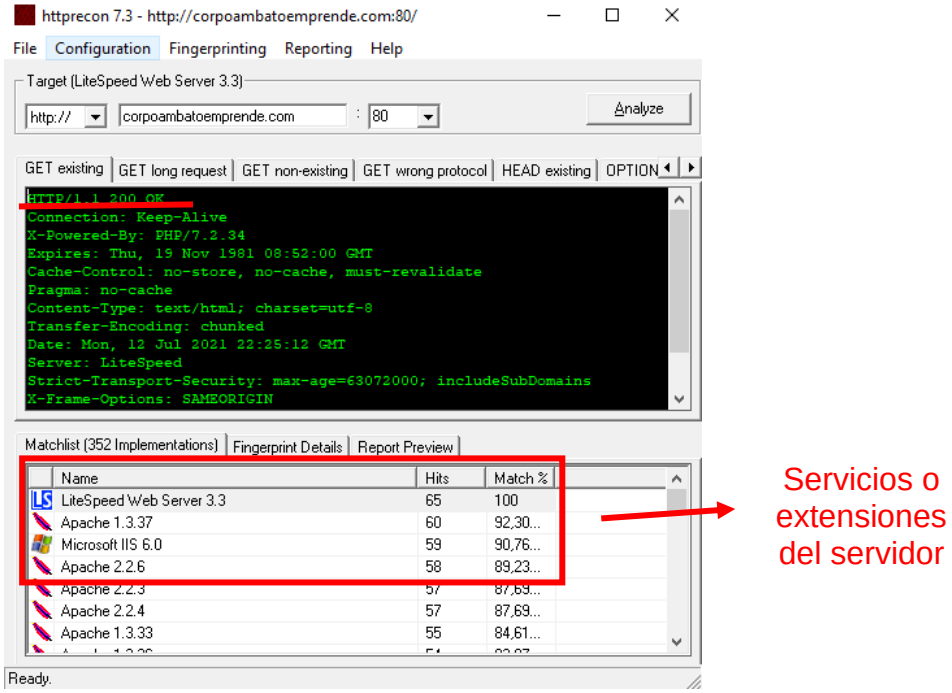
Para la ejecución de la prueba, se utiliza la herramienta *httprecon,* el cual da un resultado aproximado sobre los servicios que funcionan dentro del servidor con sus correspondientes versiones.

Figura 14. Información del tipo servidor *web* – *Httprecon* – dirección IP



Fuente: elaboración propia

Figura 15. Información del tipo de servidor *web* - *Httprecon* - URL



Fuente: elaboración propia

Como se observa en la imagen, las pruebas según la herramienta *httprecon* arrojan resultados distintos tanto para la dirección IP como para la URL, pero se mantiene dentro del margen de coincidencias en cuanto al tipo de servidor:

-*Microsoft ISS* 6.0 → **URL** = 100%, **IP** = 90,76%,

-*LiteSpeed Web Server* 3.3 → **URL** = 100%, **IP** = 96,05

-Apache → **URL** = 92,30, **IP** = 93,42%

No se sabe con exactitud que versión de Apache funciona dentro del servidor web, puesto que, como se observó en las capturas, aún no se da por hecho que el servidor funcione precisamente sobre Microsoft ISS y en conjunto con *LiteSpeed*, el porcentaje varía al escanear la URL y la dirección IP por separado, por lo que no se determina exactamente el tipo de servidor.

- **Prueba 3: Revisión de meta-archivos del servidor web en busca de fugas de información**

Objetivo de la prueba

La siguiente prueba tiene como objetivo evaluar archivos "*robots.txt*" que contienen información sobre directorios o rutas de carpetas de la aplicación o sitio *web* que se encuentre en modo acceso, los cuales son utilizados para encontrar información sensible.

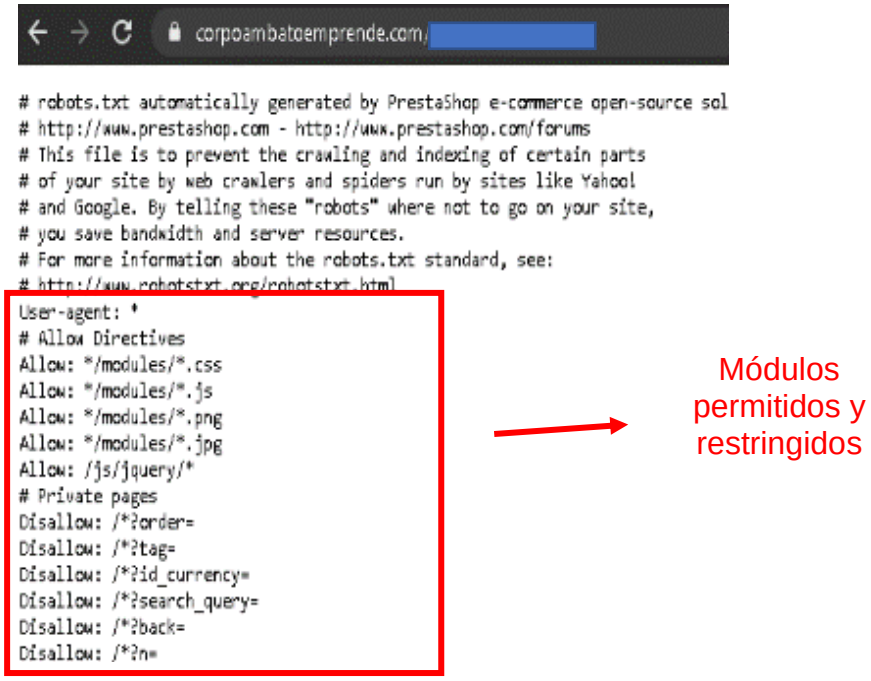
Ejecución de la prueba

Para la ejecución de la prueba, se hace uso del navegador Google para encontrar información textual sobre lo que la herramienta "robots.txt" tiene registrado. Así mismo, se espera encontrar información sobre los siguientes aspectos:

- ***User-agent:*** Muestra información sobre los motores de búsqueda y son utilizados para analizar la aplicación.
- ***Disallow:*** Permite determinar cuáles son los recursos a los que los *spiders, robots o crawlers* tienen prohibido mostrar información.
- ***Allow:*** Es la información a la que se tiene acceso para las herramientas de análisis ya mencionadas como "*robots.txt*".
- ***Sitemap:*** Esta información constituye todos los datos sobre el mapa del sitio y está en formato *xml*.

La finalidad de la prueba es encontrar archivos que posean información de contenido riesgoso que sea utilizada para realizar un ataque. Por ello, en la siguiente figura 16, se observa informacion recolectada.

Figura 16. Información de *"robots.txt"* – Google - URL



Fuente: elaboración propia

Figura 17. Información de "robots.txt" - Google - URL

Fuente: elaboración propia

Algunos de los módulos, como se observa en la figura 16, se encuentran en modo acceso, pero en realidad se encuentran limitados hasta cierto nivel, dentro de los parámetros restringidos para el acceso como se contempla en la captura 17, se muestran en modo "*Disallow*", es decir, anula dicho acceso. No obstante, mucha

información obtenida de la instrucción *robots.txt* son meras indicaciones, así que nada está asegurado.

- **Prueba 4: Enumerar aplicaciones en el Servidor *Web***

Objetivo de la prueba

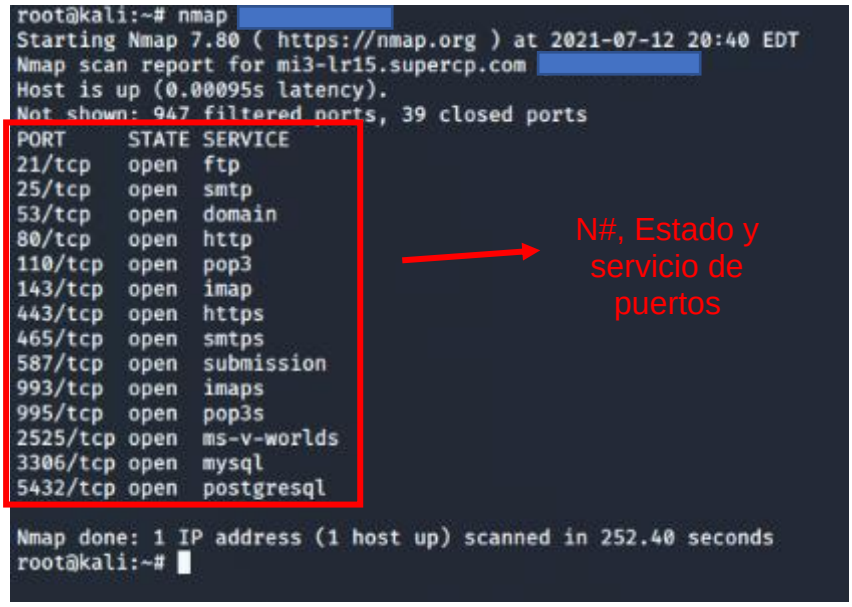
Para la siguiente prueba, se busca aplicaciones *web* que particularmente están hospedadas en el servidor *web,* pues resulta que muchas aplicaciones suelen estar mal configuradas, lo que deja expuesto a varios usuarios a ser víctimas de ciberdelincuentes que aprovechan este error para buscar vulnerabilidades.

Ejecución de la prueba

Se utiliza la herramienta *nmap* sobre el sistema operativo LINUX, el cual permite escanear puertos y reconocer servicios alojados en el servidor.

En la figura 18, se contempla los datos recolectados sobre puertos y servicios de aplicaciones que giran en torno a la ejecución del servidor *web,* el cual se aloja la plataforma de CorpoAmbato.

Figura 18. Información de puertos y servicios – Servidor *web* – Nmap - IP



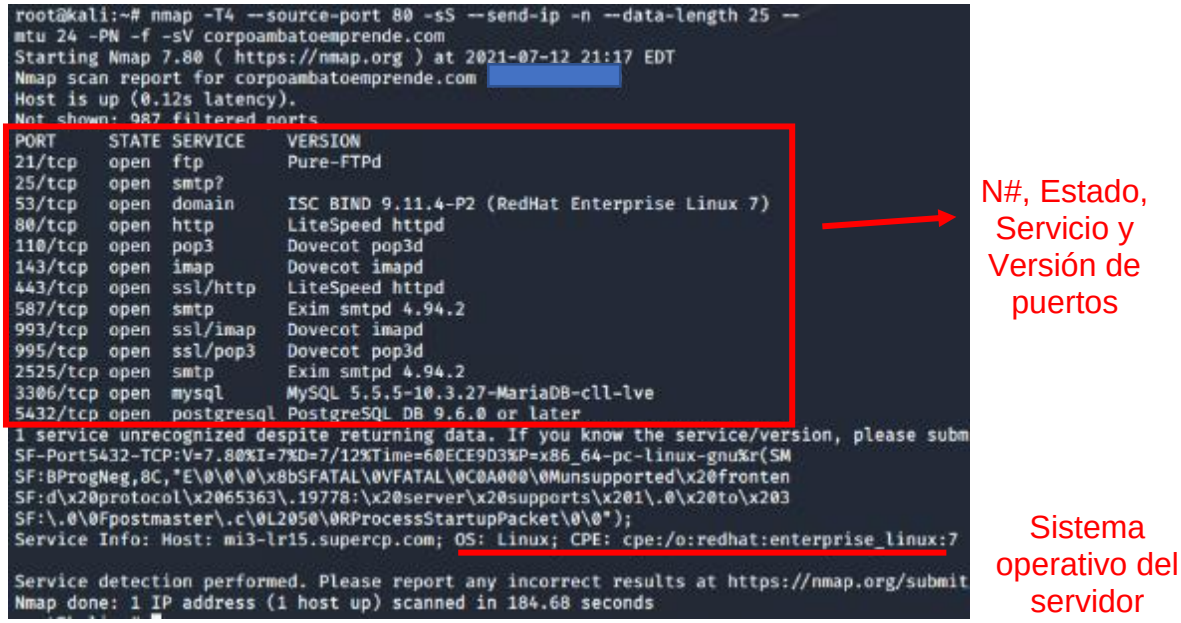
Fuente: elaboración propia

Al escanear con la herramienta mencionada da como resultado el puerto, estado y servicio en funcionamiento, pero no representa ningún riesgo por ahora, solo muestra puertos y servicios públicos.

A continuación, se realiza una búsqueda avanzada por parte de la misma herramienta *nmap* a través del siguiente comando:

nmap -T4 --source-port 80 -sS --send-ip -n --data-length 25 --mtu 24 -PN -f -sV

Figura 19. Reporte de datos *script – Nmap*



Fuente: elaboración propia

En este caso, la búsqueda dio como resultado información como: puertos abiertos, sistema operativo, servicios y su versión.

- **Prueba 5: Revisar comentarios en la página *web* y metadatos por fugas de información**

Objetivo de la prueba

La presente prueba tiene como objetivo encontrar comentarios y metadatos detallados dentro del código HTML o código fuente para hallar información interna de riesgo importante que suele estar disponible para potenciales atacantes. Las pruebas se realizan con la finalidad de determinar si existen fugas de algún tipo de información

Ejecución de la prueba

Para la ejecución de la prueba, se utiliza el navegador como herramienta para observar la estructura HTML de la plataforma por medio del visualizador de código fuente.

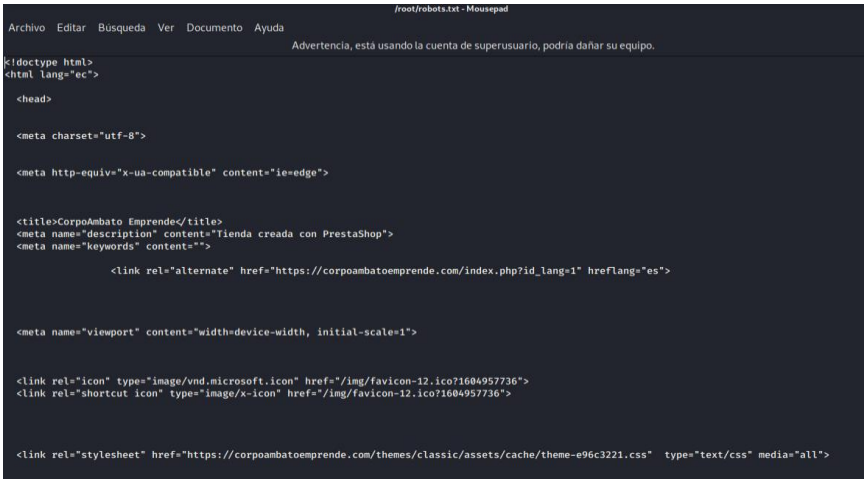
Figura 20. Código fuente de la plataforma – *Google Chrome*

Fuente: elaboración propia

Se aprecian etiquetas *html* de tipo meta, las cuales sirven para para transmitir metadatos mediante una descripción de los atributos deseados. También, se observa script de tipo JS (JavaScript) y elementos *link rel* para enlazar hojas de estilo.

Adicionalmente, se utiliza la herramienta *curl,* el cual, mediante el archivo de texto “robots.txt”, permite recolectar información sobre el código fuente de la plataforma.

Figura 21. Código fuente de la plataforma – Curl



Fuente: elaboración propia

A través del archivo de texto robots.txt, se pudo analizar la información obtenida por la herramienta mencionada para verificar de la misma forma el código fuente de la plataforma.

- **Prueba 6: Identificar los puntos de entrada de la aplicación**

Objetivo de la prueba

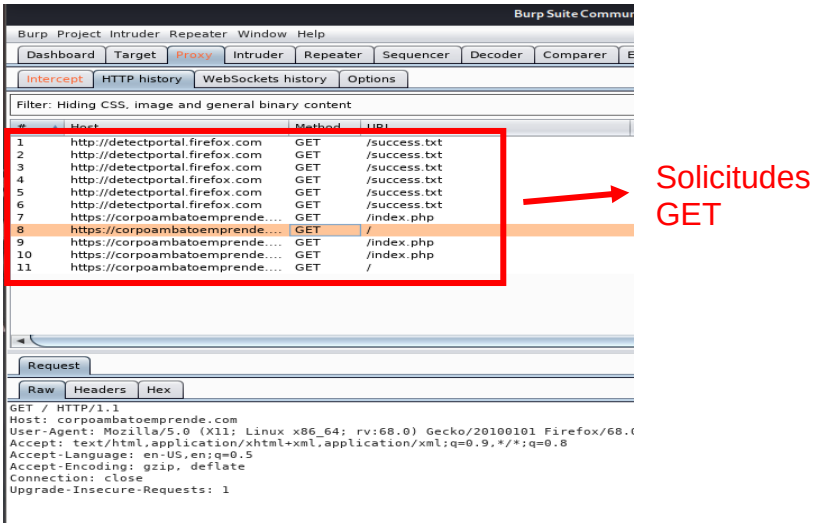
En la siguiente prueba, se establece como objetivo comprender las solicitudes y respuestas enviadas mediante la aplicación *web*, así que se identifican y analizan, por un lado, el método *GET,* que se activa cuando ejecuta una señal de envío de formulario "*Submit*" y, por otro lado, el método *POST* realiza la misma acción en un segundo plano, es decir, no es observado a simple vista por el usuario.

Ejecución de la prueba

Para la ejecución de la prueba, se hace uso de la herramienta *Burp Suite*, el cual es una herramienta de análisis que sirve para interceptar información entre el navegador y el servidor que aloja la aplicación.

En la siguiente figura 22 se contemplan los métodos *GET* que la plataforma envía a través del servidor hacia nuestro equipo.

Figura 22. Método *GET – Burp Suite*

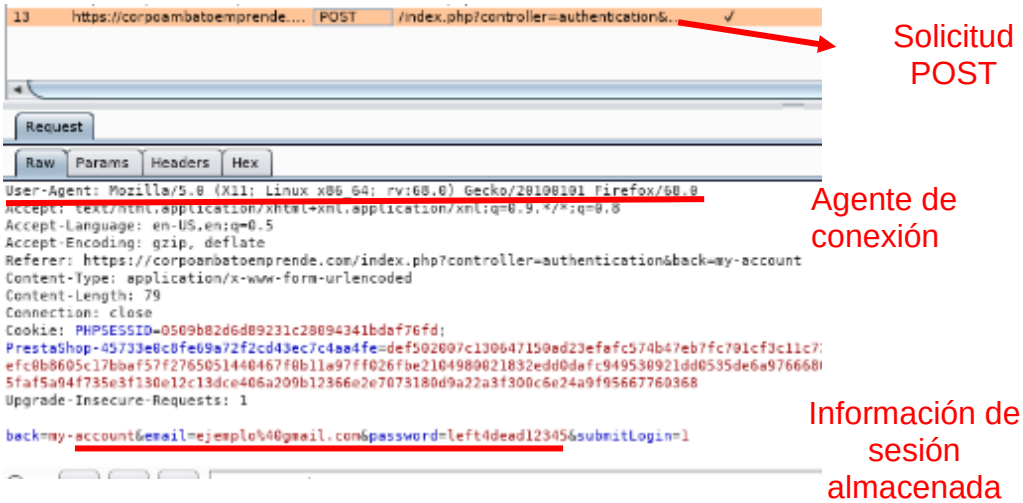


Fuente: elaboración propia

La información, que se aprecia en la siguiente imagen corresponde solicitudes de tipo *GET,* los cuales son accionados al ingresar al sitio o plataforma y la clasificación en la herramienta depende de las solicitudes presentes como: *RAW, HEADERS, HEX, HTML y RENDER* para su posterior análisis de vulnerabilidades.

Así mismo, el método *POST,* se aprecia a continuación, en la captura 23.

Figura 23. Método *POST – Burp Suite*



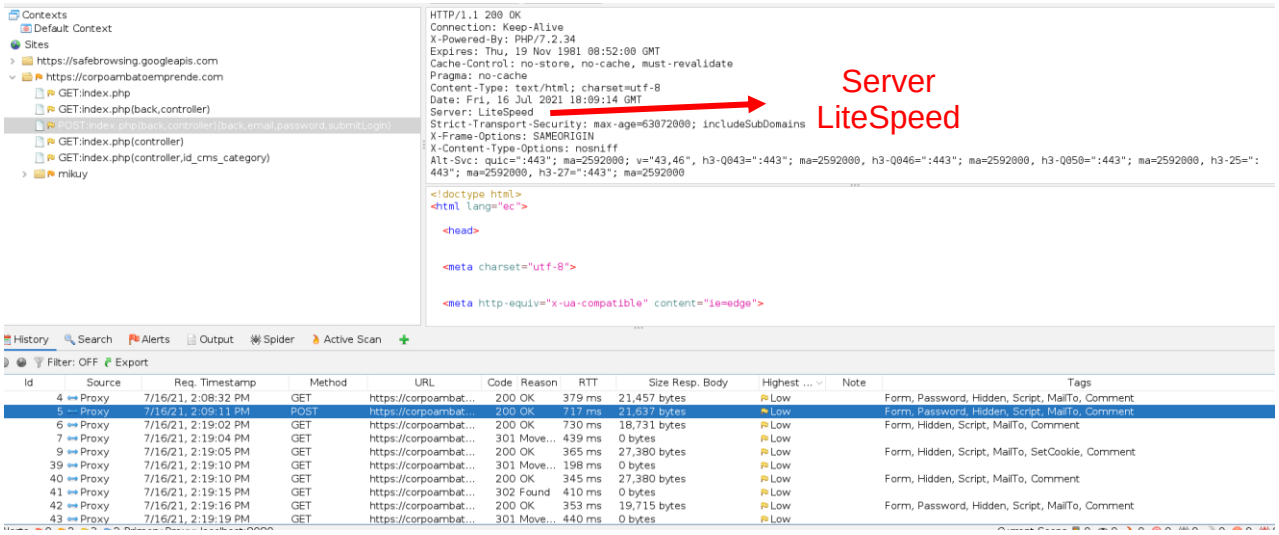
Fuente: elaboración propia

Una vez hecha la solicitud necesaria para accionar el método *POST,* se observa y analiza la información clasificada en categorías mencionadas anteriormente para identificar vulnerabilidades en la misma.

Como tal las solicitudes enviadas nunca tuvieron respuesta debido a que el servidor las bloquea y no permite que obtenga información sensible, que se detecta cuando responde dicha solicitud *BurbSuite*.

Adicionalmente, se analizan los métodos *GET* y *POST* a la vez mediante la herramienta *OWASP ZAP*, lo que permite encontrar información detallada de la misma.

Figura 24. Métodos *GET* y *POST* – *OWASP ZAP*



Fuente: elaboración propia

Un método avanzado de escaneo corresponde a la siguiente imagen, el cual, mediante la herramienta correspondiente, selecciona y clasifica información sobre Spiders o alertas de vulnerabilidades encontradas en las solicitudes de navegación por la plataforma para que en la misma ejecute ataques informáticos de tipo (SQLi, XSS, descubrimiento de ficheros, entre otros).
Se descubre información sobre la estructura de la plataforma y su relación con cada pestaña.

- **Prueba: 7 Mapear rutas de ejecución a través de la aplicación**

Objetivo de la prueba

El objetivo de esta prueba es comprender la estructura de la aplicación por medio de analizar los flujos de trabajo de los principales servicios.

Ejecución de la prueba

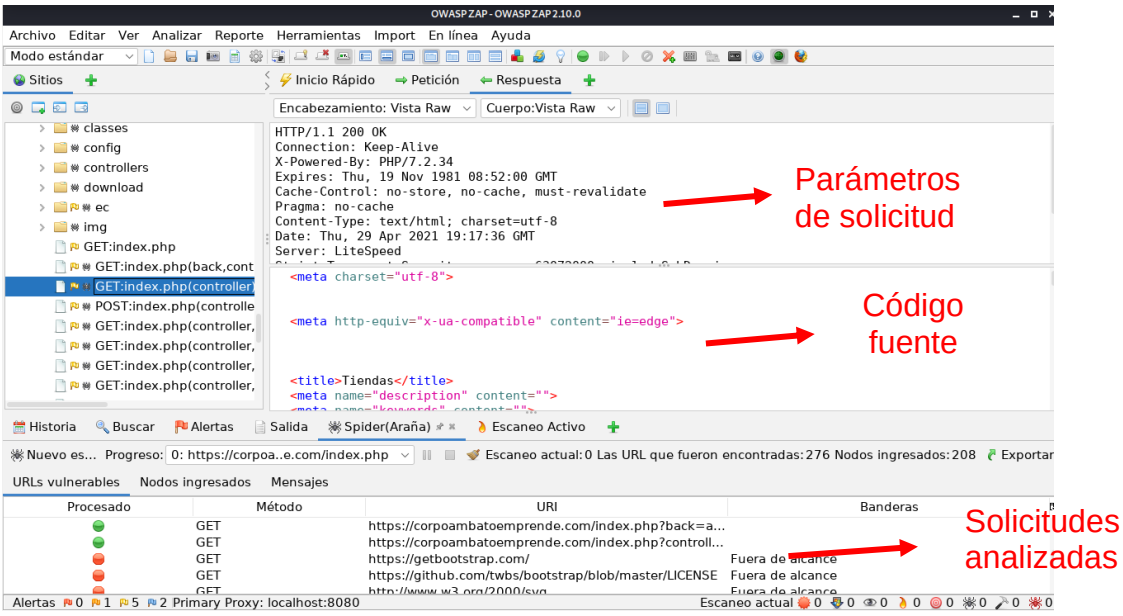
Para la ejecución de la prueba, se hace uso de la herramienta OWASP ZAP, permite descubrir nuevos recursos de la URL analizada y otorga información detallada de la misma.

Se espera encontrar información sobre los siguientes aspectos

- Árbol de directorios
- Directorios sensibles
- Archivos prohibidos
- Parámetros y variables en las URL
- Directorios Administrativos
- Mapa del sitio
- Interfaces de inicio de sesión
- Metadatos

En la siguiente figura 28, se identifican los metadatos y el mapa, en el cual está construida la plataforma y sus componentes.

Figura 25. Árbol de directorios y Metadatos – OWASP ZAP



Fuente: elaboración propia

Se aprecia el método *GET* marcado con color rojo refiriéndose a una alerta presente en la plataforma como una vulnerabilidad o simplemente un falso positivo eso depende del análisis correspondiente.

En la siguiente figura 26, se contempla la estructura de la plataforma, muestran las pestañas relacionadas unas a otras con las que cuenta y así mismo los módulos de funcionamiento.

Figura 26. Infraestructura de la plataforma – OWASP ZAP

Fuente: elaboración propia

En esta figura la herramienta encontró información a través de los *spiders* y la ordenó de forma estructurada en relación con el contenido de la plataforma.

- **Prueba 8: *Framework* referencial para el uso de huellas digitales en aplicaciones *web***

Objetivo de la prueba

El objetivo de la prueba es determinar un *framework* referencial para la búsqueda de vulnerabilidades dentro de la aplicación o sitio *web*, por lo que se espera encontrar información relevante sobre proveedores y versiones de *frameworks web.*

Ejecución de la prueba

Para la ejecución de la prueba, se hace uso de la herramienta *WhatWeb,* la cual permite escanear información tanto de forma activa como pasiva sobre varios tipos de tecnologías o datos de encabezados *HTTP* de servidores *web*.

A continuación, en la figura 30, se muestra información recolectada a través de la ejecución en la línea de comandos Linux.

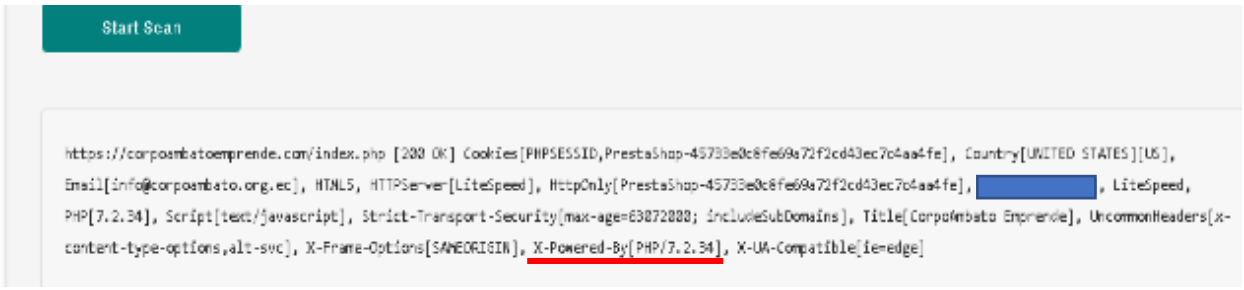
Figura 27. Comando *whatweb* – Kali Linux

Fuente: elaboración propia

Los resultados no mencionan al apartado *"X-Powered-By",* el cual almacena la versión del *framework*. No obstante, se encontró información sobre el servidor, en donde se ubica, tipo, dirección, entre otros.

En la siguiente figura 28, se observa el uso de otra herramienta para encontrar información el *framework.*

Figura 28. Escaner *Whatweb online – Hacker Target*

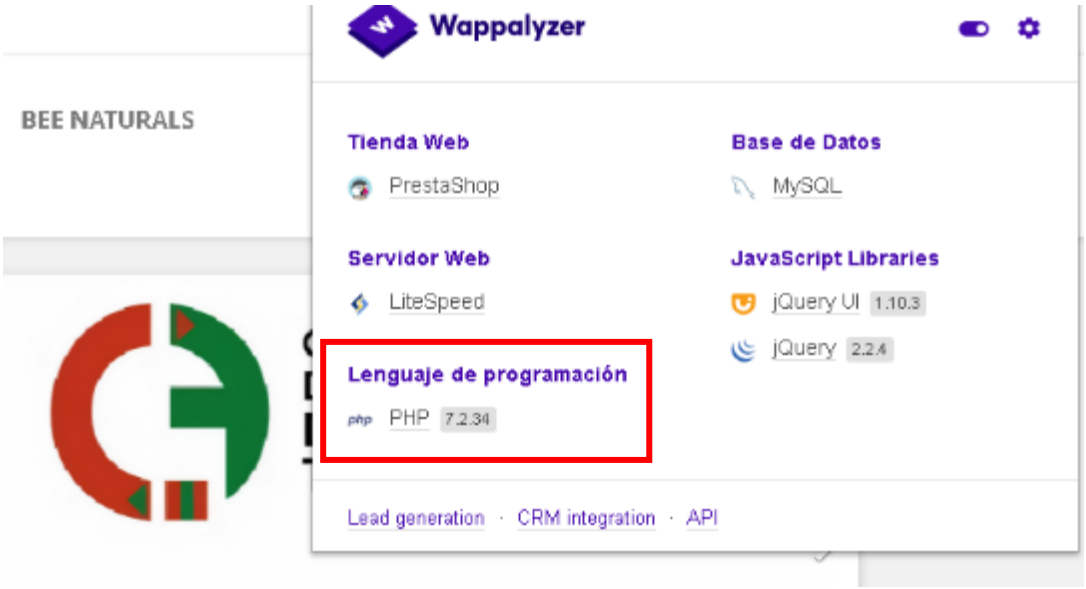


Fuente: elaboración propia

Se contempla el resultado marcado con rojo, el cual se trata de la versión PHP 7.2.34, a esta vulnerabilidad se la conoce como fuga de información.

Adicionalmente en la siguiente figura, se hace uso de una extensión del navegador *web Google Chrome* para determinar información adjunta sobre tecnologías utilizadas dentro un sitio *web*.

Figura 29. Tecnologías web – Extensión Wappalyzer



Fuente: elaboración propia

Aquí, se muestra información sobre el tipo de plataforma, servidor, base de datos, lenguajes y script de tipo JS empleados para el funcionamiento de la plataforma, lo que confirma que la misma fue creada con lenguaje PHP que por defecto *Prestashop* emplea para escribir sus plataformas.

2.3.2. Fase II – Pruebas de gestión de configuración y desarrollo

Para la siguiente fase, se realizan pruebas que están enfocadas, en su mayoría al análisis de la arquitectura de la aplicación o plataforma, con las cuales se espera obtener información sobre código fuente, métodos HTTP permitidos, métodos de autentificación, entre otros; utilizados por ciberdelincuentes para encontrar información sensible y necesaria en cuanto a realizar ataques informáticos se refiere. Al respecto, los autores Paredes et al. (2011), sostienen que la importancia de la gestión de configuración recae en la calidad de la misma, pues resulta que algunas fases como control de cambios o control de versiones dentro de una aplicación de software tienen que ser correctamente asignadas al personal responsable para su configuración, lo que en este caso, el personal de auditorías

de configuración adquiere un papel importante en la disponibilidad e integridad de la información, la aplicación respectiva es la que provee y muestra la misma.

- **Prueba 9: Configuración de la plataforma de aplicaciones de pruebas**

Objetivo de la prueba

El objetivo de la prueba es determinar errores o bugs dentro de una configuración de los elementos individuales que conforman la arquitectura de una aplicación.

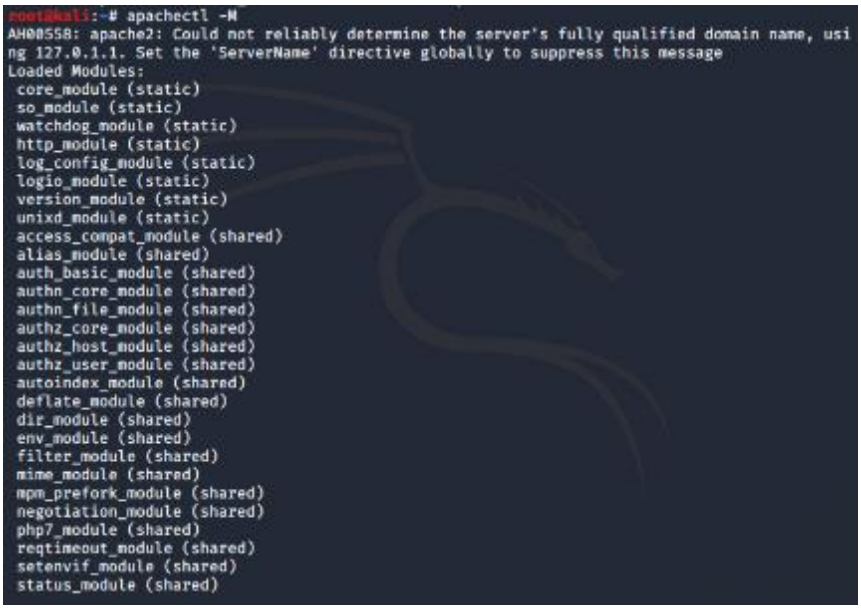
Ejecución de la prueba

Para la ejecución de esta prueba, no es necesaria la URL o dirección IP de la plataforma debido a que los comandos solo se ejecutan dentro del servidor, el cual, por seguridad, no se tuvo acceso. No obstante, se listan una seria de comandos que permiten revisar la configuración interna del servidor.

- apache2 –L
- apachectl –M
- apache2ctl –t –D DUMP_MODULES
- httpd –M
- /usr/local/apache22/bin/httpd –M

A continuación, en la siguiente figura 30, se aprecia una muestra de lo que se pudo haber obtenido si se consiguiese realizar las pruebas.

Figura 30. Módulos activos – Apache



Fuente: elaboración propia

Todos los módulos mostrados permiten a los administradores de servidores *web* de la plataforma agrupar y modular ciertas funcionalidades para su funcionamiento.

- **Prueba 10: Manejo de extensiones de archivo de prueba para información confidencial**

Objetivo de la Prueba

En la presente prueba tiene como objetivo buscar extensiones archivos de los servidores que sirven para determinar tecnologías, idiomas y accesos (*pluggins*), lo que significa que son utilizados para cumplir con solicitudes del servidor *web*. Este tipo de archivos son de suma importancia para el evaluador de vulnerabilidades en torno a penetración de información subyacente de una aplicación web, permite determinar el escenario de ataque a usar en este tipo de tecnologías.

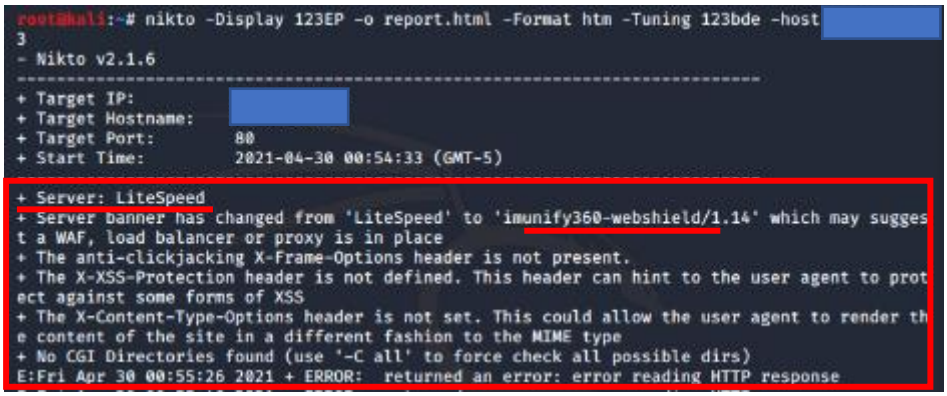
Ejecución de la prueba

Para la puesta en marcha de la prueba, se tuvo en cuenta la utilización de la herramienta *Nikto* mediante el empleo del siguiente comando:

nikto -Display 1234EP –o report.html –Format htm –Tuning 123bde –host 70.X.X.83

A continuación, en la figura 31, se procede a la ejecución de la siguiente sintaxis para el análisis correspondiente.

Figura 31. Manejo de peticiones – *Nikto*

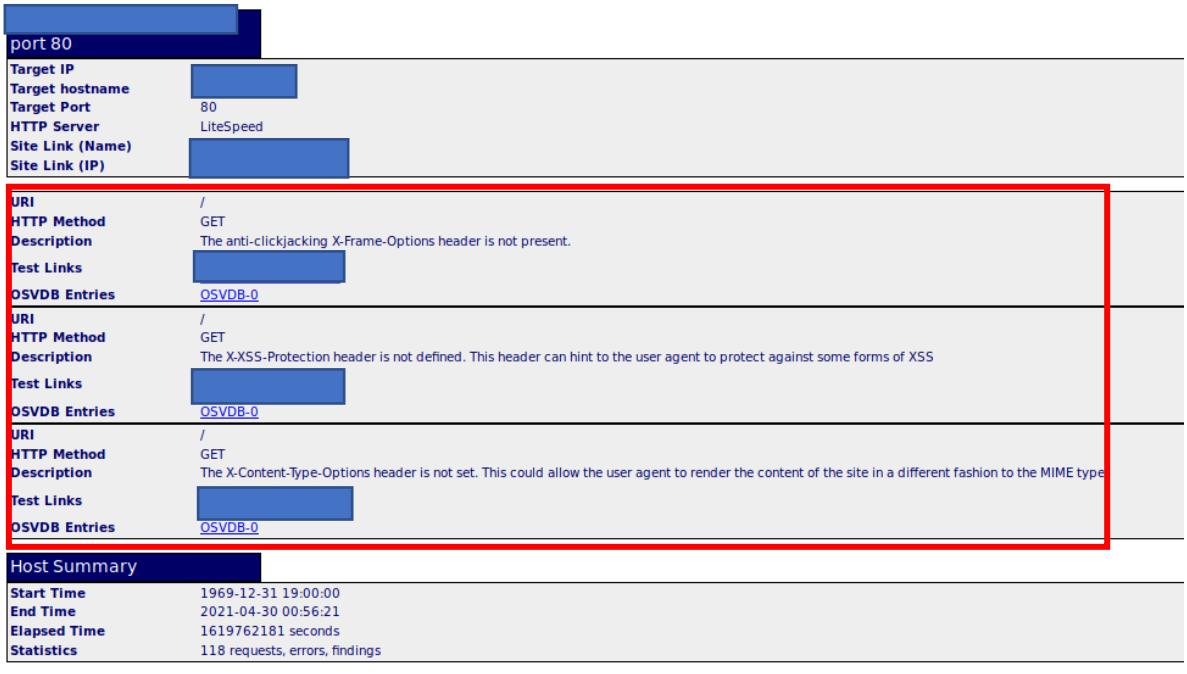


Fuente: elaboración propia

Se reconoce en base la siguiente información el tipo de servidor utilizado nombrado como *LiteSpeed*, el cual es un servidor moderno de gran velocidad de rendimiento capaz de soportar cargas de trabajo muy potentes mediante la implementación de una arquitectura basada en eventos, por lo que hace que todo el trabajo sea realizado por una menor cantidad de procesos a comparación de otros servidores. Así mismo, se evidencia que el servidor no cuenta con protección de encabezado X-XSS, que evita ataques *cross-site-scripting, es decir, aquellos* que suceden mediante la explotación de la confianza que tienen los usuarios al navegar en un sitio de mucha recurrencia en particular. No obstante, debido a que el servidor ya cuenta con seguridad para evitar mostrar información privilegiada mediante este tipo de escáner, se procedió a cancelar la prueba, pues no se pudo encontrar más información relevante dirigidos a realizar ataques informáticos.

A continuación, en la figura 32, se procede a abrir el archivo html creado al momento de ejecutar el comando

Figura 32. Reporte en formato *HTML – Nikto*



Fuente: elaboración propia

En la captura, se aprecia el mismo reporte, pero de forma más detallada y completo sobre el proceso de manejo de peticiones al realizar la prueba

- **Prueba 11: Revisar archivos antiguos, de copia de seguridad y sin referencia**

Objetivo de la prueba

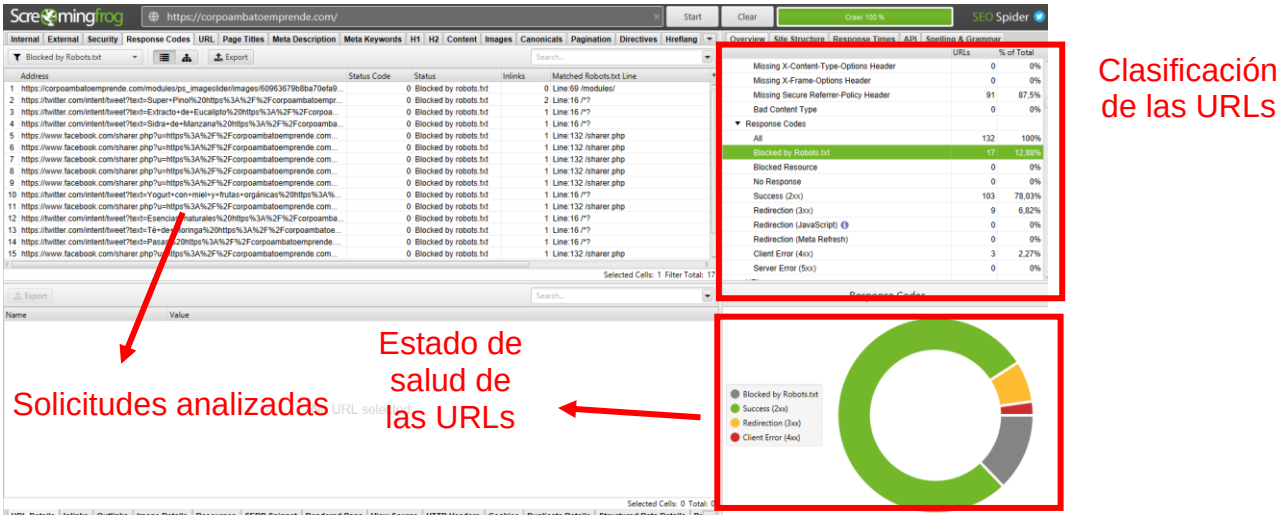
El objetivo de la siguiente prueba como lo indica el título es descubrir archivos olvidados y sin referencia, los cuales contienen información sensible sobre la infraestructura o credenciales de usuarios.

Ejecución de la prueba

Se hace uso de la herramienta de escaneo *Screaming Frog,* el cual, mediante el análisis completo hacia cualquier tipo de sitio *web,* permite comprobar estados de salud de las *urls*, enlaces internos o externos y hacer un mapa de la estructura del sitio.

A continuación, en la siguiente figura 33, se contempla el análisis de la plataforma.

Figura 33. Información salud de *URL – Screaming Frog*



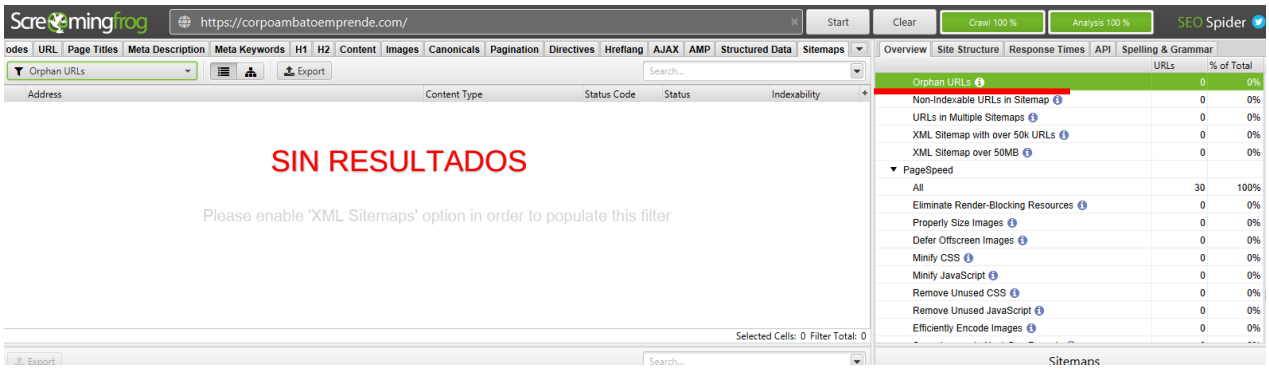
Fuente: elaboración propia

La herramienta permite identificar información detallada y ordenada en gráficos sobre la salud de la URL, como se observa en la imagen, hay un 78,03 % de *urls* que responden de forma correcta, es decir, que se encuentran en buen estado de funcionamiento, lo que deja al resto impartidos en estado bloqueado por los robots,

redireccionados y errores de ejecución de solicitudes. En este caso, las *urls* que representan un riesgo son las páginas de tipo “error 404”, que en este momento de la prueba se encontraron 3 de este tipo, los cuales son aprovechados para ataques de tipo *Pishing.*

En la figura 34, se muestra cómo se procede para encontrar antiguos y sin referencia.

Figura 34. Archivos o URL sin referencia – *Screaming Frog*



Fuente: elaboración propia

Como se muestra en la figura 38, la herramienta detecta *urls* o archivos sin referencia, existe una opción de clasificación de información llamada “*Orphan url*” que significa en su traducción al español *url* huérfanas dentro de la plataforma, por lo que se determina que no cuenta con dicha vulnerabilidad

- **Prueba 12: Infraestructura de enumeración e interfaces de administración de aplicaciones**

Objetivo de la prueba

El objetivo de la siguiente prueba es encontrar interfaces de administras dentro de la plataforma o el servidor web que poseen niveles de privilegio necesario para manipular la plataforma. La finalidad de estas pruebas es revelar como estas interfaces son accedidas por un usuario estándar o no autorizado.

Ejecución de la prueba

Para esta prueba basta con modificar el dominio de la plataforma y añadir al final palabras claves que usualmente redirigen al apartado administrativo:

https://corpoambatoemprende.com/wp-admin

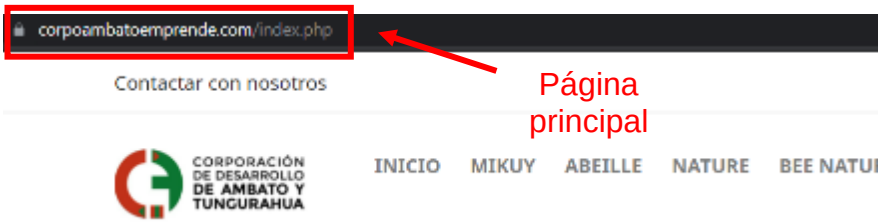
https://corpoambatoemprende.com/administrador

http://corpoambatoemprende.com/admin

https://corpoambatoemprende.com/user

A continuación, en la figura 35 se ejecuta el ingreso a la parte administrativa por medio del dominio del servidor

Figura 35. Página principal corpoAmbatoemprende.com – Navegador *web*



Fuente: elaboración propia

Cualquier intento de ingresar a la administración o *dashboard* de *prestashop* de la a través de las formas de dominio mencionadas es redirigida a la página principal, por lo que se confirma que la plataforma tiene una medida de seguridad programada para que solo los usuarios autorizados ingresen al apartado *Back End* de la plataforma.

- **Prueba 13: Métodos HTTP**

Objetivo de la prueba

El objetivo de la prueba es encontrar los diferentes tipos de métodos encargados de realizar acciones en el servidor web. Muchos de estos métodos están destinados a ayudar a los desarrolladores a implementar y testear aplicaciones que pasan por el protocolo *HTTP.* Dichos métodos son utilizados para fines adversos en cuanto a un servidor mal configurado mediante mecanismos de ataques de tipo *Cross Site Tracing (XST).*

Ejecución de la prueba

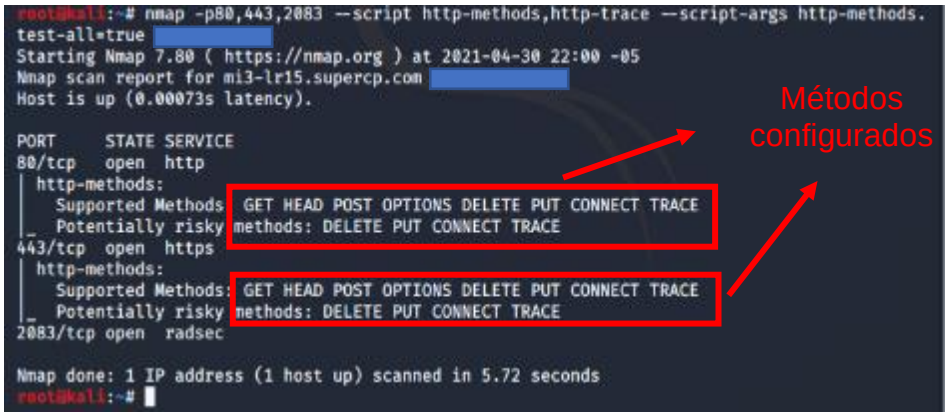
Para la puesta en marcha de la prueba, se ejecutan comandos para rastreo de puerto, por ejemplo, el siguiente comando sirve para identificar métodos realizados por el protocolo *HTTP:*

nmap -p80,443,2083 --script http-methods,http-trace --script-args http-methods.test-all=true 70.32.23.83

- **-p80:** se refiere al puerto a analizar
- **--scripth http-methods:** Detecta métodos *HTTP* mediante script
- **http-trace:** Devuelve un mensaje a lo largo de la ruta del recurso de destino
- **--script-args http-methods.test:** Retorna mensajes de tipo scripts

A continuación, en la figura 36 procede con la ejecución de la prueba para conocer los métodos funcionales en la plataforma (el proceso tarda entre 1 o más minutos).

Figura 36. Métodos *HTTP – Nmap*



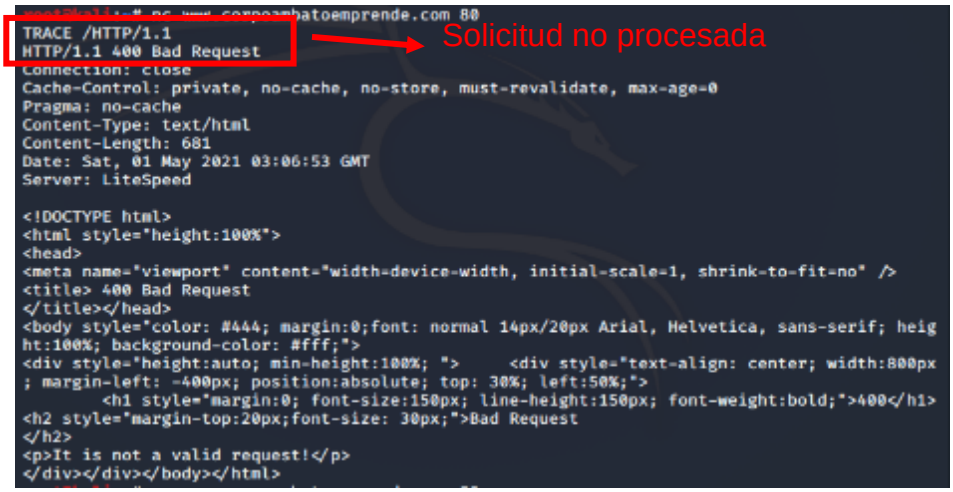
Fuente: elaboración propia

Los métodos soportados, como se observa en la imagen, poseen las siguientes vulnerabilidades:

- **PUT =** Permite al cliente subir nuevos archivos en el servidor. El atacante aprovecha este método para subir archivos ejecutables como un asp que ejecuta comandos para invocar el cmd.exe
- ***DELETE* =** Permite borrar un archivo dentro del servidor. El atacante utiliza el método para modificar el sitio web o ejecutar un ataque DoS.
- ***CONNECT* =** Este método suele permitir al atacante utilizar el servidor web como proxy.
- ***TRACE*=** Hace eco al cliente de cualquier cadena que ha sido enviada al servidor. El atacante usa este metodo a través de un ataque conocido como: Rastreo de Sitios Cruzados.

A continuación, se realiza otra prueba mediante la herramienta *netcat* para comprobar si el servidor responde a las solicitudes de los métodos encontrados mencionados anteriormente.

Figura 37. Método *TRACE – Netcat*



Fuente: elaboración propia

Al realizar la prueba, como se aprecia en la captura, se confirma que el servidor no procesa la solicitud a través del método *TRACER,* puesto que arroja el error 400, por lo que queda en constancia la ausencia de dicha vulnerabilidad.

- **Prueba 14: Seguridad de transporte escrito HTTP – HSTS**

Objetivo de la prueba

El objetivo de la prueba es corroborar que la información intercambiada entre el servidor y el usuario se realiza a través de la política de seguridad HTTP *Stric Transport Security (HSTS)* o *HTTPS.* Por eso, se espera encontrar información sobre el campo *Strict-Transport-Security,* el cual suele aparecer en la cabecera de respuestas HTTP de la aplicación, lo que indica que existe un abuso del uso del mecanismo HSTS al navegar en la aplicación o plataforma.

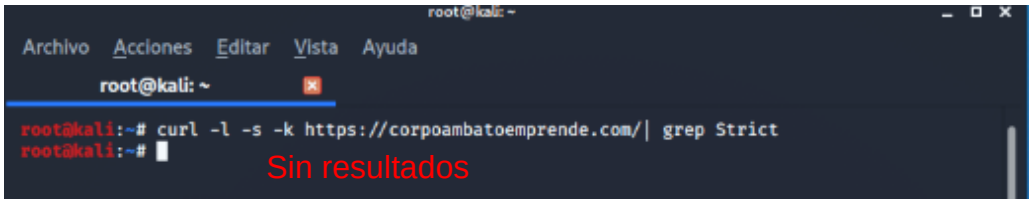
Ejecución de la prueba

Se utiliza para la puesta en marcha de la prueba un comando de la terminal como curl:

curl –I –s –k https://corpoambatoemprende.com/| grep Strict

A continuación, se procede a la ejecución del comando la siguiente figura 38.

Figura 38. Mecanismo *HSTS – Curl*

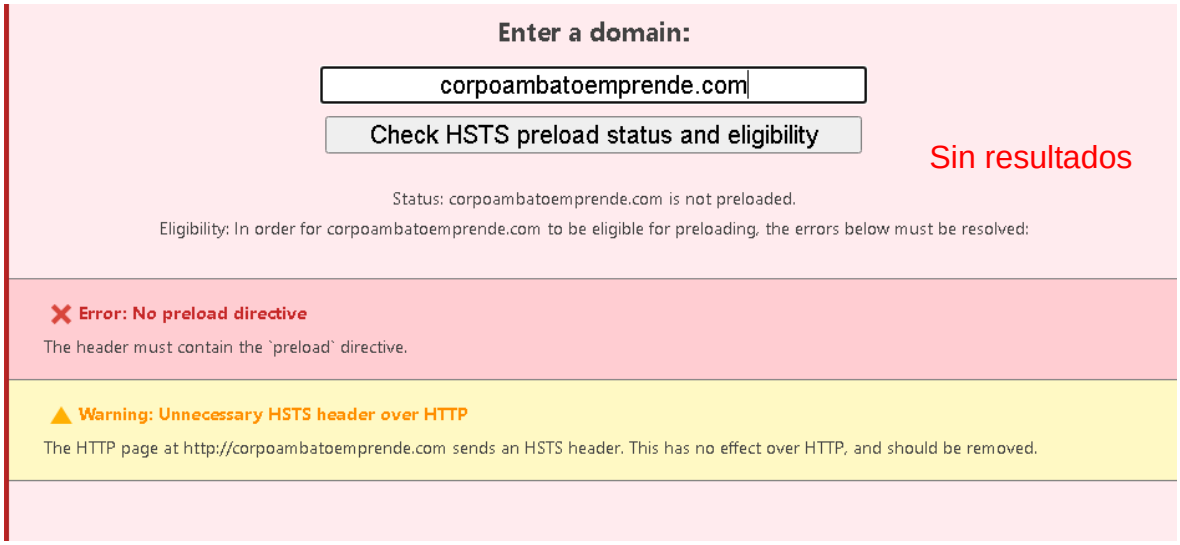


Fuente: elaboración propia

A pesar de haber ejecutado el comando, no se pudo observar la información deseada acerca del mecanismo de seguridad HSTS, por lo que se procede a utilizar herramientas alternas.

En la figura 39 observar otra herramienta de verificación del encabezado HSTS de respuesta del servidor para comprobar que este mecanismo está presente en la aplicación o plataforma

Figura 39. Encabezado *HSTS – Hstspreload*

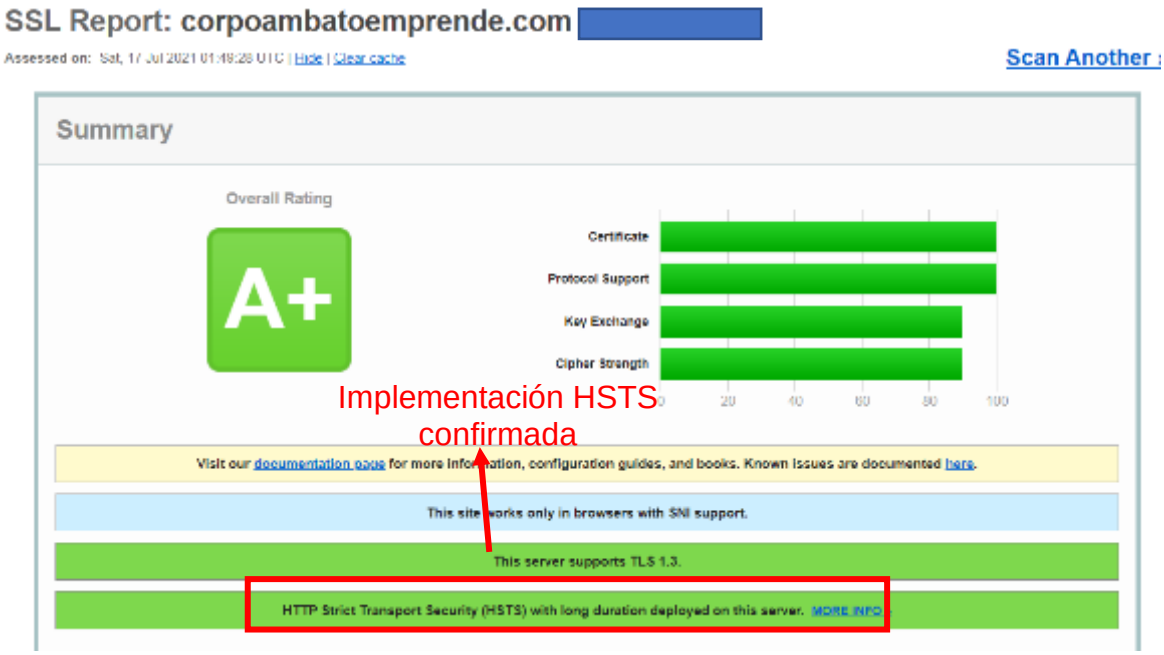


Fuente: elaboración propia

No se obtuvo un resultado al utilizar la herramienta, no muestra si cuenta con la seguridad HSTS.

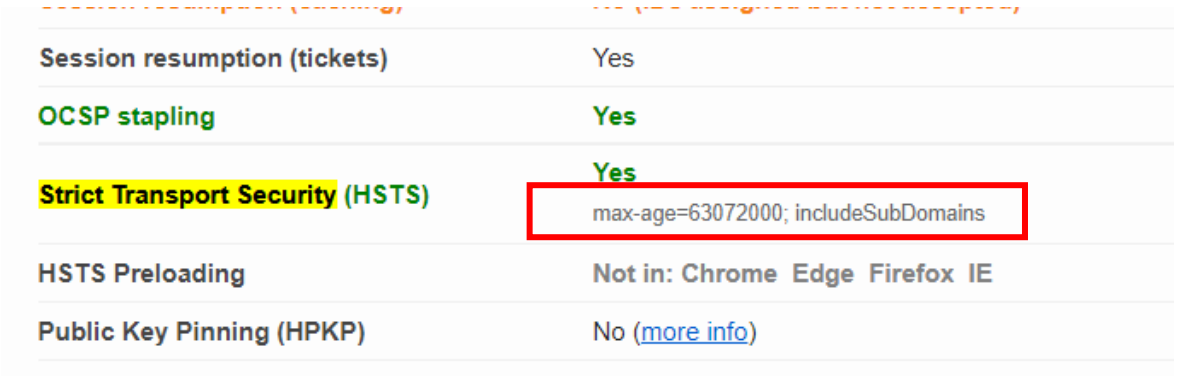
Así mismo, en la figura 40, se realizar otra prueba mediante herramientas encontradas en la red para testeo de respuestas HSTS.

Figura 40. Prueba de *HSTS – Qualys SSL labs*



Fuente: elaboración propia

Figura 41. Análisis HSTS - *Qualys SSL labs*



Fuente: elaboración propia

En este caso, sí hubo resultados, la herramienta detecta que el servidor en el que se aloja la plataforma posee la seguridad de transporte estricto HTTP (HSTS), como se muestra en la figura 40, incluso menciona la larga duración en el que convierte solicitudes HTTP en HTTPS y si los subdominios utilizan dicha seguridad (Figura 41).

- **Prueba 15: Política de dominio cruzado RIA *(Rich Internet Applications)***

Objetivo de la prueba

El objetivo de la prueba es determinar si un archivo de dominio cruzado especifica los permisos que un cliente web usa para acceder a datos en diferentes dominios. *Rich Internet Applications* (RIA) utiliza los archivos de políticas *crossdomain.xml* para permitir accesos controlados entre dominios de datos y consumo de servicios mediante tecnologías como Oracle, Java, Silverlight y Adobe, por lo que se verifica que la configuración este correcta y sin errores para evitar ataques de falsificaciones de solicitudes entre sitios.

Ejecución de la prueba

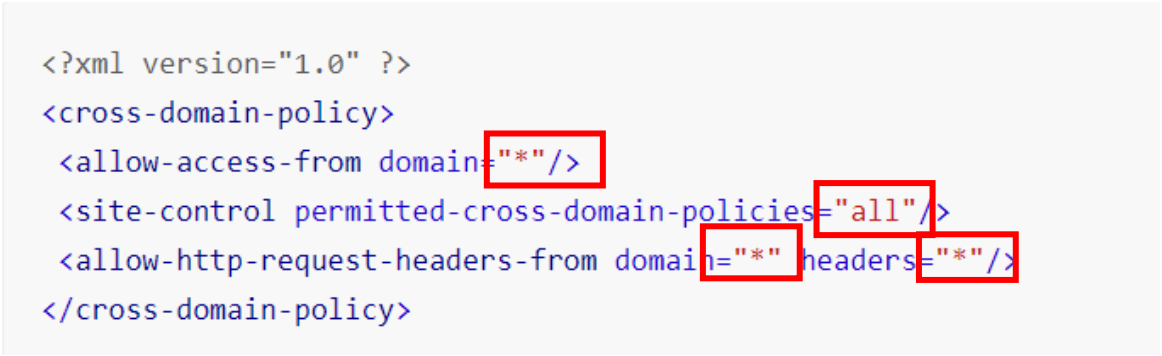
La ejecución de la prueba comprueba si existen debilidades en la política RIA, por lo que el evaluador verifica los permisos de recuperación de archivos de política *crossdomain.xml*. Para ello, se emplea la herramienta el navegador web al escribir el dominio de la siguiente forma:

corpoambatoemprende.com/crossdomain.xml

corpoambatoemprende.com/clienteaccesspolicy.xml

La prueba como tal no tuvo resultado, en pruebas anteriores, se evidenciaba que un intento de ingresar a la URL de forma modificada redirige a la página web principal, por lo que, a continuación, se presenta una captura de ejemplo sobre un archivo con políticas muy permisivas.

Figura 42. Archivo *crossdomain* – Navegador *web*



Fuente: ArcGIS Enterprise (2020)

En el ejemplo, se observa políticas con caracteres “*” o “*all*”, los cuales son excesivamente permisivas, por lo que son analizadas si presentan la vulnerabilidad asociada a falsificación de solicitudes.

El impacto que provocaría el abuso de accesos de dominios cruzados son las siguientes:

- Derrotar las protecciones CSRF.
- Leer datos restringidos o que estaban protegidos por políticas de origen cruzado.

2.3.3. Fase III – Pruebas de manejo de identidad

Esta fase tiene como objetivo validar y encontrar los roles de usuarios disponibles en la aplicación o plataforma, para lo cual se identifican los niveles de autorización de los administradores y usuarios que navegan en la plataforma, allí se configuran los permisos de acceso a información vulnerable que contiene el servidor web sobre la plataforma. Para ello, se realizan pruebas de proceso de registro para recuperar detalles de una cuenta de usuario al momento de realizar un registro o inicio de sesión fallido y a su vez comprobar la eficacia de la política de registro de nombre de usuario.

- **Prueba 16: Definición de roles**

Objetivo de la prueba

En la siguiente prueba, se busca encontrar los distintos procesos que funcionan para la creación y asignación de roles dentro de la plataforma y determinar los niveles de permisos a los cuales tienen acceso algunos usuarios y otros no.

Ejecución de la prueba

Para la ejecución de la prueba, se tiene en cuenta que, una plataforma de comercio electrónico, por lo general, tiene en operación tres tipos de usuarios encargados de controlar y navegar en la misma.

A continuación, en la siguiente tabla 4, se describen los tipos de usuarios inmersos en la plataforma.

Tabla 4. Roles y permisos

Rol	Descripción	Permisos
Cliente	Persona que entra a la plataforma web concretamente a uno de los emprendimientos y realizar las compras de los productos o servicios	Iniciar Sesión Ver información de proveedores Ver producto Añadir producto Ver carro de compra, con características como: Añadir o eliminar producto Realizar pedido en tienda, entre otros.
Visitante	Es aquella persona que solo hace ingreso a la tienda online, para ver y cotizar los productos mostrados	Ver información de proveedores Ver productos con sus características esenciales.

Fuente: elaboración propia

Se encontraron dos tipos de usuarios: el de cliente y visitante, el acceso a la parte administrativa no está disponible dentro de la plataforma al ser un área en la que ingresa exclusivamente el personal autorizado, y, por lo tanto, la forma en cómo se accede permanece oculta al público.

- **Prueba 17: De registro de usuarios**

  Objetivo de la prueba

  La siguiente prueba tiene por objetivo analizar los procesos de registro de usuario que sitios *web* tienen por defecto y en su mayoría con los correos electrónicos para comprobar que existen requisitos de identificación.

  Ejecución de la prueba

  Para la puesta en marcha de la siguiente prueba, se responden algunas preguntas orientadas a la verificación de los requisitos de identidad para que los registros de usuarios cumplan con los requerimientos de seguridad y negocios

- **¿Cualquier persona puede registrarse para acceder a los beneficios de esta?**

  En la plataforma cualquier persona con correo tiene la posibilidad de registrarse para acceder a los beneficios de esta.
- **¿Son validados por un ser humano antes de crear los registros, o se conceden automáticamente si se cumplen los criterios?**

  Al ser una plataforma para el público en general, no existe alguien que valide que usuarios tienen permiso de registrarse y cuales no, eso se comprueba a través de la ejecución del inicio de sesión una vez creada la cuenta.
- **¿Puede la misma persona o identidad registrarse varias veces?**

  Al crear una nueva cuenta es posible registrarse una sola vez, pero al momento de ingresar los mismos datos al registro de la plataforma esta, verifica que el correo electrónico ya se encuentra en uso.
- **¿Pueden registrarse usuarios para diferentes roles o permisos?**

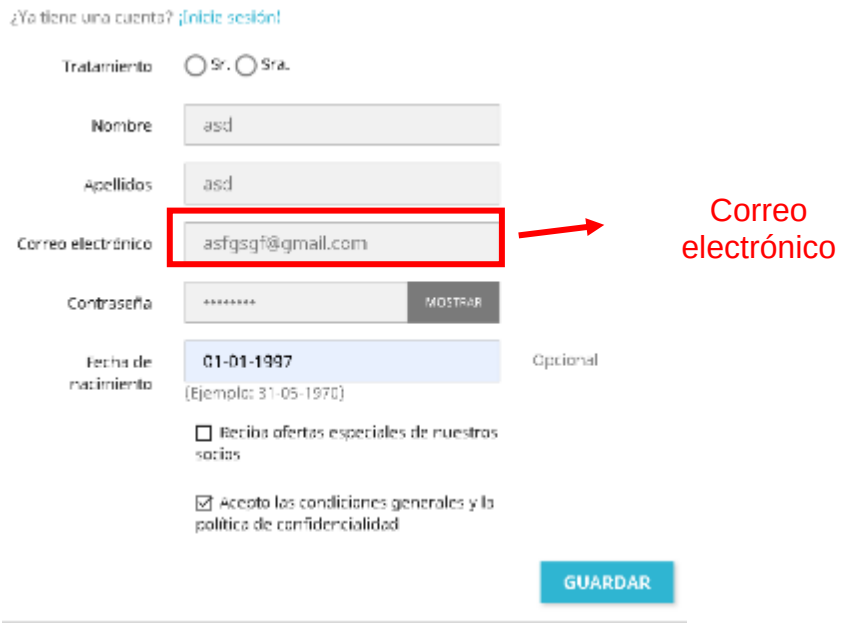
  La plataforma en si solo permite crear usuarios de tipo cliente para acceder a beneficios de perfil de usuario y guardado de productos.
- **¿Qué documento de identidad se requiere para que un registro tenga éxito?**

  No requiere de un documento de identidad para que el registro proceda a ejecutarse solo es necesario un correo electrónico ya sea verdadera o inventada.
- **¿Son las identidades registradas verificadas?**

  Las identidades registradas si son verificadas, puesto que no se repiten los mismos correos electrónicos.

A continuación, en la figura 43, se realiza por medio de la plataforma una prueba de ejemplo de registro de un usuario con correo falso.

Figura 43. Proceso de registro



Fuente: elaboración propia

En la siguiente imagen, se contempla las pruebas para responder las preguntas en torno a la verificación de requisitos de identidad.

- **¿Puede la información de identidad ser fácilmente falsificada?**

  La información no es fácilmente falsificada, debido a que, si se trata de ingresar datos no válidos, emite una alerta que afirma el error en los datos.

- **¿Puede el intercambio de información durante el registro ser manipulado?**

  No es posible, la plataforma esta alojada en un hosting privado, por lo tanto, la información de intercambio cliente-servidor es controlada por agentes externos.

- **Prueba 18: De creación de cuentas**

Objetivo de la prueba

El objetivo de la prueba es verificar qué cuentas aprovisionan a otras cuentas y de qué tipo.

Ejecución de la prueba

Para realizar la prueba, se responden las siguientes preguntas:

- **¿Existe alguna verificación, examen y autorización de las solicitudes de aprovisionamiento?**

  A través del administrador de la plataforma (CPanel), se solicita aprovisionamiento de usuario.
- **¿Puede un administrador aprovisionar a otros administradores o solo usuarios?**

  El administrador si aprovisiona a otros administradores a través de la interfaz de CPanel.
- **¿Puede un administrador u otras cuentas crear cuentas de usuario con privilegios mayores a los suyo?**

  Solo existe un administrador y cuenta con todos los privilegios y permisos disponibles, por lo que es imposible crear un usuario con privilegios mayores a los suyos.
- **¿Puede un administrador o usuario eliminar su cuenta?**

  El administrador tiene los permisos necesarios para eliminar una cuenta y un usuario común y corriente tiene la opción de eliminar su propia cuenta a través de comunicarse con el administrador de la plataforma para solicitar la eliminación permanente de la cuenta.

2.3.4. Fase lV & V – Pruebas de autenticación y autorización

En esta fase, se definen pruebas que permitan validar la seguridad que controla la forma de permitir el acceso a recursos exclusivos para aquellos que poseen permisos para ello, es decir, entender el proceso de funcionamiento de autorización, para encontrar debilidades que permitan saltarse el mecanismo de autentificación. En ese sentido, la autorización es un proceso que se activa después de la ejecución de una autentificación, por lo tanto, validaría este punto por medio de asumir credenciales validas, asociadas a un conjunto de perfiles y privilegios bien definidos. Por ende, en el desarrollo de las pruebas, se verifica la posibilidad de evitar el sistema de autorización y autenticación, mediante la detección vulnerabilidades de traspaso de rutas, o de alguna otra forma identificar maneras de escalar privilegios estipulados al evaluador.

- **Prueba 19: De transporte de credenciales en un canal encriptado**

Objetivo de la prueba

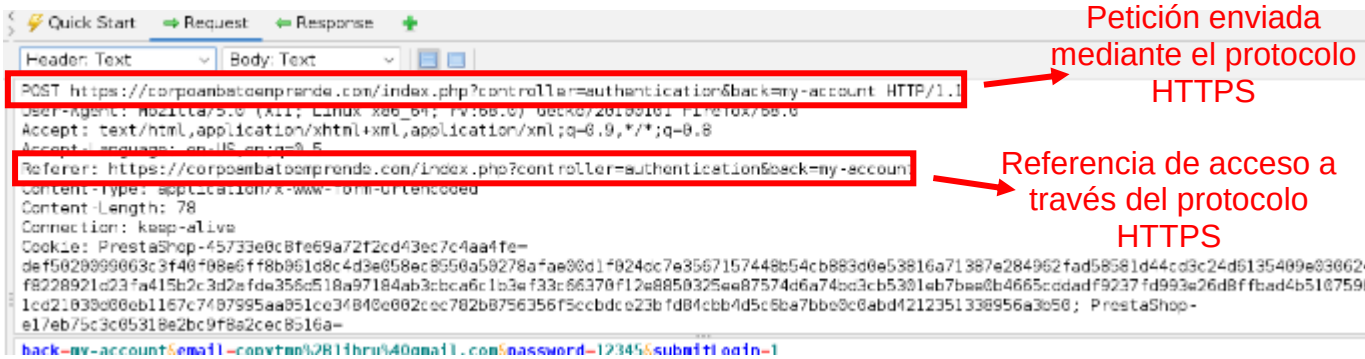
En esta prueba, se determina si existe vulnerabilidades en el transporte de credenciales por medio de canales encriptados, es decir, que al realizar solicitudes de *GET o POST* estas viajen de forma encriptada.

Ejecución de las pruebas

La forma de comprobar que el servidor responde las solicitudes GET o POST de forma encriptada es al observar las cabeceras.

A continuación, en la figura 49, se muestran los resultados del escaneo de solicitudes enfocadas a determinar la veracidad del encriptado de autentificación.

Figura 44. Solicitud *POST – OWASP ZAP*



Fuente: elaboración propia

Se confirma que la solicitud, se envía a través del protocolo HTTPS, lo que garantiza que las credenciales viajan por un canal encriptado.

- **Prueba 20: Determinar un mecanismo de bloqueo débil**

Objetivo de la prueba

Muchos sistemas de aplicaciones, servidores o sitios web utilizan para mitigar ataques de fuerza bruta el mecanismo de bloque de sesiones, es decir, el momento en que un usuario haya fallado los intentos limites que ofrece el sistema esta procede a bloquearlo e indica que lo intente más tarde. Si la plataforma no cuenta con dicho mecanismo de bloqueo estaría expuesta a ataques de fuerza bruta, por lo que un usuario mal intención tendría acceso a datos sensibles de un cliente.

Ejecución de la prueba

Para la ejecución de la prueba, se verifica que las siguientes pruebas otorguen resultados favorables:

- Evaluar la capacidad del mecanismo de bloque de cuentas para mitigar el ingreso forzado de adivinación de contraseñas.
- Evaluar la resistencia del mecanismo de liberación para abrir sin autorización una cuenta.

A continuación, se emplea la aplicación o sitio web para realizar pruebas de inicio de sesión fallidas

- **¿Cuál es el riesgo de forzado o adivinanza de contraseñas en la aplicación?**

  Existe un riesgo en exponer información personal que el cliente haya registrado en su cuenta, pero en el caso de la plataforma no existe un riesgo relevante debido a la poca probabilidad de adivinar las credenciales de una cuenta.

- **¿Basta un *CAPTCH* para mitigar el riesgo?**

  Es la forma estándar de lidiar con este ataque, así que, por el momento, es suficiente con implementarlo, no obstante, si la plataforma crece en número de usuarios, se recomienda implementar el mecanismo de seguridad de bloqueos de cuenta por intentos fallidos.

- **¿Cómo se desbloquean las cuentas?**

  A través de una solicitud enviada al correo electrónico del administrador con una explicación justificada para desbloquear la cuenta.

- **Prueba 21: De inclusión de archivos**

Objetivo de la prueba

La prueba tiene como finalidad verificar que no se incluyan archivos ubicados localmente en el servidor. Esta vulnerabilidad permite a un usuario cualquiera acceder al sistema de archivos donde este alojado la página web, por lo que es un problema de permisos mal otorgados.

Ejecución de la prueba

Para la ejecución de la prueba, se verifica a través de la búsqueda avanzada si la plataforma posee dominio con el siguiente formato:

site: ejemplo.com “php?id=”

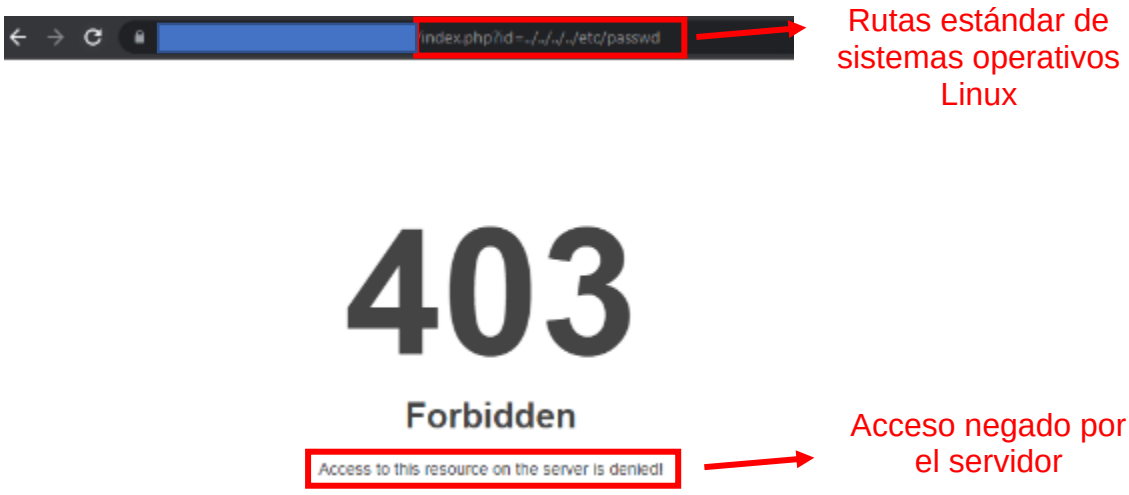
Como sabrán en pruebas anteriores, se demostró que la información indexada a Google eran los emprendimientos y la página principal, así que realizar este tipo de búsqueda no daría resultados (Figura 8). No obstante, de igual forma se ejecuta dentro de la plataforma el siguiente comando:

ejemplo.com/item?id=../../../../etc/hosts

El término “¿id=” hace referencia al vector de ataque y las posibles entradas.

Si al enviar la solicitud, el servidor en el que se aloja la plataforma responde con información sensible como especificaciones del equipo local del servidor representaría una vulnerabilidad muy grave, lo que en este caso no dio resultados, como se observa en la figura 45.

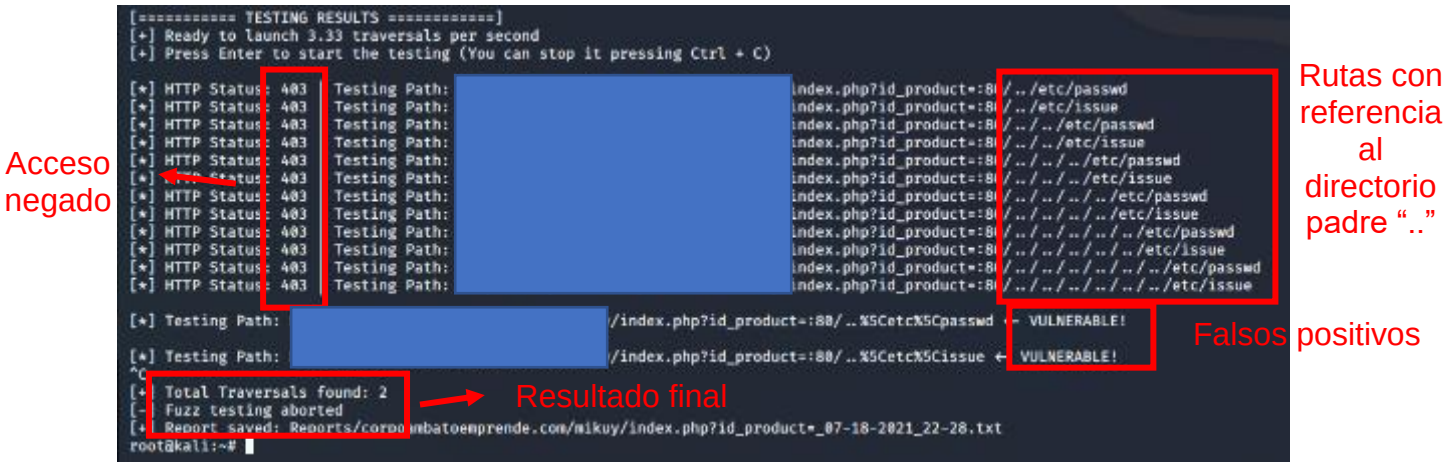
Figura 45. Ataque de inclusión de archivos - Navegador *web*



Fuente: elaboración propia

A continuación, en la figura 46, se ejecuta la misma prueba de forma automatizada a través de la herramienta *dotdotpwn.*

Figura 46. Escaneo directorio transversal – *Dotdotpwn*



Fuente: elaboración propia

Se aprecia que existen accesos con estado "vulnerable" pero al tratar de ingresar a las mismas es redirigida a la página principal de la plataforma, por lo que son falsos positivos.

- **Prueba 22: Escalamiento de privilegios**

Objetivo de la prueba

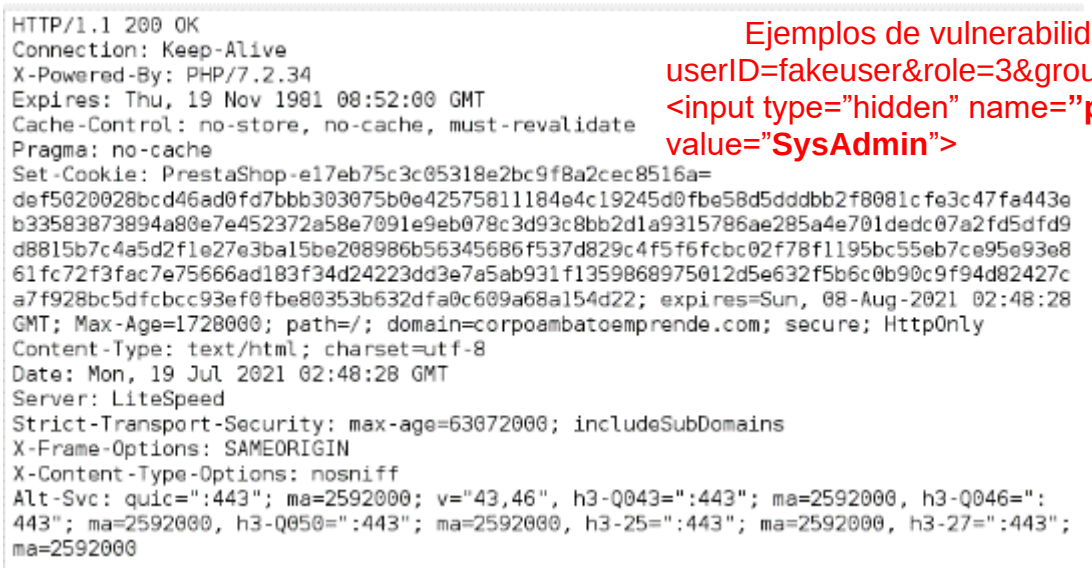
La prueba consiste en encontrar vulnerabilidades relacionadas al escalamiento de privilegios, es decir, aquellos sistemas mal configurados que permiten ganar privilegios dentro de un sistema, lo que deja expuesto a usuarios para realizar actividades ilícitas. El escalamiento sucede en forma horizontal si existen diferentes niveles de privilegios y un usuario mal intencionado accede a un nivel superior al que no fue autorizado. Por otro lado, el vertical consiste en acceder a recursos de usuarios que tienen en un mismo nivel de privilegios.

Ejecución de la prueba

Para la ejecución de la prueba, se utiliza la herramienta OWAS ZAP, el cual permite interceptar información sobre peticiones HTTP.

A continuación, la figura 47, se realiza el escaneo al sitio correspondiente.

Figura 47. Solicitud *GET – OWASP ZAP*



Al analizar la figura 47, se determina que no existen parámetros asociados al a vulnerabilidad de escarmiento de privilegios, se esperaba encontrar valores mostrados como ejemplo en la captura. Los parámetros *"group", "profile" o "SysAdmin",* por lo general son modificados y reenviados como solicitudes falsas para autentificarse como administrador del servidor.

- **Prueba 23: Referencia directa insegura a objetos**

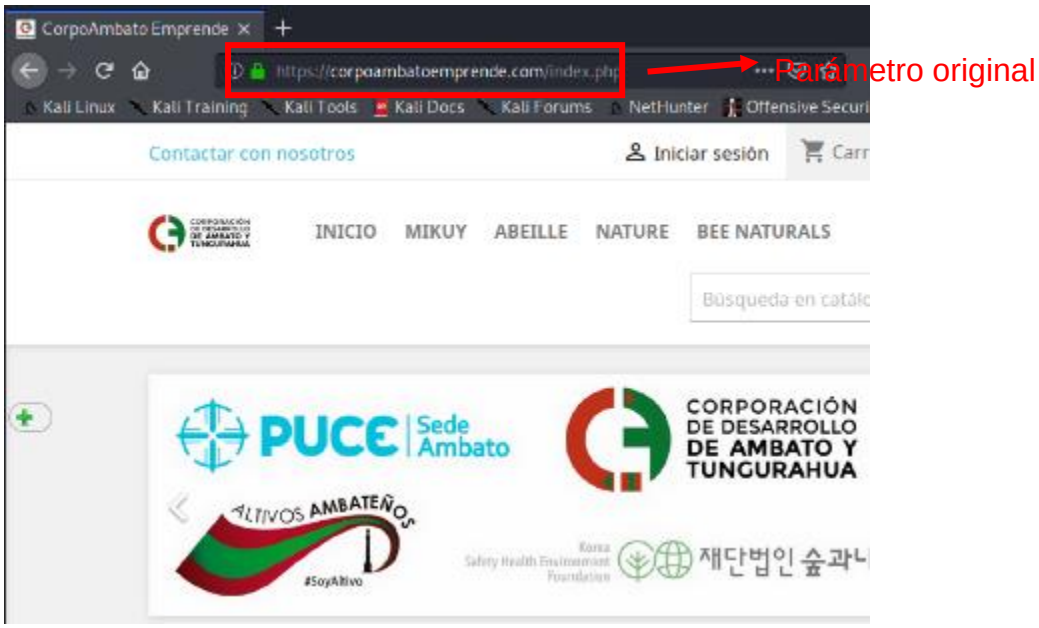
Objetivo de la prueba

El objetivo de la siguiente prueba es encontrar vulnerabilidades asociadas a accesos indebidos a objetos o archivos a través de modificar parámetros proporcionados por los usuarios.

Ejecución de la prueba

Para ejecutar esta prueba, se verifica que una plataforma cuenta de al menos dos tipos de usuario, en este caso en concreto solo existe el de visitante y cliente registrado, por lo que la prueba se enfoca en acceder a objetos que solo el cliente registrado tiene permiso de manipular. Por lo tanto, una forma fácil de probar es ejecutar una URL que con referencia a funcionalidades exclusivas para usuarios registrados tales como el perfil de usuario o cambio de datos (figura 48 y 49)

Figura 48. Página original – Navegador *web*



Fuente: elaboración propia

Figura 49. Pagina modificada – Navegador *web*

La información encontrada en base a la prueba realizada de tipo escáner, determinó que no existen parámetros de acceso a enlaces prohibidos de subcategorías dentro de lo que cabe el nivel de privilegio de un usuario visitante.

2.3.6. Fase VI – Pruebas de manejo de sesiones

En esta fase, se considera todos los aspectos relacionados al mecanismo que cubre el proceso de gestión y mantenimiento de interacción usuario y aplicación, lo que abarca el funcionamiento desde el inicio de sesión de la aplicación y hasta salir de la misma. Este proceso suele estar presente en protocolos HTTP, por lo que no cuentan con un estado que posea información sensible del usuario que solicita la información. En las pruebas, se verifica si el proceso de gestión mencionado cumple con los requisitos de seguridad para preservar la información privilegiada de los usuarios.

- **Prueba 24: Esquema de gestión de sesión**

Objetivo de la prueba

El objetivo de la siguiente prueba es verificar que las *cookies* presentes dentro de la aplicación se crean de forma segura e impredecible, caso contrario estas suelen estar expuestas a ataques que permiten la falsificación de esta, para después extraer fácilmente las credenciales de sesiones de usuarios verdaderos.

Ejecución de la prueba

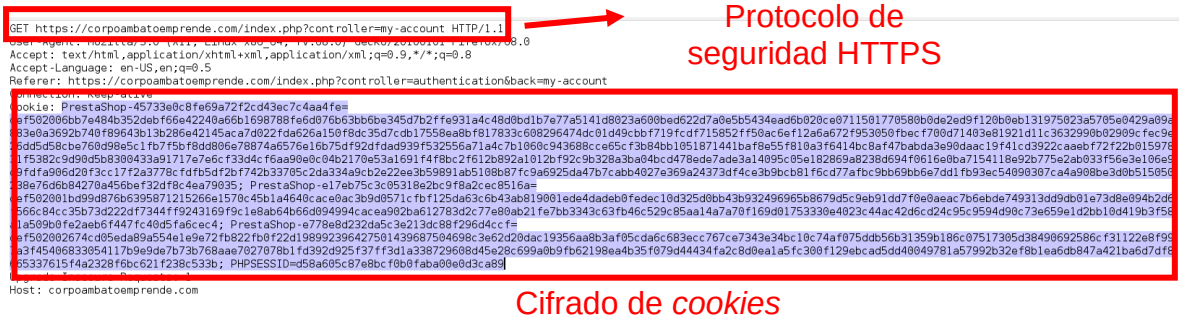
La forma de comprobar que las cookies generadas por el servidor y enviadas al cliente no sean constantes y predecibles, es realizar una acción que obligue a utilizar el mismo patrón de cookies como: el carrito de compras, se hace un seguimiento sobre todos los productos que ha elegido a largo de la sesión, por lo para reducir la carga, el servidor utilizar el mismo esquema de *cookies.*

La siguiente lista corresponde a los procesos de ataque, si se llegase a vulnerar las *cookies.*

- Recolección de *cookies:* se refiere a recopilar una cantidad suficiente de muestras de *cookies.*
- Ingeniería inversa de cookies: analizar la información encontrada sobre el algoritmo de generación de *cookies.*
- Manipulación de *cookies:* es la parte final del proceso que requiere un gran número de intentos correspondiente a llevar a cabo el ataque por medio de falsificar una *cookie* (ataque de fuerza bruta).

A continuación, la figura 50, se muestra las solicitudes y cookies identificadas en el funcionamiento de la plataforma.

Figura 50. Information *ID Cookies – OWASP ZAP*



Fuente: elaboración propia

Las cookies dentro de la plataforma no son interceptadas y manipuladas debido a la presencia del protocolo de transporte seguro HSTS (RFC 6797) (figura 40), el cual evita este tipo de vulnerabilidad al pasar el tráfico de internet a través encabezados HTTPS y no por un HTTP simple, por lo que las cookies están cifradas.

- **Prueba 25: Previsibilidad y aleatoriedad del identificado de sesión**

Objetivo de la prueba

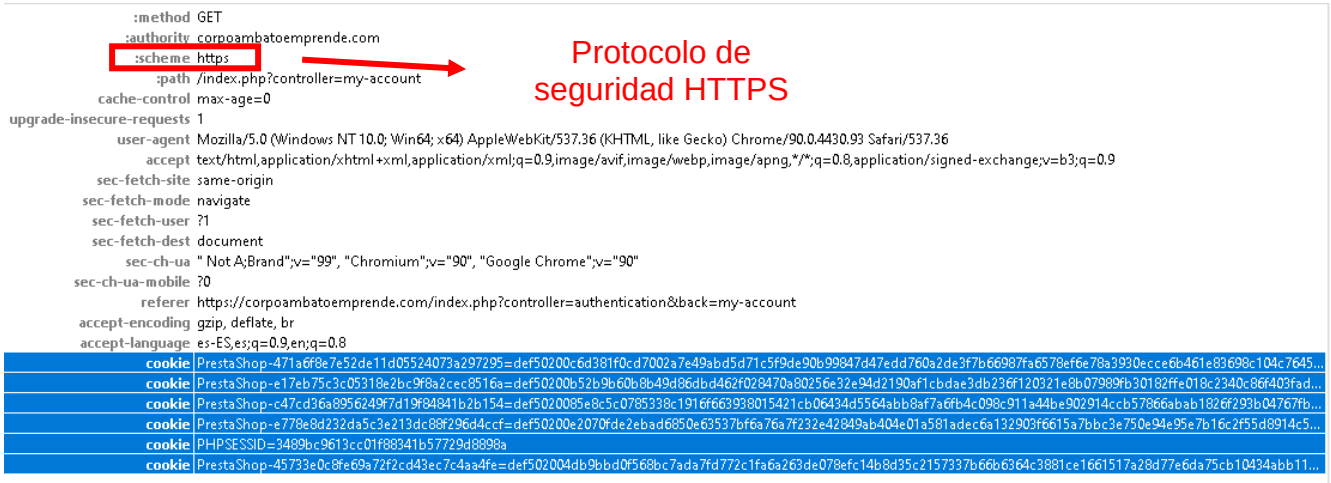
En esta prueba, se comprueba si existe una vulnerabilidad asociada a la renovación de las cookies específicamente al momento de un inicio de sesión exitoso, es decir, si al momento de la autenticación el identificador resulta ser muy corto, estaría expuesta a que el atacante adivine y robe la identificación de una sesión. Por ello, se verifica que los identificadores de sesión tengan por lo menos una longitud de 128 bits a 256 bits.

Ejecución de la prueba

Para la prueba, se utiliza la herramienta *Charles proxy* para detectar el *ID* del identificador del inicio de sesión de una cuenta de la plataforma.

A continuación, en la siguiente figura 51, se emplea la herramienta mencionada y se observan los datos encontrados

Figura 51. Contenido de la solicitud – *Charles proxy*



:method	GET
:authority	corpoambatoemprende.com
:scheme	https
:path	/index.php?controller=my-account
cache-control	max-age=0
upgrade-insecure-requests	1
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
sec-fetch-site	same-origin
sec-fetch-mode	navigate
sec-fetch-user	?1
sec-fetch-dest	document
sec-ch-ua	" Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
sec-ch-ua-mobile	?0
referer	https://corpoambatoemprende.com/index.php?controller=authentication&back=my-account
accept-encoding	gzip, deflate, br
accept-language	es-ES,es;q=0.9,en;q=0.8
cookie	PrestaShop-471a6f8e7e52de11d05524073a297295=def50200c6d381f0cd7002a7e49abd5d71c5f9de90b99847d47edd760a2de3f7b66987fa6578ef6e78a3930ecce6b461e83698c104c7645...
cookie	PrestaShop-e17eb75c3c05318e2bc9f8a2cec8516a=def50200b52b9b60b8b49d86dbd462f028470a80256e32e94d2190af1cbdae3db236f120321e8b07989fb30182ffe018c2340c86f403fad...
cookie	PrestaShop-c47cd36a8956249f7d19f84841b2b154=def5020085e8c5c0785338c1916f663938015421cb06434d5564abb8af7a6fb4c098c911a44be902914ccb57866abab1826f293b04767fb...
cookie	PrestaShop-e778e8d232da5c3e213dc88f296d4ccf=def50200e2070fde2ebad6850e63537bf6a76a7f232e42849ab404e01a581adec6a132903f6615a7bbc3e750e94e95e7b16c2f55d8914c5...
cookie	PHPSESSID=3489bc9613cc01f88341b57729d8898a
cookie	PrestaShop-45733e0c8fe69a72f2cd43ec7c4aa4fe=def502004db9bbd0f568bc7ada7fd772c1fa6a263de078efc14b8d35c2157337b66b6364c3881ce1661517a28d77e6da75cb10434abb11...

Fuente: elaboración propia

Un atacante tiene pocas probabilidades de adivinar el patrón, se encuentran cifradas y al ser cookies de identificador de sesión son únicas y solo son leídas por la plataforma.

- **Prueba 26: Falsificación de solicitudes entre sitios CSRF**

Objetivo de la prueba

Esta prueba identifica una vulnerabilidad asociada al ataque conocido como CSRF *(Cross Site Request Forgery),* que consiste en obligar al usuario a realizar acciones no deseadas en la aplicación. Se espera encontrar información relacionada al ataque como: los tokens de sesión, que permiten al atacante hacerse pasar por un usuario legitimo para acceder a la cuenta de forma ilegal.

Ejecución de la prueba

En la ejecución de la prueba, se utiliza la herramienta *OWAS ZAP*, permite identificar y agrupar los ataques de tipo *CSRF* para su posterior análisis.

A continuación, en la figura 52, se presenta la información relacionada a la vulnerabilidad de tipo *CSRF.*

Figura 52. *Anti-CSRF Tokens – OWASP ZAP*

Fuente: elaboración propia

Luego de realizar el escaneo de peticiones se observa que la herramienta detecta 4 peticiones, las cuales son falsos positivos, puesto que no almacena el formulario de inicio de sesión.

2.3.6. Fase VII – Pruebas de validación de entradas

Esta fase, se enforca en detectar una falla de seguridad que comúnmente suele encontrarse en aplicaciones mal configuradas al estar ausente el mecanismo de validación de entrada, que se ejecuta desde un usuario antes de utilizarlo. Las pruebas identifican esta falla para prevenir ataques dirigidos a aprovechar esta vulnerabilidad como: inyección SQL, inclusión de archivos, XSS, denegación de servicios, entre otros.

- **Prueba 27: De secuencia de comandos de sitios cruzados reflejados**

Objetivo de la prueba

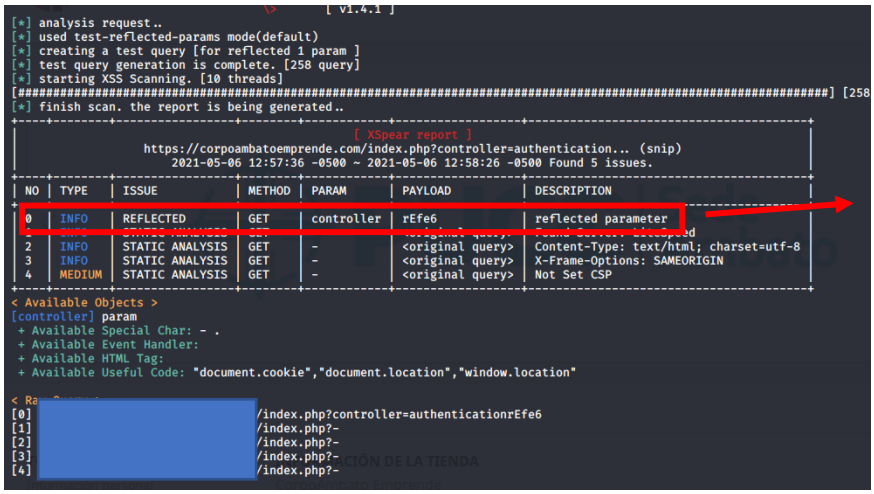
El objetivo de esta prueba es determinar si existe mediante un escáner variantes de vulnerabilidades para realizar ataques de tipo XSS no persistente. Este tipo de vulnerabilidad es aprovechado por el atacante a través de enviar un código malicioso hacia el navegador, para que el usuario lo ejecute y abra una página web de terceros.

Ejecución de la prueba

Para la ejecución, se utiliza la herramienta Xspear, el cual permite escanear de forma profunda la plataforma y encontrar vulnerabilidades de tipo XSS reflejado.

A continuacion, en la figura 53, se especifa la informacion encontrada mediante un reporte aporado por la herramienta.

Figura 53. Reporte CLI – *Xspear*



Información de parámetros reflejados

Fuente: elaboración propia

Xspear es una herramienta de escáner potente y como se aprecia, la herramienta determina que, si pudo encontrar información de parámetros reflejados, pero, está calificado en tipo en informativa, es decir, representa el nivel de riesgo más bajo en cuanto a la probabilidad de recibir ataques de este tipo.

- **Prueba 28: De manipulación verbos HTTP**

Objetivo de la prueba

Para esta prueba, se verifica que aparte de los métodos estándar que normalmente aparecen como *GET* y *POST,* se especifican otros métodos que almacenan información crítica sobre el servidor, por ejemplo, el método *HEAD, TRACE, OPTIONS, PUT, DELETE, CONNECT*, entre otros.

Ejecución de la prueba

Para la ejecución de la prueba, se utiliza la herramienta *netcat,* el cual permite enviar solicitudes personalizadas para probar distintos métodos.

A continuación, en la figura 57, se muestra la información revelada al enviar una solicitud con el método que no es común dentro de la plataforma (*TRACE)*.

Figura 54. Reporte método *TRACE – Netcat*

Fuente: elaboración propia

En base a lo observado, se interpreta que no presenta información relevante en cuanto al método enviado al dar como resultado una solicitud incorrecta, por lo que no fue capaz de comunicarse satisfactoriamente con el *host* del servidor de la plataforma.

Prueba 29: De inyección SQL

Objetivo de la prueba

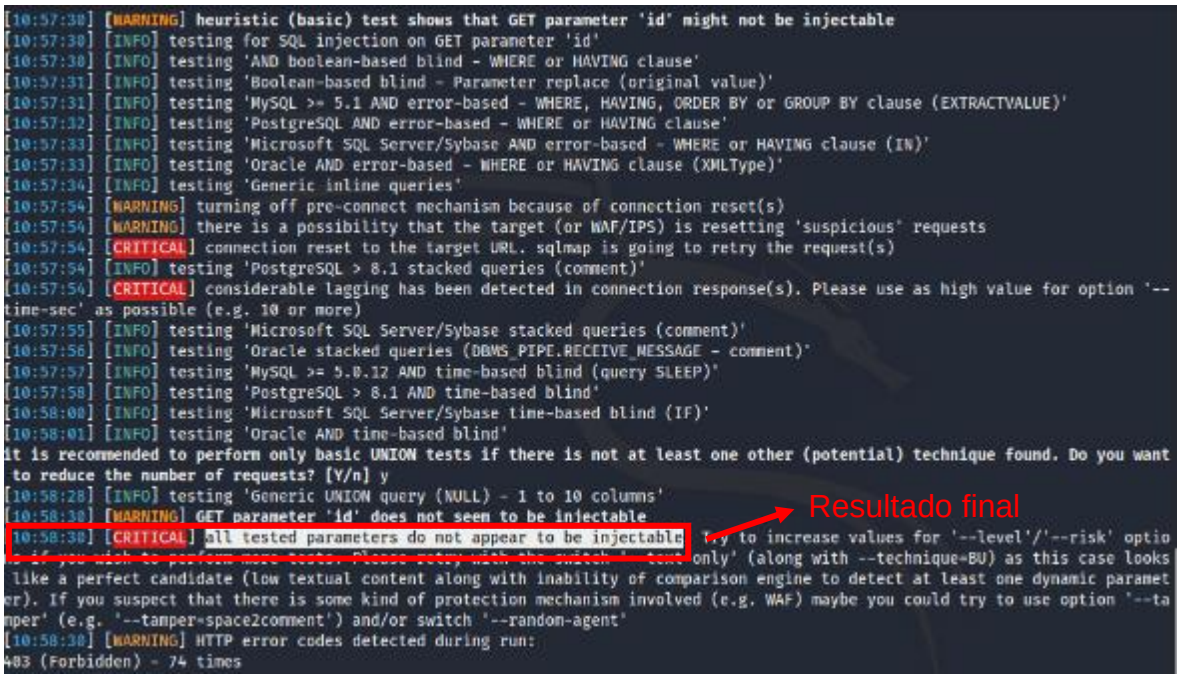
En la presente prueba, se verifica si existen vulnerabilidades orientadas a ejecutar al ataque de inyección SQL, que consiste en insertar un comando de una consulta SQL ya sea parcial o total a fin de encontrar la forma de leer, modificar o hacer operaciones con la información sensible de la base de datos.

Ejecución de la prueba

Para la ejecución de la prueba, se utiliza la herramienta *sqlmap*, el cual permite escanear y detectar vulnerabilidades relacionadas al ataque de inyección SQL.

A continuación, en la figura 55, se observa el reporte de la herramienta al ser ejecutada el escáner de vulnerabilidades.

Figura 55. Reporte de escáner – SQLmap



Fuente: elaboracion propia

Al finalizar la prueba de analisis, la misma herramienta brinda un resultado final, marcado en la figura 55, lo que afirma que todos los parametros probados no son inyectables, así que la plataforma se excluye de dicha vulnerabilidad.

2.3.7. Fase VIII – Pruebas de manejo de errores

Para esta fase, se emplean pruebas que permitan detectar los errores que aparecen cuando la aplicación o plataforma trata de ejecutar la solicitud enviada por el usuario hacia un sitio *web* inexistente, lo que a su vez, verifica si la plataforma gestiona este error. Dichos errores, son configurados y manipulados con el fin de revelar información sensible sobre el servidor.

- **Prueba 30: De análisis de códigos de error**

Objetivo de la prueba

El objetivo de esta prueba es si al momento de solicitar ingresar un apartado de la plataforma que no existe, esta tiene la capacidad de gestionar el error o responder mediante un código de estado conocido como error 400, lo que lo conduce a un enlace muerto. Muchas veces este código de error proporciona información de utilidad acerca del servidor *web* donde se ejecuta la plataforma

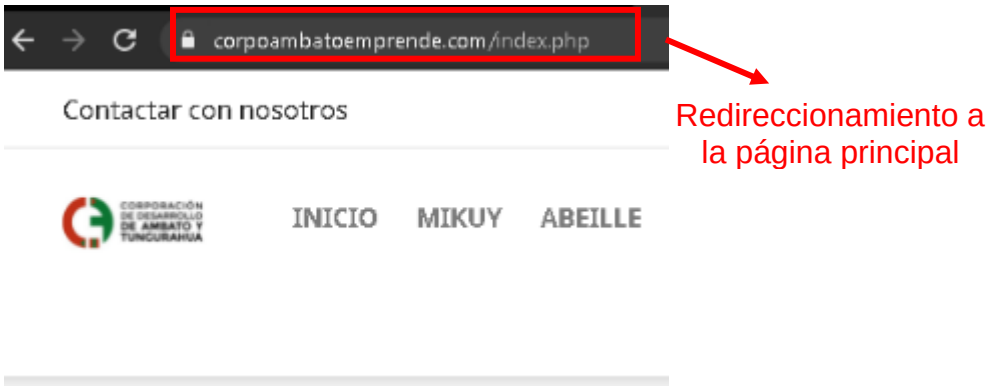
Ejecución de la prueba

Para la ejecución de la prueba, se utiliza un navegador *web,* para lo cual se ejecuta la URL modifica a partir de la URL real:

- **URL valida:** https://*******.com/index.php
- **URL modificada:** https://*******.com/index123.php

A continuación, en la figura 56, se realiza la prueba con el ingreso de la URL modificada.

Figura 56. URL modificada – *Google*

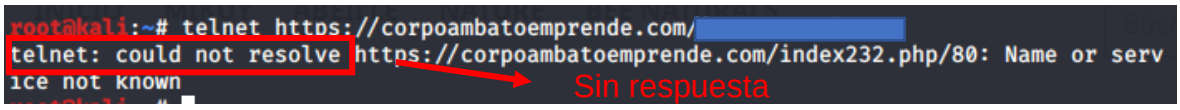


Fuente: elaboración propia

Una vez realizada la prueba, se contempla que la misma plataforma al momento del envío de una solicitud de una URL no valida, esta redirige hacia la página principal valida, la cual se muestra en el primer momento que se intenta ingresar a la URL invalida.

A continuación, en la figura 57, se emplea la herramienta *telnet* para comprobar la conectividad hacia la misma dirección modificada presentada anteriormente.

Figura 57. Reporte de conectividad – *Telnet*



Fuente: elaboración propia

Se comprueba qua la herramienta no resuelve la dirección debido a que es automáticamente redireccionada hacia la página real principal.

2.3.8. Fase IX – Pruebas de criptografía débil

En esta fase, se analiza que, al momento de realizar solicitudes de ingreso a la plataforma, se verifica si los datos transmitidos entre el usuario y la plataforma son enviados de forma segura. Las pruebas verifican que la plataforma posee los protocolos necesarios para proporcionar canales seguros a través del soporte criptográfico, además, de validar que los algoritmos de cifrado son de alto nivel ante ataques de descifrado.

- **Prueba 31: De cifrados SSL-TLS débil y protección insuficiente de capa de transporte**

Objetivo de la prueba

La prueba tiene por objetivo verificar la seguridad del envío de información entre el usuario y la plataforma, es decir, si posee para su funcionamiento el certificado TLS/SSL *(Transport Layer Security) /(Secure Sockets Layer),* permite cifrar transferencias para que no sean descifrados por usuarios terceros.

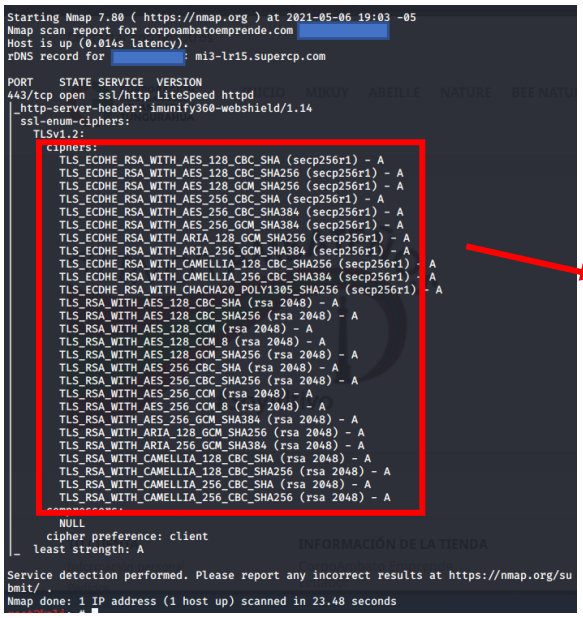
Ejecución de la prueba

Para la ejecución de la prueba, se emplea la herramienta nmap para verificar si los servicios de seguridad SSL/TLS, se encuentran activos dentro de la plataforma.

A continuación, en la figura 59, se ejecuta el siguiente comando configurado con parámetros de búsqueda y guardado de información en un archivo tipo texto:

nmap –sV –script ssl-enum-ciphers –p 443 <host>

Figura 58. Reporte *script – Nmap*



Conjunto de cifrados clasificados de (A – F)

Fuente: elaboración propia

El reporte de informe del análisis arroja como resultado una lista de comandos de todos los conjuntos de cifrado y comprensores que acepta un servidor, los cuales están clasificados de la “A” a la “F”, la calificación más alta de seguridad de cifrado es la letra “A”.

Adicionalmente, en la figura 60, se emplea una herramienta de análisis para cerciorarse de la presencia de servicios y protocolos SSL/TLS

Figura 59. Reporte del escáner – *Geekflare*

Fuente: elaboración propia

La herramienta muestra los protocolos y servicios que funcionan dentro de la plataforma, así como las vulnerabilidades a las que estaría expuesta al no poseerlas.

- **Prueba 32: De información privilegiada enviada por canales sin encriptar**

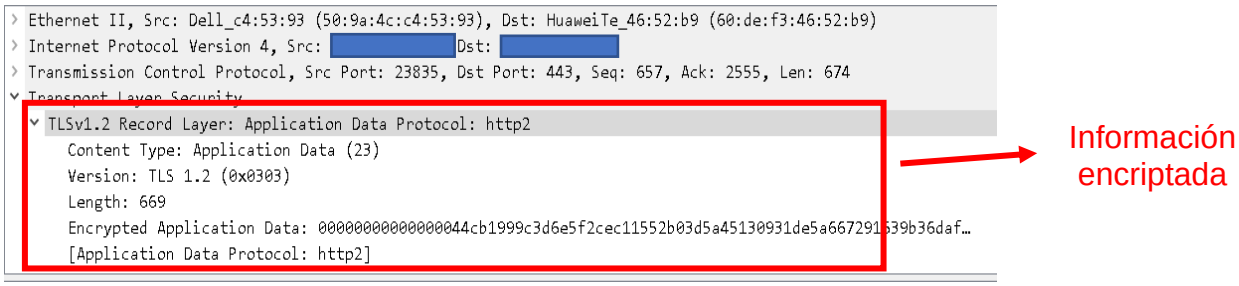
Objetivo de la prueba

La prueba tiene como objetivo verificar que los distintos tipos de información son enviados de manera segura y no en texto claro, estas suelen contener información sensible del usuario.

Ejecución de la prueba

Para poner en marcha de la prueba, se utiliza la herramienta *Wireshark* para monitorear el tráfico de red y analizar que las solicitudes viajan con protocolos y servicios de encriptación

Figura 60. Análisis de trafico de red – *Wireshark*



Fuente: elaboración propia

Se observa en base al análisis de los campos de la captura del tráfico de red al navegar por la plataforma, se verifica que estas viajan a través del protocolo SSL, por lo que la información no viaja en texto claro.

A continuación, la tabla 5 muestra un cuadro resumen de las fases, pruebas realizadas con sus correspondientes ubicaciones de ejecución y herramientas empleadas en la misma.

Tabla 5. Lista resumen de las pruebas realizadas

Fase	Nombre de la prueba	Ubicación	Herramientas utilizadas
Recopilación de información	Descubrimiento de información por motores de búsqueda	URL, IP	Google, shodan, nslookup
	Uso de huellas digitales en el Servidor Web	URL, IP	Httprecon
	Revisión de meta-archivos del servidor web en busca de fugas de información	URL	Robots.txt
	Enumerar aplicaciones en el servidor Web	IP	Nmap
	Revisar comentarios en la página web y metadatos por fugas de información	URL, IP	Navegador web, curl
	Identificar los puntos de entrada de la aplicación	URL	Burp Suite, OWASP Zap
	Mapear rutas de ejecución a través de la aplicación	URL	OWASP Zap
	Framework referencial para el uso de huellas digitales en aplicaciones *web*	URL	Whatweb linux, whatweb online, wappalyzer
Pruebas de gestión de configuración y desarrollo	Configuración de la plataforma de aplicaciones de pruebas	Equipo (PC)	Apache
	Manejo de extensiones de archivo de prueba para información confidencial	IP	Nikto
	Revisar archivos antiguos, de copia de seguridad y sin referencia	URL	Screaming Frog
	Infraestructura de enumeración e interfaces de administración de aplicaciones	URL	Navegador web
	Métodos HTTP	URL, IP	Nmap, netcat
	Seguridad de transporte escrito HTTP – HSTS	URL	Curl, Hstspreload, Qualys SSL labs
	Política de dominio cruzado RIA (Rich Internet Applications)	URL	Nikto
Pruebas de manejo de identidad	Definición de roles	Ninguna	Ninguna
	Registro de usuarios	URL	Navegador web
	Creación de cuentas	URL	Navegador web

Pruebas de autentificación y autorización	Transporte de credenciales en un canal encriptado	URL	OWASP Zap
	Determinar un mecanismo de bloqueo débil	URL	Navegador web
	Inclusión de archivos	IP	Dotdotpwn
	Escalamiento de privilegios	URL	OWASP Zap
	Referencia directa insegura a objetos	URL	OWASP Zap
Pruebas de manejo de sesiones	Esquema de gestión de sesiones	URL	Burb Suite
	Previsibilidad y aleatoriedad del identificado de sesión	URL	Charles proxy
	Falsificación de solicitudes entre sitios CSRF	URL	OWASP Zap
Pruebas de validación de entradas	Secuencia de comandos de sitios cruzados	URL	Xspear
	Manipulación de verbos HTTP	URL	Netcat
	Inyección SQL	URL	SQLmap
Pruebas de manejo de errores	Análisis de códigos de error	URL	Navegador web, telnet, OWASP Zap
Pruebas de criptografía débil	Cifrados SSL-TLS débil y protección insuficiente de capa de transporte	URL	Nmap, geekflare
	Información privilegiada enviada por canales sin encriptar	URL	Wireshark

Fuente: elaboración propia

CAPITULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Para este capítulo, se emplean matrices de escala de valoración definidas por la metodología MAGERIT de análisis y gestión de riesgos, lo que permite cuantificar los riesgos de vulnerabilidades encontradas en la investigación en base a los resultados obtenidos por la guía de pruebas OWASP. La utilización de la nueva metodología permite mediante las matrices de valoración obtener un puntaje de valoración presentada de forma cuantitativa y cualitativa, es decir, se categorizan los aspectos esenciales de seguridad como: la integridad o la confidencialidad para priorizar aquellos riesgos que tienen mayor relevancia a ser resueltos.

3.1 Análisis de riesgos

A continuación, la tabla 6, se basa en la metodología MAGERIT para determinar la probabilidad de ocurrencia, en la que Maila et al. (2015), adiciona una columna de valor cuantitativo para una mejor comprensión de la valoración de riesgos. Esta tabla sirve para asociar con los resultados obtenidos del impacto (tabla 7) y realizar el cálculo correspondiente para determinar el puntaje de riesgo definitivo correspondiente a los anexos de la tabla 9 y 10.

Tabla 6. Probabilidad de ocurrencia – Vulnerabilidad

Valor cualitativo	Valor cuantitativo	Descripción	Probabilidad de ocurrencia
Muy frecuente	4	A diario	75% - 100%
Frecuente	3	Una vez al mes	50% -75%
Frecuencia normal	2	Una vez al año	25% - 50%
Poca frecuencia	1	Cada varios años	0% - 25%

Fuente: Maila et al. (2015)

Así mismo, la tabla 7 valora la confidencialidad, integridad y disponibilidad en función de perdidas técnicas que suelen generarse en la organización por las vulnerabilidades detectadas, para después, en base al promedio de los resultados, se obtenga el valor del impacto. Los valores que resulten en un numero decimal, se redondean a su inmediato superior o inferior. Es preciso señalar que los valores

correspondientes a la triada de la información son independientes al valor resultante del impacto, por lo que se cuenta con una tabla adicional para esta, pero al poseer la misma escala de valoración, se decidió realizar una adaptación de la tabla original agrupados en una sola para simplificar el espacio.

Tabla 7. Valoración de Seguridad

Escala de valoración	Escala cuantitativa	Descripción
Muy bajo	1	**-Confidencialidad (CONF):** información relevante mínima y no sensible **-Integridad (INTE):** mínima información dañada **-Disponibilidad (DISPO):** mínima interrupción del servicio **-Impacto (IMP):** daño despreciable
Bajo	2	**-Confidencialidad (CONF):** información relevante mínima **-Integridad (INTE):** mínima información importante dañada **-Disponibilidad (DISPO):** mínima interrupción del servicio **-Impacto (IMP):** Daño menor para la empresa u organización
Medio	3	**-Confidencialidad (CONF):** importante cantidad de información no sensible revelada **-Integridad (INTE):** gran cantidad de información dañada **-Disponibilidad (DISPO):** amplia interrupción del servicio **-Impacto (IMP):** daño importante para la empresa u organización
Alto	4	**-Confidencialidad (CONF):** importante cantidad de información revelada **-Integridad (INTE):** gran cantidad de información importante dañada **-Disponibilidad (DISPO):** amplia interrupción de servicios primarios **-Impacto (IMP):** daño importante para la empresa u organización
Muy alto	5	**-Confidencialidad (CONF):** toda la información revelada **-Integridad (INTE):** toda la información destruida **-Disponibilidad (DISPO):** todos los servicios interrumpidos **-Impacto (IMP):** daño muy grave para la empresa u organización

Fuente: adaptado de Maila et al. (2015)

Por otra parte, se implementa una forma de visualizar los datos que se pronostican obtener en base las tablas ya definidas, por lo que se categoriza mediante técnicas matriciales para una mejor representación del riesgo. Para ello, en la tabla 8, se ubican los niveles de las vulnerabilidades en las filas y los niveles de impactos en las columnas.

Tabla 8. Nivel de riesgo – Cualitativo

Riesgo		**Vulnerabilidad**			
		Poco frecuente (PF)	Frecuencia normal (FN)	Frecuente (F)	Muy frecuente (MF)
Impacto	Muy alto (MA)	A	MA	MA	MA
	Alto (A)	M	A	MA	MA
	Medio (M)	B	M	A	MA
	Bajo (B)	MB	M	M	A
	Muy bajo (MB)	MB	MB	B	M

Fuente: Metodología MAGERIT

De igual forma, en la tabla 9, se elabora la respectiva matriz cuantitativa relacionada con los valores cualitativos antes presentados, en la cual la cifra se obtiene al realizar el cálculo de la siguiente formula:

Riesgo = impacto (IMP) * probabilidad de ocurrencia (PDO)

Tabla 9. Nivel de riesgo – Cuantitativo

Riesgo		**Vulnerabilidad**			
		1	2	3	4
Impacto	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Fuente: Metodología MAGERIT

Finalmente, una vez definidas las matrices de valorización, en la tabla 10, se procede a evaluar los riesgos mediante la metodología MAGERIT y con al análisis de los resultados obtenidos por las pruebas OWASP.

A continuación, para una adecuada presentación de la información, se detallan las siguientes abreviaturas a emplear en la tabla:

- **INTE:** integridad
- **CONF:** confidencialidad
- **DIPO**: disponibilidad
- **IMP:** impacto
- **PDO:** probabilidad de ocurrencia
- **RECO:** reconocimiento
- **N/A:** no aplica

Tabla 10. Evaluación de riesgo – Metodología MAGERIT

Prueba	N	Tipo de prueba	Objetivo de la prueba	Amenaza	Vulnerabilidad	INTE	CONF	DISPO	IMP	PDO	Riesgo
Recopilación de información	1	Descubrimiento de información por motores de búsqueda	Información sensible de la configuración y diseño, archivo robots.txt desactualizado	Ingeniería Social	Números telefónicos, direcciones y nombres públicos	1	1	1	1	2	2
	2	Uso de huellas digitales en el Servidor Web	Revelación de versión y tipo de servidor web para asociar vulnerabilidades conocidas	Acceso a pruebas de solicitud malformada en dependencia con el servidor	Descubrimiento de tipo de servidor	RCO	RCO	RCO	RCO	RCO	RCO
	3	Revisión de meta-archivos del servidor web en busca de fugas de información	Fuga de información de la ruta o rutas al directorio o carpeta de la aplicación web.	Acceso y almacenamiento no autorizado de contenido web	No existe	N/A	N/A	N/A	N/A	N/A	N/A

	4	Enumerar aplicaciones en el servidor Web	Enumerar aplicaciones ocultas vulnerables a ser atacadas	Posibilidad de ejecución de ataques de intrusión, accesos no autorizados.	Nombres, versión de servidor, dirección IP, dominio	1	1	1	1	2	2
	5	Revisar comentarios en la página web y metadatos por fugas de información	Comentarios que contiene información sensible sobre contraseñas, usuarios y direcciones IP	Acceso no autorizado al sistema	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	6	Identificar los puntos de entrada de la aplicación	Datos de parámetros que contiene información confidencial, como información sobre el estado, cantidad de artículos o el precio de los	Acceso no autorizado al sistema	No existe	N/A	N/A	N/A	N/A	N/A	N/A

			artículos que el desarrollador								
	7	Mapear rutas de ejecución a través de la aplicación	Información sobre el flujo de trabajo de la estructura de la plataforma	Análisis de información para ataques relacionados	Mapeo de rutas de ejecución la plataforma	RCO	RCO	RCO	RCO	RCO	RCO
	8	Framework referencial para el uso de huellas digitales en aplicaciones *web*	Versión framework sin parche, configuración errónea	Análisis de información para ataques relacionados	Revelación del campo X-Powered-By que contiene el tipo de framework	RCO	RCO	RCO	RCO	RCO	RCO

Pruebas de gestión de configuración y desarrollo	9	Configuración de la plataforma de aplicaciones de pruebas	Lista de los módulos mal configurados en el servidor web	Denegación de servicio en IIS, explotación de vulnerabilidad directory traversal	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	10	Manejo de extensiones de archivo de prueba para información confidencial	Extensiones a archivos que contengan información confidencial de credenciales de acceso	Revelación de información sensible del servidor	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	11	Revisar archivos antiguos, de copia de seguridad y sin referencia	Archivos olvidados con información de la infraestructura o credenciales	Acceso no autorizado a la interfaz administrativa o servidor de base de datos	No existe	N/A	N/A	N/A	N/A	N/A	N/A

	12	Infraestructura de enumeración e interfaces de administración de aplicaciones	Interfaces de administrador sin controles de acceso	Acceso no autorizado a la interfaz administrativa o servidor de base de datos	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	13	Métodos HTTP	Descubrimiento de métodos con potencial riesgo para deshabilitarlos	Posible aplicación de los siguientes ataques: explotación Cross-site tracing (TRACE), Inclusión de archivo ASP para ejecución de comandos (PUT), ataque DoS (DELETE), ejecución de	Métodos encontrados: PUT, DELETE, CONNECT y TRACE	1	1	1	1	2	2

				código remoto (CONNECT)							
	14	Seguridad de transporte escrito HTTP – HSTS	Mecanismo de seguridad HSTS no implementado	Ataques de intermedio (man in the middle), acceso no autorizado por canales no encriptados	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	15	Política de dominio cruzado RIA (Rich Internet Applications)	Archivos de políticas crossdomain.xml dentro de la plataforma	Ataques de Cross-site Request Forgery (Falsificación de peticiones de sitios cruzados), acceso no	No existe	N/A	N/A	N/A	N/A	N/A	N/A

				autorizado al sistema							
Pruebas de manejo de identidad	16	Definición de roles	Roles que funcionan dentro de la plataforma	Reconocimiento de roles con acceso administrativo	Descubrimiento de dos tipos de roles: administrador, cliente, visitante	RCO	RCO	RCO	RCO	RCO	RCO
	17	Registro de usuarios	Requisitos de identidad para proceso registro de usuarios no alineados con los requerimientos de seguridad y negocio.	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	3	2	2	2	1	2

	18	Creación de cuentas	Proceso de crear una cuenta válida sin la aplicación de una correcta identificación y proceso de autorización.	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	3	2	2	2	1	2
Pruebas de autentificación y autorización	19	Transporte de credenciales en un canal encriptado	Datos enviados entre el servidor y la aplicación sin encriptar	Interceptación maliciosa de datos de autenticación de usuarios	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	20	Determinar un mecanismo de bloqueo débil	Mecanismo de bloque débil o sin implementar	Ataques de fuerza bruta	Mecanismo de bloqueo direcciones IP no detectada	3	2	2	2	1	2
	21	Inclusión de archivos	Posibilidad de visualizar archivos locales del servidor	Acceso a archivos con información de credenciales	No existe	N/A	N/A	N/A	N/A	N/A	N/A

	22	Escalamiento de privilegios	Parámetros modificables de asignación de privilegios	Acceso a funciones restringidas al público	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	23	Referencia directa insegura a objetos	Acceso a objetos que contienen recursos sensibles del sistema	Acceso no autorizado a recursos del sistema	No existe	N/A	N/A	N/A	N/A	N/A	N/A
Pruebas de manejo de sesiones	24	Esquema de gestión de sesiones	Predicción y falsificación una cookie débil	Envenenamiento de cookies y acceso no autorizado a cuentas de usuario	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	25	Previsibilidad y aleatoriedad del identificado de sesión	Patrones predecibles de identificadores de sesión	Acceso no autorizado a cuentas de usuario	No existe	N/A	N/A	N/A	N/A	N/A	N/A

	26	Falsificación de solicitudes entre sitios CSRF	Vulnerabilidad asociada al ataque conocido como CSRF (Cross-site request forgery)	Ingeniería social, ataque Cross-site request forgery	Identificación de cuatro solicitudes con riesgo bajo	1	1	1	1	1	1
Pruebas de validación de entradas	27	Secuencia de comandos de sitios cruzados	Variantes de vulnerabilidades para realizar ataques de tipo XSS no persistente	Ataques XSS no persistentes	Información de menor riesgo sobre parámetros reflejados	1	1	2	1	1	1
	28	Manipulación de verbos HTTP	Buscar métodos que almacenen información crítica sobre el servidor	Respuesta a métodos que no son GET y POST	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	29	Inyección SQL	Verificar si existen vulnerabilidades orientadas a ejecutar al	Ataques de inyección SQL	No existe	N/A	N/A	N/A	N/A	N/A	N/A

			ataque de inyección SQL								
Pruebas de manejo de errores	30	Análisis de códigos de error	Enlaces muertos con información sensible del servidor	Divulgación de información sensible como: bases de datos o errores	No existe	N/A	N/A	N/A	N/A	N/A	N/A
Pruebas de criptografía débil	31	Cifrados SSL-TLS débil y protección insuficiente de capa de transporte	Certificado de transporte ausente en la transmisión de datos	Interceptación maliciosa de datos de sensibles de tarjetas o credenciales	No existe	N/A	N/A	N/A	N/A	N/A	N/A
	32	Información privilegiada enviada por canales sin encriptar	Datos enviados sin protocolos y servicios de encriptación	Interceptación del texto en claro de datos sensibles del usuario	No existe	N/A	N/A	N/A	N/A	N/A	N/A

Fuente: adaptado de Maila et al. (2015)

Al observar la tabla 10, se evidencia que se analizaron 32 pruebas realizadas mediante el seguimiento de la guía de OWASP, de las cuales ninguna de ellas alcanza un nivel alto de riesgo, así mismo, solo 8 pruebas dieron resultados, pero con un nivel bajo de riesgo y el resto no aplicaron (N/A) debido a que no se encontraron vulnerabilidades asociadas en tales pruebas. Los riesgos evaluados en nivel medio y bajo son tratados y catalogados como despreciables, es decir, que no representan una amenaza en la organización y es aceptado en la misma. Ver anexo 3 para más información. No obstante, se escogen 3 riesgos que a consideración del puntaje son riesgos de nivel muy bajo aceptable, sin embargo, tienen la opción de ser tratados a través del método de reducción para de esa forma aumentar la seguridad de la misma.

3.2 Buenas prácticas para mitigación del riesgo

Una vez realizado el análisis y valoración del riesgo con su respectivo nivel de incidencia a través de la interpretación de la información, se definen las políticas o métodos de mitigación y gestión del riesgo, a fin de elevar el nivel de seguridad dentro de la organización.

A continuación, en la tabla 11, se presentan las formas de mitigar el riesgo en función de los resultados de la evaluación y los criterios de elección de los riegos.

Tabla 11. Reducción del riesgo

Prueba	Amenaza	Vulnerabilidad	Reducción de riesgo
Registro de usuarios	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	Instalar CAPTCHA en el formulario de registro de usuarios a través de los módulos gratuitos de prestashop y añadir Modulo de verificación de edad
Creación de cuentas	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	Instalar CAPTCHA en el formulario de registro de usuarios a través de los módulos gratuitos de prestashop. Añadir módulo de confirmación de cuenta con función de código de activación enviada al correo del usuario
Determinar un mecanismo de bloqueo débil	Ataques de fuerza bruta	Mecanismo de bloqueo direcciones IP no detectada.	Instalar el módulo de bloqueo de Ips si es necesario o Instalar el módulo de “Inicio de sesión avanzado”, el cual permite restringir el número de intentos permitidos por cada sesión. Además, que permite añadir y configurar funciones adicionales en cuanto a la seguridad de los formularios de inicio y registro de usuario

Fuente: elaboración propia

La mayoría de los métodos de mitigación presentados en la tabla están orientados a la prevención de ataques de fuerza bruta, busca evitar que un *spam* automatizado, se ejecute varias veces dentro de la plataforma.

3.3 Plan de seguridad

El plan de seguridad tiene como objetivo garantizar que el contexto y el alcance de la gestión de la seguridad, se hayan establecido correctamente como lo menciona la metodología MAGERIT (2012) en su guía sobre cómo llevar a cabo planes de seguridad a través del análisis de proyectos adecuadas en relación al tratamiento del riesgo establecido. En ese sentido, la empresa MERLOS (2019) señala que es fundamental implementar un plan de seguridad para guiar al personal encargado de los sistemas en cuanto a un óptimo manejo de información, tienen a su disposición los procedimientos y medidas establecidas para hacer frente a posibles ataques cibernéticos. Por ese motivo, a continuación, se detallan las etapas a seguir en el plan de seguridad para la organización CorpoAmbato:

- Introducción a la plataforma de comercio electrónico CorpoAmbato
- Objetivo
- Alcance
- Análisis de los niveles de seguridad y riesgos
- Opciones de tratamiento del riesgo
- Descripción de buenas prácticas aplicables a la organización

En vista de que las fases fueron efectuadas en su totalidad en el transcurso de la investigación, el presente apartado está enfocado en llevar a la práctica un plan de seguridad, que de manera más resumida y legible documente el trabajo realizado. Ver en el anexo 4.

CONCLUSIONES

- La búsqueda teórica en torno a los recursos de seguridad del comercio electrónico manifiesta las razones, por el cual la seguridad de la información se ve afectada por medio de configuraciones mal implementadas al momento de instalar y configurar servidores y plataformas con versiones antiguas, como también, por descuidos en la programación del código fuente si esta es codificada desde cero y a su vez, la falta de mecanismos de seguridad como la ausencia del protocolo HTTPS en el tráfico de solicitudes, son algunos factores que señalan la presencia de vulnerabilidades.

-No se encontraron vulnerabilidades importantes que afecten la información sensible de la plataforma de comercio electrónico de CorpoAmbato, por lo que se eligieron tres riesgos de nivel bajo relacionados con los ataques de fuerza bruta, estos fueron tratados mediante la opción de reducción de riesgo.

- Se analizaron los resultados correspondientes a las pruebas de la guía OWASP para después clasificarlos en base a la metodología MAGERIT con sus correspondientes matrices de valorización del riesgo y determinar un puntaje de categorización de la confidencialidad, disponibilidad e integridad. Finalmente, el resultado fue el puntaje total del riesgo en cada prueba realizada, lo que permitió conocer que no existen amenazas con niveles altos de riesgo que requieran una atención inmediata en la seguridad de la plataforma.

- Se propone un conjunto de buenas prácticas y un plan de seguridad a través de la opción de tratamiento elegida de reducción de riesgo para la extensión de seguridad contra ataques de fuerza bruta o *spam* automatizados a través de la utilización de módulos de controles de verificación y validación de datos CAPTCHA.

RECOMENDACIONES

-Para llevar a cabo las soluciones de reducción de riesgo, se recomienda utilizar los mismos módulos gratuitos que ofrece el sistema gestor de contenidos *Prestashop* en la que la plataforma fue construida, son fáciles de descargar e implementar.

- Una vez empleadas las soluciones de seguridad, se recomienda añadir opciones de inicio de sesión "*Social Media*" para saltar la forma en que el usuario ingresa datos de forma rigurosa e ingresar directamente con cuentas que ya dispone como *Facebook, Gmail u Outlook.*

- La mayoría de las plataformas que cuentan con métodos de pago en línea requieren de un nivel de seguridad muy alto, por lo que no se recomienda añadir este módulo si aún no se establecen los requisitos de seguridad necesarios, no obstante, se recomienda añadir de forma temporal un formulario facturación con métodos de pago de transferencia directa o deposito.

BIBLIOGRAFÍA

Álamo, R. (2016). *La economía digital y el comercio electrónico: Su incidencia en el sistema tributario*. Dykinson. https://www.digitaliapublishing.com/a/46259/la-economia-digital-y-el-comercio-electronico---su-incidencia-en-el-sistema-tributario

Alonso, A. F. (2018, febrero 23). ¿Qué es un CMS? Conoce los mejores gestores de contenido. *Webempresa*. https://www.webempresa.com/blog/que-es-cms-los-mejores-gestores-de-contenido.html

Alvarez Maranon, G. (2004). *Seguridad informatica para empresas y particulares*. McGraw-Hill Espana. elibro.puce.elogim.com/es/lc/puce/titulos/50050

Ambit building Solutions Together S.a, T. (2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas

Apser Cloud Services. (2015, agosto 19). ¿Qué es la disponibilidad informática y cuál es su importancia? *apser - Cloud Computing*. https://apser.es/que-es-la-disponibilidad-informatica-y-cual-es-su-importancia/

Arriola, M. (2018, febrero 26). Los Estándares de Seguridad Informática, ¿Cuál Aplica a la Industria? Y su Estado Actual. *ISA Sección Central México*. https://www.isamex.org/intechmx/index.php/2018/02/26/los-estandares-seguridad-informatica-aplica-a-la-industria-actual/

Avellaneda, J. V., Rodríguez, J. R., & López, D. A. (2014). Servicios de Televisión sobre la Plataforma de Internet (IPTV-IMS) usando Protocolo de Flujo en Tiempo Real (RTSP) y Protocolo de Transferencia de Hipertexto (HTTP). *Información tecnológica*, *25*(1), 67–76. https://doi.org/10.4067/S0718-07642014000100008

Ayala, A. (2020, octubre 23). Investigación Bibliográfica: Definición, Tipos, Técnicas. *Lifeder*. https://www.lifeder.com/investigacion-bibliografica/

Baca Urbina, G. (2016). *Introduccion a la seguridad informatica*. Grupo Editorial Patria. elibro.puce.elogim.com/es/lc/puce/titulos/40458

Badia, R. (2015). *La proteccion de datos*. Editorial UOC. elibro.puce.elogim.com/es/lc/puce/titulos/57741

Barranco, N. J. de la, & Hernández, L. (2012). *El delito de daños informáticos: Una tipificación defectuosa*. https://minerva.usc.es/xmlui/handle/10347/4149

Basantes Andrade, A. V., Gallegos Varela, M. C., Guevara Vega, C. P., Jácome Ortega, A. E., Posso Astudillo, Á. M., Quiña Mera, J. A., & Vaca Orellana, C. F. (2016). *Comercio electrónico*. Universidad Técnica del Norte. Facultad de Ingeniería en Cienias Aplicadas. http://repositorio.utn.edu.ec/handle/123456789/6793

Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio. *Revista chilena de derecho y tecnología*, *8*(2), 111–137. https://doi.org/10.5354/0719-2584.2019.53447

Blanca, J., & Morales, C. (2016). Seguridad de la Información. *CLIP de SEDIC*. https://clip.sedic.es/article/debate-clip-no72-seguridad-la-informacion/

Bojorque, R. (2008). Sistemas Gestores de Contenido (CMS). La solución ideal en la Web. *Ingenius*, *3*. https://doi.org/10.17163/ings.n3.2008.07

Bravo, L., García, U., Hernández, M., & Varela, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica*, *2*(7), 162–167.

Cabello, A. L. C. (2015). *Implantación de aplicaciones web en entornos internet, intranet y extranet. IFCD0210*. IC Editorial.

Cárdenas, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: Revisión bibliográfica. *El Profesional de la Información*, *25*(6), 931. https://doi.org/10.3145/epi.2016.nov.10

Caser. (2019). *¿Qué es un ataque informático?* | *Caser Seguros*. https://www.caser.es/glosario-seguros/comercio/ataque-informatico

Castellanos, T., Gallego, J. C., Delgado, J. A., & Merchán, L. (2014). *Análisis comparativo entre los modelos de madurez reconocidos en la gestión de proyectos*. 28.

Chen Mok, S. (2010). Privacidad y protección de datos: Un análisis de legislación comparada. *Diálogos Revista Electrónica de Historia*, *11*(1), 111–152.

Chicaiza, G., Ponce, L., & Campos, G. V. (2020). *INYECCIÓN DE SQL, CASO DE ESTUDIO OWASP*. 9.

Chiriguayo-Lozano, S. J. (2015). Comercio Electrónico: Importancia de la Seguridad en las Transacciones Electrónicas, Amenazas y Soluciones a Implementar. *Revista Empresarial, ICE-FEE-UCSG*, *9*(35), 8–14.

Citicus. (2020). *Metodología ISF FIRM* | *Citicus*. https://www.citicus.com/blog/ISF-FIRM-methodology

Cloudflare. (2019). *¿Qué es un rastreador web?* | *Cómo funcionan las arañas web*. Cloudflare. https://www.cloudflare.com/es-es/learning/bots/what-is-a-web-crawler/

CorpoAmbato. (2018). *Quienes Somos*. https://corpoambato.org.ec/about.html

Costas-Santos, J. (2015). *Seguridad informatica*. RA-MA Editorial. elibro.puce.elogim.com/es/lc/puce/titulos/62452

Cuzcano, A. E. (2004). *EL ACCESO A LA INFORMACIÓN PÚBLICA: UN ACERCAMIENTO DOCTRINAL*. 20.

Diligent Team. (2017, abril 3). *Comparativa de las 4 plataformas de eCommerce más conocidas 2017*. Diligent. https://www.diligent.es/comparativa-de-las-5-plataformas-de-ecommerce-mas-conocidas/

Dominguez, A. H. (2018). Sistema para la detección de ataques PHISHING utilizando correo electrónico. *Telemática*, *17*(2), 60–70.

Dulzaides, M. E., & Molina, A. M. (2004). Análisis documental y de información: Dos componentes de un mismo proceso. *ACIMED*, *12*(2), 1–1.

Electronic Data Interchange. (2020). *E.D.I Basics*. 4.

Escalante, R. A. P., & Molina, A. F. G. (2018). *Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana*. 12.

Escriva Gasco, G. (2013). *Seguridad informatica*. Macmillan Iberia, S.A. elibro.puce.elogim.com/es/lc/puce/titulos/43260

Escuela de Administración, Liderazgo, Dirección y Emprendimiento. (2017). 5 elementos básicos de un Ecommerce. *EALDE Business School*. https://www.ealde.es/elementos-basicos-ecommerce/

Estruga, N. (2020, octubre 28). La importancia de la seguridad informática en el entorno empresarial. *EALDE Business School*. https://www.ealde.es/importancia-seguridad-informatica-empresas/

Eugenia, G. M. (2014). *Metodologia de la investigacion*. Grupo Editorial Patria. elibro.puce.elogim.com/es/lc/puce/titulos/40362

FourWebs. (2019). Arquitectura Web SEO para E-commerce. *4webs*. https://www.4webs.es/blog/arquitectura-web-seo-para-e-commerce

Fundación Integra de Murcia. (2010). *SEGURIDADEN EL COMERCIO ELECTRÓNICO*.

https://www.cecarm.com/Guia_Seguridad_en_el_comercio_electronico_-_CECARM.pdf-6559

Galarza, J. A., & Uriona, C. F. (2012). Modelos de Madurez en los Datos de una Organización: Caso de Estudio Universidad Católica Boliviana “San Pablo” Cochabamba. *Acta Nova*, *5*(4), 462–476.

García, M. (2017). *MVC (Modelo-Vista-Controlador): ¿qué es y para qué sirve?* https://codingornot.com/mvc-modelo-vista-controlador-que-es-y-para-que-sirve

Gasco, G. (2013a). *Seguridad informatica*. elibro.puce.elogim.com/es/lc/puce/titulos/43260

Gasco, G. (2013b). *Seguridad informatica*. Macmillan Iberia, S.A. elibro.puce.elogim.com/es/lc/puce/titulos/43260

Golan, P. (2020). *Los 5 tipos de comercio electrónico*. Shopify. https://es.shopify.com/blog/12621205-los-5-tipos-de-comercio-electronico

Gomez Vieites, A. (2015). *Seguridad en equipos informaticos*. RA-MA Editorial. elibro.puce.elogim.com/es/lc/puce/titulos/62466

González, J. (2020). Comercio electrónico en China y México: Surgimiento, evolución y perspectivas. *México y la cuenca del pacífico*, *9*(27), 53–84. https://doi.org/10.32870/mycp.v9i27.688

Heredia, M. de la C. B. (2015). *Selección, instalación, configuración y administración de los servidores de transferencia de archivos. IFCT0509*. IC Editorial.

Hernández, R., Fernández, C., & Pilar, M. (2014). *Metodología de la investigación*. McGraw-Hill.

INFOAGRO. (2005). *Características de la información para su clasificación como pública o privada.* http://www.infoagro.go.cr/Infoagro/Proyecto%20Geomar/Caracteristicas%20de%20la%20informacion%20para%20su%20clasificacion%20como%20publica%20o%20privada.pdf

Ingertec. (2019, septiembre 4). ¿Qué es la seguridad de la información? Aspectos clave, Ingertec. *Ingertec.com*. https://ingertec.com/que-es-la-seguridad-de-la-informacion/

Instituto de Ingenieros Eléctricos y Electrónicos. (2018). Estandar IEEE. *IEEE Sección España*. https://ieeespain.org/quienes-somos/

Instituto Nacional de Ciberseguridad. (2020). *Proteccion de la informacion*. 33.

Instituto Nacional de Ciberseguridad de España. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? *INCIBE*. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Instituto Nacional de Ciberseguridad de España. (2020). *Proteccion de la informacion*. 33.

Instituto Nacional de Ciberseguridad de España. (2021, mayo 25). *Información confidencial, secreto profesional. Acuerdos de confidencialidad*. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/informacion-confidencial-secreto-profesional-acuerdos-confidencialidad

JULIO, B. C., JAIME, B. M., OCTAVIO, R. R., CARMEN, R. T., Mª DEL, JORGE, R. R., GEMMA, S. A., & FRANCISCO, S. C. (2020). *Redes locales 3.ª edición 2020*. Ediciones Paraninfo, S.A.

López, P. A. (2010). *Seguridad informática*. Editex.

MAGERIT. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. 127.

Maila, A., Elías, D., Sandoval, R., & Ruperto, R. (2015). *Elaboración del Plan de Seguridad de la Información para el Fondo de Cesantía y Jubilación del MDMQ*. 112.

Martinez Rolan, X. (2019). *Diseno de paginas web: Wordpress para todos los publicos*. Editorial UOC. elibro.puce.elogim.com/es/lc/puce/titulos/106387

Medina Rojas, J. D., & Rivas Montalvo, Y. Y. (2020). Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos. *Universidad Nacional Pedro Ruiz Gallo*. http://repositorio.unprg.edu.pe/handle/20.500.12893/8074

Melo, V., & Hernando, A. (2008). EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001. *Revista de Derecho*, *29*, 333–366.

Meraz, A. I. (2018). Empresa y privacidad: El cuidado de la información y los datos personales en medios digitales. *REVISTA IUS*, *12*(41). https://doi.org/10.35487/rius.v12i41.2018.313

MERLOS. (2019, septiembre 4). ¿Para qué sirve un plan de seguridad informática? *Merlos*. https://merlos.net/para-que-sirve-un-plan-de-seguridad-informatica/

Microsoft. (2018, abril 30). *Protege tu empresa con las nuevas características de seguridad para Microsoft 365 Empresa*. Microsoft 365 Blog. https://www.microsoft.com/es-es/microsoft-365/blog/2018/04/30/safeguard-your-business-with-new-security-features-for-microsoft-365-business/

Mieres, J. (2009). Ataques informáticos. *Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf*.

Ministerio de Telecomunicaciones. (2020). *ESTRATEGIA NACIONAL DE COMERCIO ELECTRÓNICO* (p. 14). https://aportecivico.gobiernoelectronico.gob.ec/system/documents/attachments/000/000/011/original/58b9ab393399dc479d2fb43c7a305ff0de62ec96.PDF

Molina, K. (2015). *Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros*. Universidad Politécnica Salesiana Sede Guayaqui.

Monsalve-Pulido, J. A., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Facultad de Ingeniería*, *23*(37), 65–72.

Muñoz, F. (2016, marzo 31). *Ciberseguridad, documentos abiertos e información pública deben ir de la mano*. Expansión.com. https://www.expansion.com/economia-digital/protagonistas/2016/03/31/56fceea022601d2a428b457c.html

Murillo, R. S. (2009). *BENEFICIOS DEL COMERCIO ELECTRÓNICO*. 15.

Muro, J. D., & Ramírez, E. L. (2000). *Seguridad y comercio por internet*. 14.

Nerion. (2020). *Hosting web, servidores cloud y dominios | Nerion by Axarnet*. https://www.nerion.es/

Neubox. (2020). *¿Qué es un Hosting o Web Hosting?* Neubox. https://neubox.com/que-es-web-hosting

Organización de los Estados Americanos. (2013). *El Acceso a la Información Pública, un Derecho para ejercer otros Derechos*.

Organización de los Estados Americanos. (2019). Clasificación de Datos. *White paper series*, 24.

Organización Internacional de Normalización. (2020). *ISO/IEC 27009:2020*. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73907.html

Organización SSL.com. (2020). Certificados DV, OV, IV y EV. *SSL.com*. https://www.ssl.com/es/art%C3%ADculo/dv-ov-y-ev-certificados/

Ospina Díaz, M. R., Sanabria Rangel, P. E., Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: Un análisis para Colombia. *Revista Criminalidad*, *62*(2), 199–217.

OWASP. (2017). *Estándar de Verificación de Seguridad en Aplicaciones 3.0.1*. 75.

OWASP. (2020). *Los diez principales riesgos de seguridad de las aplicaciones web de OWASP | OWASP*. https://owasp.org/www-project-top-ten/

OWASP Fundation. (2020). *OWASP Foundation | Open Source Foundation for Application Security*. https://owasp.org/

Paredes, S., Hinojosa, C., & Ruiz, J. (2011). *La importancia de la Gestión de la Configuración del Software, en una Empresa de Desarrollo. 1*(3), 11.

Pérez Bustamante & Ponce. (2016, diciembre 2). Normas sobre información personal y confidencial. *PBP*. https://www.pbplaw.com/es/normas-informacion-personal-confidencial/

Pérez, E., Vergara, I., & Rodríguez, Y. (2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Ingeniería Industrial*, *35*(2), 184–198.

Pilar, A.-R., & Alfonso, G.-C. H. (2011). *Seguridad informática*. Editorial Paraninfo.

Pineda, F. A. (2017). *El delito de Hacking* [Http://purl.org/dc/dcmitype/Text, Universitat de València]. https://dialnet.unirioja.es/servlet/tesis?codigo=184249

Pinto, D. (2014). *Metodología de análisis forense orientada a incidentes en dispositivos móviles*. 11.

Ramos, X. (2020a). 60 % de transacciones bancarias se hicieron a través de internet desde la cuarentena por el coronavirus. *El Universo*. https://www.eluniverso.com/noticias/2020/04/26/nota/7822986/ventas-domicilio-coronavirus-internet-web

Ramos, X. (2020b). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. *El Universo*. https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador

Roa Buendia, J. F. (2013). *Seguridad informatica*. McGraw-Hill Espana. elibro.puce.elogim.com/es/lc/puce/titulos/50243

RockContent. (2018, noviembre 25). Conoce los 7 principales tipos de comercio electrónico del mercado. *Rock Content - ES*. https://rockcontent.com/es/blog/tipos-de-comercio-electronico/

Rodríguez, A., & Pérez, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista EAN*, *82*. https://doi.org/10.21158/01208160.n82.2017.1647

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (1a ed.). Editorial Científica 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

Rosero, A.-B. (2020). Estafas en línea, en la venta de tecnología—El Comercio. *El Comercio*. https://www.elcomercio.com/actualidad/seguridad/estafas-compras-venta-tecnologia-internet.html

Sabillón, R., & Cano M., J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33–48. https://doi.org/10.17013/risti.32.33-48

Saltos Salgado, M. F., Robalino Villafuerte, J. L., Pazmiño Salazar, L. D., Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343–351.

Sigmond, K. (2018). El comercio electrónico en los tratados de libre comercio de México. *Revista IUS*, *12*(41), 359–377.

Somalo, N. (2017, diciembre 2). Elementos de una plataforma tecnológica de ecommerce. *Nacho Somalo*. https://www.nachosomalo.com/elementos-de-una-plataforma-tecnologica-de-ecommerce/

Soriano, M. (2014). Seguridad en redes y seguridad de la información. *Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad_de_Red_e_Informacion. pdf*.

Taque, M. P. (2011). Delito en el Comercio Electrónico. *Prisma Jurídico*, *10*(1), 209–224.

Tarazona, C. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, *28*(84), 137–146.

Tatiana, B. (2016). *¿Qué es la información pública? - LegalToday*. https://www.legaltoday.com/opinion/blogs/transversal/blog-administracion-publica/que-es-la-informacion-publica-2016-06-27/

TechTarget. (2020). *¿Qué es Privacidad de datos (privacidad de información)?* SearchDataCenter en Español. https://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion

Tecon. (2019, enero 28). La Seguridad de la Información. *Tecon*. https://www.tecon.es/la-seguridad-de-la-informacion/

Tejerina, O., & Pinar, J. L. (2014). *Seguridad del estado y privacidad*. Editorial Reus. elibro.puce.elogim.com/es/lc/puce/titulos/46557

Telégrafo, E. (2012, abril 5). *Banco Pichincha implementará herramienta tecnológica para mejora de servicios y seguridad*. El Telégrafo. https://www.eltelegrafo.com.ec/noticias/economia/8/banco-pichincha-implementara-herramienta-tecnologica-para-mejora-de-servicios-y-seguridad

Torres R., A., Martínez-Rueda, R., Duarte A., N. A., Lagos S., J. A., Prieto B., F., Alba P., L. L., Moreno O., J. P., Toro C., B. A., Vilardy R., A., Castro B., D. E., Lasso O., N. A., & Buitrago R., J. A. (2015). DISEÑO DE UNA PLATAFORMA INTEROPERABLE PARA UN OBSERVATORIO DE

HÁBITOS Y ESTILOS DE VIDA SALUDABLE. *Revista Ingeniería Biomédica*, *9*(17), 45–55.

Universidad Internacional de Valencia. (2021). *Ciberamenazas en 2021: ¿cómo identificarlas?* | *VIU* [Ciencia y Tecnología]. https://www.universidadviu.com/pe/actualidad/nuestros-expertos/ciberamenazas-en-2021-como-identificarlas

Valdez Alvarado, A. (2013). *OSSTMM 3*.

Wagner, J. (2016, abril 26). Metodologías de pruebas de seguridad informática. *Noticias de seguridad informática, ciberseguridad y hacking*. https://noticiasseguridad.com/importantes/metodologias-de-pruebas-de-seguridad-informatica/

Winkels, N. (2019). *The Definitive Guide to CMS Architecture*. bloomreach.com. https://developers.bloomreach.com/blog/2019/cms-architecture.html

Woodbury, B. (2021). *Vulnerabilidades de seguridad y kits de vulnerabilidades de seguridad—Windows security*. https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/exploits-malware

Zuñiga, V. (1999). *Comercio Electrónico: Estado actual, Perspectivas y servicios*. 11.

ANEXOS

Anexo 1. Cuestionario aplicado al Gerente Técnico de CorpoAmbato

Modelo de entrevista para obtener información sobre la seguridad en plataformas de comercio electrónico

Objetivo	Recolectar información relevante en torno a la seguridad de plataformas de comercio sobre técnicas, métodos, herramientas y estrategias en general utilizadas para mantener segura la información sensible de los usuarios.
Investigador	Alejandro Javier Valle Valle Estudiante de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato

Consideraciones Generales

1. Se le solicita muy amablemente responder de forma abierta pero objetiva
2. La información aquí recolectada tiene fines investigativos

Desarrollo

1. ¿Qué mecanismo considera es el mejor para mantener segura la información de una plataforma de comercio electrónico?
2. ¿Qué niveles de seguridad emplearía en una plataforma de comercio electrónico para garantiza la información tratada?
3. ¿Qué indicadores le evidencian que una plataforma de comercio electrónico se encuentra segura?

---

4. ¿Qué medidas aplicaría para responder si se llegase a vulnerar la información de sus clientes?

---

5. ¿Qué controles implementaría para garantizar la seguridad en la información en las plataformas de comercio electrónico?
6. ¿Qué herramientas y técnicas utilizan para prevenir ataques?
7. ¿Qué tipos de ataques son comunes dentro de la organización?

Gracias por su colaboración

Anexo 2. Cuestionario aplicado a la Gerente General de CorpoAmbato

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista para obtener información sobre datos de interés asociados a proyectos de TI

Objetivo	Recolectar información de proyectos innovadores de TI realizados por la institución y planes a futuro sobre mejorar la plataforma de comercio electrónico.
Investigador	Alejandro Javier Valle Valle Estudiante de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato

Consideraciones Generales

1. Se le solicita muy amablemente responder de forma abierta pero objetiva
2. La información aquí recolectada tiene fines investigativos

Desarrollo

1. ¿Cómo están organizados para apoyar el desarrollo de proyectos de emprendimiento?
2. ¿Qué tipo de proyectos han realizado relacionados con las tecnologías de la información?
3. ¿Qué los impulsa a ayudar a otros sin obtener beneficio alguno?

---

4. ¿Actualmente qué proyectos están se llevan a cabo en la provincia dentro del área de TI?

---

5. ¿Cuál es su criterio en cuanto al proyecto de seguridad en la plataforma de comercio electrónico CorpoAmbato?
6. ¿Qué planea hacer para mejorar en un futuro la plataforma de comercio electrónico de CorpoAmbato??

Gracias por su colaboración

Anexo 3. Matrices de valorización MAGERIT

Matriz de clasificación de riesgo

Clase	Valoración cualitativa	Valoración cuantitativa	Nivel de seguridad
Crítico	Muy alto	Muy alto	Muy bajo
Grave	Alto	Posible	Medio
Moderado	Medio	Poco probable	Alto
Despreciable	Bajo y Muy bajo	Muy raro	Muy alto

Matriz de opción de tratamiento

Tratamiento	Descripción
Evitación del riesgo	Incluye evitar o retirar actividades o un conjunto de actividades planificadas que generen riesgos; o realizar cambios considerables durante la ejecución de la organización para mejorar su entorno de desarrollo para evitar riesgos.
Reducción del riesgo	Incluye implementar controles y medidas adecuadas, optimizar procesos, entre otros; para reducir al mínimo los riesgos.
Transferencia del riesgo	Implica transferir todo o parte del riesgo a una entidad externa que tenga la experiencia necesaria y los recursos suficientes para mitigar el riesgo.
Retención o aceptación del riesgo	Este enfoque es que, si ocurre un riesgo, la organización es responsable de las consecuencias, esto por lo general sucede cuando el nivel de impacto en el activo después de la evaluación es muy bajo.

Anexo 4. Plan de seguridad y buenas prácticas

PLAN DE SEGURIDAD DE LA PLATAFORMA DE COMERCIO ELECTRÓNICO DE CORPOAMBATO

Introducción

La organización CorpoAmbato sin motivos de lucro a través del desarrollo de un proyecto en conjunto con la PUCESA ha puesto a disposición una plataforma de comercio electrónico para que sus pequeños empresarios asociados a la misma comercialicen sus productos, muchos se han visto afectados por la pandemia iniciada en Ecuador a mediados del año 2020. En uno de sus planes a ejecutar en un futuro está el integrar más de mil emprendimientos o negocios dentro de la plataforma, eso implica un manejo masivo de información de todo tipo, por lo que se ve en la necesidad de precautelar la integridad de la información que allí se tramita a fin de evitar pérdidas de datos sensibles como: contraseñas, números cuenta, números de tarjetas, entre otros. Por ese motivo, se desarrolla un plan de seguridad y buenas prácticas para que la organización CorpoAmbato tenga disponible para mejorar el nivel de seguridad de la plataforma de comercio electrónico.

Objetivos

- Analizar y detectar las vulnerabilidades por medio de pruebas de escaneo dentro de la plataforma
- Determinar el nivel de riesgo de cada vulnerabilidad encontrada en base a una escala de valorización
- Proponer un conjunto de políticas o buenas prácticas a seguir para elevar el nivel de seguridad

Alcance

El alcance del plan de seguridad depende en mayor parte de las actividades a realizar en un futuro para mejorar la plataforma, en este caso, la organización planea integrar más de mil emprendimientos en su plataforma, lo que significa guardar mucha información sensible de aquellos usuarios registrados en la misma.

También, para agilizar el proceso de trabajo, se requiere de una forma rápida y segura para realizar transacciones comerciales, así que una opción es añadir a aquellos métodos de pago que usan como principal medio de comunicación a la internet, por lo que es necesaria tener un nivel de seguridad alto para proteger información relaciona a las transacciones. Es ahí donde radica la importancia de elaborar un plan de seguridad, puesto que evalúa toda la plataforma en busca de vulnerabilidades que representen un riesgo a la información sensible de usuarios, para clasificarlas en función del riesgo de modo que permita determinar pautas de prevención de la misma.

Análisis de los niveles de riesgos y seguridad

El análisis de los riesgos fue realizado a partir de los resultados obtenidos por las pruebas de la guía OWASP y la asignación de puntajes a través de las escalas de valorización del riesgo definidos por la metodología MAGERIT.

Seguidamente, la siguiente tabla, está compuesta por 7 columnas, las cuales se describen a continuación:

- Tipo de prueba: se realiza conforme al tipo de vulnerabilidad a detectar
- Objetivo de la prueba: la finalidad de la prueba
- Amenaza: surge a raíz de la vulnerabilidad
- Vulnerabilidad: es el resultado de la prueba si es detectada
- Riesgo: producto del impacto y la probabilidad (
- Nivel de seguridad: se define de acuerdo al nivel del riesgo, (Alta – Media – Baja – Muy baja) las pruebas categorizadas en N/A no se consideran en esta tabla.

N	Tipo de prueba	Objetivo de la prueba	Amenaza	Vulnerabilidad	Riesgo	Nivel Seguridad
1	Descubrimiento de información por motores de búsqueda	Información sensible de la configuración y diseño, archivo robots.txt desactualizado	Ingeniería Social	Números telefónicos, direcciones y nombres públicos	2	Alta

4	Enumerar aplicaciones en el servidor Web	Enumerar aplicaciones ocultas vulnerables a ser atacadas	Posibilidad de ejecución de ataques de intrusión, accesos no autorizados.	Nombres, versión de servidor, dirección IP, dominio	2	Alta
13	Métodos HTTP	Descubrimiento de métodos con potencial riesgo para deshabilitarlos	Posible aplicación de los siguientes ataques: explotación Cross-site tracing (TRACE), Inclusión de archivo ASP para ejecución de comandos (PUT), ataque DoS (DELETE), ejecución de código remoto (CONNECT)	Métodos encontrados: PUT, DELETE, CONNECT y TRACE	2	Alta
17	Registro de usuarios	Requisitos de identidad para proceso registro de usuarios no alineados con los requerimientos de seguridad y negocio.	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	2	Alta

18	Creación de cuentas	Proceso de crear una cuenta válida sin la aplicación de una correcta identificación y proceso de autorización.	Ataques de fuerza bruta	Falta de seguridad de identificación de usuario (Captcha)	2	Alta
20	Determinar un mecanismo de bloqueo débil	Mecanismo de bloque débil o sin implementar	Ataques de fuerza bruta	Mecanismo de bloqueo de adivinanza de contraseñas sin implementar	2	Alta
26	Falsificación de solicitudes entre sitios CSRF	Vulnerabilidad asociada al ataque conocido como CSRF (Cross-site request forgery)	Ingeniería social, ataque Cross-site request forgery	Identificación de cuatro solicitudes con riesgo bajo vulnerables al ataque	1	Muy Alta

En esta tabla, se contempla únicamente un resumen de las pruebas en las que se obtuvo resultados con respecto a las vulnerabilidades, por lo que, para observar todas las pruebas, diríjase a la tabla 10.

Opciones de tratamiento

A continuación, se elige las opciones de tratamiento definidas en el anexo 4 para determinar las siguientes acciones de mitigación.

Tratamiento	Número de prueba
Aceptación del riesgo	1,4,12,13,26
Reducción del riesgo	17,18,20
No aplica (N/A)	2,3,5,6,7,8,9,10,11,14,15,16,19,21,22,23,24,25,27,28,29,30,31,32

Las pruebas clasificadas como “N/A” (No Aplica), no se tomaron en cuenta debido a que no se encontraron evidencias de vulnerabilidades o eran pruebas de reconocimiento, por lo que no cuentan con un puntaje de riesgo.

Buenas prácticas

El siguiente apartado, se describen las buenas prácticas a implementar en base a la opción de tratamiento elegido, lo que en este caso aplicaría exclusivamente para las pruebas catalogadas en reducción del riesgo o mitigación.

- **Registro de usuarios:** instalar CAPTCHA en el formulario de registro de usuarios a través de los módulos gratuitos de prestashop y añadir Modulo de verificación de edad
- **Creación de cuentas:** instalar CAPTCHA en el formulario de registro de usuarios a través de los módulos gratuitos de prestashop. Añadir módulo de confirmación de cuenta con función de código de activación enviada al correo del usuario
- **Mecanismo de bloque:** instalar el módulo de bloqueo de IPs si es necesario o Instalar el módulo de “Inicio de sesión avanzado”, el cual permite restringir el número de intentos permitidos por cada sesión. Además, que permite añadir y configurar funciones adicionales en cuanto a la seguridad de los formularios de inicio y registro de usuario

Para más detalles acerca de las pruebas en los que se aplicaron los métodos de mitigación o reducción del riesgo. Ver tabla 22.

Políticas de seguridad

A continuación, se plantean algunas políticas de seguridad a seguir en la parte administrativa de la plataforma:

- **Política CVV y AVS:** para cuando la organización emplee métodos de pago en la misma plataforma a través del ingreso de datos de la tarjeta de crédito, por seguridad solicita del código CVV (Card Verification Value) como una condición obligatoria para realizar la transacción. Igualmente, el sistema de verificación AVS (Address Verification System), estaría presente, puesto que a través de la comunicación con el banco emisor de la tarjeta detecte

coincidencias en a la dirección de facturación del cliente y así evitar estafas si la tarjeta llegase a ser comprometida.

- **Política de creación de Backups:** así mismo, esta política, se la emplea si la organización maneja cantidades masivas de información sensible, la cual siempre presenta riesgos de perderse, por lo tanto, que de manera periódica producir una copia de seguridad para su restauración, resulta útil.
- **Política de contraseñas seguras:** para el personal que administra la plataforma es necesario contar con contraseñas robustas, es decir, que contengan una combinación de caracteres impredecible y con una longitud estándar.
- **Política de evitar almacenar información sensible:** la mejor forma de evitar robo de datos es simplemente no almacenarlos, principalmente en torno a información sensible como números de tarjeta

Unidad Gestora: Área de tecnología o área técnica
Responsable: Administrador del portal de comercio electrónico

Anexo 5. Resultado de pruebas adicionales

Herramienta de escáner Nessus

Sev	Name	Family	Count
MIXED	SMTP (Multiple Issues)	SMTP problems	4
LOW	POP3 Cleartext Logins Permitted	Misc.	1
INFO	Service Detection	Service detection	24
INFO	Nessus SYN scanner	Port scanners	23
INFO	HTTP (Multiple Issues)	Web Servers	9
INFO	Web Server (Multiple Issues)	Web Servers	6
INFO	DNS (Multiple Issues)	DNS	3
INFO	SMTP Server Detection	Service detection	3
INFO	ISC Bind (Multiple Issues)	DNS	2
INFO	TLS (Multiple Issues)	Misc.	2
INFO	IMAP Service Banner Retrieval	Service detection	2
INFO	POP Server Detection	Service detection	2
INFO	SMTP Service STARTTLS Command Support	SMTP problems	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	FTP Server Detection	Service detection	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Non-compliant Strict Transport Security (STS)	Service detection	1
INFO	OS Identification	General	1
INFO	Service Detection (HELP Request)	Service detection	1
INFO	Strict Transport Security (STS) Detection	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Traceroute Information	General	1
INFO	WebDAV Detection	Web Servers	1