UNIVERSIDAD DEL AZUAY

DEPARTAMENTO DE POSGRADOS

MAESTRÍA EN TELECOMUNICACIONES

"GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE SERVICIOS IAAS EN E-COMMERCE EN LA NUBE PÚBLICA DE PEQUEÑA Y GRAN ESCALA ENFOCADA A LA MEDIANA EMPRESA ECUATORIANA: UNA PERSPECTIVA DE CIBERSEGURIDAD"

Trabajo de graduación previo a la obtención del título de:

MAGÍSTER EN TELECOMUNICACIONES

Autor:

JOHNY FELIPE PLAZA MEJÍA

Director:

JAIME SEBASTIÁN BURBANO VILLAVICENCIO

CUENCA, ECUADOR

2024

Abstract

In the last years, public cloud providers have diversified their services to fit the needs of businesses of all sizes. In particular, medium-sized Ecuadorian e-commerce companies have shown an interest in implementing public cloud infrastructure services due to their ability to offer control, scalability, flexibility, and improved performance. However, despite these advantages, many of these companies face multiple challenges, such as economic limitations and a lack of specialized technical personnel. As a result, it is common to find cybersecurity deficiencies, allowing easily identifiable vulnerabilities to be exploited by cybercriminals. This study presents a practical guide for the implementation of secure IaaS (Infrastructure as a Service) aimed at e-commerce, using both large and small-scale cloud providers as examples. This document is offered as a tool that proposes a comprehensible technical foundation designed to help medium-sized Ecuadorian companies mitigate the most common security risks and ensure the protection of their digital assets.

Firmado electrónicamente por:
JAIME SEBASTIAN BURBANO VILLAVICENCIO

Ing. Jaime Sebastián Burbano Villavicencio. Ph.D.

Thesis Director

Ing. Johny Felipe Plaza Mejía

Author

Translated by:

Ing. Johny Felipe Plaza Mejía

Author

GUÍA PRÁCTICA PARA LA IMPLEMENTACIÓN DE SERVICIOS IAAS EN E-COMMERCE EN LA NUBE PÚBLICA DE PEQUEÑA Y GRAN ESCALA ENFOCADA A LA MEDIANA EMPRESA ECUATORIANA: UNA PERSPECTIVA DE CIBERSEGURIDAD

Johny Felipe Plaza Mejía
Escuela de Ingeniería Electrónica
Universidad del Azuay
Cuenca, Ecuador
jplaza@es.uazuay.edu.ec

***Resumen*—En los últimos años, los proveedores de la nube pública han diversificado sus servicios para adaptarse a las necesidades de las empresas de todos los tamaños. En particular, las empresas medianas de e-commerce ecuatorianas han mostrado un interés en implementar servicios de infraestructura de la nube pública debido a su capacidad para ofrecer control, escalabilidad, flexibilidad y rendimientos mejorados. Sin embargo, a pesar de estas ventajas, muchas de estas empresas enfrentan múltiples desafíos, tales como limitaciones económicas y falta de personal técnico especializado. Como resultado, es común encontrar deficiencias de ciberseguridad, lo que permite la aparición de vulnerabilidades fácilmente identificables y explotables por parte de ciberdelincuentes. En este estudio, se presenta una guía práctica para la implementación de IaaS seguros destinados a e-commerce, tomando como ejemplo proveedores de nube a gran y pequeña escala. Este documento se ofrece como una herramienta que propone una base técnica comprensible, diseñada para ayudar a las empresas medianas ecuatorianas a mitigar los riesgos de seguridad más comunes y garantizar la protección de sus activos digitales.**

***Palabras clave*—*Cloud computing*, Ciberseguridad, E-commerce, *PrestaShop*, *Linode*, AWS.**

I. Introducción y antecedentes

Cloud Computing o computación en la nube es un modelo que administra los recursos de computación necesarios y convenientes que pueden ser accedidos y compartidos mediante el Internet. Estos recursos pueden ser configurados y gestionados con una mínima interacción y desarrollo. Las principales características de este paradigma informático son: acceso a infraestructura, banda ancha, rápida elasticidad, servicio medido, servicios bajo demanda y agrupación de recursos [1]. En la Figura 1, se describen los elementos fundamentales de *cloud computing*.

La computación en la nube ofrece diferentes modelos de servicios que se adaptan según las necesidades de los usuarios. Los principales son: Infraestructura como Servicio (IaaS, sus siglas en inglés), es un servicio que ofrece recursos esenciales de procesamiento, almacenamiento, red y otros recursos computacionales relevantes. Plataforma como Servicio (PaaS, sus siglas en inglés), es un entorno de implementación y desarrollo sobre la infraestructura de la nube usando lenguajes de programación, librerías, servicios y herramientas que soporten el proveedor de la nube. *Software* como Servicio (SaaS, sus siglas en inglés) son aplicaciones completas ejecutadas en la infraestructura de la nube [2].

En cuanto al modelo de implementación, existen tres principales: privado, hibrido, público. De estos, el uso del modelo público se presenta como el más prometedor para las empresas medianas, debido a la reducción de costos en términos de adquisición y mantenimiento de infraestructura que este ofrece. La nube pública es de propiedad de terceras personas y los recursos se ofrecen a los usuarios bajo demanda, siguiendo un modelo *pay as you go*. Los proveedores de nube pública se dividen en:

- Pequeña escala diseñada para satisfacer las necesidades de pequeñas empresas. Estas nubes ofrecen servicios y recursos informáticos flexibles y escalables a un costo accesible, lo que permite a las pequeñas y medianas empresas aprovechar los beneficios de la computación en la nube sin invertir en una infraestructura propia. Un ejemplo de proveedor de nube pública de pequeña escala es *Linode*.
- Gran escala se refiere a una infraestructura de *cloud computing* amplia, robusta y escalable. Se caracteriza por tener una amplia capacidad de almacenamiento, proce-

samiento y recursos informáticos, lo que permite alojar y ejecutar aplicaciones y servicios a gran escala. Estos proveedores de servicios en la nube suelen tener centros de datos distribuidos geográficamente en diferentes ubicaciones para garantizar la disponibilidad, redundancia y rendimiento, como por ejemplo *Amazon Web Services* (AWS, sus siglas en inglés).

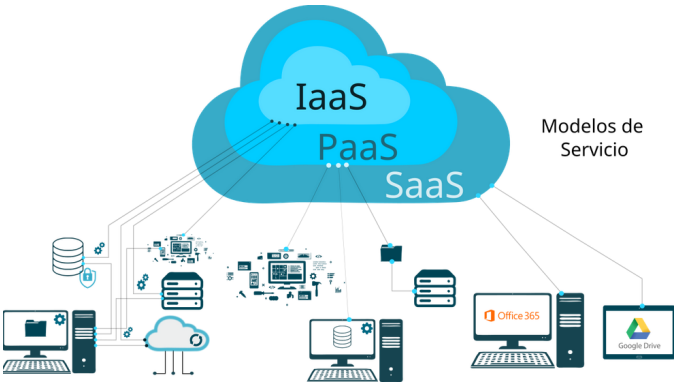

Figura 1. Cloud computing y modelos de servicio

En el Ecuador, el Servicio de Rentas Internas (SRI, sus siglas en español) define como PyMEs al conjunto de pequeñas y medianas empresas que, de acuerdo con su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos, presentan características propias [3]. En la Tabla I, se muestra la estructura empresarial ecuatoriana enfocada en dos de estas características: ingresos y número de trabajadores.

TABLA I
ESTRUCTURA EMPRESARIAL

Clasificación de las empresas	Volúmenes de ventas anuales	Personal ocupado
Micro	Menor a 100.000	1 a 9
Pequeña	100.001 a 1'000.000	10 a 49
Mediana A	1'000.001 a 2'000.000	50 a 99
Mediana B	2'000.001 a 5'000.000	100 a 199
Grande	5'000.001 en adelante	200 en adelante

Conforme las empresas medianas ecuatorianas buscan digitalizarse y expandirse en línea, la adopción de soluciones en la nube emerge como un factor crucial para asegurar escalabilidad, flexibilidad y eficiencia operativa. En este contexto, la implementación y mantenimiento de una arquitectura de nube segura basada en servicios IaaS se torna esencial, en especial, debido a la creciente sofisticación de las amenazas cibernéticas y la falta de concienciación referente a la ciberseguridad en el país.

En [4] se realizó un sondeo en Ecuador en el año 2020 a múltiples empresas con el objetivo de analizar su perspectiva hacia la seguridad informática. Los resultados revelaron que más del 50 % de las empresas encuestadas cuentan con herramientas básicas para mitigar el riesgo de ataques informáticos. Sin embargo, únicamente el 3 % de estas empresas disponen de herramientas específicas para abordar los riesgos relacionados con la computación en la nube. Además, se prevé que para el año 2025, aproximadamente el 30 % de los negocios optarán por nubes privadas, mientras que el 28 % elegirán nubes públicas como su modelo de implementación. Durante el estudio, el 75 % de las empresas encuestadas expresaron una gran preocupación en cuanto a la seguridad de la implementación de servicios en la nube pública en sus organizaciones. En este sentido, nueve de cada diez expertos en ciberseguridad coinciden en la importancia y el papel crucial de la seguridad en la nube pública, haciendo referencia a un modelo de relación compartida para garantizar la seguridad en este entorno. En [5], se establece que los riesgos tecnológicos que afronta Ecuador y el mundo es el aumento de ciberespionaje y ciberdelitos perpetuados por individuos, grupos o entidades, quienes utilizan la creciente tecnología digital para cometer delitos como la pérdida de la privacidad, fraude o robo de datos y espionaje, entre otros.

Si bien cualquier empresa puede ser víctima de ciberataques, las empresas pequeñas y medianas son especialmente vulnerables, representando el 66 % de los blancos de los atacantes [6]. Esto se debe en gran parte a la falta de inversión en seguridad, ocasionada por la limitación de recursos financieros destinados a esta área. En [7], se realizaron encuestas en el año 2023 en Latinoamérica y el Caribe a 195 empresas de diferentes tamaños. De los resultados obtenidos, se destaca que el 70 % de las empresas afirman que han experimentado un aumento en los ataques cibernéticos. Esto demuestra que, a pesar de los esfuerzos por mejorar la ciberseguridad, los ataques persisten, especialmente los ataques de ingeniería social, que son los más sufridos por estas empresas.

Para las PyMEs cuyo ingreso depende parcial o totalmente del e-commerce, el manejo adecuado de los servicios en la nube es crítico. La Estrategia Nacional de Comercio Electrónico (ENCE, sus siglas en español) [8], reconoce que el e-commerce no solo son ventas en línea, sino que abarca toda la cadena de valor, desde el acceso web hasta el servicio de posventa. Además, destaca el crecimiento de Tecnologías de Información y Comunicación (TIC, sus siglas en español), y la demanda resultante por el e-commerce en el país. Sin embargo, también se señala una brecha digital en Ecuador en comparación con otros países de la región y el mundo. Por ende, es crucial que estas plataformas de e-commerce implementen medidas sólidas de seguridad.

Por lo tanto, mientras las empresas ecuatorianas busquen expandirse digitalmente, la ciberseguridad se torna esencial, especialmente en vista de la creciente sofisticación de las amenazas cibernéticas y la falta de concienciación sobre los riesgos de seguridad. A esto se suma la complejidad tecnológica asociada al uso de *cloud computing*, que puede resultar desafiante para empresas sin experiencia en tecnologías de nube pública. Finalmente, la gran cantidad de bibliografía sobre estos temas puede hacer que abordarlos resulte complicado, y menos aún establecer una arquitectura de e-commerce segura por parte de las PyMEs que disponen personal técnico y recursos limitados. Por consiguiente, esta investigación propone el desarrollo de

una guía práctica para la implementación de servicios IaaS destinados a e-commerce en la nube pública de pequeña y gran escala, desarrollando una arquitectura que permita mitigar los riesgos más comunes de ciberseguridad en este tipo de servicios.

II. Riesgos de ciberseguridad en la nube pública para empresas de e-commerce

La ciberseguridad es el subconjunto de la seguridad de la información y se refiere a la protección de sistemas, redes y dispositivos electrónicos y de sistemas de información sobre posibles ataques cibernéticos, accesos no autorizados, robo de datos, espionaje y otras amenazas. Para definir la seguridad informática se volvió muy frecuente el uso de los tres pilares de la CIA (CIA Triad, sus siglas en inglés) [9]. Los cuales son:

- Confidencialidad: consiste en asegurar que solo el personal autorizado acceda a la información que le corresponde, mientras al mismo tiempo protege la información de divulgaciones indebidas.
- Disponibilidad: asegura que los sistemas y la información, siempre estén disponibles para quien la necesita.
- Integridad: corresponde a la propiedad de la información mediante la cual se registra, usa y mantiene, de manera que se asegure su integridad, precisión, consistencia interna y utilidad para un propósito establecido.

Las arquitecturas de nube propuestas en este trabajo se fundamentan en estos tres principios, con el fin de mitigar los riesgos de seguridad estándar asociados específicamente con los servicios de la nube pública para la implementación de un e-commerce, reforzando la correcta configuración que recaen sobre la responsabilidad del usuario de IaaS.

Generalmente, los objetivos de los ciberataques en empresas de e-commerce pueden variar dependiendo de la naturaleza y el alcance del ataque, entre ellas tenemos: Robo de datos, comprometiendo información confidencial, como datos personales, información financiera, propiedad intelectual o datos empresariales. Robo de identidad para efectuar actividades fraudulentas, como suplantación de identidad, acceso no autorizado a cuentas o realizar transacciones ilegítimas. Interrupción del servicio que puede provocar la indisponibilidad de sitios web o servicios en línea.

Existen diversos tipos de ciberataques, entre los más comunes están: el ataque Distribuido de Denegación de Servicio (DDoS, sus siglas en inglés), los cuales tienen como objetivo saturar los recursos de una aplicación, servicio o red al inundarlos con un volumen considerable de tráfico. Esta sobrecarga puede dar como resultado la interrupción del servicio. Además, los atacantes suelen aprovechar múltiples dispositivos comprometidos para lanzar una variedad de ataques, mientras la empresa se centra en mitigar el DDoS original [10].

El ataque de inyección de código en un Lenguaje de Consulta Estructurado (SQL, sus siglas en inglés) se produce cuando un atacante inserta de manera maliciosa código en un servidor que utiliza SQL, obligando al servidor a generar información delicada del sistema. Esto compromete la seguridad de la base de datos y la integridad de la información almacenada. Como resultado, el atacante puede obtener acceso no autorizado a la base de datos, robar información confidencial y manipular datos almacenados. Durante los esfuerzos de la empresa para mitigar esta vulnerabilidad, es probable que se vea obligada a interrumpir el servicio.

El ataque de día cero ocurre tras la divulgación de una vulnerabilidad en la red, pero antes de que las empresas logren implementar un parche o solución en sus servicios o productos. Durante esta brecha, los atacantes aprovechan la vulnerabilidad para cometer diversos delitos informáticos, entre ellos, el robo de información confidencial. Este tipo de ataque representa una amenaza directa para los sistemas críticos de las empresas, incluyendo servidores web, bases de datos y plataformas de e-commerce, entre otros.

En los ataques de Hombre en Medio (MitM, sus siglas en inglés), un atacante, además de interceptar la comunicación, podría alterar la misma sin que las dos partes tengan conocimiento de lo sucedido. Este tipo de ataque es perjudicial debido a que podría interceptar datos confidenciales, sean estos de la empresa vulnerada o de sus clientes. Además, que le permitiría modificar transacciones, como por ejemplo cambiar el precio del producto, los datos de envío, y sobre todo suplantar la identidad de la empresa para que el cliente realice transacciones en ella.

El *malware* se utiliza para describir *software* malicioso, que abarca categorías como *spyware*, *ransomware*, *virus*, gusanos, entre otros. Estos ataques tienen un impacto directo en las empresas, ya sea a través de *spyware*, que puede sustraer información confidencial de la empresa, o mediante *ransomware*, que bloquea el sistema hasta que se pague un rescate para liberar los equipos afectados. Además, estas amenazas pueden comprometer la seguridad de los datos de los clientes, incluyendo contraseñas, información de tarjetas de crédito y datos personales.

Los riesgos de seguridad asociados con los servicios de la nube pública, dependerá proporcionalmente del usuario y el proveedor. Por este motivo, se hace hincapié en el concepto de responsabilidad compartida, el cual define claramente las responsabilidades tanto del usuario como del proveedor en relación con los distintos servicios ofrecidos [11]. En la Figura 2, se destacan las responsabilidades del usuario como también del proveedor encargado de suministrar dichos servicios. Es esencial que tanto el usuario como el proveedor comprendan claramente estas responsabilidades compartidas y colaboren para garantizar un entorno seguro en un servicio IaaS.

En IaaS, el usuario es responsable de la seguridad de las aplicaciones que se ejecutan. Esto incluye la protección contra vulnerabilidades y amenazas específicas de la aplicación, la seguridad de las instancias computacionales como son los sistemas operativos, incluyendo la aplicación de parches y actualizaciones de seguridad, configuración y gestión de la red, incluyendo reglas de *Firewall*. La seguridad y la privacidad de los datos almacenados y transmitidos a través de IaaS, esto incluye la implementación de cifrado de Capa de Conexión Segura (SSL, sus siglas en inglés) y el manejo adecuado de las

claves, gestión de usuarios, autenticación y control de acceso a los recursos desplegados en la infraestructura.

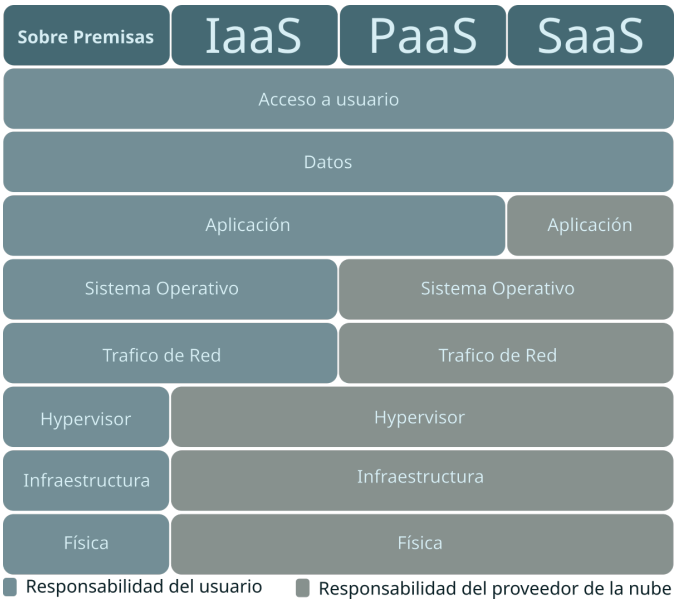

Figura 2. Responsabilidad compartida de seguridad entre el proveedor y el usuario

La responsabilidad del proveedor de la nube pública en IaaS es garantizar la disponibilidad del servicio en todo momento, asegurando que los centros de datos físicos estén siempre operativos, esto implicaría que incluyan medidas de control de acceso no autorizado, protección contra desastres naturales, seguridad de la capa de virtualización y su infraestructura, asegurar la encapsulación de datos y recursos entre diferentes usuarios de la nube pública, proporcionar servicios de *Firewall* en cuanto a red, cumplir con las normativas y estándares de seguridad predefinidos por las Organizaciones de Estandarización Internacional (ISO, sus siglas en inglés), aplicar parches y actualizaciones permanentes en su infraestructura para protegerse contra vulnerabilidades conocidas.

Las amenazas de seguridad en el acceso de usuario en la nube pública, se refiere a los accesos no autorizados, esto puede ocurrir cuando un usuario malintencionado obtiene acceso a una cuenta o recurso de la nube sin autorización por medio de diferentes tipos de ciberataques como son *malware*, inyección de código SQL, MitM, también se debe a la filtración de credenciales robadas de los usuarios, como contraseñas o claves de acceso.

En cuanto a las amenazas de seguridad en las instancias computacionales, tenemos la explotación de vulnerabilidades de seguridad en el *software* instalado o hasta en el sistema operativo, como son las vulnerabilidades de día cero. Estas vulnerabilidades son aprovechadas por los atacantes para obtener acceso no autorizado a las instancias computacionales. Además, mediante inyección de código malicioso en las instancias computacionales pueden tomar el control de los sistemas o también robar los datos.

Las amenazas de seguridad en el *Firewall* de la nube y del balanceador de carga, son por ataques de ingeniería social, y también se deben a las configuraciones incorrectas, siendo esta la principal causa de las vulnerabilidades de seguridad en la nube pública. La configuración de estos servicios pueden ser complejos, por ello es importante realizar una configuración correcta, y llevar registros de ella.

Las amenazas de seguridad en los sistemas de gestión de contenido empleados para servicios de e-commerce podrían estar en el servidor web y su base de datos, por medio de los ciberataques de día cero, inyección de código SQL, MitM, *malware* o también Las Secuencias de Comandos entre Sitios (XSS, sus siglas en inglés), que son usadas para inyectar código malicioso en el sitio web y obtener vulnerabilidades que permitan ser utilizadas para robar *cookies*, credenciales o información personal de los usuarios o clientes.

Para mitigar o reducir los ciberataques y los riesgos de seguridad, los proveedores de nube pública como AWS, [12] y *Linode*, [13], recomiendan asegurar la cuenta mediante políticas de seguridad y roles de administrador para gestionar y restringir permisos, además de configurar la Autenticación Multifactor (MFA, sus siglas en inglés) en cuentas con todos los permisos, además de monitorear eventos en toda la infraestructura levantada. En AWS se aconseja usar Redes Privadas Virtuales en la nube (VPC, sus siglas en inglés) para aislar y controlar el tráfico de la red, también recomiendan configurar los grupos de seguridad. En *Linode*, se recomienda crear redes Virtuales de Acceso Local (VLANs, sus siglas en inglés) para la comunicación interna entre instancias computacionales.

Implementar *firewalls* y *Firewalls* para Aplicaciones Web (WAF, sus siglas en inglés), permitirá mitigar ataques de web comunes descritos según el Proyecto de Seguridad en Aplicaciones Web Abiertas (OWASP, sus siglas en inglés) [14]. Además, que permitirá ingresar su propia política de seguridad. Otra recomendación es encriptar datos en reposo y en tránsito, como es utilizar Protocolos de Transferencia de Hipertexto Seguro (HTTPS, sus siglas en inglés) y Protocolo de transferencia de Archivos Seguros (FTPS, sus siglas en inglés), el cual cifrarían la información transmitida por medio de SSL y Seguridad en la Capa de Transporte (TLS, sus siglas en inglés). También se recomienda realizar mantenimientos a las instancias computacionales, con parches de seguridad, actualizaciones y opcionalmente, *firewalls* con respecto a instancia. Para mejorar la gestión de claves y acceso, por ejemplo, en *Linode*, se debería utilizar claves de *Shell* Seguro (SSH, sus siglas en inglés) en lugar de contraseñas y en AWS, utilizar el Servicio de Administrador de Llaves (KMS, sus siglas en inglés) para gestionar y proteger claves de cifrado, además se tiene que limitar el acceso a las instancias computacionales mediante direcciones de Protocolo de Internet (IP, sus siglas en inglés) específicas.

También se debe implementar herramientas de monitoreo para supervisar el rendimiento y así detectar problemas, además de configurar registros detallados para eventos de seguridad. Asimismo, se deberán realizar copias de seguridad

regularmente y almacenarlas de forma segura, probando regularmente la capacidad de restaurar desde los respaldos. De igual modo, se deben distribuir recursos en diferentes nodos o centros de datos para mejorar la alta disponibilidad, además de utilizar servicios de balanceo de carga para distribuir el tráfico eficientemente.

Finalmente, es de suma importancia que las empresas realicen auditorías de seguridad periódicas para evaluar las medidas implementadas y detectar las posibles vulnerabilidades. Desarrollar planes de respuesta a incidentes que sea compresible, detallado y especifico, además de definir acciones de respuesta claras y eficientes en caso de una brecha de seguridad, también se debe llevar a cabo actividades o cursos de formación continua a todo el personal sobre prácticas seguras de ciberseguridad y concientizarlos sobre los diferentes tipos de ciberataques que siempre están en constante desarrollo.

III. Implementación de un servicio de e-commerce en IaaS para PyMEs

Los Sistemas de Gestión de Contenido (CMS, sus siglas en inglés), son herramientas fundamentales que permiten la creación, organización y eficiente administración del contenido de un sitio web. Estas plataformas ofrecen una interfaz de administración que simplifica tanto la creación como la edición de contenido. Es importante destacar que existen CMS especializados para el e-commerce, diseñados específicamente para la creación y gestión de e-commerce. Los CMS de e-commerce se centran en proporcionar funcionalidades y herramientas orientadas a la venta de productos y servicios en el entorno digital. Permiten a los usuarios establecer y personalizar sus tiendas de manera fácil y eficiente, ofreciendo una variedad de características esenciales. Algunos de los CMS de e-commerce más comúnmente utilizados incluyen *PrestaShop*, *WooCommerce* (integrado con *WordPress*), *Shopify* y *Magento*.

En esta sección se describen los servicios y arquitectura diseñada en Linode y AWS para la implementación de un servicio IaaS de e-commerce empleando PrestaShop. Sin embargo, la arquitectura propuesta de nube puede utilizarse para otros CMS, puesto que esta se abstrae del mismo al únicamente instalarse el servicio dentro de los recursos computacionales virtuales creados en cada proveedor.

A. Servicios Linode para la implementación del e-commerce

Las instancias computacionales, denominadas *Linodes*, representan máquinas virtuales en la infraestructura de *Linode*. Con el propósito de respaldar una amplia gama de cargas de trabajo, los planes de *Linode* son de diversos tipos, cada uno con sus propios recursos, propuestas de valor y especificaciones técnicas. Cada *Linode* tiene la capacidad de ejecutar varias distribuciones Linux compatibles, incluyendo las versiones más recientes disponibles [15].

En cuanto a la seguridad de la infraestructura, es importante destacar que la responsabilidad del proveedor de *Linode* en IaaS está respaldada contra ataques DDoS en todos sus centros de datos. El objetivo de esta medida de seguridad es mitigar y eludir los posibles ataques a la infraestructura desarrollada en *Linode*.

Las VLANs están disponibles para todos los usuarios de *Linode* que utilicen los *Linodes* independientemente de la posición geográfica del centro de datos en la que fue creada. Estas operan en la capa 2 del modelo de Interconexión de Sistemas Abiertos (OSI, sus siglas en inglés) y se encuentran encapsuladas completamente de otras redes y de otros usuarios. Las VLANs desempeñan un papel fundamental al posibilitar la comunicación privada y segura entre los *Linodes*. Es importante destacar que los dispositivos externos a estas VLANs no tienen visibilidad sobre el tráfico interno de la misma, con esto se asegura un entorno de comunicación confidencial y protegido.

Los *firewalls* de *Linode* constituyen un servicio gratuito de cortafuegos basado en la nube que simplifica la protección del tráfico de red en los *Linodes*. Esta solución es accesible, robusta y fácil de usar. A través de este servicio, los usuarios tienen la capacidad de crear, configurar y agregar cortafuegos basados en la red con estado a cualquier instancia computacional.

NodeBalancer es un servicio de balanceo de carga gestionado basado en la nube, diseñado para proporcionar alta disponibilidad y escalabilidad horizontal a diversas aplicaciones, entre ellos los *Linodes*. Se clasifica como un Servicio de Balanceador de Carga (LBaaS, sus siglas en inglés) que simplifica en acceso en la infraestructura creada en *Linode*. Su función principal consiste en distribuir de manera inteligente las solicitudes entrantes entre diferentes *Linodes* que hayan sido generados y registrados, con ello permite continuar con el servicio en caso de fallo de alguna instancia. LBaaS, garantiza la alta disponibilidad y facilita el escalado horizontal para cualquier sitio web o aplicación en *Linode*.

El servicio de *Backups* de *Linode* ofrece la capacidad de realizar copias de seguridad automáticas de los discos asociados a los *Linodes*. Como parte de este servicio, se generen hasta cuatro instancias de respaldo, abarcando copias automáticas, diarias, semanales y quincenales, además de un *Backups* manual. Cada respaldo constituye una imagen completa basada en archivos de los discos respectivos de cada *Linodes*, Se pueden realizar respaldos en la franja horaria programada preferida, sin que este proceso interrumpa el funcionamiento de los *Linodes* garantizando que el servicio de copias de seguridad sea no disruptivo, proporcionando al usuario diversas opciones para una recuperación completa de sistema según sus requerimientos.

El *Linode* DNS *Manager* es una interfaz de gestión del Sistema de Nombre de Dominio (DNS, sus siglas en inglés), que facilita el uso de los dominios adquiridos en otras plataformas y la administración de los mismos. Su alcance abarca más de 250 ubicaciones en todo el mundo, permitiendo mitigar ataques de DDoS. Esta solución ofrece la capacidad de conmutar automáticamente a un servidor de nombres redundante en caso de interrupciones en el servicio en un servidor específico, lo que fortalece la fiabilidad y velocidad del sistema.

Longview es un servicio de sistema de datos gráficos que

rastrea las métricas de CPU, memoria, red, banda ancha de red tanto en agregada como en por proceso. Provee gráficas en tiempo real que pueden ayudar a exponer problemas de rendimiento.

B. Arquitectura del sistema con los servicios usados en Linode

En la Figura 3, se proporciona una representación visual de cómo los diferentes componentes y servicios interactúan entre ellos para la implementación de un servicio de e-commerce en *Linode*. La guía práctica que contiene el paso a paso para la configuración de la misma, se adjunta en: https://www.youtube.com/watch?v=KKLiUIE93i8 [16]. En este documento se detallan las características de la arquitectura implementada.

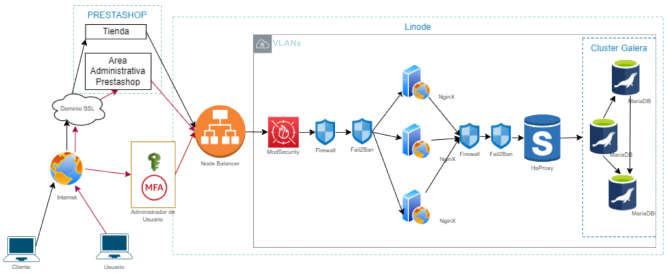

Figura 3. Arquitectura propuesta en *Linode*

Para la implementación de la arquitectura IaaS para un servicio de e-commerce en *Linode*, se utilizaron tecnologías y herramientas específicas y estables, como *PrestaShop* 8.1.1, *Debian* 11, NginX 1.2, PHP 7.4, *MariaDB* 11.3, *HAProxy* 2.8, WAF con *modsecurity*3 entre otros.

La arquitectura propuesta cuenta con las siguientes características y configuraciones:

Se han adoptado medidas de seguridad desde el inicio de la implementación, que incluyen el registro de la clave pública SSH del usuario en la plataforma *Linode* y la configuración de SSH para asegurar un acceso seguro a las instancias. La implementación de *Fail2Ban* [17], contribuye significativamente a la mitigación de ataques de fuerza bruta en SSH, lo cual fortalece aún más la seguridad de acceso a las instancias computacionales.

Se generaron duplicados de las instancias computacionales, tales como servidores web y base de datos, con el objetivo de asegurar la disponibilidad continua de los servicios. Además, se llevó a cabo la configuración de un clúster *Galera* [18]. para la base de datos, el cual permite tener redundancia y alta disponibilidad a este elemento crítico del sistema. Este enfoque fortalece la disponibilidad operativa, además de contribuir significativamente a posibles interrupciones o fallas por el cual se asegura un rendimiento consistente y confiable.

Se implementó un *NodeBalancer* para los servidores web y un *HaProxy* para los servidores de base de datos. Esto posibilita la escalabilidad mediante la creación de duplicados de los *Linodes* y la distribución de la carga entre ellos. Esto no solo simplifica la administración, sino que también garantiza un nivel óptimo de disponibilidad de *PrestaShop*.

La implementación abarca la adquisición de un dominio junto con un certificado SSL con el objetivo primordial de salvaguardar la seguridad de las comunicaciones. Esta medida resulta fundamental para preservar tanto la integridad de las transacciones como la confidencialidad de los datos de los usuarios.

Se han establecido reglas y políticas de seguridad para WAF mediante la utilización de *modsecurity* [19], con el propósito de proteger contra amenazas web comunes, según OWASP. Lo que asegura la efectiva detección y gestión de solicitudes maliciosas, reduciendo el riesgo o mitigándolo.

Se ha realizado la instalación de un ejemplo de tienda en línea de *PrestaShop* que viene por defecto, además partiendo de las recomendaciones de *PrestaShop* se han modificado los archivos de configuración tanto en NginX como para PHP. Para que estas cumplan con los requisitos necesarios para el correcto funcionamiento del e-commerce.

La configuración de *MariaDB* y la implementación de un clúster en *Galera* se desarrolló con el objetivo de garantizar un rendimiento óptimo y de redundancia para la base de datos. Esto fue posible con la creación de una instancia computacional principal y de dos secundarias que permita, en caso de fallos, que la base de datos siga disponible y que sus datos mantengan su integridad.

Se ha implementado el servicio de *firewalls*, el cual cuenta con reglas únicas de acceso a la red para los *Linodes* de servidores web, base datos y el *HaProxy*. Esto proporciona una capa adicional de seguridad en el ámbito de red, el cual fortalece la protección de la información.

C. Servicios de AWS para la implementación del e-commerce

Elastic Compute Cloud (EC2, sus siglas en inglés), proporciona una capacidad de computación escalable en la nube pública, ofreciendo la posibilidad de desarrollar e implementar aplicaciones de manera eficiente. Con EC2, es posible lanzar servidores virtuales de manera flexible, adaptándose a las necesidades específicas según se requiera. Esto permite añadir capacidad vertical para la gestión de cargas computacionales intensivas, como procesos periódicos o picos de tráfico web [20].

El Servicio de Datos Relacionales (RDS, sus siglas en inglés) simplifica la configuración, operación y escalabilidad de las bases de datos relacionales. Este servicio proporciona una solución rentable y altamente adaptable para las bases de datos y al mismo tiempo gestiona eficientemente las tareas comunes de administración.

El *Elastic Load Balancing* ofrece dos tipos de balanceadores de carga: el de aplicación y el de red, ambos disponibles para su utilización para los servicios de EC2 y otros. El balanceador de carga de aplicación es el que se va a utilizar en este documento. Este opera en la capa de aplicación (HTTP/HTTPS), permitiendo el enrutamiento basado en rutas y la capacidad de dirigir solicitudes a uno o más puertos de cada EC2. Este balanceador también admite mapeo de puertos de *host* dinámico, lo que implica que el puerto de *host* se elige automáticamente dentro del rango de puertos efímeros

de EC2 del contenedor que va a lanzar la tarea. Esto facilita la ejecución de múltiples tareas de un servicio único en EC2, ya que el balanceador de carga asigna dinámicamente el tráfico a la instancia y puerto correspondiente.

Route 53 se presenta como un servicio de DNS administrado, ofreciendo a los usuarios la capacidad de registrar nuevos dominios o administrar dominios de otros proveedores. Permite gestionar el tráfico de Internet hacia los recursos del dominio, y supervisar el estado de ellos. Este servicio se destaca por su versatilidad, permitiendo proporcionar acceso a recursos del dominio que involucren transmisión o almacenamiento.

VPC proporciona un control integral sobre su entorno de redes virtuales, abarcando aspectos como la disposición de recursos, la conectividad y la seguridad, incluso entre cuentas.

EC2 *Auto Scaling* es una herramienta diseñada para facilitar la gestión automatizada de la capacidad de aplicaciones en EC2. Con esta funcionalidad, es posible crear grupos de instancias conocidos como grupos de *Auto Scaling*, los cuales permiten establecer parámetros como un número mínimo y máximo de instancias. EC2 *Auto Scaling* asegura que el grupo nunca tenga menos instancias de la cantidad especificada como mínimo ni más instancias de la cantidad establecida como máximo. Además, se brinda la posibilidad de definir una capacidad deseada, delegando a EC2 *Auto Scaling* la tarea de mantener ese número específico de instancias.

El Administrador de Acceso e Identidad (IAM, sus siglas en inglés) es un servicio web integral, creado para administrar de manera segura el acceso a los recursos de la plataforma. IAM permite una administración centralizada de permisos para los diferentes tipos de servicios de AWS, y que estas puedan ser asignadas a los usuarios según sus requerimientos. Al crear una cuenta en AWS, se establece una identidad inicial denominada usuario *root*, la cual cuenta con el acceso total a todos los recursos y servicios. Este usuario se accede mediante el inicio de sesión utilizando el correo electrónico y la contraseña establecidos durante la creación de la cuenta. AWS recomienda no utilizar el usuario *root* para tareas diarias. En su lugar, se sugiere proteger las credenciales y emplear este usuario únicamente para funciones que requieran permisos específicos.

AWS WAF proporciona la capacidad de supervisar y gestionar las solicitudes web dirigidas a recursos protegidos. Este servicio se aplica a una variedad de recursos y servicios de AWS, entre ellos el *Eleactic Load Balancing*. Con AWS WAF, es posible proteger estos recursos al examinar las solicitudes web y verificar si cumplen con las políticas o reglas predefinidas. Como la dirección IP de origen, el valor de un componente específico de la solicitud o la velocidad de envío de las solicitudes. AWS WAF puede gestionar las solicitudes coincidentes de diversas maneras, como contándolas, bloqueándolas, permitiéndolas e incluso instaurando medidas de verificación como *CAPTCHA*.

Amazon CloudWatch es un servicio de monitoreo que supervisa en tiempo real los servicios, recursos y aplicaciones en la nube. Permite recopilar y rastrear métricas, que son variables medibles. La página de inicio de CloudWatch presenta automáticamente métricas de todos los servicios de AWS utilizados. Además, se pueden crear paneles personalizados para mostrar métricas específicas de aplicaciones y conjuntos personalizados de métricas seleccionadas. Las alarmas pueden configurarse para vigilar métricas y activar notificaciones o efectuar acciones automáticas cuando se superan umbrales predefinidos.

1) Arquitectura del sistema con los servicios de AWS: En la Figura 4, se proporciona una representación visual de cómo los diferentes componentes y servicios interactúan entre ellos para la implementación de un servicio de e-commerce en AWS. La guía práctica que contiene el paso a paso para la configuración de la misma, se presenta en: https://www.youtube.com/watch?v=n9ti0D-hju8 [21].

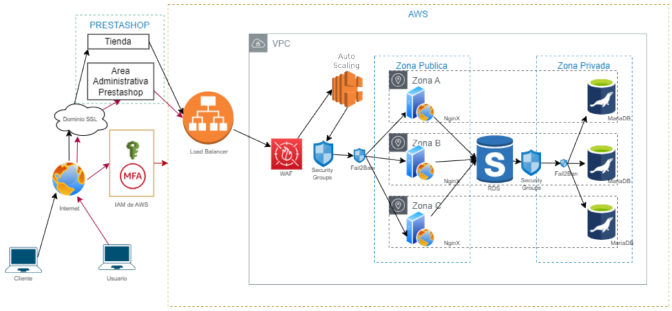

Figura 4. Arquitectura propuesta en *Amazon* AWS

Para la implementación en IaaS de un servicio de e-commerce en AWS, se utilizaron tecnologías y herramientas específicas y estables, como *PrestaShop* 8.1.1, *Ubuntu* 22.04, NginX 1.2, PHP 7.4, *MariaDB* 11.3, *HAProxy* 2.8, AWS WAF, entre otros.

La arquitectura propuesta cuenta con las siguientes características y configuraciones:

Se ha implementado una VPC que se encuentra dividida en zonas públicas y privadas. Las instancias EC2 se asignan a la zona pública, mientras para la base de datos se ha creado una subred asignada a la zona privada. Esto permite un control sobre la conectividad entre las instancias y la exposición a Internet. Además, se ha integrado un balanceador de carga de aplicaciones con grupos de seguridad definidos para la zona pública y privada para administrar de manera precisa los puertos de acceso de la infraestructura levantada.

Se ha implementado un sistema MFA en el usuario *root*, además se han realizado modificaciones en las políticas de contraseñas con el objetivo de fortalecer y asegurar un acceso seguro a la infraestructura.

La configuración de la base de datos se ha realizado mediante el uso de *RDS* y como motor de base datos *MariaDB*, se ha optado por una base datos para desarrollo y con la opción de generar instancias en reposo. Esta opción permitirá que la base de datos este siempre disponible aún en caso de fallos.

El servidor web ha sido configurado mediante la implementación de NginX, PHP y otras herramientas necesarias.

Se ha registrado un dominio con un certificado SSL, lo que garantiza la seguridad de las transmisiones de datos entre el servidor y los clientes.

Se ha establecido un grupo de *Auto Scaling* en EC2 por medio de una plantilla que contiene una imagen de la instancia, con el propósito de asegurar la escalabilidad de la infraestructura según la carga de trabajo.

Se han establecido reglas y políticas de seguridad específicas para AWS WAF, con el objetivo de proteger al sitio web contra amenazas comunes que fueron identificadas por OWASP. Por lo que permite mejorar la capacidad de bloquear o gestionar de manera efectiva las solicitudes maliciosas, y con ello agregaremos una capa de seguridad extra.

IV. Análisis de resultados

En la Figura 5, se hace un análisis de los servicios empleados tanto en AWS como en *Linode*. Este análisis permite tener una clara perspectiva entre las diferencias de un proveedor de servicios de pequeña y gran escala. Se observa que algunos servicios no están disponibles, mientras que otros servicios existen algunas similitudes en cuanto al funcionamiento del mismo. Esta comparativa destaca la relevancia de evaluar las ofertas de servicios específicos al seleccionar un proveedor de infraestructura en la nube pública.

Servicios	AWS	Linode
Administración de Usuarios	IAM	---
Instancias Computacionales	EC2	Linodes
Segmentación de Red	VPC	VLANs
Firewall	Firewall	Firewall
WAF	AWS WAF	---
Administración de Base de datos	RDS	---
DNS	Route 53	Linode DNS Manager
Balanceador de Carga	Elastic Load Balancing	Node Balancer
Monitoreo	CloudWatch	LongView

Figura 5. Comparación de servicios entre AWS y *Linode*

En la Figura 6, se llevó a cabo un análisis para evaluar las amenazas más frecuentes en relación con los recursos y aplicaciones previamente mencionados. Tanto en el entorno de AWS como en *Linode*, promueven el fortalecimiento de la seguridad mediante sus respectivas guías propietarias, las cuales proporcionan recomendaciones y configuraciones específicas por servicio para mejorar la seguridad. Estas guías abarcan el uso de herramientas internas, además de soluciones de terceros, sobre todo en *Linode*, el cual contribuyen en la implementación de prácticas seguras en IaaS, que permitan reducir o mitigar las diferentes vulnerabilidades en los servicios de la nube pública y recursos que son claves en el desarrollo de un sitio web de e-commerce.

Amenazas de seguridad \ Recursos	Acceso de usuario	Firewall como servicio	Plataforma de e-commerce	Servidor web	Balanceador de carga	Base de datos	Instancia
DDoS		SI		SI	SI	SI	SI
Contraseñas débiles o comprometidas	SI					SI	SI
Ataques de fuerza bruta	SI		SI		SI	SI	SI
Robo o exposición de credenciales	SI	SI	SI	SI			
MFA comprometida	SI						SI
Acceso no autorizado por medio de aplicaciones no seguras	SI						SI
Problemas de gestión de acceso	SI						SI
Suplantación de identidad (Spoofing)	SI				SI		SI
Exposición de puertos y servicios		SI		SI	SI	SI	SI
Malware	SI						SI
Filtración de información	SI		SI	SI		SI	SI
Reglas de firewall incorrectas		SI		SI	SI	SI	SI
Acceso no autorizado a datos, registros y configuraciones		SI	SI	SI	SI	SI	SI
Actualizaciones no oportunas	SI	SI	SI	SI	SI	SI	SI
Inyección de código SQL y XSS			SI	SI		SI	
Vulnerabilidades de software			SI	SI		SI	SI
Problemas de seguridad con aplicaciones de terceros			SI	SI		SI	SI
Inexistencia de parches y actualizaciones			SI	SI		SI	SI
Exposición de información crítica	SI	SI	SI	SI	SI	SI	SI
Errores de configuración humana	SI	SI	SI	SI	SI	SI	SI

Figura 6. Análisis de amenazas

Para evaluar la efectividad de la arquitectura y las recomendaciones de seguridad descritas en el documento, se llevaron a cabo diversas pruebas que permiten identificar posibles vulnerabilidades y evaluar la robustez en la implementación realizada en AWS y *Linode*.

Se efectuaron pruebas de inyección SQL por medio de la herramienta *SQLMap* [22]. La función de esta herramienta es automatizar el proceso de la prueba, realizando diferentes tipos de ataques comunes predefinidos por la herramienta. El objetivo es garantizar que no existan vulnerabilidades en las consultas SQL y que se encuentren adecuadamente filtradas y protegidas. Como resultado se obtuvo una prueba satisfactoria sobre la solidez del sitio web implementada en ambos proveedores. Algo que recalcar es que en AWS, *SQLMap* detecto el WAF implementado al momento de realizar el ataque, la cual produjo que los ataques predefinidos por la herramienta no fueran realizados. Mientas que en Linode se realizaron los ataques por la herramienta sin lograr ningún resultado. En la Figura 7 se presentan los resultados en *Linode* y la Figura 8 se presentan los resultados en AWS.

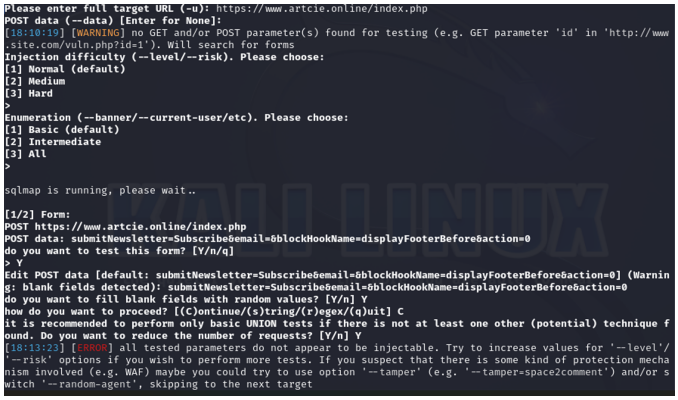

Figura 7. Resultados *SQLMap* para la implementación en *Linode*

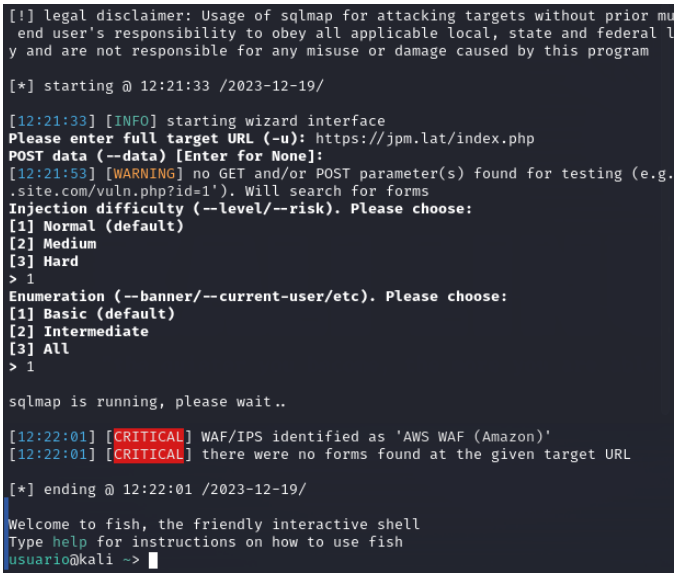

Figura 8. Resultados *SQLMap* para la implementación en AWS

Se empleó la herramienta *Nessus Essentials* [23], la cual permite automatizar el escaneo de vulnerabilidades según reglas predefinidas. Se hizo una evaluación de seguridad al sitio web. Donde se ejecutaron varios tipos de escaneos predefinidos por la herramienta, con el objetivo de identificar posibles vulnerabilidades en el sistema. Esta herramienta evalúa una vulnerabilidad por colores, tales como el azul de información, el amarillo de advertencia baja, el anaranjado de advertencia media, la roja de advertencia alta y la morada para crítica. Al realizar la exploración, los resultados obtenidos no indicaron la presencia de vulnerabilidades significativas en las instancias web analizadas. En la Figura 9 se presenta los resultados de *Linode*.

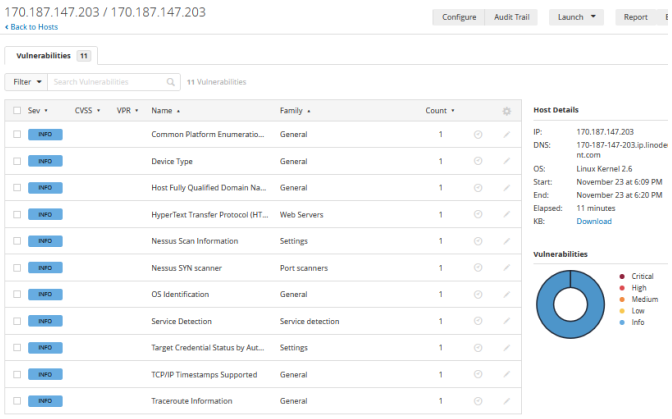

Figura 9. Resultados *Nessus* para la implementación en *Linode*

Al usar la herramienta *Nessus Essentials* en AWS se presentó una advertencia de color amarillo sobre el uso de HTTP con Seguridad de Transporte Estricta (HSTS, sus siglas en inglés) de forma predeterminada, esto se debe a que el servidor web se comunica con el balanceador de carga mediante HTTP, donde el balanceador de carga es el que se encarga de cifrar la información y redireccionar por HTTPS para efectuar la comunicación externa. La solución a esta advertencia sería utilizar certificados SSL desde las instancias computacionales por medio de *Let's Encrypt*; sin embargo, en este proyecto se utilizó un proveedor de certificados de SSL externo. En la Figura 10 y Figura 11 se presentan los resultados en AWS.

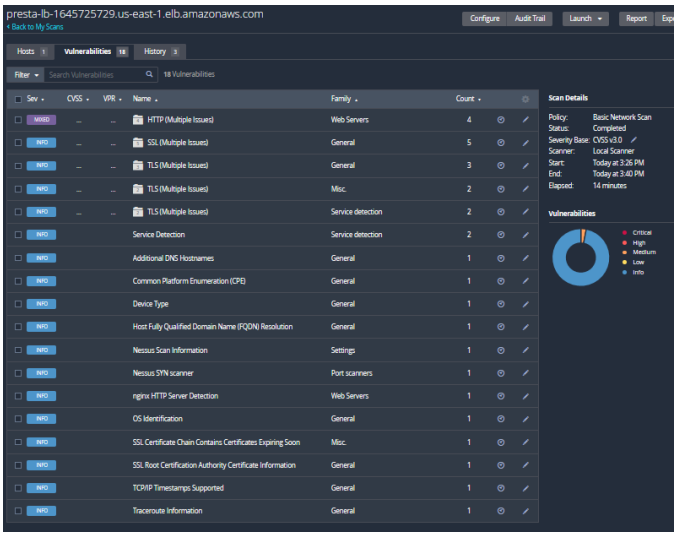

Figura 10. Resultados *Nessus* para la implementación en AWS

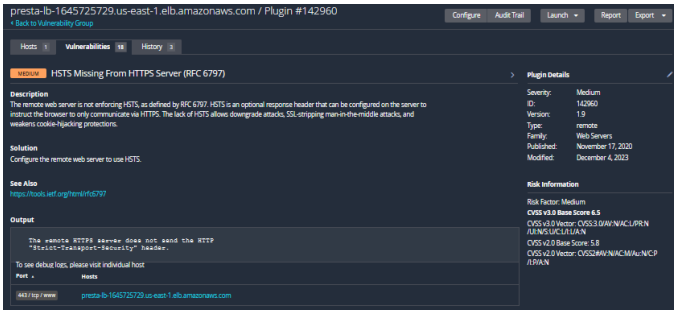

Figura 11. Resultado de alerta naranja de *Nessus* para la implementación en AWS

Se hizo una evaluación de la configuración de seguridad tanto de RDS como del clúster *Galera*. Durante este proceso, se examinaron las configuraciones de acceso a la base de datos desde el servidor web para garantizar el cumplimiento de las recomendaciones establecidas por PrestaShop. Entre estas recomendaciones incluye la vinculación de la base de datos que alberga la plataforma PrestaShop a un usuario específico. Por consiguiente, este usuario solo será capaz de administrar la base de datos designada y no tendrá el acceso a otras bases de datos que existieran en el servidor. Además, se efectuaron pruebas de disponibilidad. En *Linode* se eliminaron o se pausaron las instancias computacionales, obteniendo como resultado que cuando se las pausaba una o dos instancias el servicio se mantenía, mientras que si se detenían todas las instancias se corría el riesgo de que no iniciara el servicio de

base datos el cual tenía que ser arreglado para que vuelva a ser funcional la misma. Y en el caso de que se eliminaran todas las instancias computacionales y se alzaran nuevas instancias, a partir de clones o respaldos, sin que se haya trasladado las IPs de la instancia anterior a la nueva, llevó a que se tuviera que modificar las IPs en los archivos de configuraciones realizadas en Galera de cada servidor de base de datos además del archivo de configuración de *HaProxy*. En el caso de AWS se reinició la base de datos para comprobar que las instancias en reposo se iniciaran, cabe recalcar que este proceso es automático por parte de RDS, y su funcionalidad es similar a la de *Linode*. El resultado se considera adecuado, sin embargo, existe una interrupción del servicio mientras la instancia en reposo toma el control.

Se verificó la configuración de las reglas de seguridad de los grupos asociados a las subredes públicas y privadas en AWS, así como las reglas del *Firewall* en *Linode*. Este proceso de evaluación proporcionó una comprensión detallada de la postura de seguridad en ambos entornos. Se identificó la posibilidad de mejorar la seguridad mediante la configuración de un firewall en cada instancia computacional, asegurándose de que cumpla con las mismas reglas definidas en los servicios mencionados anteriormente.

Se realizó la verificación de la configuración de los certificados SSL en el balanceador de carga tanto en AWS como en *Linode* y se realizó un escaneo al sitio web implementando en cada uno de los proveedores por medio de *SSL Labs* [24]. Se verificó cada aspecto del proceso de la información revelada, asegurándose de que los certificados SSL estuvieran correctamente implementados en el balanceador de carga y correctamente configuradas en las instancias computacionales. Sin embargo, aunque las configuraciones son iguales, las calificaciones fueron diferentes, obteniendo una mejor calificación AWS, concluyendo que las configuraciones que se realizan internamente en la infraestructura de AWS son mejores a las realizadas por *Linode*. En la Figura 12 se presenta la calificación obtenida por *Linode* y la Figura 13 se presentan la calificación en AWS.

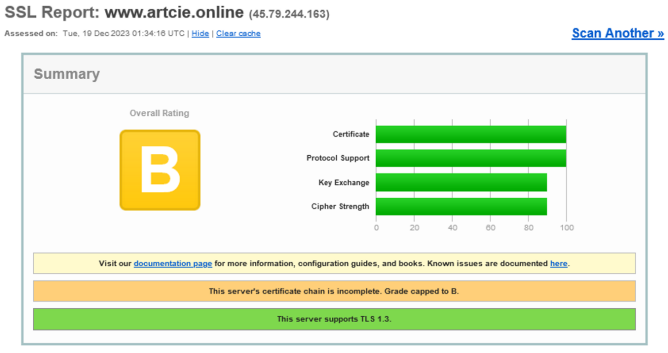

Figura 12. Calificación *SSL Labs* para la implementación en *Linode*

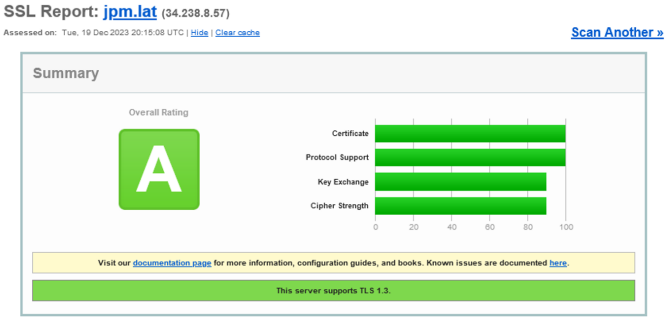

Figura 13. Calificación *SSL Labs* para la implementación en AWS

Se desarrolló una simulación de ataques DDoS mediante el uso de la herramienta *slowhttptest* [25]. El objetivo central de la simulación fue poner a prueba la capacidad del balanceador de carga, así como la resistencia y capacidad de respuesta de la infraestructura subyacente frente a este tipo de amenazas. Mediante el siguiente código: “slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 200 -t GET -u https://Dominio -x 24 -p 3”, se realizó el ataque al sitio web desplegado en *Linode* como en AWS. De manera general, el ataque fue mitigado por la infraestructura, sin embargo, en *Linode* hubo ciertos instantes no mayores de un segundo en el cual hubo caídas del servicio, esto se pudo evidenciar por los registros de la prueba y de forma visual cuando el campo, *servicio disponible* (Service Available), cambiaba a “No”. Además, al momento de realizar el ataque se llevaron a cabo diferentes pruebas de operabilidad al sitio web, donde se constataba que el sitio web tardaba más de la cuenta en abrir un enlace. En la Figura 14 y Figura 16 se presentan los resultados obtenidos, en *Linode*. En la Figura 16 se presentan los resultados en AWS.

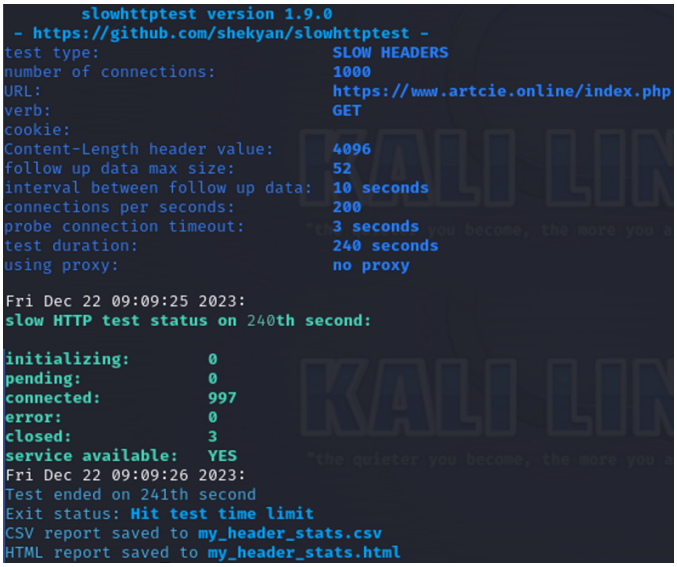

Figura 14. Resultado DDoS para la implementación en *Linode*

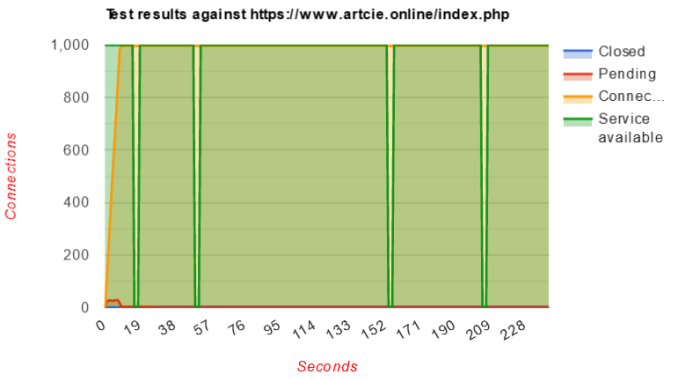

Figura 15. Resultado gráfico de DDoS para la implementación en *Linode*

```
        slowhttptest version 1.9.0
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              https://jpm.lat/index.php
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Tue Dec 19 12:20:54 2023:
slow HTTP test status on 65th second:

initializing:         0
pending:              0
connected:            257
error:                0
closed:               743
service available:    YES
Tue Dec 19 12:20:55 2023:
Test ended on 66th second
Exit status: No open connections left
CSV report saved to slowhttp.csv
HTML report saved to slowhttp.html
```

Figura 16. Resultado DDoS para la implementación en AWS

Se llevaron a cabo pruebas de escalabilidad con el objetivo de garantizar la disponibilidad del sitio web, en *Linode*, así como del autoescalado en el caso de AWS. Estas pruebas fueron realizadas deteniendo o eliminando las instancias computacionales tanto en *Linode* como en AWS, con ello se evaluó y se validó la capacidad de los sistemas para adaptarse de manera eficiente y efectiva a cambios en la carga de trabajo. En el contexto de *Linode*, las pruebas se centraron en verificar la disponibilidad del sitio web, es decir, la capacidad del sistema para manejar caídas de los servidores web y que el sitio web siga funcionando hasta levantar los respaldos de las instancias computacionales. También se eliminaron las instancias computacionales, y al momento de crear unas nuevas instancias a partir de respaldos o clones, sin haber sido transferido la IP anterior, estas nuevas IPs debían ser ingresadas en el balanceador de carga para que el sitio web vuelva a ser funcional. En el caso de AWS, además de detener las instancias computacionales, se efectuaron pruebas específicas de autoescalado, donde se evaluó la capacidad del entorno para adaptarse automáticamente a cambios en la demanda sin intervención humana. Se verificó la configuración de las políticas de autoescalado, la efectividad de la detección automática de la carga de trabajo, en la cual concluyó que solo se requería del mínimo de instancias configuradas.

Se realizó una revisión de la configuración SSH y *Fail2Ban*. Con el objetivo de garantizar su eficaz detección y bloqueo de intentos de acceso no autorizado. Este proceso incluyó la verificación de cada parámetro y ajuste relacionado con SSH y *Fail2Ban* implementados en los *Linodes*, para asegurar que estén correctamente configurados y alineados con las mejores prácticas de seguridad. En SSH se comprobó que solo los dispositivos que estén autorizados y que su llave pública esté registrada correctamente puedan ingresar a la instancia computacional, sin embargo, para hacer las pruebas en *Fail2Ban* se habilitó el acceso por contraseña en el archivo de configuración de SSH. Esto permitió confirmar por medio de los *logs* de *Fail2Ban* que los mecanismos de detección de intentos de acceso no autorizado estén activos y funcionando de manera óptima, y se aseguró que las políticas de bloqueo y las reglas estén adecuadamente establecidas para proporcionar una capa sólida de seguridad contra posibles amenazas. En AWS se comprobó su seguridad en SSH, lo cual utiliza políticas de acceso a las instancias computacionales por medio de KMS, y al realizar las mismas pruebas que se efectuaron en *Linode*, se comprobó que se puede asegurar las instancias en *Linode* a un similar grado de seguridad de AWS, agregando una capa de seguridad adicional con *Fail2Ban*. En la Figura 17 y la Figura 18 se presentan los resultados obtenidos en *Linode*.

```
usuario@kali -> ssh -p 9146 usuario@170.187.147.203
The authenticity of host '[170.187.147.203]:9146 ([170.187.147.203]:9146)' can't be established.
ED25519 key fingerprint is SHA256:PywnWQ9ZOxLKXrdOGVFiDFaFjVtwNYBjna6fWvY9FCE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[170.187.147.203]:9146' (ED25519) to the list of known hosts.
usuario@170.187.147.203: Permission denied (publickey).
usuario@kali ~ [255]> ssh -p 9146 usuario@170.187.202.221
The authenticity of host '[170.187.202.221]:9146 ([170.187.202.221]:9146)' can't be established.
ED25519 key fingerprint is SHA256:GKVdHAqgLjdQetxphK7gsKFvtyVmFt+8Fk/l17EyA28.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[170.187.202.221]:9146' (ED25519) to the list of known hosts.
usuario@170.187.202.221's password:
Permission denied, please try again.
usuario@170.187.202.221's password:
Permission denied, please try again.
usuario@170.187.202.221's password:
usuario@170.187.202.221: Permission denied (publickey,password).
usuario@kali ~ [255]> ssh -p 9146 usuario@139.144.27.38
The authenticity of host '[139.144.27.38]:9146 ([139.144.27.38]:9146)' can't be established.
ED25519 key fingerprint is SHA256:RyAqkIB4+xQjJDyBPa5QO5tal1MQCJx4rnizVGH0u9Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[139.144.27.38]:9146' (ED25519) to the list of known hosts.
usuario@139.144.27.38's password:
Permission denied, please try again.
usuario@139.144.27.38's password:
Permission denied, please try again.
usuario@139.144.27.38's password:
usuario@139.144.27.38: Permission denied (publickey,password).
usuario@kali ~ [255]>
```

Figura 17. Resultados de acceso en SSH en *Linode*

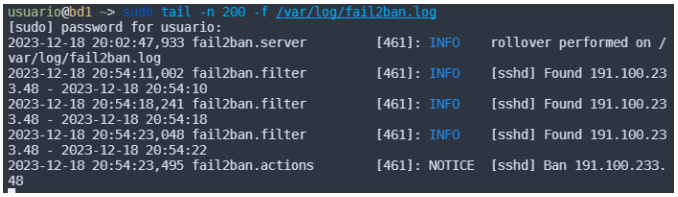

Figura 18. Resultado de Fail2Ban al errar la contraseña en *Linode*

Se evaluó la eficacia de MFA mediante la ejecución de pruebas de inicio de sesión con el objetivo de confirmar su implementación. Esta prueba implicó verificar que MFA esté funcional y que, de hecho, sea un requisito esencial para completar el proceso de inicio de sesión, siendo que en *Linode* es la única forma permitida de acceso, mientras que en AWS se puede optar por otros factores de acceso de respaldo. En la Figura 19 se presenta el resultado de *Linode*. La Figura 20 y la Figura 21 se muestra el resultado obtenido en AWS.

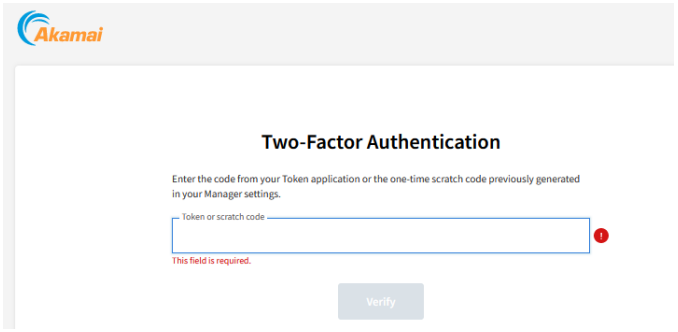

Figura 19. Resultado MFA en *Linode*

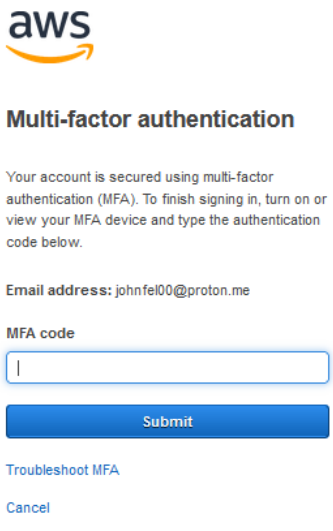

Figura 20. Resultado MFA en AWS

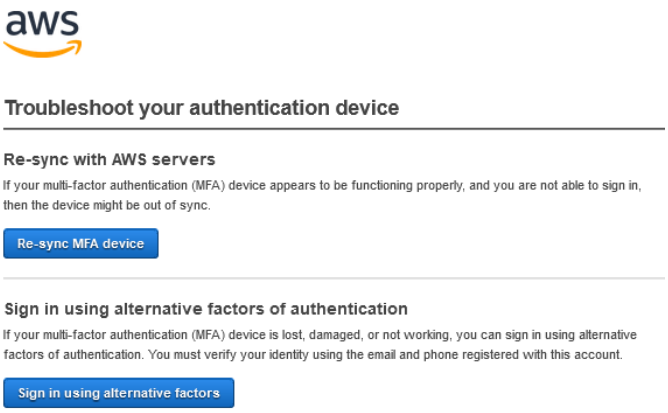

Figura 21. Resultado MFA en AWS: Problemas de acceso MFA

V. Conclusiones

Si bien los servicios de proveedores de nube pública ofrecen innumerables ventajas para las empresas medianas de e-commerce, es crucial reconocer y abordar los riesgos de seguridad asociados. Para mitigar estos riesgos, las empresas de e-commerce deben adoptar una estrategia de seguridad de nube pública robusta y coherente. Esto implica la implementación de políticas sólidas para la protección de datos, gestión de accesos y contraseñas, monitorización continua de la seguridad, aplicar actualizaciones y parches de seguridad, realizar copias de seguridad y recuperación de datos, así como proporcionar una formación continua de los empleados.

Es recomendable realizar un Monitoreo continuo con herramientas avanzadas a los diferentes elementos que conforman la infraestructura levantada en busca de anomalías del cual puedan dar como resultado brechas de seguridad. Esto permitiría estar alerta y reducir el impacto en caso de que se haya vulnerado algún servicio o aplicación. En este sentido, esta guía se presenta como una solución, sin embargo, las PyMEs deben considerar a la ciberseguridad no como un gasto sino como una inversión y considerarla prioritaria en las futuras etapas. El tener en cuenta la necesidad de un rubro que permita contratar empresas especializadas que ayuden a mitigar o reducir el riesgo que enfrenta una PyMEs y sobre todo un e-commerce. Esta estrategia ayudaría a tener una gestión eficiente y especializada de los recursos, permitiendo a las PyMEs de e-commerce, concentrarse en sus objetivos empresariales sin comprometer la integridad, disponibilidad y confidencialidad de la seguridad de la información.

La elección entre un proveedor de nube de gran escala y uno de menor escala dependerá de las necesidades específicas y el presupuesto disponible de las PyMEs. Los proveedores de gran escala como AWS, *Microsoft Azure* y *Google Cloud Plataform* (GCP, sus siglas en inglés) ofrecen una amplia gama de servicios, pero también implican mayores costos y una configuración de servicios más compleja, por lo que requerirían una inversión significativa en los recursos de TI. Por otro lado, los proveedores de menor escala como *Linode*, *DigitalOcean* y *Vultr* pueden ser más asequibles y personalizados, aunque su

presencia global puede ser limitada, y pueden ofrecer menos servicios en comparación con los proveedores de gran escala.

A lo largo de este estudio, se efectuó la implementación de un e-commerce en dos nubes públicas, AWS y *Linode*. Lo cual permitió entender las fortalezas y debilidades de cada uno de ellos, por tal razón, si las PyMEs de e-commerce cuentan con el presupuesto necesario para adquirir los servicios de nube pública de gran escala, es preferible realizar la implementación en AWS, por múltiples factores. Entre ellos se destacan los servicios de IAM, RDS, VPC, EC2 *Auto Scaling* y AWS WAF, los cuales no están presentes o no se encuentran completamente desarrollados en *Linode*. Estos servicios de AWS ofrecen capas adicionales de seguridad, permiten un escalado automático de los servidores web y garantizan la disponibilidad constante de la base de datos gracias a la funcionalidad proporcionada por RDS.

REFERENCIAS

[1] J. A. J. Celleri and S. Rodriguez, "Cloud computing para pymes," *Utmach*, 2018.
[2] D. K. Judith S. Hurwitz, *Cloud Computing For Dummies, 2nd Edition*. John Wiley and Sons, Inc.,, 2020.
[3] G. Avalos, "Pymes en el ecuador," *Camara de comercio*, 2020.
[4] R. Chavez, "Estado actual de la ciberseguridad 2020 ecuador," 2020.
[5] WorldEconomicForum, "The global risks report 2023 18th edition," *World Economic Forum*, 2023.
[6] J. W. Jackie., "Why cybersecurity for small businesses is more necessary now than ever before.," 2021.
[7] D. university Latam ciso, "Perspectivas de ciberseguridad de los lideres de la industria," 2023.
[8] M. t. Ministerio de PCEIP and S. privado, "Estrategia nacional de comercio electrónico," 2021.
[9] D. Kosutic, *Ciberseguridad en 9 pasos el manual sobre seguridad de la información para el gerente*. EPPS Services Ltd, Zagreb, 2012.
[10] IBM, "What is a cyberattack." https://www.ibm.com/topics/cyber-attack.
[11] J. S. Enrique Javier, "Riesgos de ciberseguridad en las empresas," 2017.
[12] AWS, "Documentación de aws sobre seguridad." https://aws.amazon.com/security/.
[13] Linode, "Documentación de linode sobre seguridad." https://www.linode.com/docs/guides/security/.
[14] OWASP, "Project modsecurity core rule set." https://owasp.org/www-project-modsecurity-core-rule-set/.
[15] Linode, "Documentación de linode." https://www.linode.com/docs/.
[16] J. Plaza, "Implementación de un e-commerce de alta disponiblidad con linode." https://johnyfelipe.github.io/cloud-computing/Linode-Implementacion/.
[17] Fail2Ban, "Fail2ban." https://github.com/fail2ban/fail2ban.
[18] Galera, "Documentación de galera cluster." https://galeracluster.com/library/documentation/index.html.
[19] S. Labs, "Modsecurity." https://github.com/SpiderLabs/ModSecurity.
[20] Amazon, "Documentación de amazon aws." https://aws.amazon.com/es/?nc1=h_ls.
[21] J. Plaza, "Implementación de un e-commerce de alta disponiblidad con aws." https://johnyfelipe.github.io/cloud-computing/AWS-implementacion/.
[22] SQLMapProject, "Sqlmap." https://sqlmap.org/.
[23] Tenable, "Nessus essentials." https://www.tenable.com/.
[24] Qualys, "Ssl labs." https://www.ssllabs.com/.
[25] Shekyan, "Slowhttptest." https://www.kali.org/tools/slowhttptest/.