Escuela Politécnica Superior de Jaén
Máster Universitario en Ingeniería Informática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior (Jaén)

Trabajo Fin de Máster

PLANIFICACIÓN Y DISEÑO DE UN SERVICIO SEGURO EN LA NUBE

Alumno/a: **Méndez Lugo, María Dolores**

Tutor/a: Prof. D. José Ramón Balsas Almagro
Dpto.: Departamento de Informática

Septiembre, 2021

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don José Ramón Balsas Almagro, tutor del Trabajo Fin de Máster titulado Planificación y diseño de un servicio seguro en la nube, que presenta María Dolores Méndez Lugo, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Septiembre de 2021

El alumno: Los tutores:

María D. Méndez L.

María Dolores Méndez Lugo José Ramón Balsas Almagro

RESUMEN

El presente trabajo de fin de máster tiene como objeto de estudio la planificación y diseño de un servicio seguro en la nube, enfocado en una aplicación web dedicada al comercio electrónico. El objeto de estudio se basa en una implementación de una tienda virtual sobre la plataforma Magento desplegada en una infraestructura de Amazon Web Services donde se aplicarán políticas y buenas prácticas de seguridad, siguiendo los estándares definidos por OWASP, CSA, ENS, así como, aspectos relacionados a legislación aplicable.

ABSTRACT

The purpose of this master's thesis is the planning and design of a secure cloud service, focused on a web application dedicated to electronic commerce. The object of study is based on an implementation of a virtual store on the Magento platform deployed in an Amazon Web Services infrastructure where security policies and good practices will be applied, following the standards defined by OWASP, CSA, ENS, as well as aspects related to applicable legislation.

Palabras clave: Ingeniería Informática, Seguridad Informática, Nube, CMS, Magento, AWS.

Planificación y diseño de un servicio seguro en la nube

Índice

Lista de tablas

Lista de ilustraciones

Definiciones, Acrónimos y Abreviaturas

E-Commerce	Comercio Electrónico
PYME	Pequeña y mediana empresa
CMS	Content Management System
ERP	Enterprise Resource Planning
SEO	Search Engine Optimization
SSL	Secure Sockets Layer
SaaS	Software as a Service
IaaS	Infraestructure as a Service
PaaS	Platform as a Service
DIPRODAP	Dirección de Protección de Datos Personales
CONAMI	Comisión Nacional de Microfinanzas
SIBOIF	Superintendencia de Bancos y otras Instituciones Financieras
ENS	Esquema Nacional de Seguridad
RGPD	Reglamento General de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
CVE	Common Vulnerabilities and Exposures
NVD	National Vulnerability Database
OWASP	Open Web Application Security Project
CWE	Common Weakness Enumeration
SQL	Structured Query Language
LDAP	Lightweight Directory Access Protocol
URL	Uniform Resource Locator
MITM	man-in-the-middle
CSP	Content Security Policy
RPC	Remote Procedure Call
IPC	Inter-Process Communication
EC2	Elastic Compute Cloud
MFA	Multi-Factor Authentication
AWS RAM	AWS Resource Access Manager
ACL	Access Control List
DAST	Dynamic Application Security Testing

1.- **INTRODUCCIÓN**

Con los avances tecnológicos y al crecimiento acelerado de conexiones de internet en el mundo y alcance de la mano principalmente por medio de dispositivos móviles, así como, cambios inesperados en estos dos últimos años a causa de la conocida pandemia producida por el virus SARS-CoV-2, se ha impulsado el crecimiento de las ventas online. Este hecho ha sido la consecuencia de las medidas adoptadas para la seguridad de la población (mantenerse en casa), y en Latinoamérica no ha sido una excepción. Algunos especialistas en la materia de economía como Forbes [1], Insider Intelligence [2], Euromonitor International [3], nos explican que para América Latina el E-Commerce es un terreno fértil de más rápido crecimiento y por lo que obliga a las Pymes a reinventarse en su modelo de negocio.

En Nicaragua no ha ocurrido de manera diferente, por lo que ha forzado a las Pymes a reestructurar su modelo de negocio y adaptarse a los cambios con una transformación digital trasladándose al comercio electrónico. De hecho, podemos mencionar algunas de las ventajas de este frente al comercio tradicional, tales como:

- Obtención de mayor número de clientes tanto online como offline debido al aumento de visibilidad que permite internet.
- Facilidad de mostrar los productos por parte del empresario, así como facilidad de encontrar los productos por parte del cliente.
- Vencer limitaciones geográficas, accesibilidad.
- Ahorrar tiempo a la hora de realizar las compras, comodidad.

Existen diferentes tipos de E-Commerce y estos están clasificados por algunos criterios según Marketing4Ecommerce [4]:

- **E-Commerce según los bienes y servicios que distribuyen:**
    - e-commerce de productos analógicos con empresas que solo venden online y empresas que venden online y offline, según la forma de construir la tienda online.

- **E-Commerce según la forma de construir la tienda online:**
    - open source e-commerce**,** plataformas de código abierto a disposición de cualquiera permitiendo gestionarlas en sus propios servidores, ejemplos de ellas, Magento.

- **E-Commerce según los agentes que participan en las transacciones:** entre los más conocidos están:
    - B2B**:** es el comercio Business to Business o de Empresa a Empresa, donde se realizan las transacciones comerciales o de productos a grandes escalas entre dos empresas y no intervienen consumidores finales.
    - B2C**:** comercio Business to Customer o de Empresa a Cliente, estas establecen relaciones comerciales con consumidores finales.

Así como las Pymes han tenido que adaptarse a los cambios y modificar su modelo de negocio, apuntando al comercio electrónico de igual forma sucede con el cliente. Debido a que está acostumbrado a realizar sus compras visitando las tiendas físicas, guiado por la necesidad de ver y tocar el producto para además garantizar la máxima fiabilidad en sus compras.

Es ahí donde la seguridad informática juega un papel fundamental para que las empresas brinden a sus clientes la misma tranquilidad, seguridad y confianza, asegurando de que las compras realizadas a través de su tienda virtual son igual de confiables que al hacerlo en su tienda física.

1.1 Motivación

Tras un breve análisis de cómo los últimos acontecimientos han incidido en el modelo de negocio de las Pymes, basado en el uso de internet como medio de comunicación y de cuán importante es la seguridad informática, el presente trabajo pretende profundizar en este último aspecto, no solo con el objetivo de que las empresas protejan sus datos, sino que también brindar la confianza a sus clientes garantizando que los servicios que ofrecen son seguros. Adicionalmente, en mi situación particular de mi plan de estudios en el que, aunque he cursado el Máster de Informática, opté por especializarme en asignaturas específicas de seguridad

informática lo que ha servido de motivación para profundizar aún más con este trabajo en estos aspectos tan importantes hoy en día.

Por lo tanto, este Trabajo de Fin de Máster se enfocará en el despliegue de un servicio de comercio electrónico de forma segura en la nube.

1.2 Objetivos

Los objetivos propuestos para la realización de este Trabajo de Fin de Máster, de acuerdo a las competencias requeridas, se resumen de la forma siguiente:

- Familiarizarse con las competencias habituales de los responsables de seguridad de proyectos que impliquen el desarrollo y explotación de servicios en la nube.
- Analizar diferentes aspectos relacionados con aspectos legales y seguridad que deban ser considerados en el ciclo de vida de un sistema informático.
- Estudiar, integrar y utilizar de forma segura tecnologías y servicios habituales proporcionados por terceros que contribuyan a garantizar la explotación segura de un servicio web en la nube.

1.3 Metodología a desarrollar

Esta memoria constará de la siguiente estructura:

- Primeramente, se definirá el tipo de servicio a desplegar y que será objeto de estudio para este TFM.
- A continuación, en el capítulo 3 se realizará un análisis de los aspectos de seguridad para su diseño tales como, legislación aplicable, recomendaciones de seguridad, estudio y análisis de amenazas a los que podría estar expuesto el servicio, así como requisitos de seguridad propios específicos del sistema.
- Seguidamente, en el capítulo 4 se determinarán las medidas de seguridad y buenas prácticas para el diseño seguro del sistema, así como la arquitectura del sistema.

- Acto seguido, en el capítulo 5 se llevará a cabo el diseño, configuración y despliegue del servicio en la nube, además de un breve análisis de coste operativo.
- Luego, en el capítulo 6 se desarrollará una evaluación de la seguridad del sistema de objeto de estudio y los resultados obtenidos de las pruebas realizadas, con el objetivo de obtener una valoración final de la efectividad de las medidas propuestas.
- Para finalizar, en el capítulo 7 se comentará en qué medida se han alcanzado los objetivos propuestos y las conclusiones del trabajo realizado.

En adición, esta memoria dispondrá de un apartado de Apéndice con detalles sobre la instalación y despliegue del sistema de experimentación y aspectos más relevantes de configuración en lo referente a la seguridad.

2.- **DEFINICIÓN DEL SERVICIO**

Para establecer el punto de partida del presente proyecto, se definirán las características y necesidades de una empresa ficticia, que denominaremos LUMA. Dicho nombre es definido por defecto por el gestor de contenido Magento.

LUMA es una Pyme que ofrece artículos deportivos y que tiene presencia de forma local en diferentes puntos del país. Con el objetivo de poder llegar a más clientes, tiene la necesidad de adaptar su estrategia de crecimiento a la era digital del comercio electrónico a través de una tienda virtual y para poder brindar mayor confianza a sus clientes requiere que su plataforma de venta on-line sea segura.

Actualmente LUMA cuenta entre 1 y 6 sucursales, con aproximadamente 40 trabajadores, ofreciendo a sus clientes 1200 artículos deportivos para todas las edades, con un promedio de visitas diarias entre todas las sucursales de 9.000 clientes y un estimado de ventas de 3.000 ventas diarias.

Con la finalidad de complementar su línea de negocio tradicional de “tienda física”, brindar un mejor servicio y captar clientes, principalmente en lugares donde no cuentan con presencia física, se precisa que la plataforma tenga un nivel de disponibilidad que garantice que el servicio esté siempre a disposición del cliente, así como, asegurar un alto nivel de seguridad. Este debería brindarle al cliente la confianza para que al realizar una compra y proporcionar datos sensibles como el método de pago “tarjetas de crédito y/o débito” y sus datos personales “información sobre una persona natural o jurídica que la identifica o la hace identificable” estos estén siempre protegidos.

2.1 Gestores de contenido (CMS E-Commerce)

Para una Pyme una opción habitual a la hora de entrar en el comercio electrónico y por cuestiones económicas es optar por una plataforma ya desarrollada frente a tener que costear el desarrollo de una opción a medida.

Existe una variedad de CMS o gestores de contenidos disponibles, así como proveedores de servicios en la nube. A continuación, se detalla una breve descripción,

las características de cada uno de ellos, aspectos de seguridad, ventajas y desventajas.

Los CMS o gestores de contenidos son software diseñado para la creación y administración de páginas web, sin embargo, algunos están diseñados específicamente para la creación de una tienda online y que detallaremos a continuación [5] [6] [7] [8]:

Análisis de CMS por Funcionalidades

Magento

Fuente: [9]

Magento Community Edition lanzada en 2007 como primera versión beta al público, es una plataforma de solución integral Open Source gratuita para desarrollar páginas web orientada a e-commerce. Al ser de código abierto tiene detrás una gran iniciativa, apoyada por miles de desarrolladores de todo el mundo, lo que le permite ser una de las mejores plataformas de ecommerce de la actualidad. Además, cuenta con una versión de pago con mayores características y soporte técnico. Magento se caracteriza por ser multiplataforma, multilenguaje, tiene a disposición miles de plantillas, ofrece plugins gratuitos, configuración de pagos, estadísticas y reportes, entre otros.

Ventajas:

- Escalable, ideal para Pymes y grandes empresas
- Multilenguaje y multi moneda
- Integración nativa de ERPs, óptimo para tiendas que desean tener una tienda física y virtual.
- Optimización SEO
- Encriptación SSL
- Cuenta con herramienta de análisis de seguridad gratuita
- Comunidad activa de desarrolladores manteniéndolo siempre actualizado.
- Ofrece soluciones con temas ya preparados y tiene una capacidad ilimitada para personalizar el sitio con un código propio.

Desventajas:

- Panel de control algo complejo lo que dificulta un poco su adaptación.
- Curva de aprendizaje lenta a pesar de que cuenta con mucha documentación, requiere tener conocimientos previos de programación.
- Consumo de recursos, se requiere de servidores con alta capacidad.
- La Licencia Enterprise es muy costosa.

Shopify

Fuente: [10]

Shopify es otra plataforma destinada para crear tiendas virtuales, con un modelo de servicio SaaS. Este CMS ha ganado mucha popularidad principalmente en Estados Unidos por ser una plataforma intuitiva, práctica, fácil de usar que no requiere de conocimientos técnicos.

Ventajas:

- No requiere de conocimientos técnicos.
- Interfaz intuitiva y fácil de usar. En pocos pasos, puedes tener una tienda virtual montada permitiendo cambiar la apariencia y funcionalidad con una variedad de plantillas y apps.
- Plataforma integral y completa.
- No requiere de un hosting, al ser una plataforma SaaS.

Desventajas

- Plataforma de pago, no cuenta con una versión gratuita. Ofrece un periodo de prueba de 14 días.
- No es un software open source, lo que impide poder modificarlo. Además, no cuenta con una comunidad disponiendo sólo del servicio soporte que ofrecen para aclaración de dudas.
- No es multi moneda ni multilenguaje. Disponible sólo en el idioma nativo inglés.
- Al ser un servicio SaaS, los datos de compras y de clientes se almacenan en sus propios servidores por lo que dicha información se encuentra en manos de terceros.

WordPress – WooCommerce

Fuente: [11]

WordPress es un CMS de los más utilizados para la creación de cualquier sitio web, una plataforma open source flexible con una interfaz intuitiva y fácil de usar. Se caracteriza por ser una herramienta que puede ser aprovechada por los usuarios con cualquier nivel de conocimiento técnico. Sin embargo, WordPress no es una plataforma nativa de e-commerce, por lo que requiere del uso del plugin gratuito *WooCommerce [12]* que convierte una instalación de wordpress en una tienda online.

Ventajas:

- Panel de administración muy fácil de configurar.
- Plugin gratuito a excepción que si se desea extensiones con funcionalidades extras.
- Dispone de plantillas gratis estilizadas y muy customizables. Así como, una variedad de plantillas de pago.
- SEO Friendly, cuenta con un plugin SEO muy detallado permitiendo implantar técnicas para un buen posicionamiento de la tienda.
- Cuenta con una comunidad que tiene a disposición tutoriales, artículos, foros.

Desventajas:

- No es un software nativo de e-commerce, al ser una extensión depende de WordPress.
- Puede darse incompatibilidad de plugin con el tema elegido causando problemas en el funcionamiento correcto de la web.
- Propenso a vulnerabilidades.
- Tiende a ralentizar el proceso de gestión y dinamismo cuando tienes muchos artículos y/o referencias.
- No es escalable.

Prestashop

Fuente: [13]

Prestashop es un CMS de uso exclusivo para la creación de tiendas online de gran popularidad. Software Open Source diseñado para Pymes. Permite configurarlo de forma gratuita, aunque si se desea instalar módulos en específicos se requiere de un pago. Software de fácil instalación, aunque la ruta de aprendizaje para configurar un sitio es más lenta y complicada comparado con otros CMS.

Ventajas:

- Herramienta Open Source gratuita.
- Óptimas para pequeñas y medianas empresas.
- Interfaz amigable e intuitiva
- Optimizable permitiendo albergar una gran cantidad de artículos sin afectar su rendimiento.
- Cuenta con una comunidad de expertos.
- SEO friendly

Desventajas:

- Módulos de alto costo, si se desea incorporar módulos con mejores funcionalidades estas son de pagos y muy elevados.
- No es tan flexible si se requiere realizar modificaciones más específicas.
- Propenso a vulnerabilidades.

Comparativa de funcionalidades

En este apartado se realiza una comparativa donde se refleja si cumplen o no ciertas características (Ver Tabla 1).

Características	*Magento*	*Shopify*	*Woocommerce*	*Prestashop*
Gratis	X		X	X
Escalable	X			X
Seguridad	X			
Comunidad	X		X	X
Módulos Incluidos	X	X		
SEO	X	X	X	X
Open Source	X		X	X
Fácil Configurar		X	X	

Tabla 1 Comparativa de funcionalidades

Como se puede observar en la tabla 1, se aprecia que cada CMS cuenta con una variedad de funcionalidades diferentes e iguales. Sin embargo, la opción que cuenta con más características es Magento, seguida de Prestashop.

Magento se caracteriza por ser una plataforma e-commerce robusta, su variedad de funcionalidades, características y seguridad brinda una pequeña ventaja en comparación con otros CMS de similares características. Cabe señalar que Magento cuenta con tres ediciones diferentes, Community Edition, Enterprise Edition y Enterprise Cloud Edition.

Análisis de CMS a nivel de Seguridad

En este apartado se realiza un breve análisis de cómo los CMS mencionados anteriormente gestionan las amenazas y aspectos de seguridad de la aplicación.

Magento

En el tratamiento de la seguridad, Magento brinda una serie de recomendaciones y pautas a seguir, así como, herramientas propias para el manejo de la seguridad del software [14], entre ellas:

- Guía de mejores prácticas de seguridad de Magento.
- Documentación con plan de acción de seguridad en caso de que el sitio ha sido comprometido.
- Herramienta de análisis de seguridad (gratis).
- Centro de Seguridad: Al suscribirse recibe alertas de seguridad, Boletín de Seguridad (informa últimas vulnerabilidades y parches de Magento).
- Canales para informar problemas de seguridad.
- Soporte 24/7
- Políticas de Seguridad de Contenido (CSP).
- Herramientas para el cumplimiento de la industria:
    - Reglamento General de Protección de Datos (GDPR).
    - Ley de Privacidad del Consumidor de California (CCPA).

Shopify

Shopify, para el tratamiento de seguridad del software tiene a disposición [15]:

- Centro de ayuda de Shopify: brinda una serie de recomendaciones a sus clientes de cómo tratar la seguridad de su cuenta, entre ellas:
    - Creación de contraseñas exclusivas por medio de cajas fuertes de contraseñas.
    - Autenticación segura.
    - Monitoreo de actividades sospechosas de inicio de sesión.
- Servicio de atención al cliente.
- Foro de la comunidad Shopify – Soporte Shopify.
- Cumplimiento con las leyes de privacidad:
    - Reglamento General de Protección de Datos (GDPR).

- Ley de Privacidad del Consumidor de California (CCPA).
- Aplicaciones de banners de privacidad de clientes.

Woocommerce

Woocommerce para el tratamiento de la seguridad dispone en su sitio web [16]:

- Guía de autoservicio: Documentación con recomendaciones y configuraciones básicas como medidas de protección del sitio Woocommerce.
- Herramienta de análisis de seguridad gratis, aunque la mayoría de las extensiones de análisis son de pago.
- Cumplimiento de PCI-DSS (Estándar de seguridad de datos de la industria de tarjetas de pago).
- Cumplimiento con Reglamento General de Protección de Datos (GDPR).
- HelpDesk por sistema de ticket.

PrestaShop

PrestaShop para el tratamiento de la seguridad tiene a disposición en su sitio web [17]:

- Documentación con guías y recomendaciones básicas de protección del sitio web.
- Centro de ayuda: asistencia técnica con planes de soporte adaptable a las necesidades del cliente.
- Foro de la comunidad PrestaShop
- Cumplimiento de Ley:
  - Reglamento General de Protección de Datos (GDPR) GDPR

Comparativa de aspectos de seguridad de los CMS

En este apartado se muestra una comparativa de cómo los CMS tratan los aspectos de seguridad (Ver Tabla 2).

Seguridad	*Magento*	*Shopify*	*Woocommerce*	*PrestaShop*
Documentación	X	X	X	X
Guía de buenas prácticas	X	X	X	X
Herramienta de Análisis Seguridad	X		X	
Políticas de Seguridad Contenido (CSP)	X			
Centro Seguridad	X			
Soporte	X	X	X	X
Canales Informar Problemas Seguridad	X			
Cumplimiento Ley	X	X	X	X
Herramientas Cumplimiento de Ley	X			X
Comunidad - Foro	X	X	X	X

Tabla 2 Comparativa de aspectos de seguridad

En la tabla 2, refleja que aspectos de seguridad son tomados en cuenta por los gestores de contenido e identifica que algunos de ellos son tratados de forma similar. No obstante, Magento tiene a disposición una diversidad de recursos en el tema de seguridad, liderando con respecto a los otros gestores de contenido e-commerce mencionados en este apartado.

2.2 Propuesta de Solución

Según lo estudiado en el apartado 2.1, se opta finalmente por Magento como CMS, por variedad de recursos, múltiples funcionalidades, características y documentación. Además, en el tratamiento de la seguridad del software tiene a

disposición una diversidad de recursos; brindando una pequeña ventaja en comparación con otros CMS de similares características.

2.2.1 Recursos para implementación del CMS

CMS Magento

Magento Community Edition es la plataforma e-commerce seleccionada para la implementación del servicio, dado a las diferentes características y bondades que la destacan entre los otros CMS para comercio electrónico.

Este tipo de CMS al ser un software Open Source, permite modificar el código fuente de la versión Community. Además, ofrece como ventaja a los interesados en implementar este CMS no tener que construir desde cero una web ya que viene construida con una plantilla por defecto que puede ser reemplazada por alguna plantilla gratis o de pago de su preferencia.

Magento Community Edition desde su primer lanzamiento en el 2007 dispone de varias versiones, la última versión estable disponible en Julio de 2021 es **Magento 2.4.2 y 2.4.2-p1 (Incluye parche de seguridad)** y de la cual se utilizará para la implementación del proyecto.

Magento 2.4.2-p1

Magento en su página web establece una serie de requisitos mínimos de sistema para su instalación [18], los utilizados son:

- Sistema Operativo recomendado (Linux x86-64): Ubuntu Server 20.04
- Servidor Web: Apache 2.4
- PHP: 7.4
- Servidor Base de Datos MySQL 8
- Servidor de Correo SMTP: Postfix
- Elasticsearch 7.X
- Composer 2.X

Magento cita en su documentación oficial algunas recomendaciones de hardware para su funcionamiento [19], entre ellas: **memoria PHP** “Magento 2 según como se implemente en el sistema, tiene diferentes requisitos de memoria PHP. En el caso de configurar una tienda de servidor único, recomiendan configurar la memoria PHP para 2G. En caso de configurar un sitio mediante la implementación de canalización, sugieren 2 GB en el servidor de compilación y 1 GB en el de nodo web”.

Por lo tanto, tomando en cuenta estas consideraciones se requiere los siguientes recursos como mínimo y que serán tomados en cuenta más adelante, para el diseño de la arquitectura del sistema con el proveedor de servicio en la nube:

- Memoria RAM: >= 4G
- CPU: >= 2 Cores
- Almacenamiento: >= 80G

2.2.2 Proveedores de servicios en la nube

Las infraestructuras de comunicaciones y hardware necesarias para publicar un servicio de estas características en Internet son demasiado costosas para una PYME y que estas, por lo tanto, suelen contratar estos servicios a empresas especializadas como son los proveedores de servicio en la nube.

Cloud Computing, o computación en la nube es más que todo un sistema de computación y almacenamiento de datos a través de internet, donde dicha información se almacena en lo que hoy se le conoce como la nube o cloud en inglés. En síntesis, la nube es un conjunto de servidores que nos permite acceder a los datos e información almacenada desde cualquier lugar, siempre y cuando se tenga acceso a internet.

En la actualidad existe una variedad de proveedores de servicio en la nube y estos se destacan por el tipo de servicio que ofrecen, tales como: **SaaS** (Software como un Servicio), **IaaS** (Infraestructura como un Servicio) y **PaaS** (Plataforma como un Servicio).

El tipo de servicio que se requiere para la implementación de la aplicación, es el tipo de servicio **IaaS** (Infraestructura como un Servicio), este proporciona un recurso

de hardware flexible que puede escalarse en función de sus necesidades de almacenamiento y procesamiento. Algunos expertos en tecnología exponen en su último artículo, el top 5 de los principales proveedores en la nube en 2021 [20] [21]: **AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform, Alibaba Cloud y IBM**; destacando como el líder en **IaaS** y su ramificación a **AWS.**

El proveedor de servicio en la nube elegido para la realización del proyecto es **AWS**. La decisión de elegir este proveedor es por destacar entre los proveedores de servicio en la nube, la gran documentación que existe sobre el uso de sus productos. Además, de forma personal lo considero interesante y enriquecedor para mi currículum profesional.

3.- **ANÁLISIS DE ASPECTOS DE SEGURIDAD**

Este capítulo está orientado al estudio y análisis de aspectos de seguridad, legislación aplicable, así como, las vulnerabilidades a las que puede estar expuesta la aplicación y que deben ser tomados en cuenta en la implementación del servicio.

3.1 Legislación Aplicable

3.1.1 Protección de Datos Personales

La protección de datos personales en Nicaragua está regulada por la Ley de Protección de Datos Personales N ° 787 publicada en marzo de 2012; y el Reglamento de la Ley N ° 787, Decreto N ° 36-2012 de octubre de 2012 [22][23]. Esta ley consolida el derecho de los nicaragüenses a la privacidad de sus datos personales, así como saber con qué finalidad se tiene su información personal. El alcance de esta ley es territorial, es decir, se aplica a cualquier dato recopilado en Nicaragua.

Esta ley tiene por objeto:

- Garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa.
- Otorgar el derecho que tiene toda persona de vigilar y saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales.

La ley y el reglamento ampara a la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados. Se entiende por datos personales a toda la información sobre una persona natural o jurídica que la identifica o la hace identificable, datos personales informáticos son los que pueden ser tratados a través de medios electrónicos o automatizados y datos personales sensibles. Los datos personales sensibles es toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas,

económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación. La entidad reguladora y que controla la correcta aplicación de la Ley es la Dirección de Protección de Datos Personales “DIPRODAP”.

Los principios y garantías recogidos por la ley son:

- Finalidad legítima: El tratamiento de los datos sólo podrán ser tratados, cuando sean adecuados, proporcionales y necesarios en relación con el alcance y las finalidades específicas, explícitas y legítimas para las que han sido solicitados.
- Brindar el derecho de solicitar información sobre sus datos personales, así como el derecho a rectificar, modificar, suprimir o complementar, incluir, actualizar o cancelar cualquiera de sus datos y estas acciones para el interesado serán de forma gratuita.
- Derecho al Olvido Digital

El consentimiento es un requisito importante según la ley, especialmente para recopilar y procesar datos y este deberá ser informado al titular de forma previa al tratamiento que serán sometidos sus datos personales y las de otorgar su consentimiento. Como regla general, será válido el consentimiento tácito, salvo que la Ley exija el consentimiento expreso del titular de datos. Cuando se utilicen mecanismos como medios electrónicos que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular de datos hace contacto con los mismos, en ese momento se deberá informar al titular sobre el uso de esas tecnologías, que a través de las mismas se obtienen datos personales y la forma en que se podrán deshabilitar.

La ley establece que el responsable del fichero de datos deberá adoptar las medidas técnicas y organizativas que sean necesarias para garantizar la integridad, confidencialidad y seguridad de los datos personales, para evitar su adulteración, pérdida, consulta, tratamiento, divulgación, cesión o divulgación no autorizada, y que permitan detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o de los medios técnicos utilizados. Dichas medidas deberán ser proporcionales a sus operaciones, a los riesgos inherentes a éstas y al tamaño de los ficheros de datos que administren, y estarán

sujetas a la aprobación de la DIPRODAP, la cual podrá establecer estándares mínimos de seguridad mediante normativa de carácter general que dicte al efecto.

Actualmente la DIPRODAP aún no ha sido designada, por lo que, la falta de una autoridad de protección de datos ha afectado la aplicación de la Ley y el Reglamento. Por tanto, en la práctica, la Ley no es aplicable, según lo explica una experta en la materia [24].

Dado a que la entidad reguladora en Nicaragua aún no ha sido designada y como propuesta para aplicar las medidas de seguridad necesarias que nos permitan identificar la naturaleza de los datos a tratar, así como para que esta aplicación en un futuro pueda prestar sus servicios fuera del territorio nacional, se utilizará como modelo de referencia el Esquema Nacional de Seguridad, ENS, que adapta los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO o Reglamento General de Protección de Datos “RGPD” [25] y la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales “LOPDGDD” [26].

3.1.2 Comparativa

En este apartado se realiza una comparativa de los reglamentos mencionados previamente, donde refleja algunos aspectos que no son contemplados por la Ley y el Reglamento de Protección de Datos Personales de Nicaragua con respecto a la RGPD y LOPDGDD que, si están establecidas, y de los que se indican a continuación:

- La Ley y el Reglamento no considera el nombramiento del delegado de Protección de Datos. La RGPD y LOPDGDD si lo contempla.
- El consentimiento puede ser tácito, salvo que la ley exprese lo contrario con el consentimiento expreso del titular. La RGPD y LOPDGDD, ordena el consentimiento expreso.
- En el consentimiento tácito con aviso informativo por medios electrónicos, el titular deberá responder o manifestar su negativa en un periodo de cinco días hábiles, en caso de no hacerlo, se entenderá que el titular ha otorgado su consentimiento. La RGPD y LOPDGDD no aplica este tipo de consentimiento.

- Ante una filtración de datos, la ley no obliga a notificar al cliente, DIPRODAP o cualquier otra autoridad a excepción si la persona es policía nacional o militar. La RGPD y LOPDGDD obliga la notificación a las instituciones correspondientes y al afectado a excepción que los datos filtrados no representen ningún perjuicio al afectado.
- En Nicaragua, la Ley y el Reglamento no fija una edad para ofrecer el consentimiento de manera autónoma. La RGPD y LOPDGDD define en 14 años.

3.2 Recomendaciones en seguridad

Un aspecto muy importante que debemos de tener en cuenta, es con respecto a la seguridad de las aplicaciones en la nube, ya que estas están expuestas permanentemente a amenazas por ataques malintencionados con el objetivo de explotar vulnerabilidades propias. Por lo tanto, la seguridad de aplicaciones en la nube debe tener en cuenta los aspectos específicos de seguridad derivados de los servicios en la nube, además de los aspectos clásicos de seguridad informática. De modo que, para definir las medidas de protección es fundamental la identificación y el seguimiento de amenazas a las que pueden estar propensas.

La identificación, el estudio y análisis de seguridad en las aplicaciones en la nube es un proceso muy importante que ayuda a minimizar el riesgo de que una vulnerabilidad sea explotada, así como, aplicar las medidas de mitigación de forma ágil ante una ruptura de brecha de seguridad.

En la actualidad existen organismos u organizaciones que ayudan a la identificación, categorización, consulta y seguimiento de vulnerabilidades. A su vez, crear conciencia sobre las amenazas, los riesgos y las vulnerabilidades en la nube, brindar las mejores prácticas para ayudar a garantizar un entorno seguro en la nube. Y que podemos tomar como referencia para planificar la seguridad del sistema:

CSA

Cloud Security Alliance, CSA, es una organización líder mundial que tiene como objetivo crear conciencia sobre las amenazas, los riesgos y las vulnerabilidades en la nube, así como, brindar las mejores prácticas para ayudar a garantizar un entorno seguro en la nube. Estos problemas suelen ser el resultado de la naturaleza compartida y bajo demanda de la computación en la nube.

CSA, recopila información de expertos en seguridad y genera informes que pone a disposición. Estos ayudan a mantenerse actualizado sobre las últimas amenazas, riesgos y vulnerabilidades en la nube.

Su último informe, “Principales amenazas para la computación en la nube: Egregious Eleven” [27], expone y clasifica por orden de importancia las 11 amenazas, riesgos y vulnerabilidades que destacan actualmente sobre problemas de seguridad en la industria de la nube.

ENS - Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010, de 8 de enero, tiene como finalidad crear las condiciones necesarias de confianza en el uso de los medios electrónicos [28]. Su objetivo es adaptar medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos que permitan una adecuada protección de la información.

El ENS está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información, aplicando las medidas de seguridad necesaria que deben ser proporcionales a las dimensiones de seguridad y categoría del sistema a proteger. Para lograr el cumplimiento, se debe determinar la categoría de un sistema de información, basándose en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas.

Aunque el ENS fue creado para ser aplicado a las Administraciones públicas, se tomará como referencia para determinar la categoría del sistema y poder definir

las medidas de seguridad que serán aplicadas en la aplicación web que es objeto de estudio.

OWASP Top 10

El OWASP Top 10, “Los diez riesgos más críticos en aplicaciones web” [29], es un documento estándar de metodología de análisis de riesgo, donde muestra un consenso sobre los riesgos de seguridad más críticos para las aplicaciones web.

Su objetivo es concientizar acerca de las consecuencias de las debilidades más comunes de la seguridad de las aplicaciones web y que elementos pueden influir en una amenaza:

- Agentes
- Tipo de ataque utilizado
- Vulnerabilidad y/o controles de seguridad explotados
- Posible impacto de la amenaza

OWASP Top 10 se enfoca en identificar los riesgos más críticos independientemente del tipo de empresa u organización. Para determinar el riesgo general, se evalúa la probabilidad asociada a cada agente de amenaza, vector de ataque, debilidad de seguridad y combinarlo con una estimación del impacto técnico y de negocio. En la ilustración 1, ejemplifica como un atacante puede utilizar diferentes rutas a través de la aplicación para perjudicar un negocio.

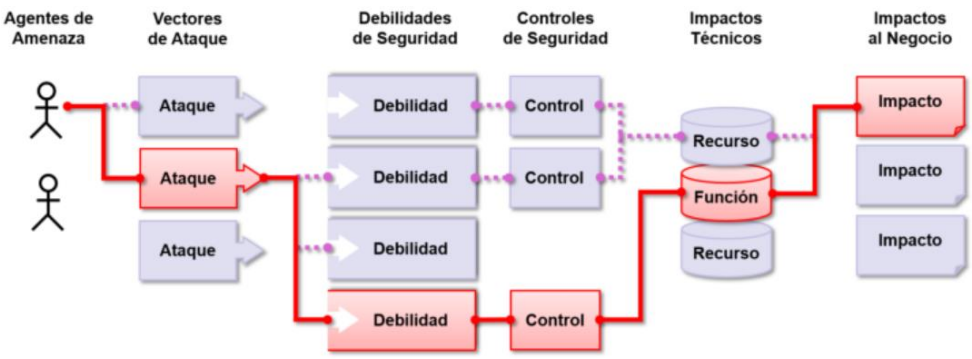


Ilustración 1 Riesgos en seguridad de aplicaciones

Independientemente de la empresa u organización estas deben de adoptar este documento e iniciar el proceso para garantizar que sus aplicaciones web minimicen estos riesgos. Por lo tanto, se tomará como referencia para identificar los riesgos a los que podría verse expuesta la aplicación.

Los factores de clasificación OWASP Top 10 son genéricos y estos son medibles en función de:

- Probabilidad de la amenaza
  - Por la facilidad de realizar el ataque.
  - Conocimiento de la vulnerabilidad.
  - Capacidad para detectar la vulnerabilidad
- Impacto
  - Técnico
  - De negocio

En la ilustración 2, muestra el esquema de evaluación utilizado, basado en la Metodología de Evaluación de Riesgos de OWASP.

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Ilustración 2 Esquema de evaluación de riesgo

3.3 Análisis de Amenazas a los que se puede enfrentar el sistema

En este apartado se realizará un análisis de las amenazas, riesgos, vulnerabilidades que destacan actualmente y a las que podría enfrentarse el sistema. Además, determinar el nivel de sistema a través del ENS y qué impacto tendría la aplicación ante un incidente de seguridad. Tomaremos como referencia, las recomendaciones de organismos expertos en materia de seguridad y que han sido mencionados en el apartado 3.2 de esta memoria.

3.3.1 CSA

CSA, en su informe “Principales amenazas para la computación en la nube: Egregious 11”, describe y clasifica las 11 amenazas de seguridad en la nube que destacan actualmente. Se realizará un estudio de cómo estos riesgos y vulnerabilidades pueden afectar a la empresa, y por lo tanto supone una amenaza que más adelante, los requisitos de seguridad deberán contemplarse.

1.- Divulgación de datos privados: Puede ser debido a ataques o usos no apropiados. Este tipo de ataque es un riesgo para la empresa, dado a que una violación de datos puede traer consecuencias negativas, tales como:

- Posibles sanciones legales y contractuales.
- Impacto en la reputación y la confianza de los clientes.
- Gastos financieros incurridos debido a la respuesta a incidentes y análisis forense.

2.- Errores en configuración y control de cambios inadecuado: Una mala configuración de los recursos en la nube, componentes y frameworks pueden utilizarse como vectores de ataque. Esto puede conllevar a filtraciones de datos, eliminación o modificación de recursos, interrupción del servicio, ocasionando un impacto negativo hacia la empresa:

- Posibles sanciones legales.
- Pérdida de fiabilidad de los clientes.
- Pérdidas financieras.

3.- Falta de arquitectura y estrategia de seguridad en la nube: Una mala arquitectura y estrategia de seguridad puede dejar a la empresa vulnerable a ciberataques, provocando un impacto severo, incluidas:

- Pérdidas financieras.
- Daños a la reputación de la empresa.
- Repercusiones legales.

4.- Gestión insuficiente de identidad, credenciales, claves y control de acceso: Un acceso no autorizado puede causar, manipulación y revelación de datos sensibles,

colapsar los recursos del sistema, y como consecuencia causar daños a la empresa, entre ellas:

- Sanciones legales.
- Daños financieros.
- Mala reputación y falta de credibilidad.

5.- Robo de Identidad: De llevarse a cabo este tipo de ataque representa una amenaza para la empresa, entre ellas, robo de datos sensibles y/o tarjetas bancarias. Causando consecuencias catastróficas para la empresa, entre ellas:

- Pérdidas financieras.
- Sanciones legales.
- Pérdida de prestigio y credibilidad.

6.- Amenazas por parte del personal: Usuarios con acceso legítimo a los recursos que hacen daño al negocio, pudiendo realizar actos deliberados, manipulación y exposición de datos confidenciales, anulación de pruebas. Este tipo de amenazas puede originar daños a la empresa:

- Gastos financieros incurridos debido a la respuesta a incidentes y análisis forense.

7.- Interfaces y APIs inseguras: Son las partes más expuestas de un sistema y atacadas continuamente, provocando manipulación, exposición y uso indebido de datos sensibles. Este tipo de amenaza es un riesgo para la empresa, causando:

- Posibles sanciones legales.
- Impacto en la reputación y la confianza de los clientes.
- Pérdidas financieras.

8.- Plano de control débil: No tener el control total de la lógica, la seguridad y la verificación de la infraestructura de datos podría provocar daños, falta de disponibilidad o fugas de datos a la empresa, como consecuencia podría generar:

- Impacto comercial.
- Posibles sanciones legales.
- Pérdidas financieras.

9.- Fallos en arquitectura del proveedor y del cliente: Este tipo de vulnerabilidad puede permitir ataques que generen brecha de privacidad, robo de información, indisponibilidad del servicio. Puede perturbar la empresa:

- Financieramente.
- Operacionalmente.

10.- Visibilidad limitada del uso de la nube: Una amenaza provocada por el uso de servicios en la nube que no cumplen con las políticas de seguridad establecidas. La empresa puede estar expuesta a un amplio abanico de brechas de seguridad, entre ellas, introducción de Malware, acceso no autorizado a datos y pérdida de los mismos. Impactando negativamente:

- Las finanzas en la empresa.
- Disponibilidad operacional.
- Posibles sanciones legales.

11.- Abuso y uso malintencionado de servicios en la nube: Una vulnerabilidad provocada por el uso malintencionado de los recursos de computación en la nube. Exponiendo a la empresa a ataques de "Minería" para moneda digital, campañas de correo electrónico no deseado y phishing, fraude de simulación de clicks automatizados. Afectando al negocio:

- Inversión financiera, sin aprovechamiento de recursos.
- Disponibilidad operacional.

3.3.2 ENS

El ENS establece una serie de medidas de seguridad que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría de seguridad (artículo 43) del sistema de información de que se trate [30]. Para determinar la categoría del sistema, se tomará en cuenta el impacto que tendría la aplicación ante un incidente de seguridad.

1. Para precisar el impacto de una aplicación sobre un incidente, se tendrá en cuenta cada una de las dimensiones de seguridad: confidencialidad [C],

integridad [I], trazabilidad [T], autenticidad [A], y disponibilidad [D]. La aplicación puede verse afectada en una o más de las dimensiones de seguridad. En caso que una dimensión de seguridad no sea afectada, no se vincula a ningún nivel.

2. Cada dimensión de seguridad se aplica a un nivel: ALTO, MEDIO o BAJO.
    a. Nivel BAJO: Se utiliza cuando las consecuencias de un incidente de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
    b. Nivel MEDIO: Se utiliza cuando las consecuencias de un incidente de seguridad supongan un daño grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
    c. Nivel ALTO. Se utiliza cuando las consecuencias de un incidente de seguridad supongan un quebranto muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
3. El ENS establece tres categorías de seguridad para los sistemas de información: BÁSICA, MEDIA y ALTA.
    a. Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
    b. Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO y ninguna alcanza un nivel superior.
    c. Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO y ninguna alcanza un nivel superior.

Dado que los datos que la empresa de referencia, LUMA, va a recopilar del usuario son datos personales y por el tipo de servicio que ofrece, tomando todo esto en cuenta, propondremos una clasificación de las dimensiones de la forma siguiente: (Ver Tabla 3).

DIMENSIONES					
SISTEMA	Trazabilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad
	(T)	(A)	(C)	(I)	(D)
NIVEL	ALTO	ALTO	ALTO	ALTO	MEDIO

Tabla 3 Categorías del sistema según ENS

Los resultados obtenidos en la tabla 3, define a un sistema de categoría ALTA. Estos datos, nos permitirá más adelante establecer los requisitos de seguridad del sistema.

3.3.3 Posibles agentes interesados en atacar el sistema

Habitualmente, cuando hablamos acerca de la seguridad y de cómo proteger nuestro sistema, nos enfocamos principalmente sobre qué tipos de ataques, amenazas y/o vulnerabilidades puede estar expuesto. En cambio, muy pocas veces nos detenemos a reflexionar acerca de los posibles agentes interesados en llevar a cabo un ataque. Los motivos pueden variar y puede influir o no el tipo de sistema a atacar. Estos actores pueden ser motivados por muchos factores, principalmente obtener un beneficio:

- Clientes: su intención es aprovecharse para obtener compras gratis, modificar precios.
- La competencia: afectar el servicio y/o reputación de la empresa para captar más clientes, utilizando ataques, tales como, denegación de servicio, exposición de datos sensibles, entre otros.
- Grupos de extorsión: ataques Ransomware, secuestrando información valiosa para la empresa y obtener dinero a cambio de liberarla.
- Aprovechamiento de computación en la nube: usando recursos con fines ilícito “criptomoneda” mientras la empresa paga las facturas.
- Ex-empleados descontentos: afectando el servicio por medio de ataques de denegación de servicio, robando y/o exponiendo datos sensibles afectando la fiabilidad de la empresa.
- Reconocimiento: para algunos actores representa un reto o son motivados por el ego de ser reconocidos ante la comunidad.

3.4 Requisitos de Seguridad Específicos

Una vez atendiendo las posibles amenazas a las que puede estar expuesto el sistema y que han sido mencionadas en el apartado anterior, podemos plantear los requisitos y necesidades concretas.

3.4.1 ENS – Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin específico. En las tablas/ilustraciones del presente se emplean las siguientes convenciones [31]:

a) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz ‘aplica’.
b) ‘n.a.’ significa ‘no aplica’.
c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo “=”.
d) Para indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad, se utilizan los signos "+" y "++".
e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial I, D, C, A, T.
f) En las tablas del presente se han empleado colores verde, amarillo y rojo de la siguiente forma: el color verde para indicar que una cierta medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría MEDIA o superior; el rojo para indicar las medidas que sólo son de aplicación en categoría ALTA.

1. **Control de acceso [op.acc]**: conjunto de actividades preparatorias para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

1.1 Identificación [op.acc.1]: Para que el cliente pueda darse de alta al sistema, será necesario un identificador singular, ejemplo: cuenta correo, que será asociado a una cuenta única.

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

Ilustración 3 Dimensiones y nivel de seguridad

1.2 Requisitos de acceso [op.acc.2]: Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Ilustración 4 Dimensiones y nivel de seguridad

1.3 Acceso remoto [op.acc.7]: Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros. Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades.

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	=

Ilustración 5 Dimensiones y nivel de seguridad [op.acc.7]

2. Explotación [op.exp].

2.1 Configuración de seguridad [op.exp.2]: El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste. El usuario tiene que realizar acciones conscientes.

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Ilustración 6 Dimensiones y nivel de seguridad [op.exp.2]

2.2 Gestión de la configuración [op.exp.3]: Se gestionará de forma continua la configuración de los componentes del sistema de forma que mantenga la

funcionalidad mínima, seguridad por defecto, y garantizar que el sistema sea adaptable y reacciones ante vulnerabilidades o incidentes.

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Ilustración 7 Dimensiones y nivel de seguridad [op.exp.3]

2.3 Gestión de cambios [op.exp.5]: Se mantendrá un control continuo de cambios realizados en el sistema, de forma que los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, se determinará si los cambios son relevantes para la seguridad del sistema.

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Ilustración 8 Dimensiones y nivel de seguridad

2.4 Protección frente a código dañino [op.exp.6]: Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Ilustración 9 Dimensiones y nivel de seguridad [op.exp.6]

2.5 Gestión de incidentes [op.exp.7]: Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo reporte de incidentes reales o sospechosos, toma de medidas urgentes, asignación de recursos para investigar las causas, informar a las partes interesadas, prevenir que se repita el incidente.

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Ilustración 10 Dimensiones y nivel de seguridad [op.exp.7]

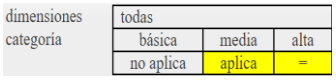
2.6 Registro de la actividad de los usuarios [op.exp.8]: Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, el registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

Ilustración 11 Dimensiones y nivel de seguridad [op.exp.8]

3. Servicios externos [op.ext].

3.1 Contratación y acuerdos de nivel de servicio [op.ext.1]: Se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes.



dimensiones / categoría	todas		
	básica	media	alta
	no aplica	aplica	=

Ilustración 12 Dimensiones y nivel de seguridad [op.ext.1]

4. Monitorización del sistema [op.mon].

4.1 Detección de intrusión [op.mon.1]: Se hará uso de una herramienta de detección de intrusiones.

dimensiones / categoría	todas		
	básica	media	alta
	no aplica	aplica	=

Ilustración 13 Dimensiones y nivel de seguridad [op.mon.1]

5. Gestión del personal [mp.per]

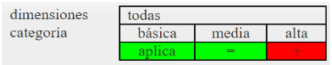
5.1 Concienciación [mp.per.3]: Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

dimensiones / categoría	todas		
	básica	media	alta
	aplica	=	=

Ilustración 14 Dimensiones y nivel de seguridad [mp.per.3]

6. Protección de las comunicaciones [mp.com].

6.1 Perímetro seguro [mp.com.1]: Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejará transitar los flujos previamente autorizados. El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.



dimensiones / categoría	todas		
	básica	media	alta
	aplica	=	+

Ilustración 15 Dimensiones y nivel de seguridad [mp.com.1]

6.2 Protección de la autenticidad y de la integridad [mp.com.3]: Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Ilustración 16 Dimensiones y nivel de seguridad [mp.com.3]

7. Protección de las aplicaciones informáticas [mp.sw].

7.1 Aceptación y puesta en servicio [mp.sw.2]: Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se realizará inspecciones, análisis de vulnerabilidades, pruebas de penetración.

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Ilustración 17 Dimensiones y nivel de seguridad [mp.sw.2]

8. Protección de la información [mp.info]

8.1 Datos de carácter personal [mp.info.1]: Se aplicará cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Ilustración 18 Dimensiones y nivel de seguridad [mp.info.1]

8.2 Copias de seguridad (backup) [mp.info.9]: Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

dimensiones	D		
nivel	bajo	medio	alto
	aplica	=	=

Ilustración 19 Dimensiones y nivel de seguridad [mp.info.9]

9. Protección de los servicios [mp.s]

9.1 Protección de servicios y aplicaciones web [mp.s.2]: Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias:

- Se garantizará la imposibilidad de acceder a la información obviando la autenticación: ataques de manipulación de URL, ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web conocido en terminología inglesa como "cookies", inyección de código.
- Prevención de intentos de escalado de privilegios.
- Prevención ataques de "cross site scripting"
- Se emplearán "certificados cualificados de autenticación del sitio web" SSL.

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Ilustración 20 Dimensiones y nivel de seguridad [mp.s.2]

9.2 Protección frente a la denegación de servicio [mp.s.8]: Se establecerá un sistema de detección de ataques de denegación de servicio, además, procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Ilustración 21 Dimensiones y nivel de seguridad [mp.s.8]

3.4.2 OWASP

En el apartado 3.2, se realizó un breve análisis de los diferentes organismos u organizaciones que ayudan a la identificación, categorización, consulta y seguimiento de vulnerabilidades. El OWASP Top 10, se enfoca en identificar los riesgos más críticos para las aplicaciones web independientemente del tipo de empresa u organización.

Con el objetivo de reducir la confusión, los nombres de los riesgos en el Top 10 están alineados con las debilidades de CWE para promover convenciones de nomenclatura generalmente aceptadas. Los riesgos definidos por OWASP y que pueden afectar a la aplicación son:

A1.- Inyección

Las fallas de inyección ocurren cuando un atacante envía datos hostiles que no son verificados en el servidor. Como consecuencia, la aplicación puede procesar datos manipulados con un intérprete SQL, LDAP, comandos del OS o ejecutar código binario arbitrario. Esto puede resultar en pérdida de datos, corrupción o divulgación a partes no autorizadas, pérdida de responsabilidad o denegación de acceso.

Para prevenir este tipo de ataque:

- Revisar todos los datos provenientes de cualquier fuente externa no confiable y variables que los contengan.
- Uso de bibliotecas o utilidades de los frameworks para procesar entradas., e.g. escapado de caracteres no permitidos.
- Uso de listas blancas de información válida, e.g. Expresiones Regulares.
- Utilización de herramientas de análisis estático de código.
- Utilizar cortafuegos a nivel de aplicación.

A2.- Gestión incorrecta de autenticación

Un atacante o usuario autorizado intenta hacerse pasar por otro obteniendo información que permita identificarlo por el sistema, principalmente debido a gestión propia del proceso autenticación y gestión de credenciales del usuario.

Posibles contramedidas para prevenir este tipo de ataque:

- Utilizar sistemas de gestión de autenticación y facilidades del framework de desarrollo o bibliotecas especializadas.
- Gestión adecuada de operaciones que puedan afectar a las credenciales del usuario, uso de políticas adecuadas de claves válidas, limitación de operaciones fallidas.
- Cifrado adecuado de credenciales en reposo y tránsito, incluso evitar que estén en memoria.

- Protección de identificadores de sesión: evitar que aparezcan en la URL.
- Doble autenticación o doble factor en operaciones críticas.
- Registro de operaciones sobre credenciales.

A3.- Exposición de datos sensibles

El atacante consigue acceso a información confidencial: MITM, claves, información sin cifrar, datos en el navegador.

Posibles contramedidas para prevenir este tipo de ataque:

- Cifrado de datos y credenciales.
- Uso de algoritmos de cifrados seguros y adecuados.
- Evitar almacenar información sensible no relevante en servidor y cliente.
- Ofuscar/tokenizar información sensible, e.g. su tarjeta de crédito ***69**.
- Control de políticas de claves de cifrado.
- Protección ID de sesión.
- Uso de encabezados de seguridad adecuados cuando se envía información sensible.
- Evitar autocompletado de campos.

A5.- Insuficiente control de acceso

Usuarios, identificados o no, pueden manipular la URL, parámetros, encabezados, cookies que permiten acceder a recursos que no les corresponden.

Posibles contramedidas para prevenir este tipo de ataque:

- Políticas de control de acceso sobre URLs.
- Verificar privilegios del usuario para acceder a cualquier recurso específico.
- Evitar uso de llaves primarias en URLs: utilizar referencias temporales en URLs que tengan asociadas las llaves primarias en contexto de sesión.
- Procesar sólo la información esperada en una petición.
- Utilizar mecanismos del framework para controlar el acceso en diferentes capas.
- Restringir acceso a metadatos.
- Restringir acceso a metadatos

A6.- Configuración incorrecta de seguridad

El atacante se aprovecha de valores de configuración por defecto, entre ellas credenciales, elementos/servicios no usados ni asegurados pero accesibles...

Posibles contramedidas para prevenir este tipo de ataque:

- Configuración de seguridad de servicios en la nube.
- Seguridad del SO, servicios y red.
- Seguimiento de CVE y actualizaciones periódicas.
- Revocar o modificar credenciales por defecto.
- Omitir detalles de versiones o errores internos en producción.
- Estudiar y configurar elementos de seguridad en servidores y frameworks.
- Análisis automatizado.

A7.- Secuencia de Comandos en Sitios Cruzados - Cross-Site Scripting (XSS)

El atacante consigue ejecutar código javascript no autorizado en el navegador del usuario, incluso autenticado y realizar acciones sin su consentimiento. Estos tipos de ataques pueden ser: *Según persistencia del código malicioso* (Almacenado, Reflejado) y *Punto de entrada del código malicioso* (Server XSS, Client XSS).

Contramedidas para prevenir este tipo de ataque:

- Comprobación de integridad de recursos externos JS y CSS (SRI).
- Codificación adecuada, según contexto de datos en salida HTML generada al usuario, tanto desde el servidor como del cliente.
- Uso de funcionalidades anti-XSS en frameworks de desarrollo y/o Uso de bibliotecas especializadas para codificación.
- Validación adecuada de datos del usuario (servidor y cliente).
- Evitar elementos inseguros de Javascript.
- Uso de directivas de seguridad de contenidos en el navegador (CSP)
- Evitar plugins externos.
- Análisis dinámico y estático.

A9.- Uso de componentes con vulnerabilidades conocidas

El atacante detecta una vulnerabilidad de forma automática o manual en alguno de los componentes utilizados por la aplicación. Muchas vulnerabilidades no llegan a ser

divulgadas de forma pública, o al menos hasta bastante tiempo después de haberse producido.

Posibles contramedidas para prevenir este tipo de ataque:

- Registro actualizado de versiones de componentes y dependencias.
- Actualizaciones periódicas.
- Seguimiento de vulnerabilidades de componentes de la pila de desarrollo.
- Uso de herramientas de análisis estático.

A10.- Registro y Monitorización Insuficientes

La falta de monitorización y respuestas adecuadas frente a acciones no convencionales facilita al atacante la experimentación y explotación de vulnerabilidades en el sistema.

Posibles contramedidas para prevenir este tipo de ataque:

- Registro sistemático y detallado de fallos en procesos de identificación, control de acceso y validación de datos de entrada.
- Registro de operaciones críticas en el sistema.
- Centralización de logs en servicios especializados en gestión y detección.
- Sistemas de alerta y respuesta frente a amenazas.

3.4.3 Otras necesidades concretas

Además de tener en cuenta los requisitos de seguridad de organismos que son referencia en aspectos de seguridad, y con el objetivo de reforzar dichas recomendaciones, se requiere que el sistema cuente con:

- *Alta disponibilidad y tolerancia a fallos*, con el objetivo de que el servicio esté disponible para los clientes el mayor tiempo posible tratando de mitigar posibles problemas debidos a incrementos puntuales de conexiones (e.g. usando balanceo de carga) o caídas de nodos debidas a cuestiones de mantenimiento o problemas hardware o software (e.g. seleccionando servicios con SLAs adecuados a las necesidades de la empresa).

- *Monitorización,* tener una visión de los eventos que se generan en el sistema, permite anticiparnos y detectar vulnerabilidades, para poder evitar y solucionar cualquier problema.
- *Firewall de aplicaciones,* para proteger al sistema contra ataques comunes.

4.- MEDIDAS DE SEGURIDAD Y BUENAS PRÁCTICAS

Una vez realizado el estudio de la legislación aplicable, análisis de amenazas, recomendaciones y requisitos de seguridad aplicables al sistema, se plantearán las medidas de seguridad y buenas prácticas; así como, las características que tendrá la arquitectura del sistema y funcionalidades concretas.

4.1 Recomendaciones CMS Magento

Magento en los aspectos de seguridad como buenas prácticas en la parte de implementación y despliegue, brinda una serie de recomendaciones generales. Además, considera seguir las siguientes cinco recomendaciones que son de máxima prioridad [32].

1. Habilitar el doble factor de autenticación (2FA): Para mejorar la seguridad en el panel de administración, brinda la opción de requerir la autenticación de dos pasos para acceder a la interfaz de usuario de Magento Admin. La extensión admite múltiples autenticadores, incluidas las claves Google Authenticator, Authy, Duo y U2F.

2. Configurar y utilizar una URL de administrador que no sea la predeterminada: Aunque esto no protegerá el sitio completamente, su uso ayudará a prevenir ataques automatizados a gran escala. Asimismo, Adobe crea de forma aleatoria un URL de administrador cuando se realiza la instalación. Otra recomendación para el panel de administrador, es limitar el número máximo de errores de inicio de sesión antes de que se bloquee la cuenta, limitar el número de solicitudes de restablecimiento de contraseña por hora y que el tiempo de bloqueo sea en un mínimo de 30 minutos.

3. Mantener el código actualizado instalando todas las versiones de parches: Adobe-Magento, recomienda usar la última versión de la aplicación, así como todos los parches actuales, es la primera y mejor línea de defensa contra posibles compromisos. Magento Commerce publica actualizaciones de seguridad trimestralmente.

4. Implementar las variables de entorno "lock config" y "lock env": Esta opción permite bloquear los archivos env.php y config.php para que no se pueda editar en el administrador de Magento o cambia una configuración que ya está bloqueada en el administrador de Magento.

5. Configurar y ejecutar el servicio de escaneo de seguridad de Magento Commerce: El servicio Security Scan está disponible de forma gratuita, realiza un análisis en busca de riesgos de seguridad conocidos, recibe actualizaciones de parches y notificaciones de seguridad. Dentro de sus ventajas de esta herramienta:

- Informa sobre el estado de seguridad en tiempo real.
- Ejecución de análisis de seguridad programable.
- Informes de los resultados obtenidos con recomendaciones de acciones correctivas.
- Historial de informes de seguridad.

Así mismo, Magento en su guía de instalación, brinda una serie de recomendaciones de seguridad posterior a su instalación [33] [34] [35]:

- Asegurar la configuración correcta del encabezado HTTP X-Frame-Option.
- Prevenir secuencias de comandos entre sitios (XSS), validando cualquier valor proveniente de las solicitudes.
- Prevención de ataques DoS y fuerza bruta.
- Prevención de secuestro sesiones de usuarios.
- Configurar informe de seguridad de problemas.

4.2 Requisitos operacionales ENS (funcionalidades concretas)

A su vez, para cumplir con los requisitos operacionales establecidos por el ENS, se requiere que la aplicación cuente con los siguientes requisitos:

- Uso de framework de gestor de contenido con su última versión disponible, que integre conexiones seguras entre el servidor y los clientes. Incluyendo clave de cifrado para proteger contraseñas y datos confidenciales.
- Uso de certificado SSL/TLS para establecer conexiones seguras.

- Gestor de logs para registro de actividades.
- Firewall de aplicaciones web (WAF) para proteger la aplicación contra ataques.
- Uso de plugin de pasarela de pago.
- Copias de seguridad automatizadas.
- Alta disponibilidad:
    - Balanceador de carga.

4.3 Arquitectura del Sistema

La arquitectura propuesta para la implementación de la aplicación web con el proveedor de servicio en la nube AWS, tendrá las siguientes características:

- Una nube virtual privada (VPC) que abarca una zona de disponibilidad, en ella estará configurada una subred pública y una subred privada.
- Para la subred pública, contará con un host bastión Auto Scaling que abarca varias zonas de disponibilidad para conceder acceso mediante Secure Shell (SSH) al servidor web de Magento.
- Gateways de traducción de dirección de red (NAT) para lograr conectividad a Internet de salida a todas las instancias EC2 que se inician en la red privada.
- Instancia de servidor web de Amazon EC2 Auto Scaling iniciada en una subred privada.
- Una instancia Amazon Relational Database Service (Amazon RDS) con un motor de base de datos MariaDB iniciada en una subred privada.
- Un balanceador de carga de aplicaciones para equilibrar la carga de tráfico HTTP y HTTPS.
- Grupo de seguridad adecuado para la instancia EC2 y base de datos con el objetivo de restringir el acceso a los protocolos y puertos necesarios.
- Implementación de certificados de capa de conexión segura/seguridad de la capa de transporte (SSL/TLS).
- Nombre de dominio *“lumates.es” adquirido a través de un proveedor de nombre de dominios.*

- Servicio Amazon Route 53 para el direccionamiento del tráfico de Internet a los recursos del dominio: "*lumatest.es*"
- Servicio SMTP para el servidor web Magento.
- Firewall de aplicaciones web (WAF).
- Servicio de monitoreo de Amazon Guard Duty.
- Servicio de Amazon Inspector para evaluar la seguridad de la aplicación ejecutada en la instancia.

En la ilustración 22 se muestra de forma gráfica la arquitectura del sistema propuesto

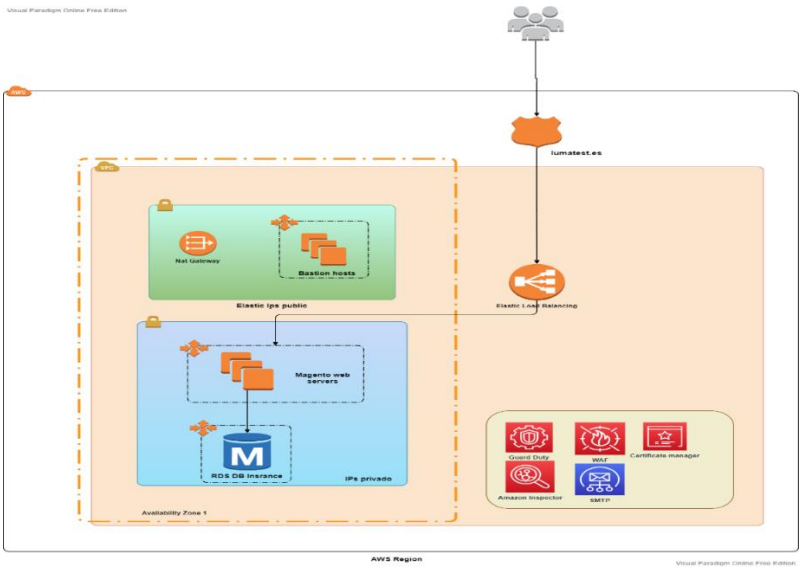


Ilustración 22 Arquitectura de la aplicación web en la nube propuesta

4.4 Buenas prácticas a nivel organizativo y operacional

La importancia de implantar medidas de seguridad y buenas prácticas, también aplica a nivel organizacional de una empresa. Es por ello que, se plantean las siguientes recomendaciones, algunas de ellas extraídas del Marco Organizativo del ENS [36]:

- Definir los roles o funciones de seguridad del personal, determinando para cada uno, los deberes y responsabilidades del cargo a desempeñar. Con el objetivo de fijar, quién o quiénes, tendrán privilegios de administrador del panel

de control del CMS y del proveedor de servicios en la nube y que será el o los responsables de gestionar las cuentas de usuarios.

- Disponer de material orientativo como apoyo al personal, que detalle acerca:
  - Las actividades operacionales habituales.
  - Procesos de cómo reportar e identificar comportamientos anómalos.
  - Medidas de contingencia que se deben aplicar ante un evento o afectación del servicio.
- Puntualizar la frecuencia de:
  - Rotación de cambio de contraseñas.
  - Uso de herramienta de análisis de vulnerabilidades.
- Definir políticas de copias de seguridad automatizadas, estableciendo la frecuencia de ejecución, (eg. frecuencia semanal mientras no haya mucha afluencia al sistema). Además, programar simulacros periódicos de recuperación del sistema a partir de dichas copias de seguridad.
- Eliminar cuentas de usuarios del personal que ya no es parte de la empresa.

4.5 Medidas de seguridad que aporta el proveedor de servicio en la nube

Cuando nos referimos a la nube y en lo que se refiere a la seguridad, los proveedores de servicio hoy en día, han optado por la implantación de un modelo que ayuda a aliviar la carga operativa del cliente. AWS es un pionero de la implantación de este modelo conocido como modelo de responsabilidad compartida [37]. Este modelo consiste en que AWS toma la responsabilidad de administrar, operar y controlar los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios. El cliente es responsable de la administración del sistema operativo invitado (incluye actualizaciones, parches de seguridad), de cualquier aplicación asociada y de la configuración del firewall del grupo de seguridad que brinda AWS. Por otro lado, estas responsabilidades variarían según los servicios que utilice el cliente.

A este modelo de responsabilidad compartida se diferencia como seguridad "*de*" la nube y seguridad "*en*" la nube como se muestra en la ilustración 23.

Ilustración 23 Modelo de responsabilidad compartida en torno a la seguridad de AWS

Fuente: AWS Seguridad en la nube

Seguridad de la nube: AWS es responsable de garantizar y proteger la infraestructura que ejecuta todos los servicios que aprovisiona en la nube de AWS. Esto se refiere a toda la infraestructura que está conformada por hardware, software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Seguridad en la nube: Se refiere a la responsabilidad que debe de asumir el cliente y estará determinada por los servicios de la nube de AWS que este seleccione. Una forma de ejemplificar cómo determinar el alcance de trabajo y las responsabilidades de seguridad por parte del cliente sería: un servicio Amazon EC2, clasificado como un servicio IaaS, en este caso el cliente asume la responsabilidad de realizar las tareas de administración y configuración de seguridad necesarias, incluyendo la administración del sistema operativo huésped (parches de seguridad y actualizaciones), así como, cualquier otra aplicación instalada por el cliente y de la configuración del firewall que proporciona AWS.

Dentro del "*Marco de Buena Arquitectura de AWS y su Pilar de la Seguridad*" [38], se basa en saber cómo aprovechar las tecnologías de la nube para proteger los datos, los sistemas y los activos.

Como fase previa AWS dedica un apartado acerca de la separación y administración de cuentas de AWS. En ella recomienda organizar las cargas de trabajo en cuentas individuales y agrupar las cuentas según la función, los requisitos de conformidad o un conjunto común de controles. Para AWS, las cuentas son un contenedor de confianza cero con límites estrictos para los recursos, es por ello que nos brinda algunas recomendaciones, entre ellas:

- Separar las cargas de trabajo mediante el uso de cuentas: Este enfoque establece límites y controles entre las cargas de trabajo. Ejemplo, separar a nivel de cuenta para aislar las cargas de trabajo de producción de las de prueba.
- Administrar las cuentas de forma centralizada: AWS Organizations, es una herramienta que ayuda a administrar las cuentas, establecer controles y configurar servicios en las cuentas.
- Establecer controles de manera centralizada: Por ejemplo, uso de políticas de control de servicios (SCP) para aplicar medidas de seguridad de permisos a nivel de organización, unidad organizativa o cuenta.

El Pilar de Seguridad de AWS es conformado por:

Administración de Identidades y Accesos: Esta se divide en dos áreas principales:

- Administración de la identidad: Consta de dos tipos de identidades, *identidades de humanos* que se refiere a los miembros de una organización, e *identidades de máquinas* que se refiere a las aplicaciones que se ejecutan dentro del entorno AWS. Para tratar la parte de seguridad, recomienda:
    - Uso de mecanismo de inicio de sesión seguro: Estableciendo longitud de contraseña mínima, y la autenticación MFA.
    - Uso de credenciales temporales.
- Administración de permisos: tiene el objetivo de controlar a qué se tiene acceso, quién puede acceder y bajo qué condiciones lo hace. Algunas prácticas que recomiendan:
    - Establecer un principio de privilegios mínimos.
    - Compartir recursos de forma segura con AWS RAM.

Detección: La detección es una parte esencial del ciclo de vida de la seguridad que permite la identificación de una posible configuración errónea de seguridad, una amenaza o un comportamiento inesperado. AWS hace uso de diferentes enfoques para abordar los mecanismos de detección, entre ellos:

- Configuración del registro de servicios y aplicaciones: Esta base de mecanismos, está diseñada para registrar y detectar una amplia gama de

acciones en todos los recursos de la cuenta. AWS proporciona una serie de servicios que se pueden implementar, tales como:

- Historial de eventos.
- Monitoreo y registro de las configuraciones aplicadas.
- Monitoreo de detección de amenazas.
- Gestor centralizado de alertas.

Protección de la infraestructura: Es una pieza fundamental, su objetivo es garantizar que los sistemas y los servicios de la carga de trabajo estén protegidos contra el acceso no intencionado o no autorizado, y contra posibles vulnerabilidades. AWS, dispone de varios enfoques para la protección del mismo:

- Protección de redes: Planificar, administrar, diseñar de forma ordenada la red constituye la base de cómo se proporciona aislamiento y se establecen límites para los recursos de la carga de trabajo. Algunas prácticas que recomiendan:
  - Crear capas de red, segmentando en capas formadas por subredes a los componentes que comparten requisitos de accesibilidad.
  - Controlar el tráfico en todas las capas, examinar la conectividad de cada componente, si requiere accesibilidad a Internet, aplicar controles para el tráfico de entrada y de salida, uso de firewall, ACL.
  - Implementar inspección y protección, para los componentes que operan a través del protocolo HTTP, el uso de un firewall de aplicaciones como AWS WAF es una herramienta que protege contra ataques comunes, así como, monitorear y bloquear solicitudes HTTP(s) que coincidan con las reglas configurables.
- Protección de recursos informáticos: La administración de vulnerabilidades por medio de análisis y aplicación de parches, permite detectar las vulnerabilidades del código, las dependencias y la infraestructura. Las buenas prácticas recomiendan:
  - Uso de herramientas para el análisis de código estático y dependencias de terceros para detectar problemas de seguridad, vulnerabilidades y exposiciones comunes de CVE recientes.
  - Evaluar la configuración de las instancias con el fin de detectar vulnerabilidades y exposiciones comunes conocidas, herramientas

como Amazon Inspector permiten evaluar, notificar y comparar con los puntos de referencia de seguridad.

Protección de los datos: A la hora de plantear acerca de la protección de datos, se debe de establecer como una práctica fundamental la clasificación de los datos, ya que proporciona un método de cómo categorizar los datos de una organización en función de su criticidad y confidencialidad. Este método tiene como objetivo determinar los controles de protección y retención adecuados, así como, prevenir la manipulación indebida o cumplir con las obligaciones normativas.

Por otro lado, se debe de tener en cuenta a la hora de aplicar medidas de protección de los datos, que estos se dividen en dos tipos de datos:

- Datos en reposo: son datos que residen en un almacenamiento no volátil a lo largo del tiempo, tales como, las bases de datos, los archivos, y cualquier otro medio de almacenamiento donde se conserven los datos. Algunas de las medidas para proteger este tipo de datos son:
    - Uso de tokenización, es un proceso que define un token para sustituir información confidencial, por ejemplo, el número de una tarjeta de crédito.
    - El cifrado, es un método que transforma el contenido a un modo ilegible.
    - Aplicar control de acceso.
- Datos en tránsito: son todos aquellos datos que se envían de un sistema a otro, incluyendo la comunicación entre otros servicios y los usuarios finales. Algunas medidas para proteger los datos en tránsito son:
    - Implementación de certificados de capa de conexión segura/seguridad de la capa de transporte (SSL/TLS) públicos y privados. Servicio como AWS Certificate Manager permite aprovisionar, administrar e implementar los certificados SSL/TLS.
    - Aplicar cifrado en tránsito utilizando protocolos de puntos de enlace seguros HTTPS mediante TLS para la comunicación.
    - Automatizar la detección del acceso no deseado a los datos por medio de herramientas que detecten automáticamente los intentos de trasladar datos fuera de los límites definidos. Herramientas como Amazon GuardDuty, brindan este tipo de análisis.

Otro tema importante a tomar en cuenta acerca de las medidas de seguridad que aporta el proveedor, es referente a los "*Acuerdos de nivel de servicios (SLA)*" y el nivel de disponibilidad que ofertan para los servicios. Como hemos visto en apartados previos, una afectación del servicio puede llegar a causar pérdidas para la empresa, entre ellas la económica. AWS en su catálogo de servicio, ofrece los siguientes niveles de disponibilidad [39], e.g. 99,99% para elementos virtualizados y balanceador de carga; 99,9% para gestor de monitoreo y un 99,95% para firewall de aplicaciones web. En el caso de que cualquiera de los servicios no cumpla con el compromiso de servicio, AWS otorga al cliente un crédito por servicio y serán aplicados contra pagos futuros.

4.6 Matriz de resumen – requisitos de seguridad / medidas de seguridad

A continuación, en la tabla 4 se describe una matriz de resumen donde para cada requisito de seguridad establecido que medidas seguridad contribuyen a garantizarlos.

Activos de Información	Requisito de Seguridad	Medida/s de seguridad concretas
Magento	Seguridad panel de administración	Habilitar 2FA
	URL administrador	Se usará URL aleatorio generado por Magento.
	Código actualizado	Última versión disponible Magento 2.4.2-p1
	Bloquear archivos env.php y config.php	Implementar las variables de entorno "lock config" y "lock env".
	Proteger encabezado HTTP X-Frame-Option	Editar en archivo env.php estableciendo valor “DENY”.
	Prevenir ataque XSS	A través de CSP como “restrict mode”.
	Prevenir ataques DoS y Fuerza bruta	Utilizando CAPTCHA y habilitando Gestión de sesiones.
	Prevenir secuestro de sesiones usuario	Activar opción en panel administrador.
	Protección Datos sensibles	Uso de plugin “Pasarela de pago”
AWS	Mecanismo inicio de sesión segura	Estableciendo MFA
	Administración de permisos	Establecer privilegios mínimos a excepción del administrador.
	Protección datos en reposo	-Uso tokenización. -Uso de cifrado.
	Protección datos en tránsito	Certificado SSL/TLS.
	Protección de componentes que operan por HTTP	Uso firewall de aplicaciones “AWS WAF”.
	Alta disponibilidad	-Balanceador de carga: AWS Elastic Load Balancing. -Copias automáticas.

Tabla 4 Matriz de resumen de requisitos y medidas de seguridad

5.- **DISEÑO Y CONFIGURACIÓN**

En este apartado se detallarán algunos aspectos relevantes referente al despliegue de la aplicación en la nube, así como, las medidas de seguridad aplicada como parte de las buenas prácticas mencionadas previamente.

5.1 Despliegue del servicio en proveedor del servicio

Para el despliegue de la aplicación con el proveedor del servicio AWS, se parte del diseño de arquitectura propuesto en el apartado 4.3 de esta memoria. Cabe mencionar que, para la implementación y entorno de prueba, no se hace uso del servicio Auto Scaling por motivos de costo de recursos.

Los recursos utilizados para la implementación del servicio de aplicación web como entorno de prueba son los siguientes:

Servidor web Magento: Se configuran los siguientes recursos:

- *Instancia EC2 [40] de tipo "t2.medium":*
  - *Requisitos de infraestructura:* memoria RAM de 4G; 2CPU virtuales; volumen de almacenamiento 30G; IP pública y privada asignada por AWS. Para el acceso a la instancia por SSH, AWS asigna un par de claves de tipo RSA. En las ilustraciones 24, 25 y 26 se muestra un resumen de las configuraciones de la instancia.

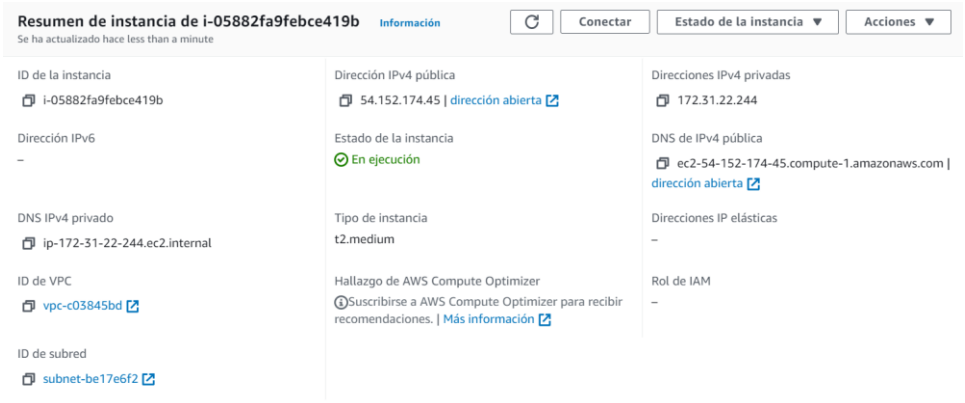


Ilustración 24 Información del tipo de instancia y direccionamiento IP asignado

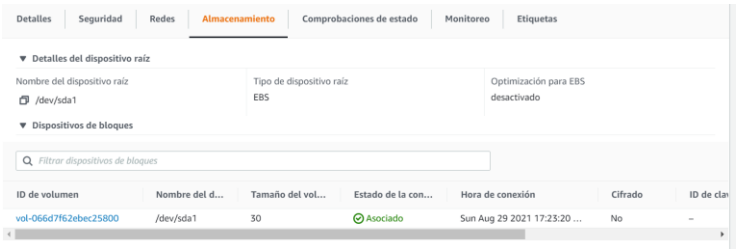


Ilustración 25 Tamaño del volumen de almacenamiento

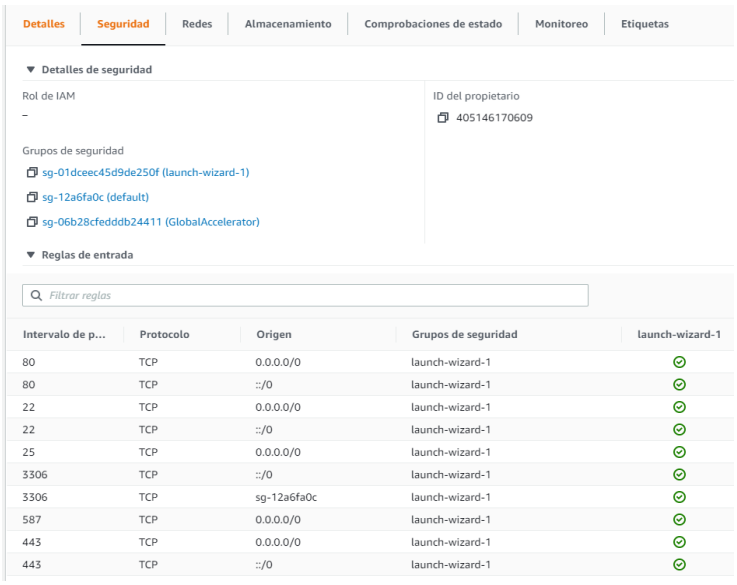


Ilustración 26 Grupos de seguridad y puertos permitidos

- *Requisitos de sistema:* Para la instalación del CMS Magento 2.4.2-p1, se requiere de los siguientes recursos adicionales: SO (Linux x86-64) Ubuntu Server 20.04; Apache 2.4, PHP: 7.4; servidor SMTP: Postfix; Java openjdk-8-jdk; Elasticsearch 7.9; Composer 2.X. En las ilustraciones 27, 28 y 29 se muestra un resumen de los servicios instalados.

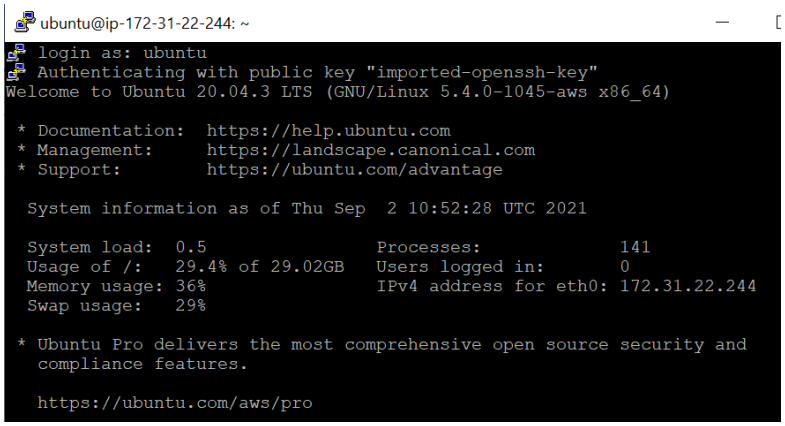


Ilustración 27 SO Linux Ubuntu 20.04

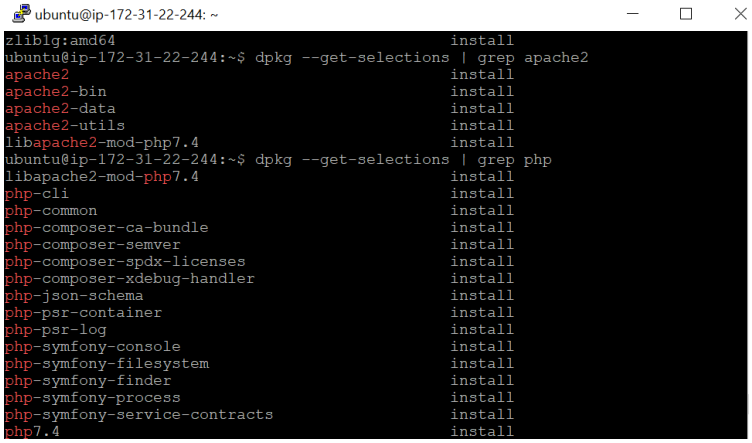


Ilustración 28 Servicios instalados

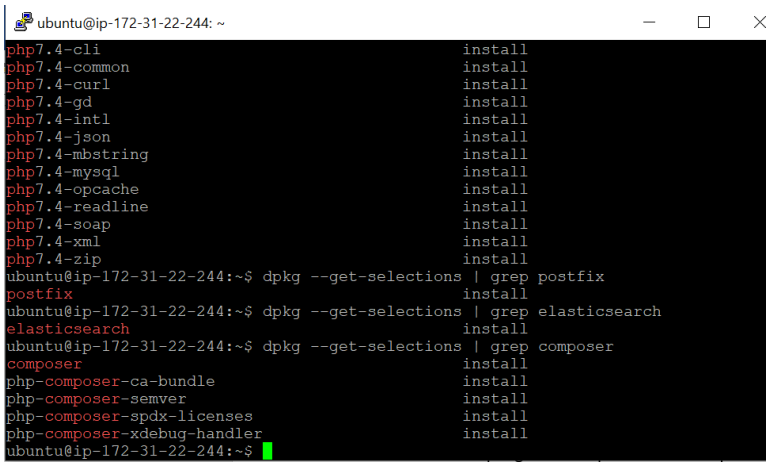


Ilustración 29 Servicios instalados

- *Instancia Amazon RDS [41] clase* “db.t2.micro” de la capa gratuita*: En las ilustraciones 30 y 31 se detalla información resumida de la instancia RDS.*
  - *Requisitos de infraestructura:* memoria RAM de 1G; 1CPU virtual.
  - *Requisitos del sistema:* motor de base de datos MariaDB 10.4.13; base de datos de nombre magento242.
  - *Seguridad:* Para el acceso público a la base de datos, se asocia al grupo de seguridad de la instancia EC2. Dicha configuración, permite el

acceso únicamente a través de la instancia utilizando el par de claves como método de autenticación.

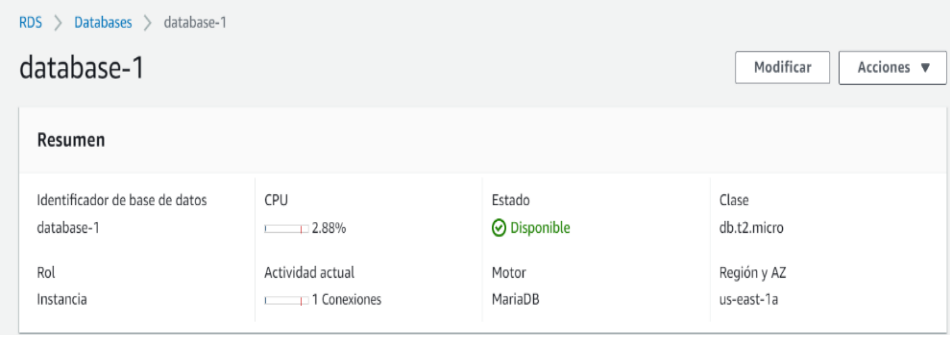


Ilustración 30 Información RDS - database-1

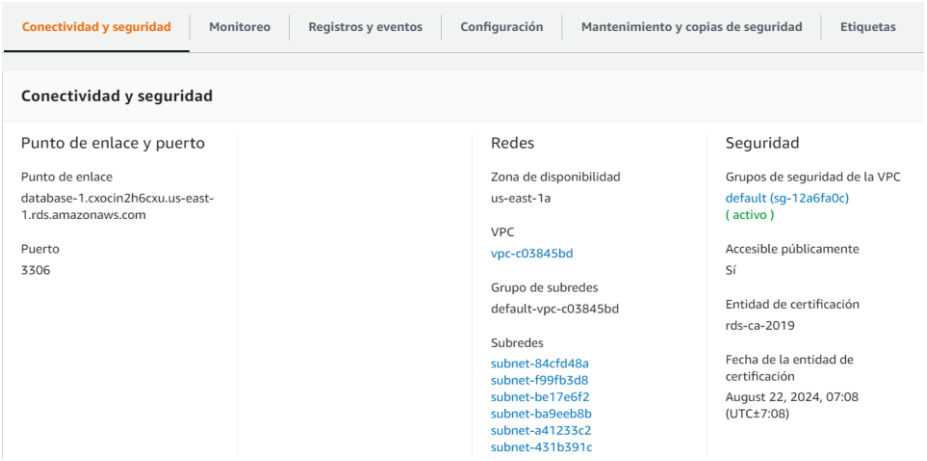


Ilustración 31 RDS conectividad y seguridad.

A continuación, siguiendo las recomendaciones de buenas prácticas del proveedor de servicio en la nube, así como, garantizar la disponibilidad del servicio se procede aplicar las siguientes configuraciones definidas previamente:

- ***Mecanismo de inicio sesión segura:*** AWS categoriza los tipos de usuarios para el inicio de sesión. Ellos son el usuario raíz que es el propietario de la cuenta y usuario de IAM asignado para tareas diarias. AWS asigna una capa de seguridad adicional para el inicio de sesión, ella es el Multi-Factor Authentication (MFA). Por tanto, se aplica capa de seguridad al usuario raíz. En las siguientes ilustraciones se detalla la configuración:

- *Usuario Raíz:*

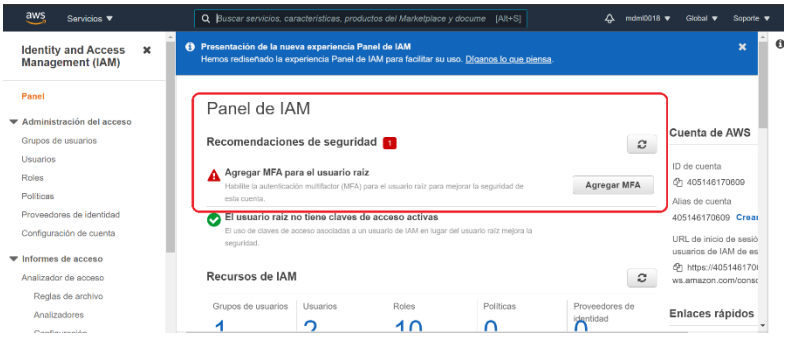


Ilustración 32 Usuario Raíz sin MFA

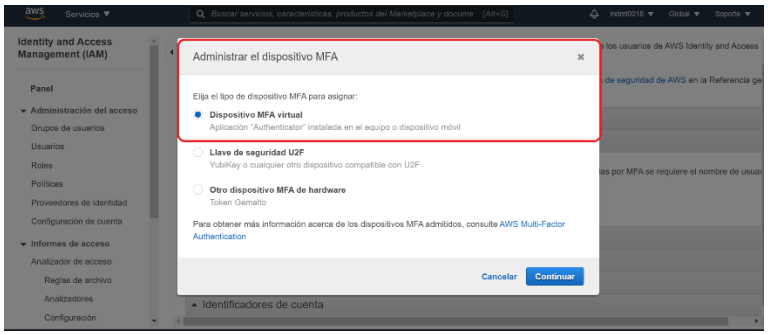


Ilustración 33 Activación MFA virtual

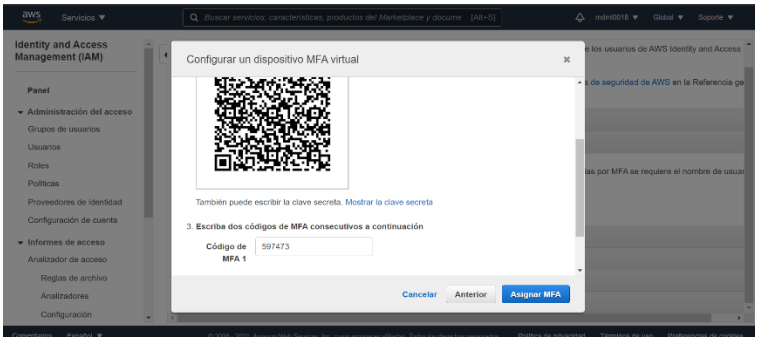


Ilustración 34 Validación de código QR a través app Google Authenticator

Ilustración 35 MFA activado

Ilustración 36 Validación correcto funcionamiento MFA

Ilustración 37 Capa seguridad añadida de AWS CAPTCHA por default

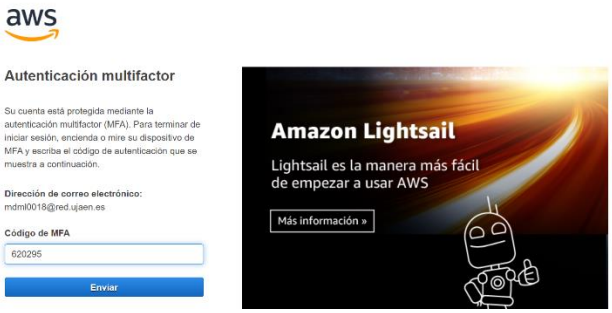


Ilustración 38 Ingreso de Código seguridad asignado por app Authenticator

- ***Administración de permisos:*** Amazon como parte de las recomendaciones de buenas prácticas, sugiere asignar un usuario IAM con permisos de administrador. Este usuario, se designa para la realización de tareas diarias con el objetivo de evitar trabajar con la cuenta propietaria.
  - *Usuario IAM:* Se configura el grupo de usuario "*Administrator*" con el usuario del mismo nombre. Se asigna la política "*AdministratorAccess"* brinda acceso completo a los servicios y recursos de AWS. Dicha cuenta administrador, tiene los privilegios para crear cuentas de usuarios y

asignar los privilegios según la asignación de tareas. En la siguiente ilustración se muestra información del usuario Administrator.

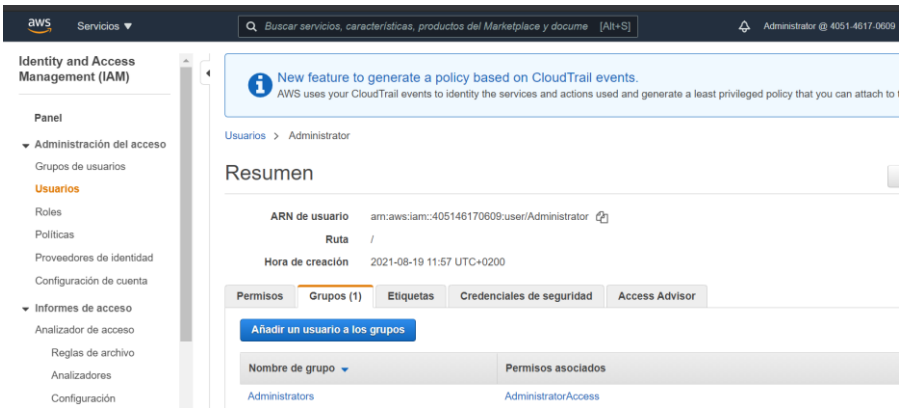


Ilustración 39 Grupo de usuario Administrator

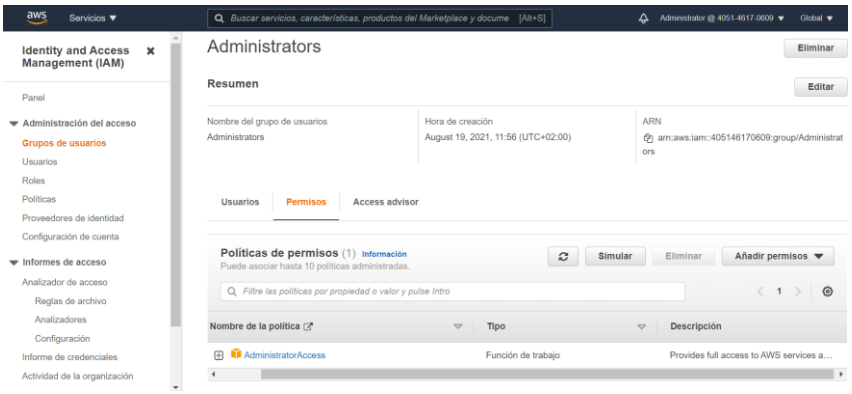


Ilustración 40 Política de permisos

- ***Protección de datos en reposo:*** AWS proporciona una capa adicional en las instancias RDS (Base de Datos), por medio del cifrado de base de datos. Amazon RDS hace uso de una clave maestra de cliente (CMK) de AWS Key Management Service (KMS) para cifrar los recursos. El algoritmo de cifrado utilizado para las instancias de BD es el estándar AES-256. Este tipo de servicio actualmente no se encuentra disponible en la capa gratuita, por tanto, no se ha implementado en el despliegue de prueba del servicio objeto de estudio. No obstante, se recomienda el uso de este servicio como medida de protección de los datos almacenados.
- ***Protección de datos en tránsito:*** Para la protección de los datos en tránsito, se agrega una capa adicional de protección, a través, de la implementación de un certificado de capa de conexión segura/seguridad de la capa de transporte (SSL/TLS). Para ello se hace uso de un nombre de dominio "*lumatest.es*",

asignado por medio de un proveedor de nombres de dominio (IONOS.es) [42], así como, uso del servicio Amazon Route 53 para el direccionamiento del tráfico de Internet a los recursos del dominio “lumatest.es”. En el caso del certificado SSL_TLS, se prescinde del certificado proporcionado por el proveedor de nombre de dominios IONOS por motivos de obligatoriedad de renovación de contrato después de pasado el periodo de prueba gratis. Por lo que se solicita un certificado a la entidad de certificación gratuita Let’s Encrypt[1], se requiere que el certificado SSL/TLS esté disponible para redes IPv4 e IPv6 para un correcto funcionamiento.

En las ilustraciones 41, 42 y 43 podemos observar parte de las configuraciones.

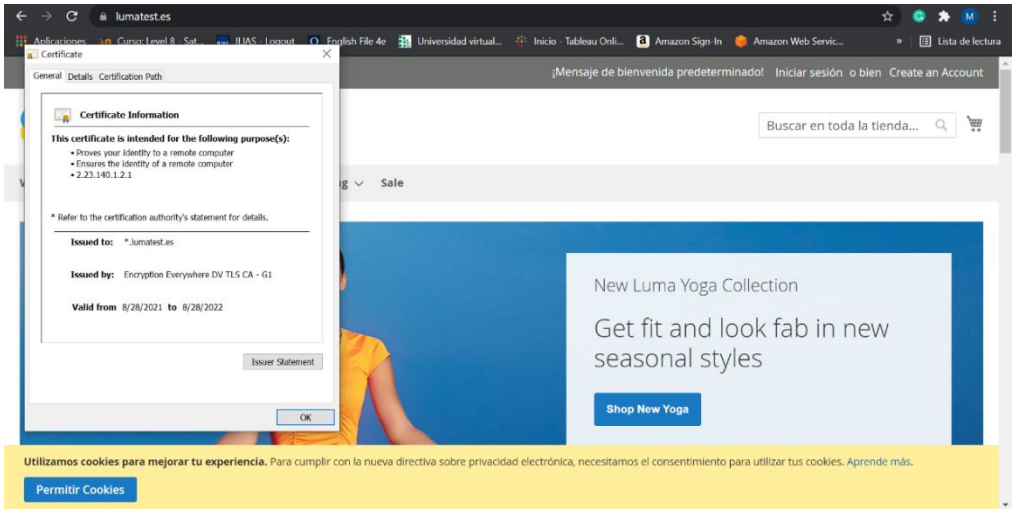


Ilustración 41 Certificado SSL para el dominio lumatest.es

[1] Fuente: https://letsencrypt.org/es/

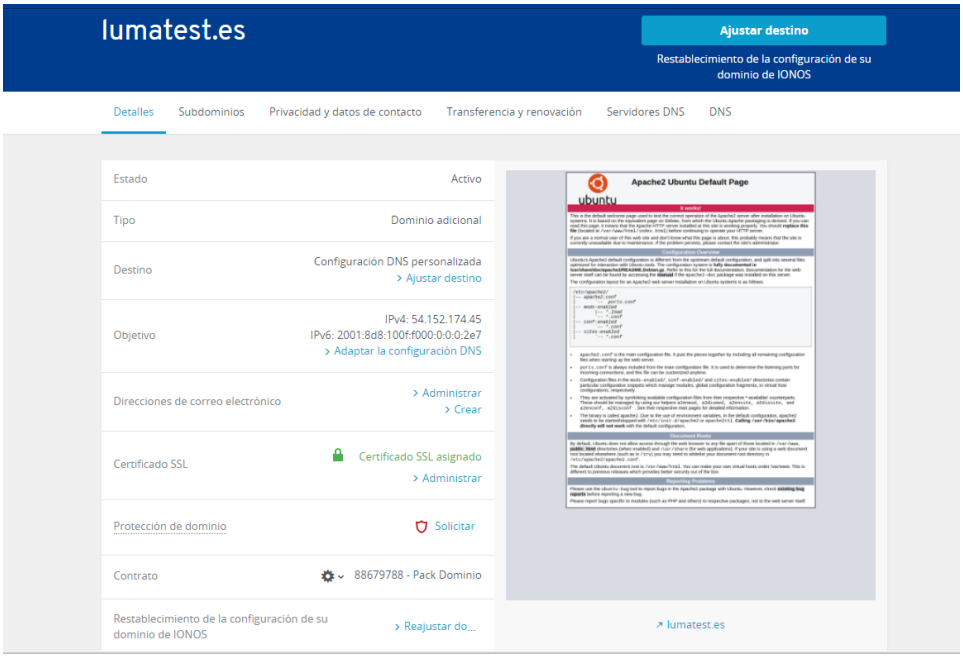


Ilustración 42 Registro de dominio lumatest.es

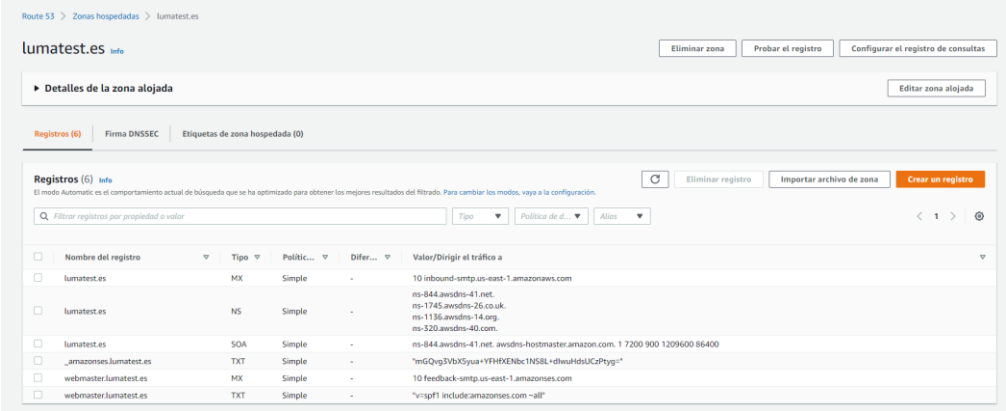


Ilustración 43 Servicio Route 53 para direccionamiento tráfico de internet hacia el dominio

- ***Alta disponibilidad:*** Con el objetivo de brindar una alta disponibilidad del servicio, se dispone de lo siguiente:
  - ***Uso del servicio Elastic Load Balancing:*** Específicamente se hace uso de un balanceador de carga de aplicaciones, siendo el más adecuado para brindar un equilibrio de carga del tráfico HTTP y HTTPS. La configuración aplicada a la instancia, permite que la carga de tráfico HTTP y HTTPS esté equilibrada en 6 zonas de disponibilidad, en la misma región. Adicionalmente, se integra el servicio de un acelerador global de tipo estándar, permitiendo dirigir el tráfico a los puntos finales óptimos a través de la red Global de AWS. En las ilustraciones a continuación se muestra un resumen de la configuración.

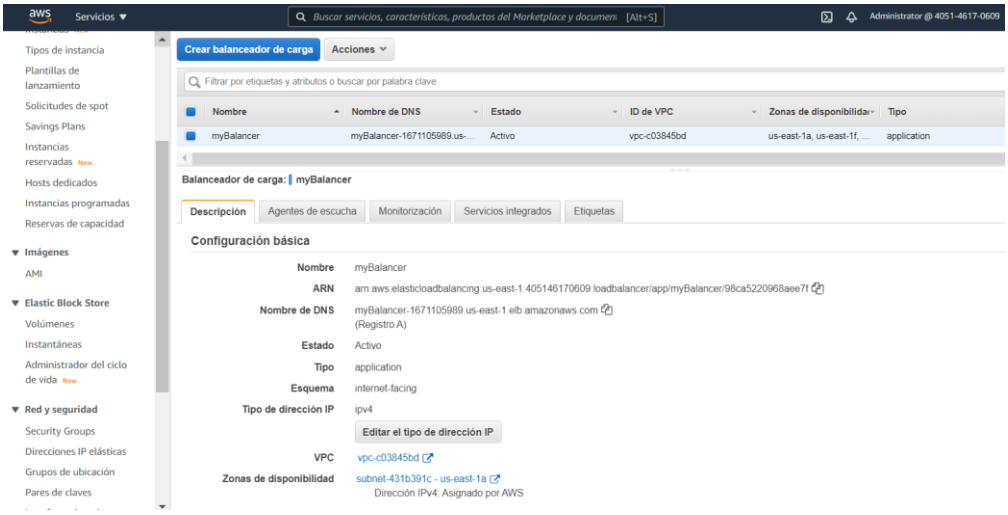


Ilustración 44 Configuración de balanceador de carga

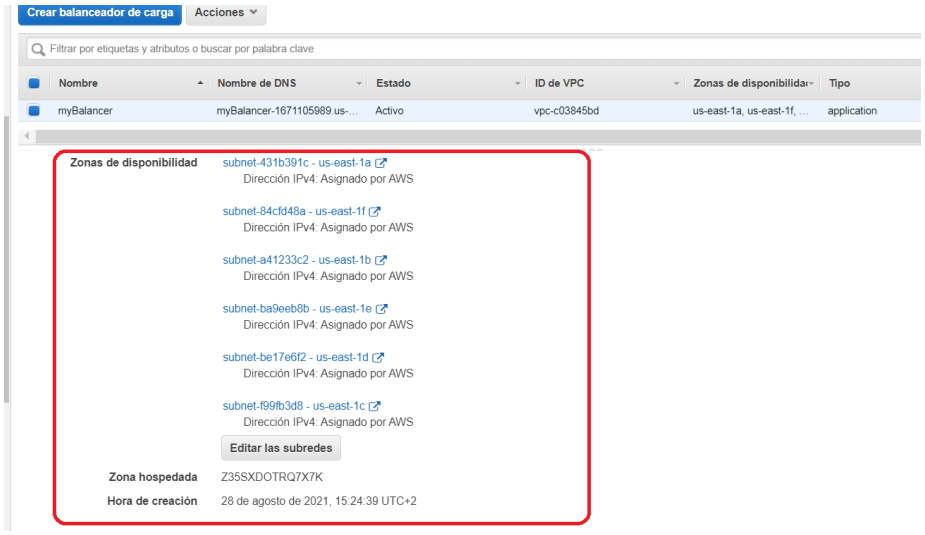


Ilustración 45 Zonas de disponibilidad

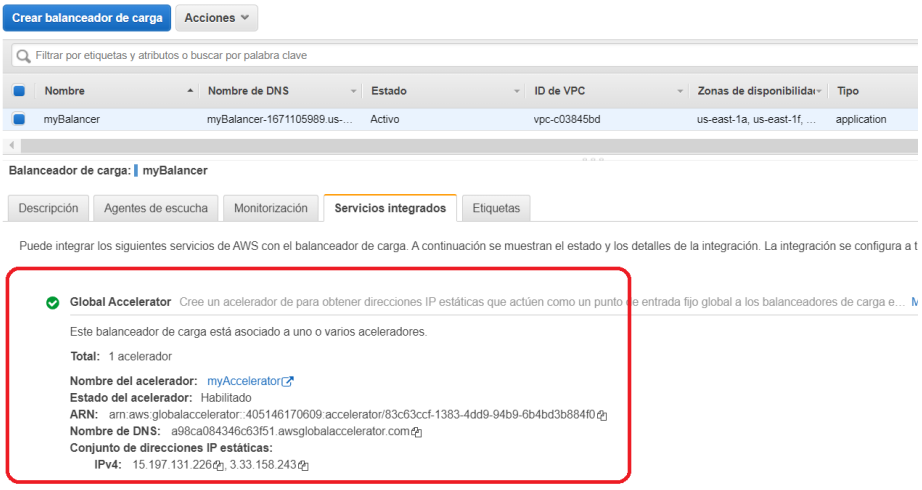


Ilustración 46 Integración del servicio Acelerador Global

- ***Sistema de copias de seguridad automáticas:*** Se configura un plan de copias de seguridad automática del recurso EC2, se designa una frecuencia semanal mientras no haya mucha afluencia al sistema. A medida que crezca el volumen de peticiones se aumentará la frecuencia. En el caso de las RDS (Base de Datos), en el momento de su creación se habilitó la opción copia de seguridad automatizada. En las siguientes ilustraciones se muestra las configuraciones aplicadas:

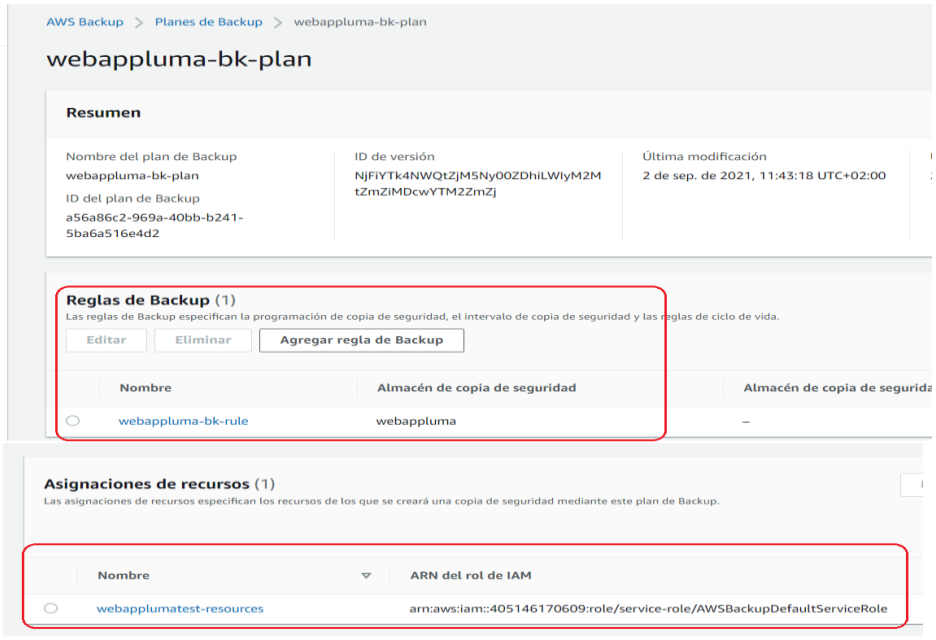


Ilustración 47 Configuración copias de seguridad automatizada instancia EC2

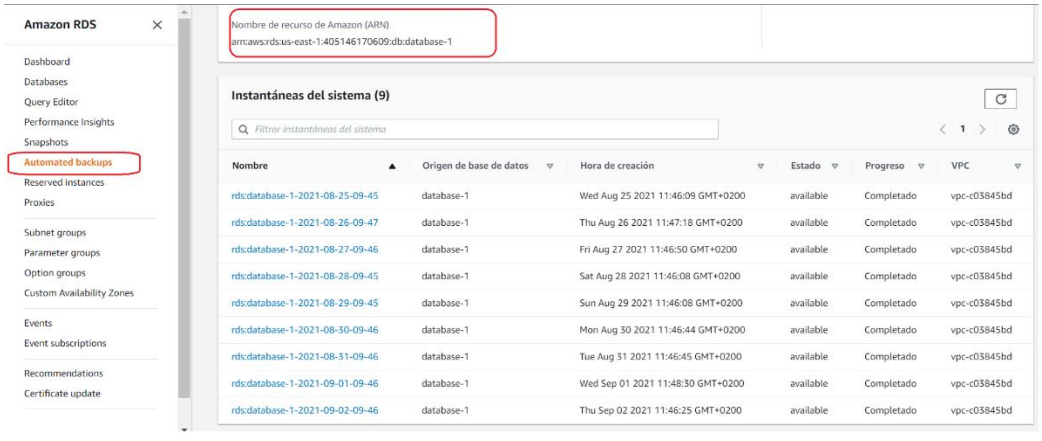


Ilustración 48 Panel de copias de seguridad instancia RDS

- ***Protección de componentes que operan en el protocolo HTTP(s):*** Una de los métodos de protección, es por medio del uso de un firewall de aplicaciones como "*AWS WAF" [43]*. Esta es una herramienta que protege contra ataques comunes, así como, monitorear y bloquear solicitudes HTTP(s) que coincidan con las reglas configurables. AWS WAF tiene compatibilidad de integración con recursos, tales como, Balanceador de carga de aplicaciones, que será el recurso sobre el que integraremos una Lista de Control de Acceso (ACL). Una de las ventajas encontradas en AWS WAF, es que posee una lista de reglas administradas por AWS, entre ellas:
  - *Core rule set:* Esta regla bloquea y previene ataques de un rango de vulnerabilidades conocidas, incluidas el Top 10 amenazas de OWASP.
  - *SQL database:* Contiene reglas que bloquean ataques de tipo inyección SQL.
  - *Known bad input:* Bloquea patrones de solicitud no válidas asociadas con ataques conocidos o descubrimiento de vulnerabilidades.
  - *Admin protection:* Evita que el atacante pueda escanear el sitio web en busca de la ruta administrador para escalada de privilegios.

  En las siguientes ilustraciones, se muestra la creación de una ACL que se integra al recurso Aplicattion Load Balancing.

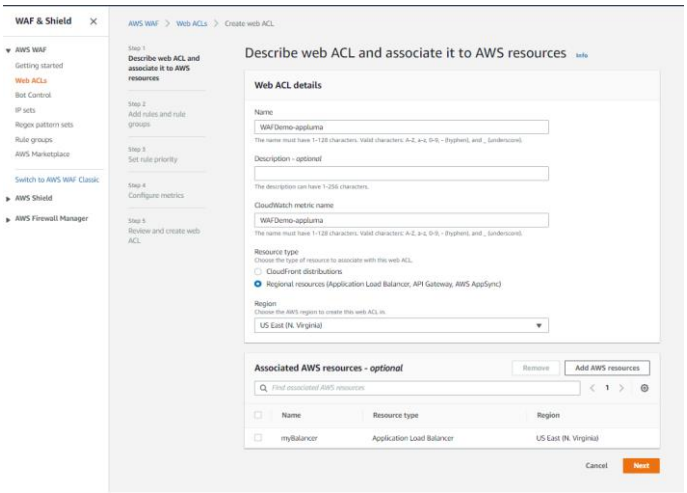


Ilustración 49 Configuración ACL asociada al recurso myBalancer

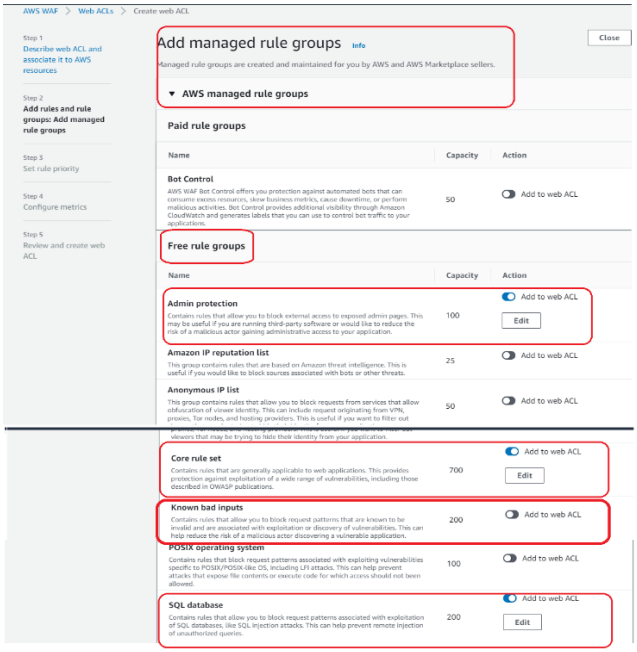


Ilustración 50 Habilitación de reglas de la capa gratuita de AWS

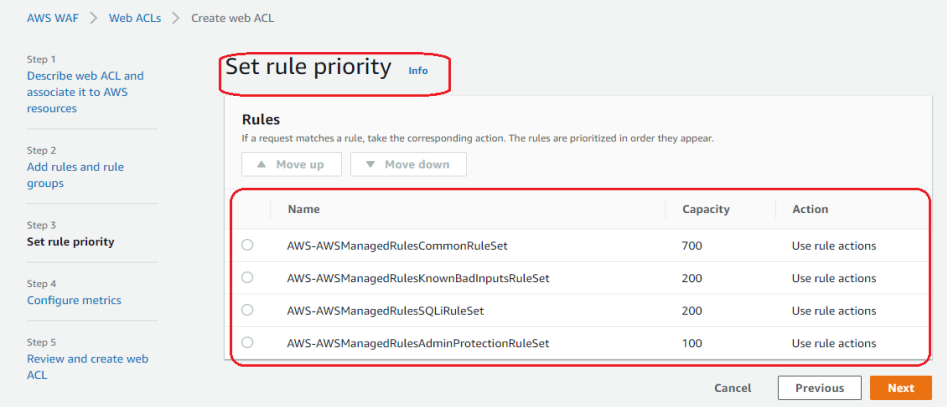


Ilustración 51 Configuración de orden de prioridad de las reglas

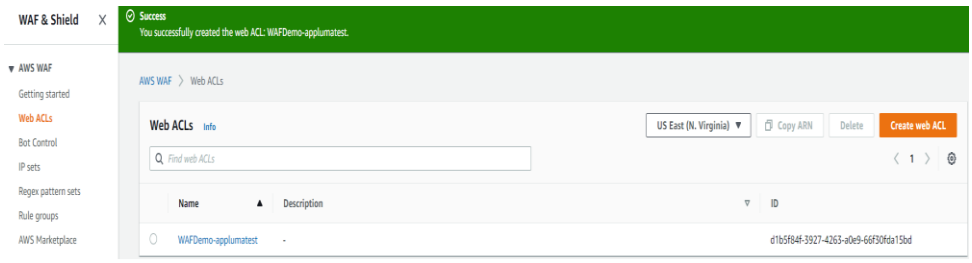


Ilustración 52 Confirmación de web ACL creada

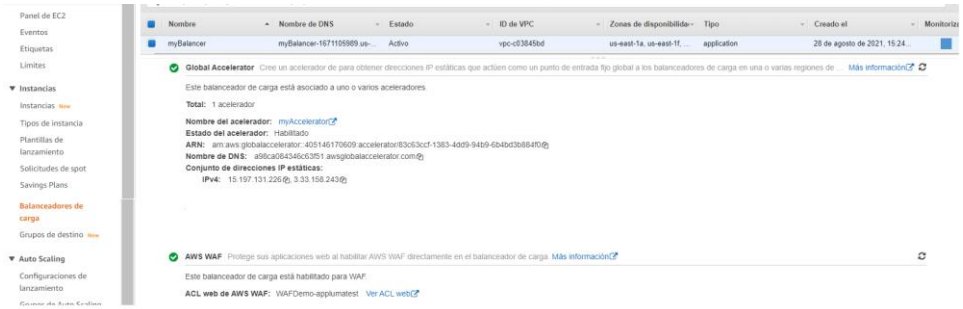


Ilustración 53 Validación de la integración de AWS WAF al recurso myBalancer

Una vez llevado a cabo el despliegue del servicio en la nube, como parte de las buenas prácticas y siguiendo las recomendaciones de Magento post instalación, se procederá a configurar / aplicar las medidas de seguridad establecidas para cada requisito de seguridad mencionados en el apartado 4.6 de esta memoria y que contribuirán a garantizar la seguridad de la aplicación.

- ***Código actualizado:*** Se hace uso de la última versión estable disponible con su parche de seguridad: *Magento 2.4.2-p1.*

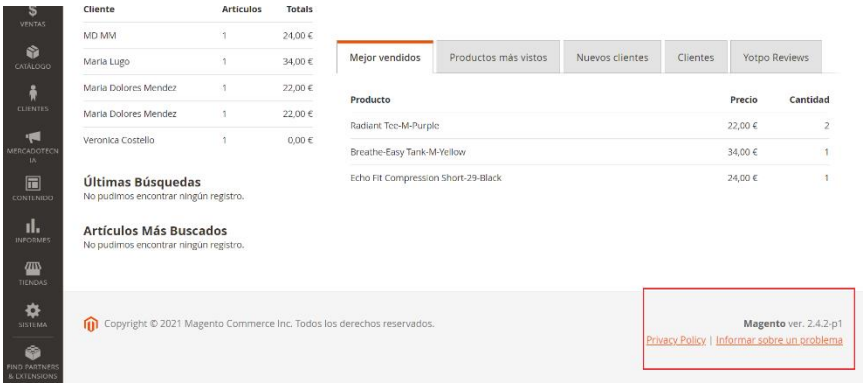


Ilustración 54 Versión estable Magento 2.4.2-p1

- ***Seguridad Panel de Control:***
  - *URL administrador:* Se hace uso del url creado por Magento de forma aleatoria, obteniendo url admin backend*: "lumatest.es/admin_jga6ep".*
  - *Habilitar Doble Factor de Autenticación "2FA": Magento dispone de varias opciones, se hace uso de Google Authenticator.*

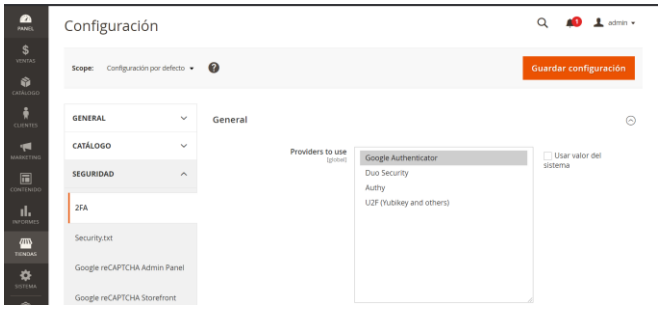


Ilustración 55 Activación de 2FA

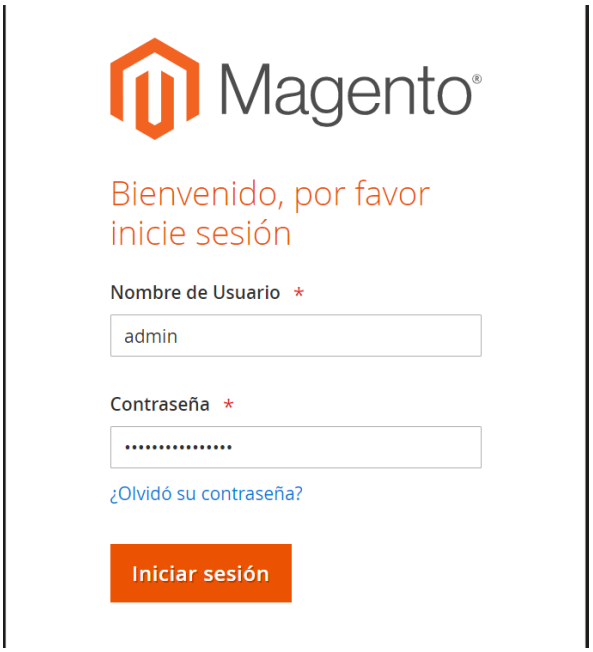


Ilustración 56 Inicio de sesión panel admin

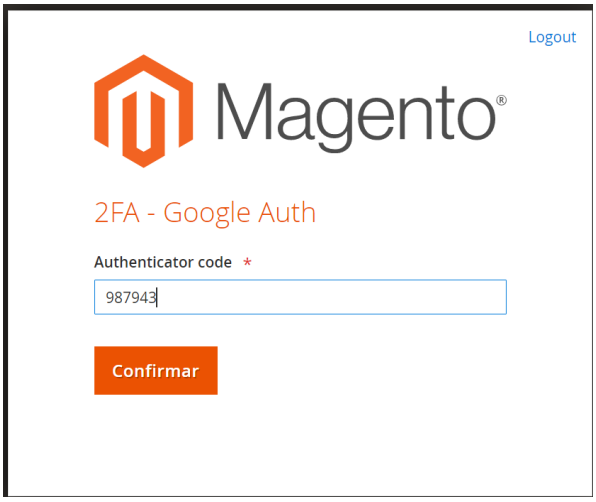


Ilustración 57 Código asignado por app Authenticator

- ***Protección de encabezado HTTP X-Frame-Option:*** Se modifica en el archivo de configuración "env.php": 'x-frame-options' => 'DENY'.

Ilustración 58 Protección encabezados x-frame-options

- ***Prevención contra ataques XSS:*** Se modifica el fichero XssProtection.php, cambiando *const HEADER_ENABLED = '1; mode=block';* por *const HEADER_ENABLED = '0';*

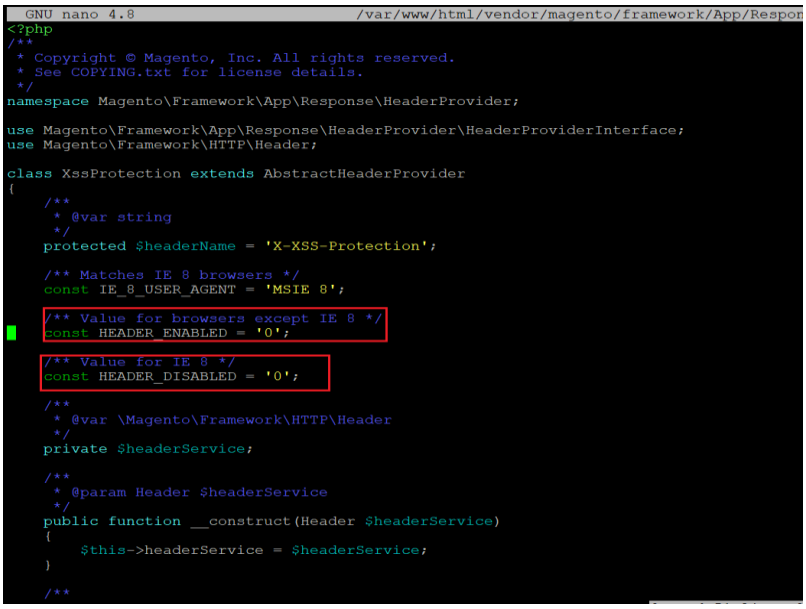


Ilustración 59 Protección ataques XSS

- ***Prevención ataques DoS y Fuerza bruta:*** Magento recomienda como medida de prevención de estos tipos de ataques, utilizar "*CAPTCHA/Google recaptcha.* Es un dispositivo visual que garantiza que un ser humano, en lugar de una computadora (o "bot"), esté interactuando con el sitio. Este método se

puede utilizar tanto para el acceso de administrador como para una variedad de acciones de escaparate iniciadas por clientes registrados.

Para el *panel admin*, se utiliza el método CAPTCHA para recuperación de contraseña y después de tres intentos fallidos de inicio de sesión, como se muestra a continuación:

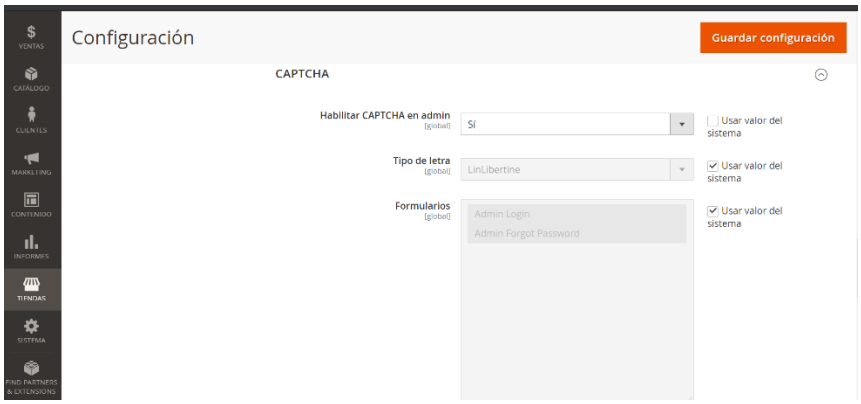


Ilustración 60 Habilitación método CAPTCHA panel admin

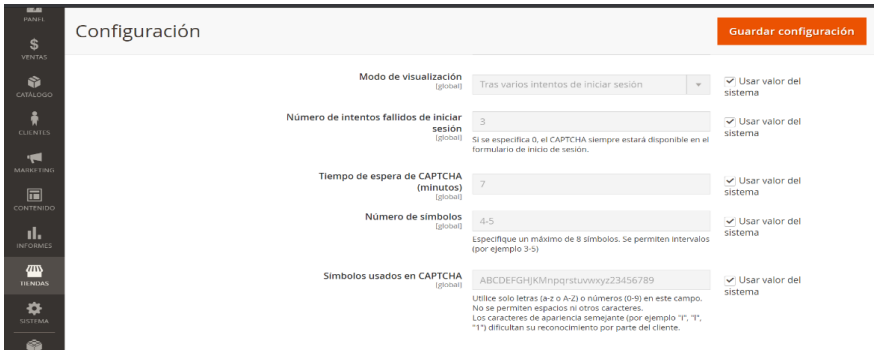


Ilustración 61 Configuración de parámetros método CAPTCHA panel admin

Ilustración 62 Ejemplo recuperación de contraseña método CAPTCHA

Habilitación de CAPTCHA de escaparate para una serie acciones del cliente:

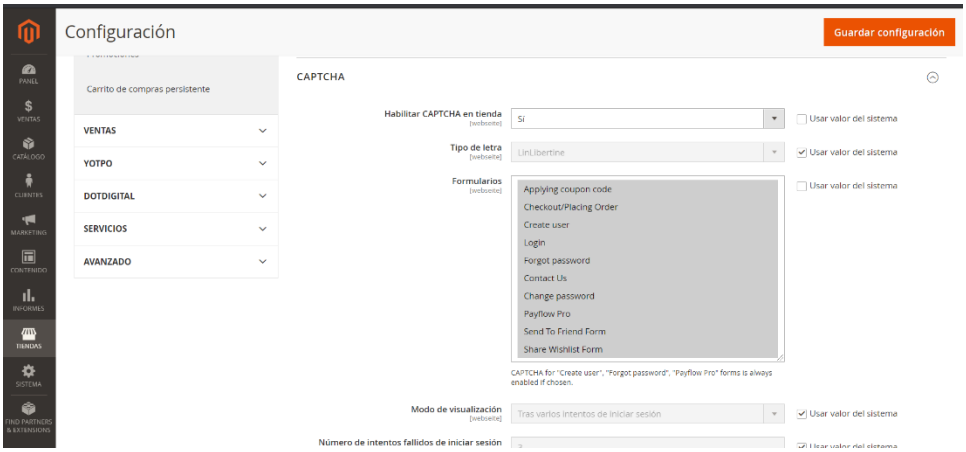


Ilustración 63 Habilitación CAPTCHA escaparate

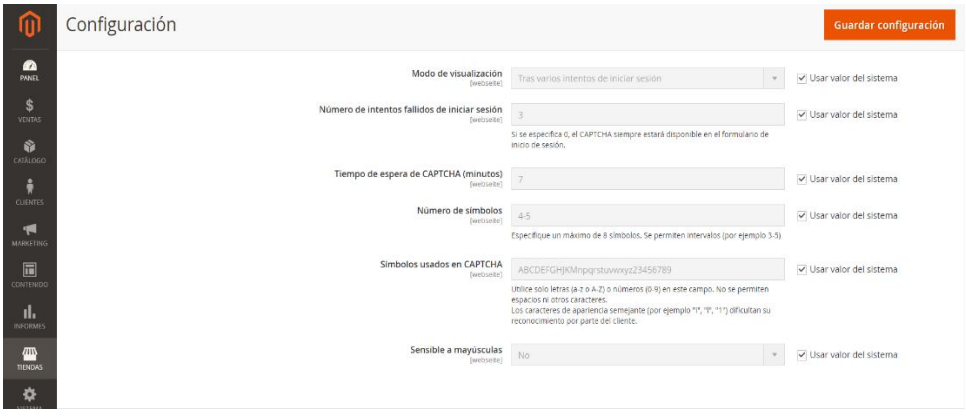


Ilustración 64 Configuración de parámetros método CAPTCHA escaparate

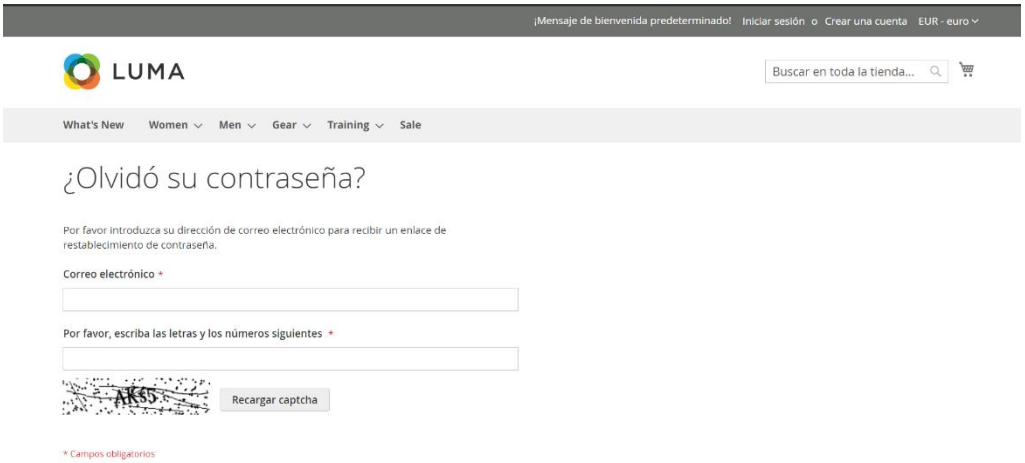


Ilustración 65 Ejemplo recuperación de contraseña método CAPTCHA

- ***Prevención secuestro de sesiones usuario:*** Magento permite validar las variables de sesión como medida de protección contra posibles ataques de fijación de sesiones o intentos de envenenar o secuestrar sesiones de usuario.

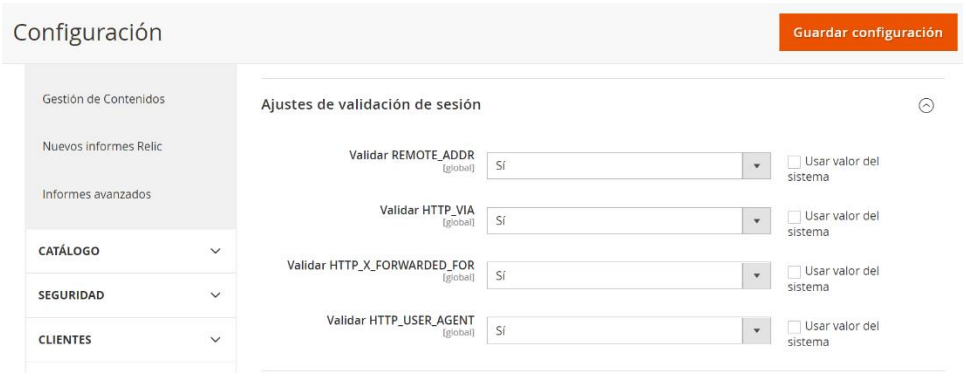


Ilustración 66 Habilitación de validación de sesión

- ***Gestión de Cookies:*** Las cookies son pequeños archivos que se guardan en la computadora de cada visitante del sitio web y se utilizan como lugares de almacenamiento temporal. Aunque la Ley de Proteccion de Datos en Nicaragua no obliga un consentimiento expreso para la recopilación de este tipo de datos, como propuesta de mejora, se toma de referencia la LOPDGDD que establece el consentimiento expreso. Por tanto, se habilita el modo de restricción de cookies.

Ilustración 67 Habilitación de cookies modo restrictivo

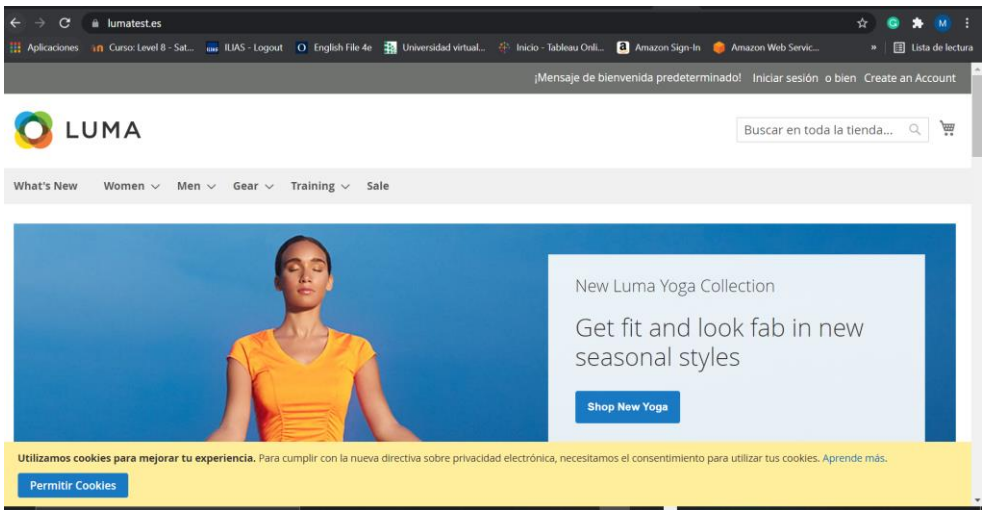


Ilustración 68 Notificación de confirmar cookies al acceder al url "https://lumatest.es"

- ***Protección de datos sensibles:*** Con el objetivo de proteger los datos sensibles para el usuario como lo es el método de pago, se hace uso de un plugin de pasarela de pago. Dicha pasarela de pago, se encargará de enlazar con la entidad bancaria quien será la responsable del tratamiento y protección de estos datos. La pasarela utilizada como método de prueba para la aplicación que es objeto de estudio es "*Stripe Mode Demo*".

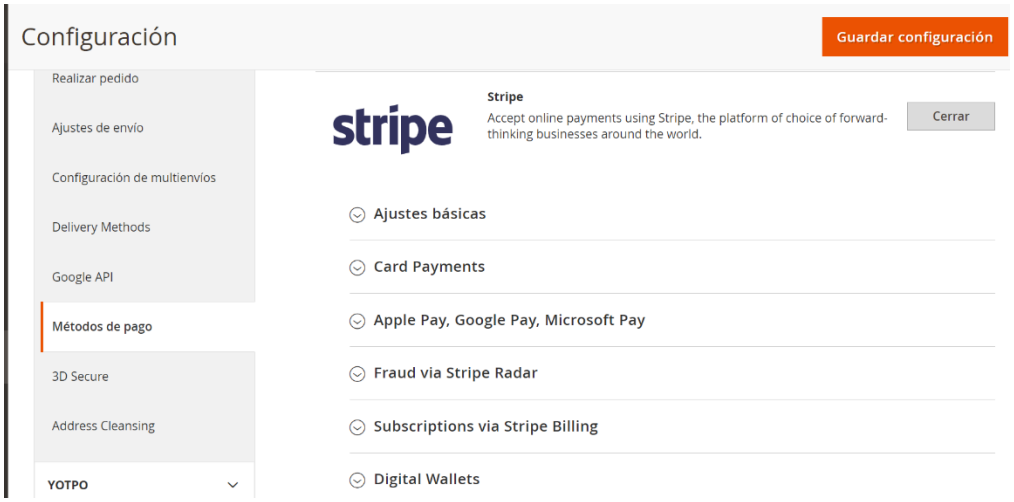


Ilustración 69 Configuración plugin de pasarela de pago

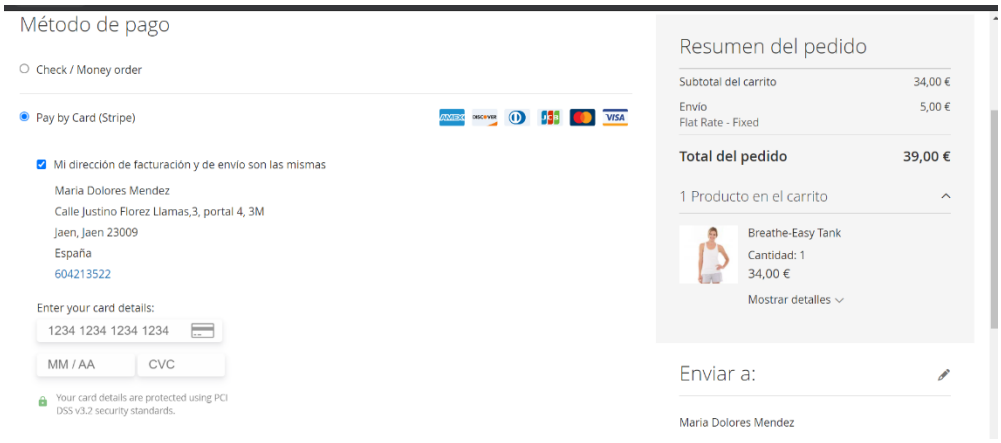


Ilustración 70 Pasarela de pago Stripe

- ***Seguridad Panel admin:*** Parte de las recomendaciones de Magento, es gestionar una buena configuración de seguridad del panel admin. Por tanto, se configuran los siguientes parámetros:
  - Medio para recuperación de contraseña: correo electrónico.
  - Número máximo de solicitudes de restablecer contraseña: 3.
  - Duración de la sesión del administrador: 180 segundos.
  - Número de intentos fallidos de inicio de sesión: 3.
  - Tiempo de vida de la contraseña (días): 90.

Ilustración 71 Configuración seguridad panel admin

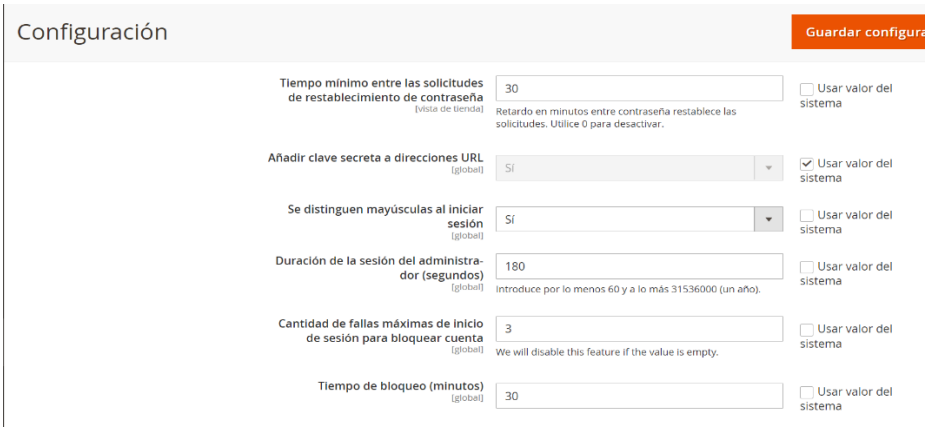


Ilustración 72 Configuración seguridad panel admin (parte 2)

Ilustración 73 Configuración seguridad panel admin (parte 3)

- ***Informe de problemas de seguridad:*** Magento dispone del servicio “Informe de problemas de seguridad”, siendo este de gran utilidad ante alguna incidencia de seguridad que pueda presentarse en la aplicación. Consiste en un archivo “txt” que contiene información de contacto, entre otros datos y que puede utilizarse como un canal para informar a los investigadores acerca de problemas de seguridad sobre el sitio.

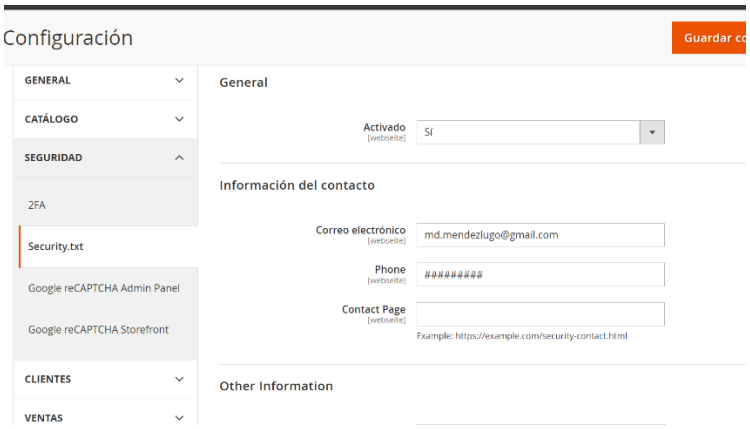


Ilustración 74 Habilitación informe de seguridad

- ***Monitorización:*** Parte de las recomendaciones de buenas prácticas, es tener una visión de los eventos que se generan en el sistema que nos permita anticiparnos para tomar medidas correctivas de forma proactiva y ágil. AWS dispone de una variedad de recursos para monitorizar el estado de los servicios, (eg. EC2), dispone de su propia herramienta de monitoreo para evaluar el uso de recursos del sistema y monitoreo de peticiones, como se muestra en la ilustración 75.

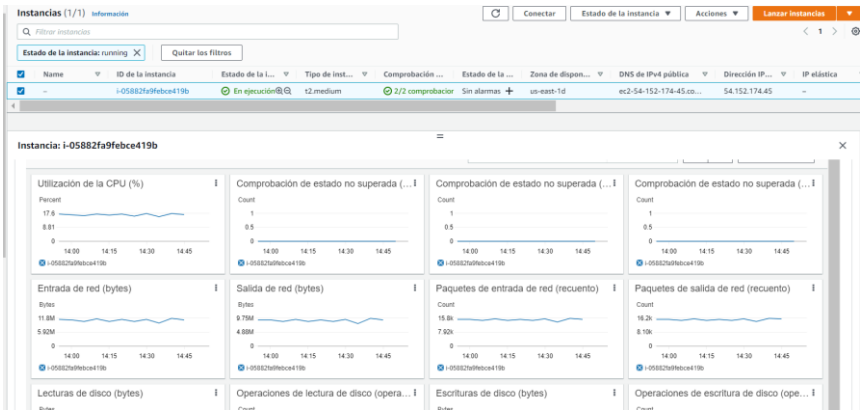


Ilustración 75 Panel de monitoreo EC2

También, dispone de herramientas de monitoreo como Amazon GuardDuty [44], que identifica actividades inesperadas y potencialmente no autorizadas y maliciosas dentro del entorno de AWS. Este servicio tiene un costo adicional para su utilización, por lo que no pudo ser utilizado en el entorno de prueba, sin embargo, se recomienda hacer uso de este servicio. En la ilustración 76, muestra un ejemplo del tipo de análisis que realiza esta herramienta.

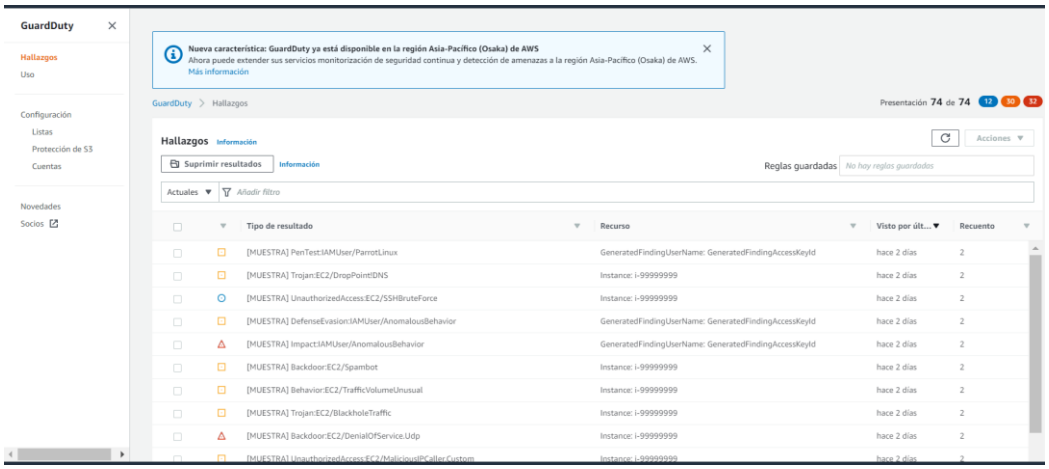


Ilustración 76 Panel de hallazgos Amazon GuardDuty

5.2 Análisis de coste operativo

Para la estimación económica se hace uso de la herramienta online proporcionada por el proveedor de servicios en AWS[2], así como, proveedor de nombre de dominio IONOS[3], en ella se agregan los servicios necesarios para la implementación inicial. En la tabla 5 y 6 se detallan los recursos con características básicas para el buen funcionamiento de la aplicación.

[2] Fuente: https://calculator.aws/#/
[3] Fuente: https://www.ionos.es/

Estimación de costo por servicio AWS				
Descripción	***Servicio***	***Divisa***	***Mensual***	***Resumen de configuración***
Instancia EC2	Amazon EC2	USD	62,1066	SO (Linux), Almacenamiento SSD (80 GB), Carga de trabajo (Monthly, Punto de referencia: 1, Punto máximo: 2, Duración del pico: 3 Día 0 Hr 0 Min), Frecuencia de instantáneas (Semanal), Cantidad cambiada por instantánea (3 GB), Instancia EC2 (t2.large) 2vCPU – 8GB RAM.
RDS Base de Datos	Amazon RDS for MariaDB	USD	210,10	Volumen de almacenamiento (SSD de uso general (gp2)), Almacenamiento (40 GB al mes), Cantidad (1), Tipo de instancia (db.t2.large ”2vCPU – 8GB RAM”), Implementación (Multi-AZ), Almacenamiento copias de seguridad adicional (40 GB).
Route 53 hostedzone	Amazon Route 53	USD	0,9	Zonas alojadas (1)
Load Balancing Aplication	Application Load Balancer	USD	22,27	Número de balanceadores de carga de aplicaciones (1)
WAF	AWS Web Application Firewall	USD	9,6	Número de listas de control de acceso web (ACL web) utilizadas (1 por mes), Número de reglas agregadas por ACL web (4 por mes)
GuardDuty	Amazon GuardDuty	USD	4,00	Análisis de eventos de administración de AWS CloudTrail (1 millones por mes)
Amazon Inspector	Amazon Inspector	USD	1,8	Primeros 90 días Gratis. Estimación de 4 evaluaciones al mes. Evaluación de host: 0,30 USD por evaluación, Capacidad de alcance de red: 0,15 USD por evaluación.
Coste Total Mensual		**USD**	310,77	
		EUR	261,87	

Tabla 5 Estimación de costo de operación

Estimación de costo registro de nombre de dominio IONOS		
Dominio	**Divisa**	**Anual**
lumatest.com	USD	1 (Primer año)
	USD	15 (Siguiente año)

Tabla 6 Estimación de costo registro nombre de dominio

* Según la propia herramienta los costes operativos en el proveedor de servicio AWS son una estimación y pueden estar sujetos a cambios.

6.- **EVALUACIÓN DE LA SEGURIDAD**

En este apartado se llevará a cabo una evaluación de las medidas de seguridad aplicadas en el capítulo 5 y los resultados obtenidos.

6.1 Técnicas y herramientas

La importancia de auditar una aplicación nos permite identificar el estado de salud del sistema, las vulnerabilidades, amenazas a las que puede estar expuesto para poder agilizar el proceso en la toma de decisiones y aplicar las medidas correctivas necesarias.

Existen diferentes tipos de pruebas a la hora de evaluar una aplicación, entre ellas, las pruebas dinámicas de seguridad de aplicaciones DAST es un método de **"prueba de caja negra"**. Este tipo de prueba se basa en torno a la introducción de fallos para probar la funcionalidad de código en una aplicación al ser ejecutada. Además, detecta otros tipos de fallos como defectos de autenticación, control de acceso, etc.

Para llevar a cabo la auditoría de la aplicación que es objeto de estudio, realizaremos una auditoría dinámica a través del uso de herramientas propias de Magento y AWS, así como, herramientas de análisis de terceros.

Las herramientas que se harán uso para realizar un análisis de la aplicación son:

- ***Magento Scan Security Tool [45]:*** Esta herramienta realiza un análisis para detectar riesgos de seguridad conocidos, malware, y recibir actualizaciones de parches y notificaciones de seguridad. Esta herramienta se encuentra disponible de forma gratuita, y permite programar el análisis de seguridad para se ejecute diariamente, semanalmente o bajo demanda.
- ***Análisis de arquitectura – Amazon Inspector [46]:*** Parte de la seguridad de una aplicación es analizar la arquitectura donde se ejecuta el sistema. AWS dispone del servicio Amazon Inspector que comprueba la accesibilidad de red de las instancias EC2 y el estado de seguridad de las aplicaciones que se ejecutan en dichas instancias. También, evalúa la exposición, vulnerabilidades y las desviaciones de las prácticas recomendadas de las aplicaciones. El uso

de este servicio tiene un costo adicional, sin embargo, dispone de un periodo de prueba de 90 días gratis.

- ***Zed Attack Proxy (ZAP) [47]:*** Es una herramienta gratuita para prueba de penetración (Pentesting) se mantiene bajo la cubierta de OWASP. Permite realizar escaneo de forma activa y pasiva para encontrar algunas vulnerabilidades y como una forma de tener una idea del estado de seguridad básico de una aplicación web.

6.2 Resultados de evaluación

Primeramente, se realizó un análisis a la arquitectura donde se ejecuta el sistema a través de la herramienta Amazon Inspector, dicho análisis tuvo una duración de 1 hora, tiempo recomendado por el proveedor. Se obtiene los siguientes resultados del análisis:

En la ilustración 75, muestra el panel principal con un breve resumen de los hallazgos notables, estado de la evaluación y las últimas evaluaciones recientes.

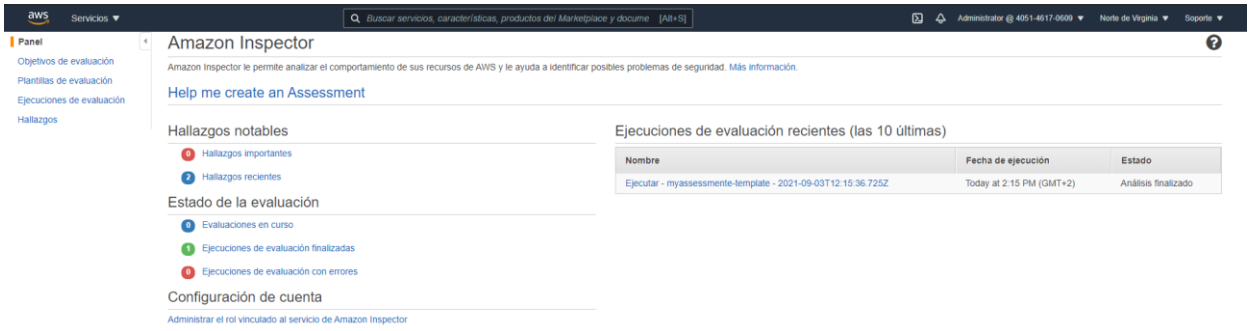


Ilustración 77 Panel principal Amazon Inspector

En la ilustración 76 se obtiene un resumen de los hallazgos encontrados, el nivel de gravedad y el tipo de vulnerabilidad detectada.

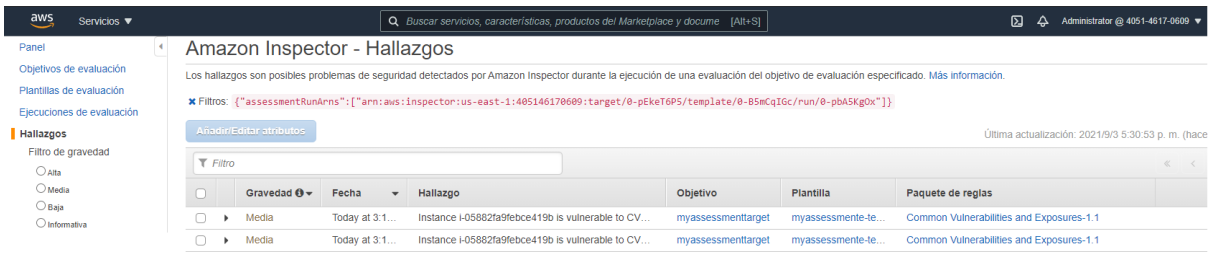


Ilustración 78 Panel Hallazgos

Amazon Inspector te permite obtener mayor información acerca del hallazgo encontrado seleccionándolo, también, puedes descargar un informe PDF. En las ilustraciones 77 y 78 detalla información cómo el número de CVE de las vulnerabilidades encontrada en la EC2, el nivel de gravedad, una breve descripción del tipo de vulnerabilidad y recomendaciones para solventarlo.

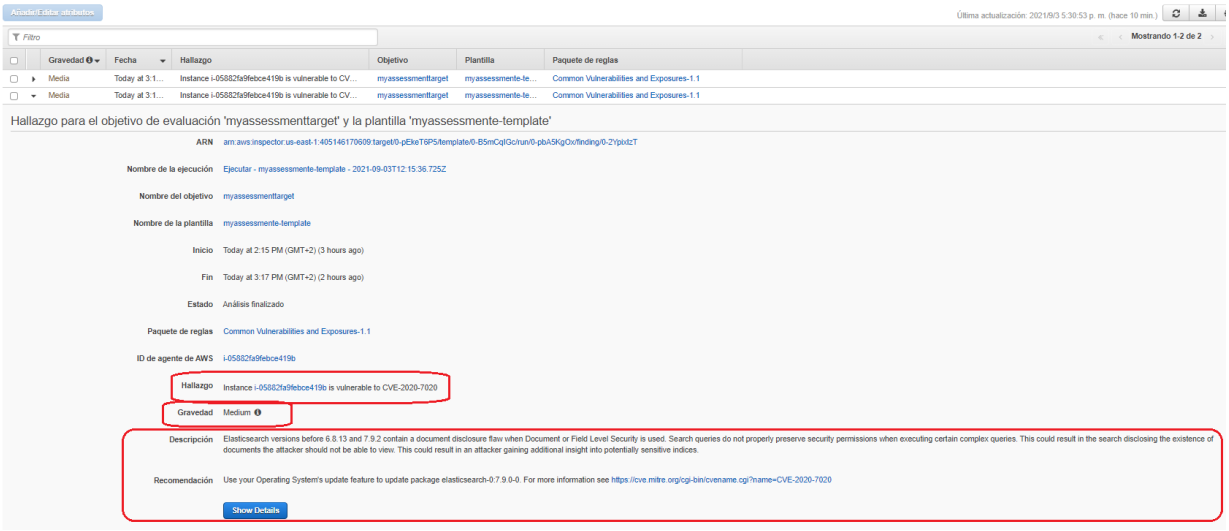
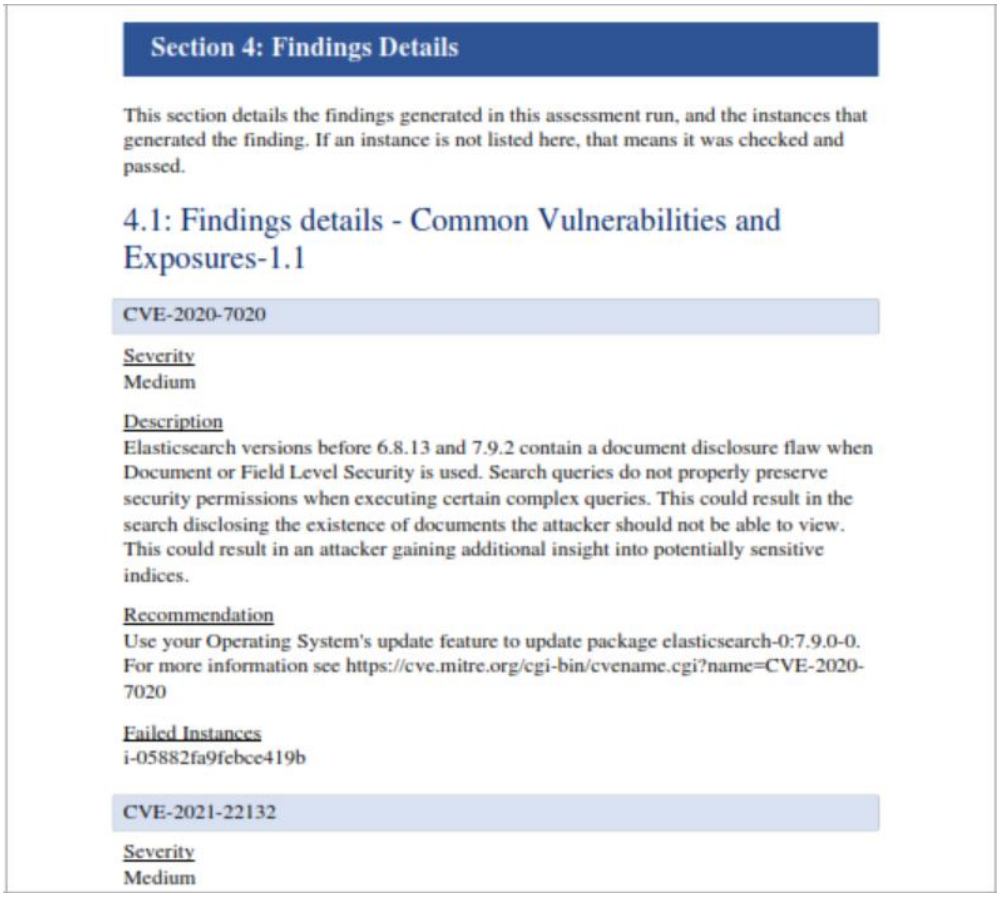


Ilustración 79 Información del tipo de hallazgo y recomendaciones para solventar



Section 4: Findings Details

This section details the findings generated in this assessment run, and the instances that generated the finding. If an instance is not listed here, that means it was checked and passed.

4.1: Findings details - Common Vulnerabilities and Exposures-1.1

CVE-2020-7020

Severity
Medium

Description
Elasticsearch versions before 6.8.13 and 7.9.2 contain a document disclosure flaw when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries. This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

Recommendation
Use your Operating System's update feature to update package elasticsearch-0:7.9.0-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7020

Failed Instances
i-05882fa9febce419b

CVE-2021-22132

Severity
Medium

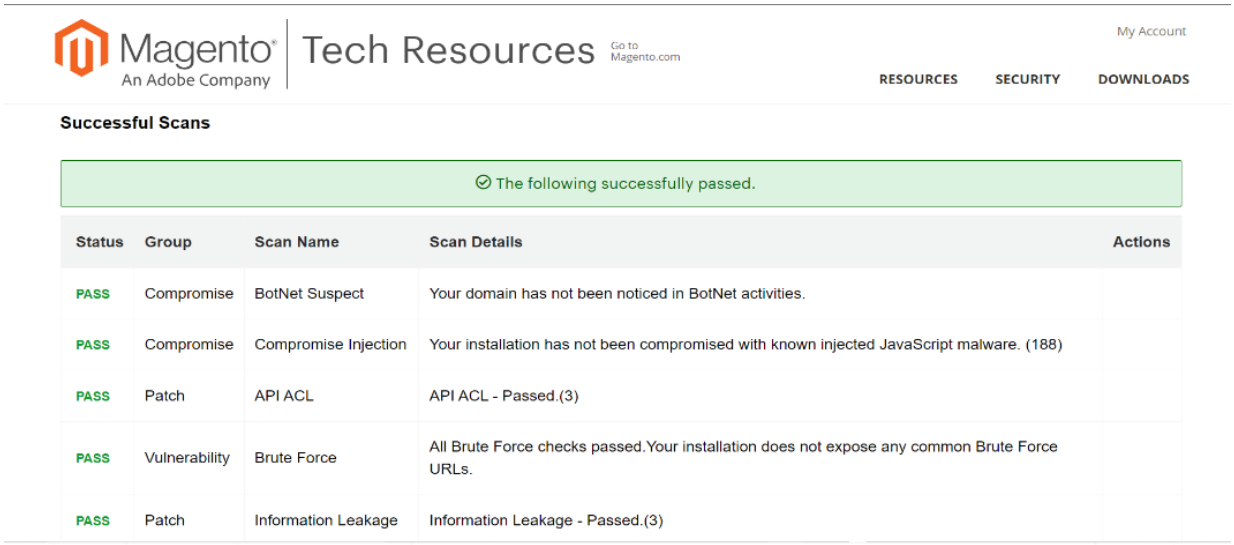
Ilustración 80 Ejemplo de resultados del Informe PDF

Las vulnerabilidades de severidad media encontradas describen problemas en las versiones de Elasticsearch anteriores a la 6.8.13 y 7.9.2 con ID CVE-2020-7020 [48], estas no conservan correctamente los permisos de seguridad al ejecutar determinadas consultas complejas ocasionando divulgación de documentos y las versiones de Elasticsearch 7.7.0 a 7.10.1 con ID CVE-2021-22132 [49], las consultas de búsqueda asíncrona almacenan incorrectamente los encabezados HTTP ocasionando divulgación de información en la API de búsqueda asíncrona.

Recomendaciones: Una medida para mitigar esta vulnerabilidad es actualizar la versión de Elasticsearch a una versión superior a la 7.9.0, versión utilizada para la implementación del entorno de prueba. Por lo tanto, se recomienda en mantenimientos futuros realizar actualización del paquete. Dado que el sistema no es accesible desde el exterior se dificulta que la vulnerabilidad pueda llegar a explotarse.

Posterior al análisis de arquitectura con la herramienta Amazon Inspector se ejecutó el análisis al sitio Magento con la herramienta *Security Scan de Magento*. El tipo de vulnerabilidades en general que ha estudiado la herramienta y

que podemos mencionar, por ejemplo, que no esté en una botnet, que no tenga extensiones vulnerables o compromisos frente a inyección, que no presente extensiones vulnerables. En la ilustración 81 muestra los resultados siendo satisfactorios.



Status	Group	Scan Name	Scan Details	Actions
PASS	Compromise	BotNet Suspect	Your domain has not been noticed in BotNet activities.	
PASS	Compromise	Compromise Injection	Your installation has not been compromised with known injected JavaScript malware. (188)	
PASS	Patch	API ACL	API ACL - Passed.(3)	
PASS	Vulnerability	Brute Force	All Brute Force checks passed.Your installation does not expose any common Brute Force URLs.	
PASS	Patch	Information Leakage	Information Leakage - Passed.(3)	
PASS	Vulnerability	JS Libraries	Outdated JS Libraries - Passed.(2)	
PASS	Vulnerability	Base /pub/	Your Web server is configured to run Magento from %MAGENTO_ROOT%/pub	
PASS	Patch	RCE Vulnerability	No known RCE Vulnerability found (200)	
PASS	Vulnerability	Unprotected XML	Your installation's configuration files are protected.	
PASS	Vulnerability	Vulnerable Extensions	Vulnerable Extensions - Not found	
PASS	Vulnerability	SSL Basic	Your server uses a valid SSL certificate and SSL chain certificate.	
PASS	Vulnerability	SSL Frontend	All secure URL checks passed. Your installation uses SSL for secure URLs.	
PASS	Vulnerability	Full Time SSL	Your installation appears to redirect all unsecured traffic to HTTPS.	
PASS	Vulnerability	Full Time SSL	Your installation appears to redirect all unsecured traffic to HTTPS.	
PASS	Vulnerability	SSL TLS	Your server does not support TLSv1.0.	
PASS	Vulnerability	Unprotected VCS	Your VCS folder is protected/.git/config /.hg/requires /.svn/entries	
PASS	Compromise	Visbot Malware	'Visbot' malware was not detected on your installation.	

Ilustración 81 Análisis Scan Security Magento

Análisis de pentesting con ZAP (OWASP): El tipo de análisis de vulnerabilidad realizado con esta herramienta fue un escaneo automático que combina ataques de fuerza bruta, este tipo de pruebas son altamente intrusiva. La primera acción que ejecutará el escáner activo es el spider/araña cuyo objetivo es identificar todos los recursos referenciados en el dominio, es importante destacar que en función de las dimensiones del dominio el tiempo empleado con este proceso puede variar significativamente. El tiempo de análisis spider ejecutado para la identificación de recursos referenciados fue de 48 horas con un porcentaje de escaneo del 58%. En la ilustración 82 podemos observar estado de la prueba.

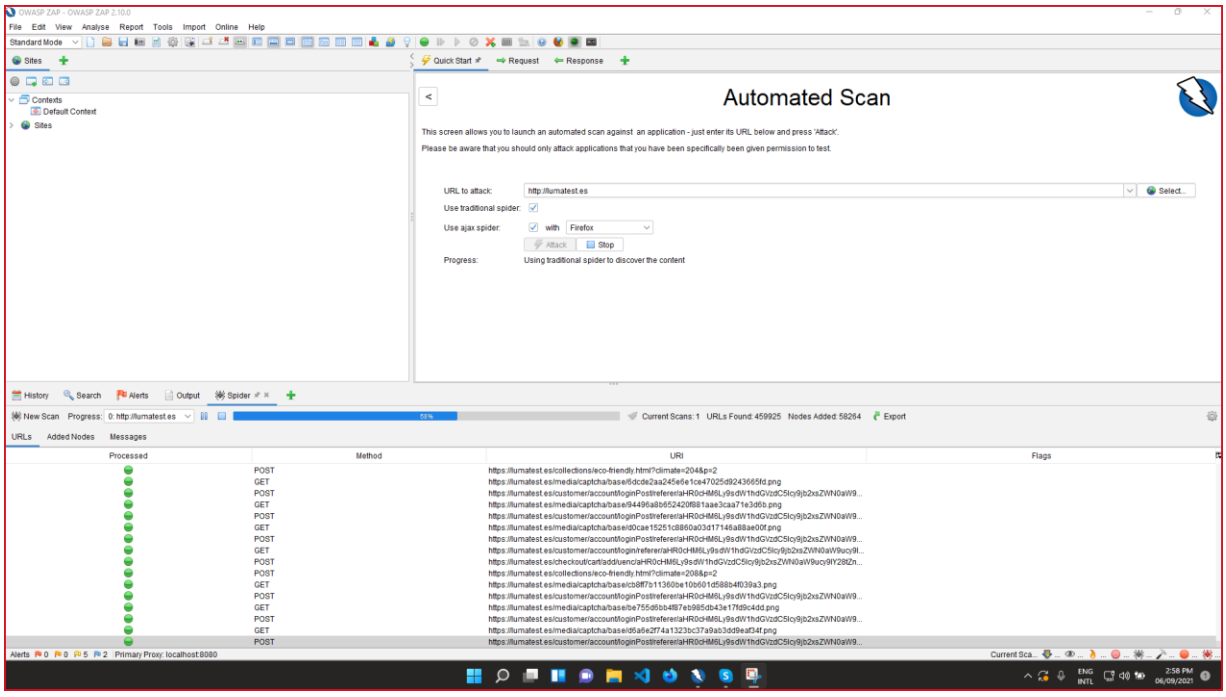
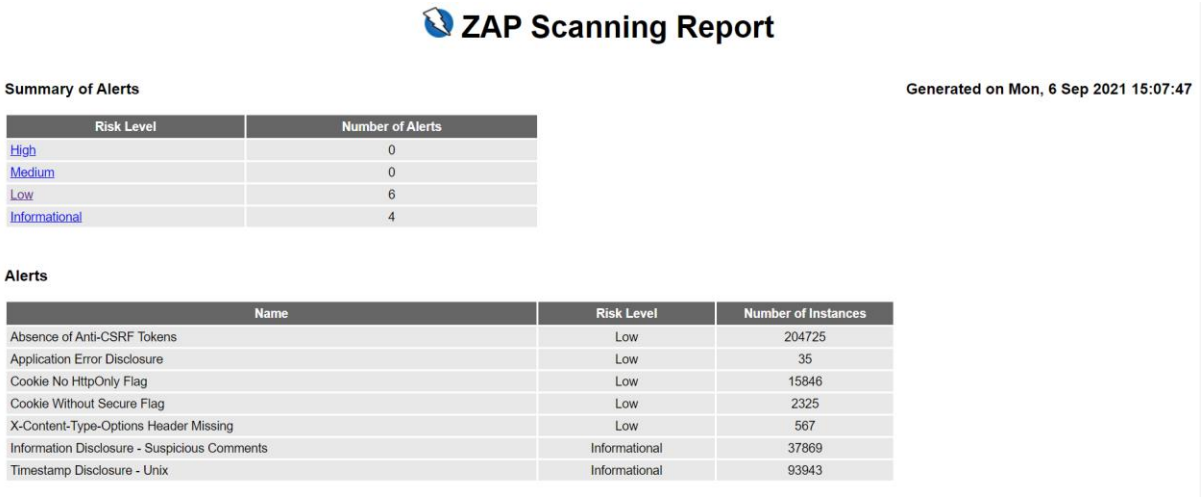


Ilustración 82 ZAP OWASP - Progreso del análisis

Transcurrido un periodo de 48 horas se forzó la finalización del proceso, posteriormente comenzó a realizar múltiples test de seguridad a medida en función de las tecnologías y recursos detectados, una vez finalizado los test de seguridad se obtiene un informe “ZAP Scanning Report” de las vulnerabilidades identificadas y categorizadas por criticidad que será anexado a la memoria.

Los resultados obtenidos en el informe muestra 6 alertas de nivel bajo como se muestra en la ilustración 83 y que procederemos a analizar cada una de ellas.



ZAP Scanning Report

Summary of Alerts

Generated on Mon, 6 Sep 2021 15:07:47

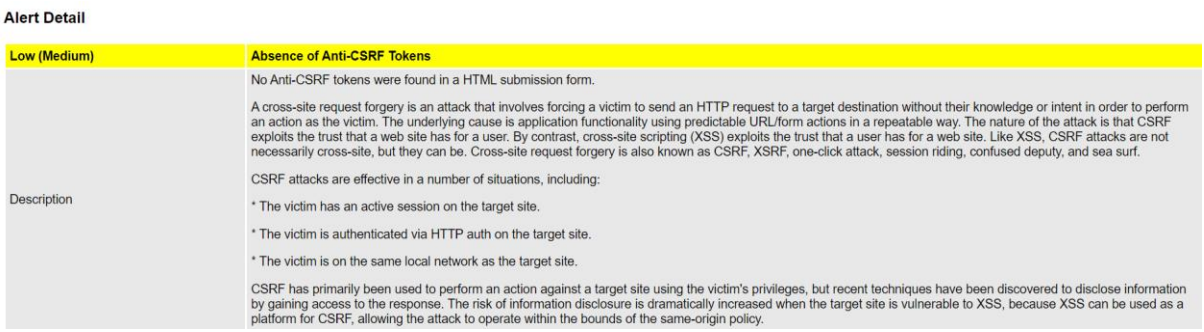
Risk Level	Number of Alerts
High	0
Medium	0
Low	6
Informational	4

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Low	204725
Application Error Disclosure	Low	35
Cookie No HttpOnly Flag	Low	15846
Cookie Without Secure Flag	Low	2325
X-Content-Type-Options Header Missing	Low	567
Information Disclosure - Suspicious Comments	Informational	37869
Timestamp Disclosure - Unix	Informational	93943

Ilustración 83 Informe ZAP - Resumen

Ausencia de Anti-CSRF Tokens: Las primeras dos vulnerabilidades detectadas hace referencia a la ausencia de tokens Anti-CSRF en formulario HTML, ilustración 84. Una forma de mitigar este tipo de vulnerabilidad es a través del método Synchronizer Token Pattern mediante la generación de un token una vez por sesión de usuario o para cada solicitud o mediante el cifrado basado en Token Pattern[4]. Se aplica la configuración correcta para solventar vulnerabilidad como se muestra en la ilustración 85.



Alert Detail

Low (Medium)	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Ilustración 84 Información de vulnerabilidad encontrada

[4] Fuente: https://devdocs.magento.com/guides/v2.4/extension-dev-guide/security/csrf.html

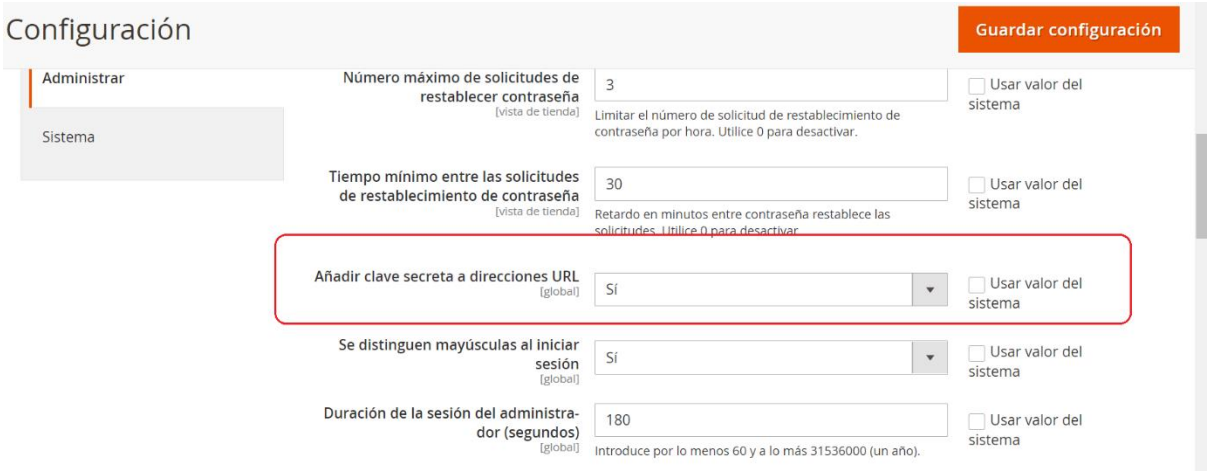


Ilustración 85 - Añadir token a direcciones url

Cookie No HttpOnly Flag: Esta vulnerabilidad indica que las cookies fueron configuradas sin el indicador HTTPOnly. Se considera este tipo de alarma como un falso positivo, ya que fue previamente configurado, queda constancia en el apartado 5, ilustración 67 de esta memoria. En la ilustración 86 muestra información de la alarma.

Low (Medium)	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://lumatest.es/men/tops-men/tanks-men.html?material=38
Method	POST
Parameter	private_content_version

Ilustración 86 Alarma Cookie No HttpOnly Flag

Falta el encabezado X-Content-Type-Options: Este tipo de vulnerabilidad permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que podría hacer que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido distinto del tipo de contenido declarado, en la ilustración 87 podemos ver detalles de la alarma. Una forma de mitigar es establecer el encabezado Content-Type de manera adecuada, por lo que, se procedió a habilitar Magento a "*mode: production"* cómo se muestra en la ilustración 88 con el objetivo de optimizar cache y ver si insertaba las cabeceras de seguridad. Se recomienda dar seguimiento a la solución aplicada con el objetivo de validar el correcto funcionamiento.

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and

Ilustración 87 Alarma X-Content-Type-Options Header Missing

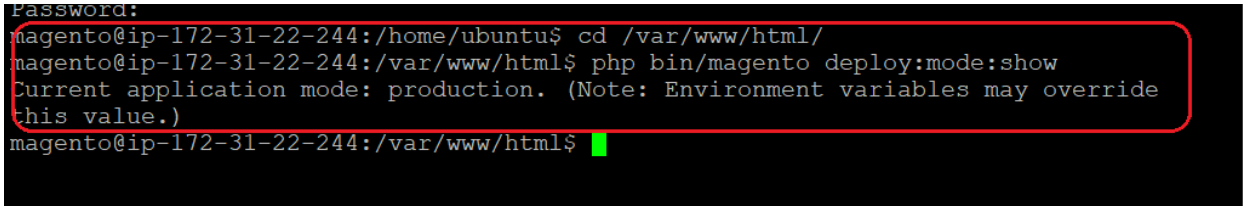


Ilustración 88 - Habilitación Magento mode: production

El uso de estas herramientas de análisis de vulnerabilidades y fuerza bruta nos permite poder obtener una visión del alcance de las medidas de seguridad aplicadas. Lo que nos indica que la seguridad debe de permanecer en constante evaluación y cuán importante es la concientización de ella a nivel organizativo.

7.- **CONCLUSIONES**

En este apartado se valorará el trabajo realizado y el nivel de cumplimiento de los objetivos propuestos.

Con la realización de este proyecto se ha podido validar la importancia de planificar de forma previa y hacer un estudio de cómo el uso de plataformas ya desarrolladas y albergar estos servicios en infraestructura de terceros puede influir en el ciclo de vida del sistema.

Tras hacer un estudio y familiarizarse con las competencias habituales de los responsables de seguridad de diferentes proveedores de servicio en la nube, así como, plataformas ya desarrolladas para el comercio electrónico se considera que, Magento y AWS, brindan una amplia gama de funcionalidades incluyendo aspectos de seguridad que nos permitió tomar la decisión de hacer uso de ellos. En adición, se ha podido validar que realización de un estudio de la legislación aplicable, así como un análisis de posibles amenazas a los que se podría enfrentarse el servicio nos permitió poder clasificar las dimensiones del sistema y determinar su categoría de según el ENS de nivel “ALTO” respecto a sus requisitos de seguridad. A su vez, esto ha facilitado aplicar las medidas necesarias según los estándares de seguridad como parte de las buenas prácticas recomendadas.

Después de llevar a cabo una implementación de entorno de pruebas se considera que los servicios seleccionados y aplicando las medidas de seguridad y buenas prácticas propuestas se han alcanzado los objetivos dando como resultado un servicio de tienda virtual con un nivel razonable de seguridad.

Estas medidas propuestas son solo el punto de partida, la seguridad del sistema debe continuar evaluándose y mejorándose periódicamente a lo largo de su vida, siguiendo las recomendaciones de buenas prácticas, una organización adecuada por parte del personal, dar seguimiento a las alertas de seguridad de los proveedores, etc.

Cabe señalar que los servicios seleccionados para la implementación, a pesar de la gran gama de funcionalidades de que disponen, y que los hace resaltar de los demás, se han podido identificar pequeños inconvenientes. Por ejemplo, la política de seguridad de AWS es tan restrictiva que llega a tornarse un poco compleja poder

integrar los diferentes recursos que dispone ya que para cada uno de ellos deben de configurarse políticas y reglas asociadas a la cuenta para poder hacer uso de dichos recursos. Sin embargo, en algunos casos esta información no se encuentra disponible en la documentación, provocando que la curvatura de aprendizaje del uso de los servicios sea un poco más lenta o teniendo que recurrir al servicio de soporte. Del mismo modo, Magento dispone de una gran cantidad de documentación para el proceso de instalación y configuración, pero, al igual que en el caso anterior, se pudo experimentar durante el proceso de instalación algunas configuraciones adicionales que no están disponibles en su documentación o se encuentran dispersas sin una lógica de proceso de instalación.

Referente a la utilidad de las herramientas de evaluación de seguridad propuestas, podemos mencionar algunas ventajas e inconvenientes encontrados. Con respecto a la herramienta que dispone Magento podemos mencionar como características positivas, es su facilidad de uso, herramienta gratuita, sin embargo, el tipo de análisis de vulnerabilidad que realiza es limitado. AWS Inspector tiene como ventaja su facilidad de uso, también, es una herramienta dedicada al análisis propio de la accesibilidad de red de la instancia EC2 y de las aplicaciones que se ejecutan sobre esa instancia. Un aspecto negativo de esta herramienta es que es de pago, su precio dependerá del número de evaluaciones realizadas. En referencia a la herramienta ZAP se caracteriza por ser robusta, muy reconocida ante la comunidad de ciberseguridad, gratis, dispone de documentación, pero limitada lo que dificulta poder aprovechar todas las bondades que ofrece de forma ágil.

De cara al mantenimiento o ampliación futura, una de las ventajas que tiene el CMS propuesto, Magento, es la actualización a la nueva versión 2.4.3 disponible a partir de finales de agosto 2021, y que no se pudo incluir para su análisis en el presente trabajo, dicha versión incluirá mejoras de seguridad que incluyen la expansión de la cobertura de reCAPTCHA, dependencias principales de composer y las bibliotecas de terceros se han actualizado a las últimas versiones que son compatibles con PHP 8.x. Por ahora no es recomendable pasarla a producción y esperar un tiempo prudencial. El inconveniente que podría presentarse de cara a una ampliación es que sería necesario un periodo de prueba de la misma, antes de pasar

a producción, por parte de los responsables de seguridad de *LUMA* para su evaluación siguiendo las pautas y utilizando las herramientas que se han propuesto.

Desde el punto de vista personal la realización de este proyecto me ha permitido poder poner en práctica los conocimientos adquiridos en el Máster. También he logrado ampliar la visión previa que entendía en aspectos de seguridad y que solo eran aplicados a nivel de infraestructuras de redes dada a mi experiencia trabajando en empresas de telecomunicaciones, llegando a comprender que la seguridad es igual de importante y necesaria en otros tipos de tecnologías. Por todo ello se ha incrementado mi interés por continuar ampliando mis conocimientos en infraestructuras de la nube y seguridad para enriquecer mi curriculum profesional.

8.- **BIBLIOGRAFÍA**

1. Advertorial, F. (2021, 5 marzo). Latinoamérica, terreno fértil para el ecommerce. Forbes Colombia. https://forbes.co/2021/03/05/negocios/latinoamerica-terreno-fertil-para-el-ecommerce/
2. Ceurvels, M. (2020, 14 diciembre). Latin America will be the fastest-growing retail ecommerce market this year. Insider Intelligence. https://www.emarketer.com/content/latin-america-will-fastest-growing-retail-ecommerce-market-this-year
3. Euromonitor Communications. (2018, 27 marzo). E-Commerce Is the Fastest Growing Global Retail Channel Through 2022. Market Research Blog. https://blog.euromonitor.com/e-commerce-is-the-fastest-growing-global-retail-channel-through-2022/
4. Guibert, Y. (2017, 14 septiembre). 12 tipos de eCommerce para construir tu negocio digital con éxito. Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce. https://marketing4ecommerce.net/tipos-de-ecommerce/
5. P. (2021, 25 marzo). Los 3 CMS para e-commerce más utilizados. AT Language Solutions. https://www.at-languagesolutions.com/atblog/cms-ecommerce-mas-utilizados/
6. Torres, D. (2021, 3 febrero). La lista definitiva de los mejores CMS en 2021. Mejores-CMS. https://blog.hubspot.es/marketing/mejores-cms
7. SeQura. (2021, 18 junio). Mejores CMS para eCommerce. Mejores CMS E-Commerce. https://www.sequra.es/post/mejores-cms-para-ecommerce
8. C. (2021b, abril 1). Comparativa de los 10 mejores CMS para crear tu web 2021. Café con SEO. https://www.cafeconseo.es/los-10-mejores-cms-para-crear-tu-web
9. Adobe Commerce Developer Guide. (s. f.). Magento. Recuperado 4 de septiembre de 2021, de https://devdocs.magento.com/
10. La Mejor Plataforma de eCommerce | Shopify España. (s. f.). Shopify. Recuperado 4 de septiembre de 2021, de https://www.shopify.es/

11. WordPress. (s. f.). Herramienta de blog, plataforma de publicación y CMS. WordPress.org España. Recuperado 4 de septiembre de 2021, de https://es.wordpress.org/
12. Trường, K., Owens, S., Whicker, E., Medeiros, L., Montague, H., & Eisenbarth, S. (2021, 17 agosto). WooCommerce. WordPress.org España. https://es.wordpress.org/plugins/woocommerce/
13. Please Wait. . . | Cloudflare. (s. f.). Prestashop. Recuperado 4 de septiembre de 2021, de https://www.prestashop.com/es?__cf_chl_jschl_tk__=pmd_B7Yw5xNYVsLCFACOcyKkbq_DQCRKVJyYSrzuZ5qL6E8-1630755428-0-gqNtZGzNAdCjcnBszQoR
14. Security | Adobe Commerce 2.4 User Guide. (2021, 24 junio). Security Adobe. https://docs.magento.com/user-guide/stores/security.html
15. S. (s. f.). Account security. Shopify Help Center. Recuperado 8 de julio de 2021, de https://help.shopify.com/en/manual/your-account/account-security
16. WooCommerce. (2018, 24 junio). WooCommerce site and data security FAQ. WooCommerce Docs. https://docs.woocommerce.com/document/woocommerce-security-faq/
17. Dashboard - PrestaShop documentation. (s. f.). PrestaShop Documentation. Recuperado 8 de julio de 2021, de https://doc.prestashop.com/dashboard/
18. System requirements | Adobe Commerce Developer Guide. (2021, 11 junio). Adobe Commerce. https://devdocs.magento.com/guides/v2.4/install-gde/system-requirements.html
19. Hardware recommendations | Adobe Commerce Developer Guide. (2021, 16 febrero). Adobe Commerce Developer Guide. https://devdocs.magento.com/guides/v2.4/performance-best-practices/hardware.html
20. Dignan, L. (2021, 2 abril). Top cloud providers in 2021: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players. ZDNet. https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/
21. Jones, E. (2021, 29 abril). Cuota de mercado de la nube - una mirada al ecosistema de la nube en2021. Kinsta. https://kinsta.com/es/blog/cuota-de-mercado-de-la-nube/

22. LEY DE PROTECCIÓN DE DATOS PERSONALES. (s. f.). legislacion.asamblea.gob.ni. Recuperado 12 de julio de 2021, de http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

23. REGLAMENTO DE LA LEY NO. 787 “LEY DE PROTECCIÓN DE DATOS PERSONALES”. (s. f.). legislacion.asamblea.gob.ni. Recuperado 12 de julio de 2021, de http://legislacion.asamblea.gob.ni/Normaweb.nsf/9e314815a08d4a6206257265005d21f9/7bf684022fc4a2b406257ab70059d10f?OpenDocument

24. Nicaragua - Data Protection Overview. (2021, 16 junio). DataGuidance. https://www.dataguidance.com/notes/nicaragua-data-protection-overview

25. BOE.es - DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (s. f.-b). https://www.boe.es/. Recuperado 4 de agosto de 2021, de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

26. BOE.es - BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018, 5 diciembre). https://www.boe.es/eli/es/lo/2018/12/05/3. https://www.boe.es/eli/es/lo/2018/12/05/3

27. Top Threats Working Group | CSA. (s. f.). cloudsecurityalliance. Recuperado 17 de julio de 2021, de https://cloudsecurityalliance.org/research/working-groups/top-threats/

28. ENS. (s. f.). ENS. Recuperado 12 de julio de 2021, de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001

29. OWASP Top Ten Web Application Security Risks | OWASP. (s. f.). OWASP Top Ten Web Application Security Risks. Recuperado 16 de julio de 2021, de https://owasp.org/www-project-top-ten/

30. ENS. (s. f.-b). ENS. Recuperado 9 de agosto de 2021, de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1065
31. ENS. (s. f.-c). ENS-Marco operacional. Recuperado 9 de agosto de 2021, de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1073
32. Adobe-Magento-Commerce-Best-Practices-Guide. (2021). Adobe-Magento-Commerce-Best-Practices-Guide. https://www.adobe.com/content/dam/cc/en/security/pdfs/Adobe-Magento-Commerce-Best-Practices-Guide.pdf
33. Configure the application | Adobe Commerce Developer Guide. (2021, 20 mayo). Https://Devdocs.Magento.Com/Guides/v2.4. https://devdocs.magento.com/guides/v2.4/install-gde/install/post-install-config.html
34. Content Security Policies | Adobe Commerce Developer Guide. (2020, 20 agosto). Https://Devdocs.Magento.Com/Guides/v2.4/. https://devdocs.magento.com/guides/v2.4/extension-dev-guide/security/content-security-policies.html
35. Security | Adobe Commerce 2.4 User Guide. (2021b, junio 24). Https://Docs.Magento.Com/User-Guide/. https://docs.magento.com/user-guide/stores/security.html
36. ENS. (s. f.-d). ENS. Recuperado 4 de septiembre de 2021, de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1074
37. Modelo de responsabilidad compartida – Amazon Web Services (AWS). (s. f.). Amazon Web Services, Inc. Recuperado 22 de julio de 2021, de https://aws.amazon.com/es/compliance/shared-responsibility-model/
38. Bases de seguridad - Pilar de seguridad. (s. f.). aws-security-pillar. Recuperado 23 de julio de 2021, de https://docs.aws.amazon.com/es_es/wellarchitected/latest/security-pillar/security.html
39. Acuerdos de nivel de servicios (SLA) de AWS. (s. f.). Amazon Web Services, Inc. Recuperado 17 de agosto de 2021, de https://aws.amazon.com/es/legal/service-level-agreements/

40. ¿Qué es Amazon EC2? - Amazon Elastic Compute Cloud. (s. f.). AWS EC2. Recuperado 2 de septiembre de 2021, de https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html
41. ¿Qué es Amazon Relational Database Service (Amazon RDS)? - Amazon Relational Database Service. (s. f.). Amazon RDS. Recuperado 2 de septiembre de 2021, de https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/Welcome.html
42. Comprueba la disponibilidad de tu dominio | IONOS de 1&1. (s. f.). 2001–2021 1&1 IONOS España S.L.U. Recuperado 2 de septiembre de 2021, de https://www.ionos.es/domaincheckresult
43. Cómo funciona AWS WAF - AWS WAF, AWS Firewall Manager y AWS Shield Advanced. (s. f.). AWS WAF. Recuperado 2 de septiembre de 2021, de https://docs.aws.amazon.com/es_es/waf/latest/developerguide/how-aws-waf-works.html
44. What is Amazon GuardDuty? - Amazon GuardDuty. (s. f.). Amazon GuardDuty. Recuperado 5 de septiembre de 2021, de https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html
45. Security Scan | Adobe Commerce 2.4 User Guide. (2021, 20 julio). Magento Security Scan. https://docs.magento.com/user-guide/magento/security-scan.html
46. ¿Qué es Amazon Inspector? - Amazon Inspector. (s. f.). AWS Amazon Inspector. Recuperado 5 de septiembre de 2021, de https://docs.aws.amazon.com/es_es/inspector/latest/userguide/inspector_introduction.html
47. OWASP ZAP – Getting Started. (s. f.). OWASP ZAP. Recuperado 5 de septiembre de 2021, de https://www.zaproxy.org/getting-started/
48. cve.mitre.org. (s. f.). cve.mitre.org. Recuperado 6 de septiembre de 2021, de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7020
49. cve.mitre.org. (s. f.-b). cve.mitre.org. Recuperado 6 de septiembre de 2021, de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22132
50. Troubleshoot an unresponsive website on an EC2 instance. (s. f.). Amazon Web Services, Inc. Recuperado 6 de septiembre de 2021, de

https://aws.amazon.com/es/premiumsupport/knowledge-center/ec2-instance-hosting-unresponsive-website/

APÉNDICE

En este apartado se detallarán algunos aspectos sobre la instalación y despliegue del sistema de experimentación.

1. Manual de instalación del CMS Magento

1.1 Creación de instancias EC2 y RDS en AWS[5]

Como fase previa a la instalación de Magento se requiere crear una instancia EC2 con requisitos mínimos planteados en el apartado 2.2.1 y un RDS con motor de Base Datos de preferencia (eg. MariaDB, MySQL) en el proveedor de servicio. El proceso para el lanzamiento de ambas instancias es bastante intuitivo, solo se necesita seguir los pasos recomendados por AWS. Por lo que se omite la explicación del proceso en esta memoria.

1.2 Instalación Magento

En el apartado 2.2.1 se mencionan los requisitos del sistema para el funcionamiento de Magento. A continuación, se brinda una serie de pasos para la instalación de los paquetes necesario:

1.2.1 Instalar Apache 2.4

- Actualizar repositorios: *sudo apt update*
- Instalar Apache: *sudo apt install apache2 -y*
- Modificar archivo config Apache para permitir archivos .htaccess en el directorio web: *sudo nano /etc/apache2/sites-available/000-default.conf*
- Agregar las siguientes líneas:
    - *<Directory "/var/www/html">*
    - *AllowOverride All*
    - *</Directory>* Nota: Estas líneas indican donde se instalará Magento.
- Modificar configuración apache2 y establecer el nombre del servidor global: *sudo nano /etc/apache2/apache2.conf (agregar línea debajo de HostnameLookups Off)*

    ServerName IP del servidor AWS

[5] *Es necesario haberse dado de alta previamente en AWS.

- Comprobar si hay errores de sintaxis: *sudo apache2ctl configtest*
- Habilitar la reescritura de Apache (resuelve la mayoría errores 404 posterior a la instalación): *sudo a2enmod rewrite*
- Reiniciar apache para aplicar los cambios: *sudo systemctl restart apache2*
- Habilitar apache a través de firewall: *sudo ufw allow 'Apache Full'*
- Probar Apache ingresando vía web a la dirección IP AWS

Resolución de problemas: Un inconveniente que se presentó después de instalar el servidor Apache fue que no se alcanzaba vía web con la IP de AWS. La causa fue que el firewall del sistema operativo no tenía permitida los puertos de escucha 80 y 443 [50]. Como solución se agrega regla al firewall de Ubuntu permitir los puertos 80 y 443 aplicando los siguientes comandos:

- Ejecute el siguiente comando para verificar puertos permitidos en firewall UFW: sudo ufw status verbose
- Comando para permitir solicitudes de conexión entrantes en los puertos 80 y 443: sudo ufw allow in 80/tcp y sudo ufw allow 443/tcp.
- Se requiere agregar los siguientes puertos que serán necesarios durante el ciclo de instalación: puertos: 22, 587, 3306, 25, 9200

1.2.2 Instalar PHP 7.4

- Aplicar la siguiente línea de comando que instala PHP y extensiones necesarias de Magento 2.4: *sudo apt install php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-soap php7.4-bcmath php7.4-xml php7.4-mbstring php7.4-gd php7.4-common php7.4-cli php7.4-curl php7.4-intl php7.4-zip zip unzip -y*
- Modificar el siguiente archivo de config para indicar al servidor web que prefiera archivos PHP: *sudo nano /etc/apache2/mods-enabled/dir.conf Nota: Modificar de la lista: index.html por index php y index.php por index.html "es decir que index.php este al principio de la lista".*
- Modificar dos variables predeterminadas en el archivo de config de php: *sudo nano /etc/php/7.4/apache2/php.ini* editar líneas:
  - date.timezone = Europe/Madrid (eg. Europe/Madrid).
  - memory_limit = 4G (Por defecto viene en 128M) → Magento no corre en menos de 4G.

- Reiniciar apache para aplicar cambios: *sudo systemctl restart apache2*

1.2.3 Instalación de servidor de correo SMTP – Postfix

- Postfix agente de transferencia de correo, maneja el correo en un servidor. Para instalar aplicar el siguiente comando: *sudo apt install mailutils -y*
- Seleccionar *Ok*
- Seleccionar: *Internet Site, OK*.
- En system mail name escribir nombre dominio: (eg.nombre ec2), *Ok*.
- Modificar archivo de config de postfix: *sudo nano /etc/postfix/main.cf, buscar la línea "inet_interfaces = all" y modificarla con: inet_interfaces = loopback-only*
- Reiniciar postfix para aplicar cambios: *sudo systemctl restart postfix*

1.2.4 Instalación de Elasticsearch 7.9.0

1.2.4.1 Instalar Kit de desarrollo Java

- Aplicar la siguiente línea de comando: *sudo apt install openjdk-8-jdk -y*
- Verifique instalación con: *java -version*

1.2.4.2 Instalar Elasticsearch

- Descargar los 2 archivos Elasticsearch 7.6 con los siguientes comandos: *wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.9.0-amd64.deb y*
  wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.9.0-amd64.deb.sha512
- Comprobar integridad de los archivos: *shasum -a 512 -c elasticsearch-7.9.0-amd64.deb.sha512 debe de indicar OK*.
- Agregar el archivo descargado al administrador de paquetes del S.O: *sudo dpkg -i elasticsearch-7.9.0-amd64.deb*

1.2.4.3 Configurar elasticsearch para ejecución automática

- Aplicar comando: *sudo /bin/systemctl daemon-reload*
- Agregar elasticsearch al inicio del sistema: *sudo /bin/systemctl enable elasticsearch.service*
- Ejecutar elasticsearch: *sudo systemctl start elasticsearch*

- Validar Elasticsearch: *curl -X GET 'http://localhost:9200'*

1.2.4.4 Modificar de Elasticsearch:

- Modificar lo siguiente en el archivo de configuración: *sudo nano /etc/elasticsearch/elasticsearch.yml y cambiar lo siguiente: Nombre del cluster: "cluster.name: Magento Cluster" (Nombre a eleccion)*
- Nombre del nodo: *node.name: Node Magento*
- Actualizar host de red: *cambiar por la IP de AWS*.
- Reiniciar el servicio para aplicar los cambios: *sudo systemctl restart elasticsearch*
- Validar que los cambios han sido aplicados: *curl -X GET 'http://localhost:9200' debe de salir el nuevo nombre del nodo y cluster*

1.2.5 Instalacion de Composer 2.X

1.2.5.1 Crear un usuario de Magento

- Aplicar comando: *sudo adduser magento*
- Ingresar claves para el nuevo usuario: *xxxxxxxx*
- Hacer que el grupo de servidores web sea el grupo principal para el nuevo usuario: *sudo usermod -g www-data magento*

1.2.5.2 Dar permisos de carpeta

Al instalar Apache, se crea automáticamente un directorio web para almacenar archivos web. Este se crea con el usuario predeterminado www-data (o incluso root). Se requiere actualizar los permisos para que el nuevo usuario magento funcione correctamente.

- Aplicar el comando: *sudo chown -R magento:www-data /var/www/html/*

1.2.5.3 Instalar Composer

- Aplicar comando descargando el archivo desde la web: *sudo curl -sS https://getcomposer.org/installer | php*
- Mover el archivo descargado de Composer a otro directorio: *sudo mv composer.phar /usr/local/bin/composer*
- Aplicar comando: *sudo composer install*

1.2.6 Descargar Magento 2.4 con Composer

- Ubicarse en el directorio donde se instalará Magento: *cd /var/www/html*

- Cambiar al usuario magento creado previamente: *su magento, poner password del usuario magento.*
- Validar que el directorio se encuentre vacío con el comando: *ls -la*
- Si se encuentra el archivo de prueba index.html, borrarlo con el comando: *rm index.html*
- Instalar magento - pedirá claves públicas y privadas asignadas al darse de alta en Magento: *composer create-project --repository-url=https://repo.magento.com/ magento/project-community-edition=2.4.2-p1 .*
- Establecer permisos de preinstalación: *find var generated vendor pub/static pub/media app/etc -type f -exec chmod g+w {} + && find var generated vendor pub/static pub/media app/etc -type d -exec chmod g+ws {} + && chown -R :www-data . && chmod u+x bin/magento*

1.2.7 Instalar Magento 2.4 a través de línea de comandos

1.2.7.1 Ejecutar script de instalación: reemplazar con datos propios

bin/magento setup:install \

--base-url=http:// ip aws \

--db-host= punto enlace RDS y Puerto conexion \

--db-name=nombre BD \

--db-user= nombre BD \

--db-password=pasword \

--admin-firstname=admin \

--admin-lastname=admin \

--admin-email=mail@gmail.com \

--admin-user=admin \

--admin-password=password\

--language=es_ES \

--currency=EUR \

--timezone=Europe/Madrid \

--use-rewrites=1

1.2.8 Actualizar memory_limit de PHP

- Abrir archivo .htaccess: nano .htaccess
- Modificar en memory_limit, linea php_value memory_limit: *reemplazar 756MB por 4G*

1.2.9 Instalar tareas cron

Estas son tareas programadas que deben de ejecutarse en segundo plano, ayudan en tareas de indexación, copias de seguridad, actualizaciones, etc.

- Ejecutar el siguiente comando: *bin/magento cron:install*
- Validar que Magento está funcionando ingresando a la dirección IP de AWS

1.2.10 Instalar Sample Data

- Cambiar a modo desarrollado con la siguiente línea de comando: *bin/magento deploy:mode:set developer*
- Remover archivos generados en cache previamente: *rm -rf generated/metada/* generated/code/**
- Limpiar la cache: *bin/magento cache:clean*
- Se recomienda realizar un BK de los datos.
- Intalar sample data: *bin/magento sampledata:deploy* (pedirá claves públicas y privadas)
- Aplicar un upgrade: *bin/magento setup:upgrade*

1.2.11 Descargar Paquete de Idioma Español

- Acceder con el usuario magento: *su magento*
- Acceder a carpeta donde está instalado magento: *cd /var/www/html*
- Aplicar comando para descargar paquete idioma español: wget https://github.com/mageplaza/magento-2-spanish-language-pack/raw/master/es_ES.csv
- Aplicar comando para mover el paquete a la carpera es_ES: *bin/magento i18n:pack -m replace es_ES.csv -d es_ES*
- Aplicar comando para desplegar el español en todo magento: *bin/magento setup:static-content:deploy -f es_ES*
- Aplicar comando para borrar cache: *bin/magento cache:flush*

- Para buscar el directorio donde se desplego el archivo es_ES.csv: *sudo find / type f -name "es_ES.csv"*
- Ir al backend:
    a. *Ir a la config de la cuenta admin,*
    b. *interface locale cambiar a: Español/Spain*
    c. *agregar clave usuario administrador del backend*
    d. *clic a guardar*
    e. *Para el front end:*
        i. *Clic en stores*
        ii. *Clic configuration*
        iii. *En país por defecto, seleccionar país*
        iv. *Modificar config regional y poner el país*
        v. *Modificar la unidad medida y el día del primer día de la semana*
        vi. *Clic guardar configuración*
        vii. *En administración de cache, clic a vaciar almacenamiento cache*
        viii. *Validar que el front end está completamente en español.*

1.3 Configuraciones adicionales AWS

1.3.1 Reglas de entrada y salida grupos de seguridad EC2

En el grupo de seguridad de la instancia ubicada en la pestaña seguridad, acceder al grupo de seguridad creada al lanzar EC2 como se muestra en la ilustración 82, en reglas de entrada, editar y agregar los puertos como se muestra en la ilustración 83.

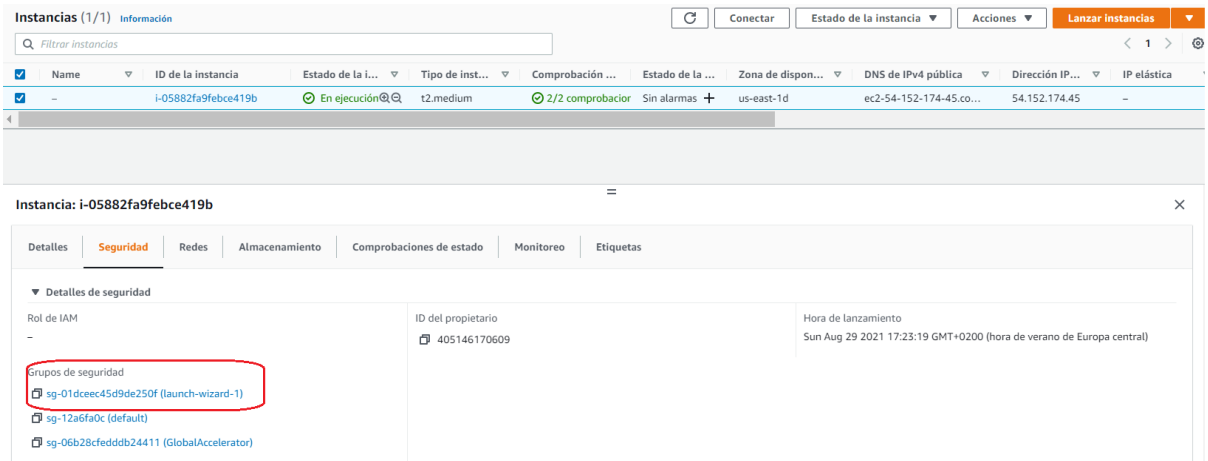


Ilustración 89 Grupos de seguridad EC2

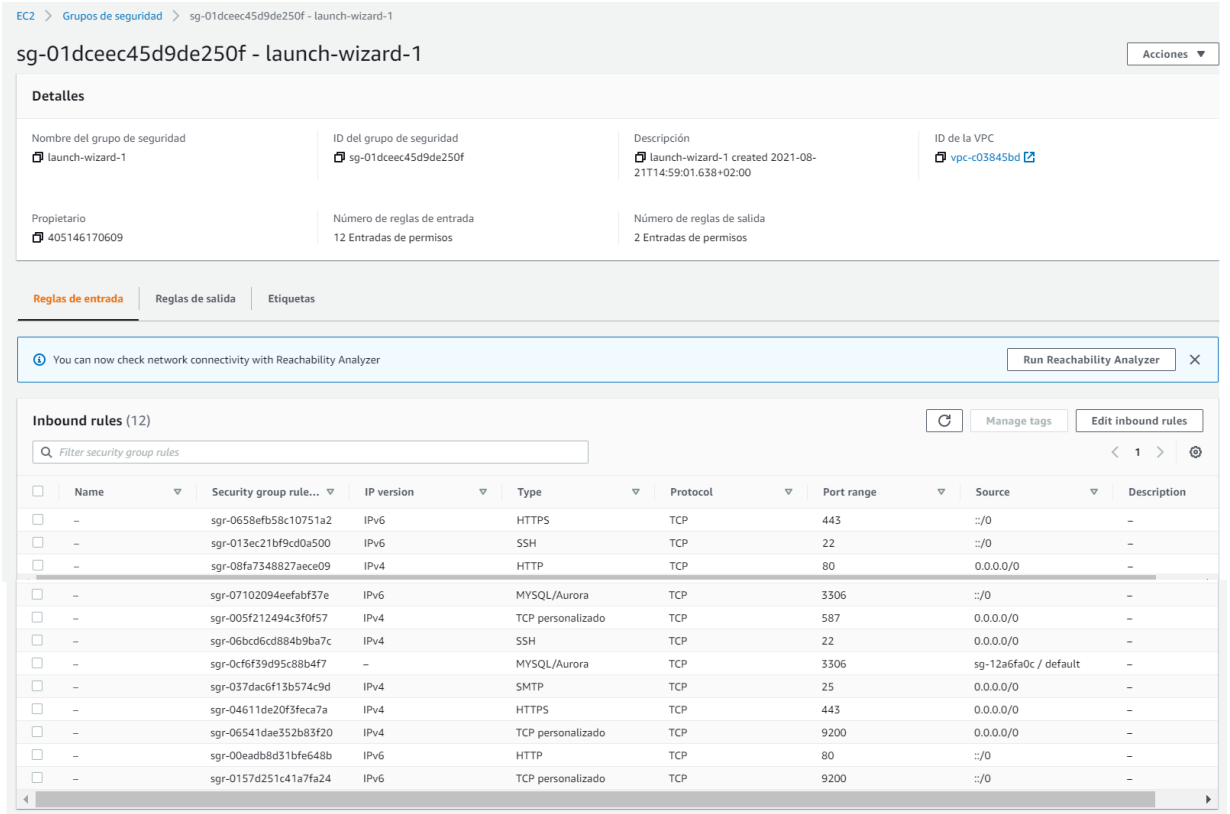


Ilustración 90 Reglas de entrada instancia EC2

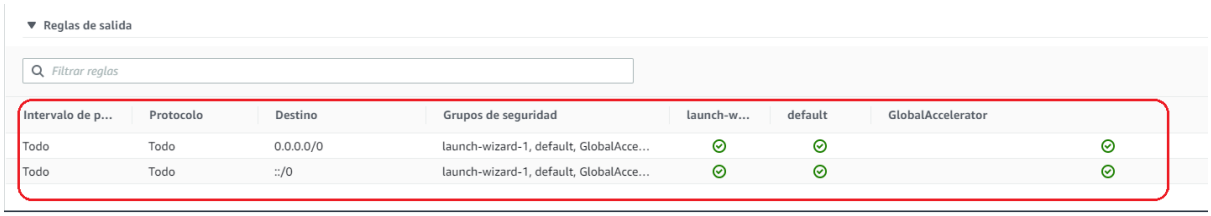


Ilustración 91 Grupo de seguridad - reglas de salida

1.3.2 Grupo de seguridad RDS

En el grupo de seguridad del RDS creado previamente, acceder a las reglas de entrada, seleccionar editar y crear la regla que se muestra en la ilustración 85 y 86.

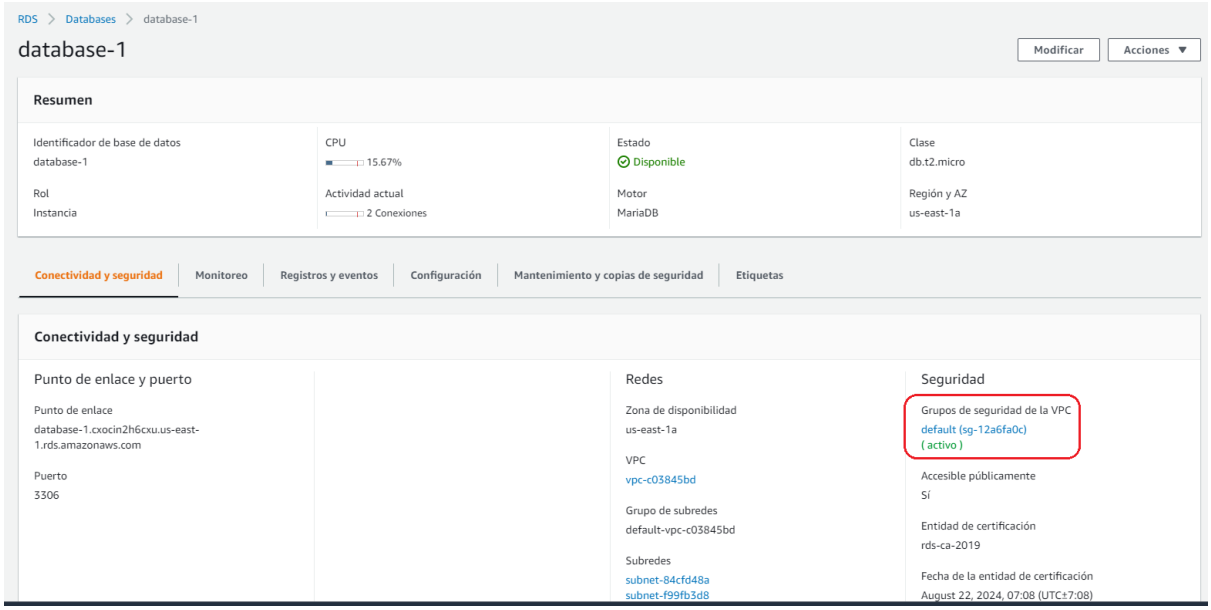


Ilustración 92 Grupo de seguridad RDS-database-1

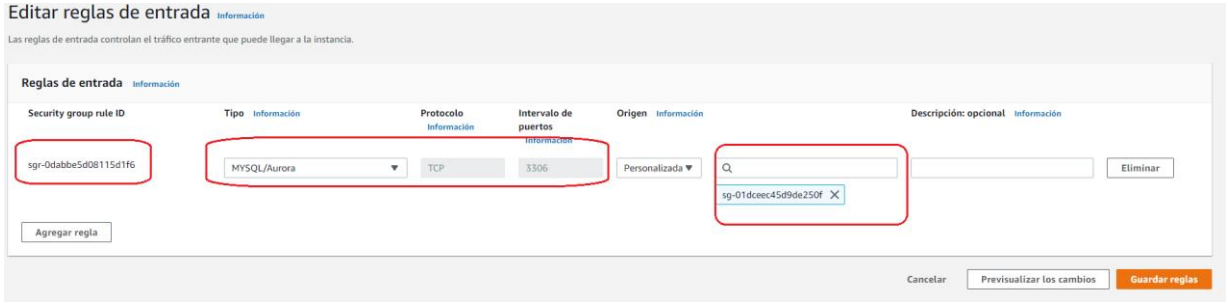


Ilustración 93 Grupo de seguridad - Reglas de entrada