UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Metodología basada en la implementación de una infraestructura en la nube

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Masias Ordinola, Carlos Gabriel (orcid.org/0000-0001-6224-0286)

ASESOR:

Tavara Ramos, Anthony Paul (orcid.org/0000-0002-4159-930X)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de Servicio de Redes y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Apoyo a la reducción de brechas y carencias en la educación en todos sus niveles

PIURA – PERÚ

2023

DEDICATORIA

Dedico este trabajo a mi madre, que día a día me apoya en todo, sus sacrificios y hace todo lo posible para que cumpla mis sueños y que salga adelante, a mis hermanas por todo el apoyo que me han brindado desde siempre, a mi padre por todo lo posible que hizo para que ayudarme con mis estudios, a mis amigos, a las demás cercanas a mí y a mí por esforzarme cada día para ser un profesional que enorgullezca a mi familia.

AGRADECIMIENTO

El agradecimiento es para mi madre, mis hermanas, para mi padre y demás personas cercanas a mí por su apoyo, por todo lo que se sacrificó para que hoy esté aquí y a mí por llegar a este punto, uno de los más importantes en mi vida.

ÍNDICE DE CONTENIDOS

Índice de tablas

Índice de figuras

RESUMEN

El uso de la tecnología en la nube ha aumentado en los últimos años, siendo Amazon Web Services (AWS) uno de los proveedores más utilizados. La norma ISO 27017:2015 asegura la seguridad de estos servicios. Por ello, se tuvo como objetivo proponer una guía metodológica para la implementación de una infraestructura en la nube. El tipo de investigación fue aplicado con un diseño de estudio no experimental de nivel descriptivo. Se analizó la variable “Infraestructura en la nube” a través de fichas de observación y la estadística inferencial a través de la prueba no paramétrica U Mann Whitney. El resultado principal destacó que la implementación de los controles de seguridad en la nube está condicionada por diversos factores, entre ellos, económicos; complejidad y tecnológico. Por ende se concluye que es posible proponer una guía metodológica para la implementación de controles de seguridad en la nube, sin verse afectada por las variaciones entre las diferentes empresas. Además, se destaca la importancia de adherirse a estándares y normas para salvaguardar la seguridad de la información en la nube y maximizar sus ventajas.

Palabras clave: Norma, seguridad de los datos, gestión de recursos, tecnología de la información.

ABSTRACT

The use of cloud technology has increased in recent years, with Amazon Web Services (AWS) being one of the most widely used providers. ISO 27017:2015 standard ensures the security of these services. Therefore, the objective of this study was to propose a methodological guide for the implementation of a cloud infrastructure. The research conducted was applied in nature, employing a non-experimental descriptive study design. The variable 'Cloud Infrastructure' was analyzed through observation cards, and inferential statistics were employed using the non-parametric Mann-Whitney U test. The main finding highlighted that the implementation of cloud security controls is influenced by various factors, including economic, complexity, and technological aspects. Consequently, it is concluded that it is possible to propose a methodological guide for the implementation of cloud security controls, unaffected by variations among different companies. Furthermore, the importance of adhering to standards and regulations to safeguard cloud information security and maximize its advantages is emphasized.

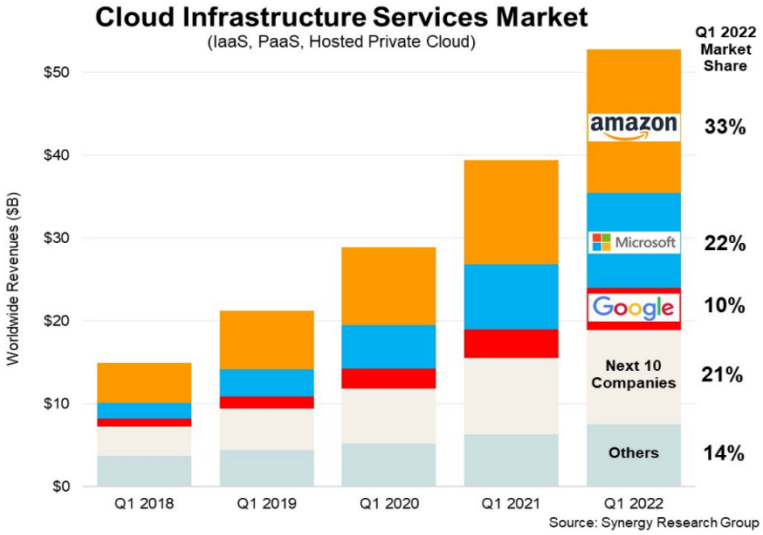
Keywords: Standard, data security, resource management, information technology.

I. INTRODUCCIÓN

En la actualidad, las empresas tienen dos opciones principales para alojar su software: tener un servidor propio o utilizar servicios en la nube como AWS, Azure o Google Cloud. Ambas opciones tienen ventajas y desventajas. La administración de servidores físicos ofrece mayor control y personalización, pero implica altos costos y requerimientos de personal especializado. Por otro lado, los servicios en la nube ofrecen escalabilidad y reducen los costos iniciales, pero pueden plantear preocupaciones de seguridad y dependencia de terceros.

Según el estudio de Synergy Research Group (2022) sobre la evolución de la cuota de mercado de los proveedores de nube, los servicios de los proveedores de la nube han ido impulsando aún más durante la pandemia. Los servicios públicos crecieron un 37% en el primer trimestre del 2021. La demanda de servicios en la nube está experimentando un crecimiento significativo, mayoritariamente en la pública, donde se destaca la presencia dominante de los tres principales proveedores y su acaparamiento en un 71% de esta industria. (Synergy Research Group 2022)

Figura 1. Crecimiento de servicios en la nube, 2022



Fuente: Synergy Research Group, 2022

Esto refleja el por qué las empresas de los distintos sectores económicos están utilizando tecnologías basadas en la nube. Donde cada vez se está migrando a la nube y dejando de usar los servidores físicos. Distintos sectores, como el financiero o salud, utilizan estas tecnologías para sus distintos usos, desde almacenar datos hasta alojar servicios o sus sistemas.

El uso de la computación en la nube va más allá de simplemente subir un software, se trata de diferentes elementos que se relacionan a fin de tener una mayor seguridad, accesibilidad y confiabilidad. Desde la implementación de estándares de seguridad, como el ISO 27017:2015, hasta la adecuada gestión y mantenimiento mediante buenas prácticas basadas en protocolos y estándares en la nube, se establece un marco de seguridad integral. Dentro de este contexto, se pueden identificar dos actores fundamentales:

En primer lugar, está la seguridad de la nube, donde el proveedor de servicios en la nube adopta una serie de protocolos destinados a garantizar la protección de sus servicios. En segundo lugar, está la seguridad en la nube, donde el cliente desempeña un papel fundamental en la protección de sus propias cargas de trabajo.

Hasta la fecha, no se encuentra suficiente información que asimile una guía metodológica para poder realizar un plan de aprovisionamiento, desde la elección del proveedor cloud, la arquitectura hasta el despliegue a entornos como pruebas o producción. No se tiene en cuenta sobre cuál proveedor utilizar sin primero tener en cuenta la necesidad del cliente para su software.

Por ejemplo, una empresa nueva dedicada al rubro tecnológico, empiece un proyecto de software sobre un sistema de inventario. Ha seguido de acuerdo a su metodología ágil sus actividades programadas y demás acciones. Sin embargo, ahora se necesita llevar a un entorno de QA y/o producción. Al no tener servidores propios, una opción es solicitar servicios en la nube en algún proveedor para subir su software y sea accesible. Antes de configurar en la nube, es necesario elaborar

un plan detallado que aborde aspectos clave como la capacidad y alcance del software, el tráfico esperado, los costos involucrados, así como las ventajas y desventajas de los principales proveedores de servicios. También se deben considerar aspectos como la capacidad de los servidores, los servicios adicionales necesarios, el tiempo de uso requerido, los estándares de seguridad y las mejores prácticas, entre otros. Este plan garantizará una implementación exitosa y un aprovechamiento óptimo de la infraestructura en la nube.

Cloud computing nube tiene consigo grandes beneficios como la flexibilidad, donde los usuarios pueden escalar sus servicios e ir aumentando o disminuir en relación a sus necesidades. La eficiencia, donde se pueden desarrollar, administrar y desplegar aplicaciones y/o servicios de manera rápida y automatizada y el valor estratégico, ya que al ser tecnología innovadora, hay una ventaja competitiva solo por proveer y/o utilizar estos servicios.

Las empresas pueden optar por construir su infraestructura o usar servicios en la nube. En la nube, se encuentran tres modelos de servicios: SaaS, PaaS e IaaS. SaaS permite acceder a aplicaciones alojadas en la nube, mientras que PaaS proporciona una plataforma completa para el desarrollo de aplicaciones. Por último, IaaS ofrece recursos de infraestructura virtualizada. Las empresas eligen el modelo de servicio en la nube que se ajuste a sus necesidades, además del tipo del modelo de despliegue que utilicen, como privado, público, híbrido o comunitario. Para desplegar una aplicación, por ejemplo: el sistema de una empresa, lo general es utilizar servidores, almacenamiento, base de datos, etc.; sin embargo, aprovisionar estos servicios requieren un nivel de seguridad aplicando estándares como lo es el ISO 27017:2015.

Como se mencionó, aplicar estándares que realicen buenas prácticas y una correcta administración de estos servicios, requieren un riguroso seguimiento a fin de cumplir dichos estándares. Sin embargo, hay empresas que aún no migran a la nube o están por hacerlo, y resalta el crecimiento de las empresas en el ámbito de la nube el cual es evidente y se refleja en su interés por adoptar estos servicios.

Sin embargo, es común que muchas empresas solo estén familiarizadas con los nombres de los proveedores más destacados de servicios. Este crecimiento implica que las nuevas empresas, y las que ya utilizan estos servicios, empiecen a utilizar con más frecuencia los servicios en la nube.

Con el fin de ilustrar ciertos conceptos y demostrar la aplicabilidad de los métodos propuestos, se utilizan algunos datos de referencia en este trabajo de investigación en lo que respecta a usuarios, contraseñas, configuraciones de red, servidores, base de datos, direcciones IP y relacionados cuando se realizan las configuraciones mostradas en el presente trabajo de investigación. Esto solo afecta en lo mencionado anteriormente, mas no en los datos obtenidos ni los resultados, estos datos son verídicos. Asimismo, todos los datos de referencia, serán eliminados y descartados cuando se termine con el desarrollo de proyecto de investigación.

Como justificación social, el análisis a revisar permitirá establecer una guía metodológica para cuando se requiera aprovisionar servicios en la nube relacionados a servidores, redes, almacenamiento y seguridad. Como justificación metodológica, este proyecto de investigación permitirá aplicar y probar una secuencia de pasos para seleccionar, implementar y desplegar servicios y aplicaciones en la nube aplicando estándares. Como justificación práctica, el estudio de esta investigación se realiza porque existe la necesidad de conocer lo relacionado a proveedores en la nube y su manera de aprovisionar ciertos recursos y servicios en su respectiva plataforma con el uso de estándares, como la ISO 27017:2015.

En lo explicado anteriormente surge la incógnita del estudio, ¿Cuál es la aplicabilidad de los controles de seguridad de la norma ISO 27017:2015 en la implementación de servicios en la nube?

El objetivo general del presente trabajo es Proponer una guía metodológica para la implementación de una infraestructura en la nube.

Con el fin de lograr el objetivo general, se han establecido los siguientes objetivos específicos: Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento; Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube y Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta.

Como hipótesis general se sostiene que una guía metodológica basada en Amazon Web Services (AWS) facilita la selección, implementación y despliegue de servicios y aplicaciones en la nube.

II. MARCO TEÓRICO

Con el propósito de desarrollar una correcta base teórica, se sintetizaron e incluyeron algunos antecedentes a nivel nacional e internacional.

Garay Gómez (2016) aplicó un modelo de negocio con TIC teniendo como base al cloud computing. También se establece y asegura que las propiedades y diagramas de servicios que añade y da a las compañías. Se incorporan algunos servicios que presentan la nube pública (Arquitectura Hibrida); paralelamente que los marcos y normativas para el desempeño para realizar una migración e integración con los servicios que ofrece el cloud computing. Se puede concluir que se desarrolla y aplica buenas prácticas de seguridad para migrar de entornos de QA. (Garay Gómez 2016)

Mientras que Figueroa Lozano (2019) en su investigación tuvo como objetivo utilizar una metodología de riesgos en una aplicación de salud. Además de que se detalla la aplicación de una metodología de administración de peligros, teniendo en cuenta sobre cómo se aplicará la norma ISO/IEC 27005. No obstante, esta normativa ISO, utiliza la ejecución de la interpretación de forma que explica la estabilidad y examinar los riesgos, planteando los controles mitigantes para los peligros identificados. (Figueroa Lozano 2019)

Peralta Trejo y Laura Ochoa (2019) en su investigación se desarrolló una guía con el propósito de agilizar el proceso de migración para el INEI. Se realizó un estudio y constataron que el INEI reporta adecuadamente la información relacionada con los registros y censos estadísticos del país. Como resultado, se estableció una secuencia de productos o entregables que incluyeron la exploración de servicios en AWS, el identificar sistemas de información críticos, el plan y diseño de la migración. Estas acciones tenían como objetivo aumentar la disponibilidad de los sistemas del INEI y contribuir al logro del objetivo final del plan. (Peralta Trejo, Laura Ochoa 2019)

Del mismo modo, Lin, Pan y Liu (2022) discutieron ampliamente sobre los

métodos para mejorar la disponibilidad de las instancias spot. Este artículo presenta un estudio sobre los trabajos relacionados con las instancias spot, introduciendo en primer lugar la historia del desarrollo de los modelos de fijación de precios de las instancias spot, resumiendo a continuación los métodos que pueden mejorar la disponibilidad de las instancias spot y, por último, discutiendo cómo entender y utilizar mejor las instancias spot. Se espera que los usuarios de la nube puedan obtener suficientes conocimientos en este artículo para poder utilizar las instancias spot de varios proveedores de la nube para proveerse de recursos informáticos baratos y estables. (Lin, Pan, Liu 2022)

En su artículo, Zeadally, Das y Sklavos (2021) explican sobre cómo los fabricantes de productos para dispositivos y electrodomésticos de IoT, especialmente en el ámbito del consumidor, ofrecen soluciones de seguridad mal implementadas. Asimismo, se cumple con requisitos de seguridad generales de seguridad en IoT como la autenticación, integridad, privacidad, entre otros. Es crucial adoptar normas y estándares en relación a los protocolos de criptografía para servicios en la nube basados en IoT, más en el ámbito de los sistemas GSI. Una norma relevante en este sentido es la ISO 27017:2015, la cual resulta crucial para los fabricantes de dispositivos y electrodomésticos IoT. (Zeadally, Das, Sklavos 2021)

Mientras que Kim, Kim, Park, Kim y Chang (2020) explican la correlación sobre cómo los esfuerzos para fortalecer la privacidad del historial del paciente en los Sistemas de Gestión de Emergencias (EMS) basados en 5G incluyen la búsqueda de certificaciones internacionales como ISO 27001 y ISO 27799. Estas certificaciones son estándares reconocidos a nivel mundial que establecen requisitos para los SGSI y la gestión de la información de salud en organizaciones de atención médica. Al obtener estas certificaciones, los sistemas EMS demuestran su compromiso con la protección de la privacidad del historial del paciente, asegurando prácticas confiables y alineadas con estándares internacionales. Estas certificaciones buscan establecer estándares de seguridad y protección de la información médica en los EMS. Se espera que

estas certificaciones contribuyan a un entorno más seguro donde la información del paciente esté protegida de manera integral a nivel internacional. Específicamente, se anticipa que los Sistemas de Gestión de Emergencias (EMS) basados en la nube cumplan con regulaciones suplementarias establecidas en certificaciones. (Kim et al. 2020)

En Australia, Ali, Shrestha, Chatfield y Murray (2020) explican la adopción que ha generado la seguridad de los datos con respecto a la tecnología cloud, ya que los estándares actuales carecen de requisitos específicos. Esta investigación propuso un nuevo modelo de requisitos de seguridad en la nube, que considera prácticas de mitigación de riesgos, responsabilidad compartida y entornos complejos. El objetivo es establecer un marco sólido y adaptado a la realidad actual para garantizar la protección de la información. Estas implicaciones teóricas son relevantes para promover una adopción segura y responsable de la tecnología en la nube, especialmente para los gobiernos locales. Se destaca la importancia de establecer relaciones sólidas entre proveedores de servicios en la nube y gobiernos locales para abordar preocupaciones y crear entornos propicios. (Ali et al. 2020)

Asimismo, Avula, Nela, Gudapati y Velagapudi (2012) en su investigación, implementan una infraestructura en la nube, específicamente para el servicio almacenamiento, con un sistema existente pero no alojado, con la finalidad de que las historias médicas estén al alcance en varios doctores a nivel mundial. Por ejemplo, haciendo uso de los servicios en la nube, un doctor que reside en Japón y necesite subir un historial médico y que este se almacene en la nube. Posteriormente, esta información se podrá visualizar y acceder del servicio de almacenamiento en la nube o en la misma aplicación, que podría estar alojada en la nube. Finalmente, dicha información podrá ser leída a través de un doctor que esté, por ejemplo, en Londres. (Avula et al. 2012)

El Instituto Nacional de Estándares y Tecnología (NIST), ubicado en Estados Unidos, Mell y Grance (2011) proporcionan una descripción del cloud computing

como un enfoque que permite acceder de manera remota y ubicua a través de servicios configurables. Esto significa que los usuarios pueden acceder a recursos y servicios informáticos, como almacenamiento, aplicaciones y procesamiento de datos, de manera flexible y según sus necesidades, sin la necesidad de poseer o administrar infraestructura física. La computación en la nube proporciona una forma eficiente de consumir y utilizar recursos tecnológicos, ya que se adaptan fácilmente a la demanda y se pueden configurar según los requerimientos específicos de cada usuario, sin tener que acceder a su ubicación física. Estos recursos están ubicados de manera física en un data center del proveedor cloud y los usuarios de estas plataformas pueden acceder a estos de manera virtual, pudiéndose realizar de manera remota sin importar la ubicación donde se encuentre alguien, con una conexión a internet y configurar, por ejemplo, redes, servidores, almacenamiento, base de datos, etc. (Mell, Grance 2011)

Bagaeen, Al-Zoubi, Al-Sayyed y Rodan (2019) determinan que la tecnología cloud ofrece un acceso eficiente a recursos remotos y distribuidos a través del uso de proveedores de servicios. Sin embargo, la seguridad, la privacidad y la disponibilidad de los datos alojados en la nube son preocupaciones importantes tanto para los usuarios individuales como para empresas. Se compromete con la protección de los datos confidenciales y la disponibilidad para asegurar una experiencia confiable y satisfactoria para los usuarios y las organizaciones. (Bagaeen et al. 2019)

Una de las aplicaciones con cloud computing, teniendo como referencia a Bora y Ahmed (2013) presentan las ventajas de utilizar la computación en nube para el e-learning. Hay muchas instituciones educativas que no pueden permitirse este tipo de inversiones, y la computación en nube es la mejor solución, especialmente en las universidades, donde el uso de los ordenadores es más intensivo y lo que se puede hacer para aumentar los beneficios de las aplicaciones comunes para estudiantes y profesores. (Bora, Ahmed 2013)

Büyüközkan, Uztürk y Maden (2023) en su investigación relatan sobre la disponibilidad de los servicios cloud y se refiere a esta como el tiempo en que los servidores están activos y el servicio en la nube se encuentra funcional y accesible. Además de la disponibilidad, la confiabilidad de los sistemas para garantizar una capacidad de alta calidad también es un factor clave. Se sugiere que la empresa se enfoque en estos aspectos para mejorar el rendimiento al implementar su software. Se recomienda prestar menos atención a la latencia (tiempo), ya que es común que la empresa elija la medida más cercana de retraso temporal para lograr el rendimiento deseado en la capacidad. Además, la implementación es importante debido a los procesos automatizados que reducen la carga y facilitan la implementación en la nube. (Büyüközkan, Uztürk, Maden 2023)

Según Bahrami (2015) en su investigación lista a Azure, AWS y GCP como los tres grandes proveedores y los servicios que mejorarán los negocios de las aplicaciones móviles. Estos servicios abarcan el almacenamiento, computación, bases de datos, autenticación y autorización, notificaciones push, así como servicios de análisis y monitoreo. Estos servicios proporcionan una infraestructura escalable, segura y flexible al mejorar la experiencia del usuario, también logran reducir los costos operativos. Por último, se analiza algunas de las prácticas más avanzadas en este campo y presenta algunas oportunidades de desarrollo a futuro. (Bahrami 2015)

De acuerdo con Bhardwaj, Subrahmanyam, Avasthi y Sastry (2016), con la creciente concienciación y preocupación por el cloud computing y la seguridad de la información, cada vez hay más conciencia y uso de algoritmos de seguridad en los sistemas y procesos de datos. Su artículo presentó una breve visión general y una comparación de los algoritmos criptográficos, con énfasis en los algoritmos simétricos que deberían utilizarse para las aplicaciones y servicios que estén ejecutándose en la nube que requieren el cifrado de datos y enlaces. En este artículo se revisan los algoritmos simétricos y asimétricos,

haciendo hincapié en los algoritmos simétricos para considerar la seguridad de los mismos en las aplicaciones y servicios que estén ejecutándose. (Bhardwaj et al. 2016)

Kewate (2022) relata sobre cómo AWS ofrece tecnología cloud y que, además brinda alta tecnología y aspectos como la seguridad, integridad y mantener disponibles los datos de los usuarios. “AWS proporciona los recursos necesarios. Los servicios de TI están disponibles a precios asequibles y no se requiere una inversión previa en los servicios. El cliente debe pagar por los servicios que utiliza regularmente.” (Kewate 2022).

Según lo mencionado, se puede destacar lo siguiente:

Se enfatiza que AWS proporciona los recursos necesarios, lo que sugiere que AWS cuenta con una amplia variedad de recursos de TI disponibles para sus clientes. Esto puede incluir servidores, almacenamiento, herramientas para análisis de datos y otras tecnologías de TI. Además, se menciona que los servicios de TI están disponibles a precios asequibles, lo que sugiere que AWS ofrece precios competitivos para sus servicios en comparación con otras soluciones de TI en el mercado. Esto puede ser beneficioso para las organizaciones que buscan reducir sus costos de TI. No obstante, se destaca que no se requiere una inversión previa en los servicios. Esto puede ser atractivo para las organizaciones que buscan reducir sus costos de capital al evitar la necesidad de realizar una inversión inicial en hardware y software.

También, se menciona que el cliente solo debe pagar por los servicios que utiliza regularmente, lo que sugiere que AWS ofrece un modelo de pago por uso, lo que puede ser beneficioso para las organizaciones que buscan controlar y reducir sus costos de TI, aunque esto puede variar si se desea un servicio a largo plazo, donde convendría algún tipo de plan que esté sujeto a un periodo de tiempo fijo y reduzca el costo de dicho servicio.

Del mismo modo, Kamaruddin, Mohamed, Jarno y Daud (2020) con su

investigación, la seguridad de la información es uno de los elementos cruciales en las operaciones organizacionales, requisito esencial tanto para el suscriptor como para el proveedor cloud en diferentes áreas del cloud computing. Esto sugiere que se necesita considerar, en su mayoría con empresas, la seguridad al implementar soluciones en la nube y tomar medidas para mitigar los riesgos asociados. Aplicar herramientas, métodos y/o estándares como la ISO 27001:2013 o ISO 2017:2015 permitirá salvaguardar la información del cliente. Las organizaciones que utilizan la nube deben cumplir con requisitos de seguridad específicos. Estos requisitos pueden abarcar la configuración de controles de acceso apropiados, la gestión de identidades y acceso, el cifrado de datos, así como la detección y respuesta a incidentes de seguridad. (Kamaruddin et al. 2020)

Xu, Goteng y He (2021) en su investigación explican sobre la relación entre la latencia y la disponibilidad en los servicios en la nube y su importancia para la satisfacción del usuario y el éxito empresarial. Donde se considera que una latencia elevada y una disponibilidad deficiente tienen repercusiones negativas para las empresas. Los usuarios experimentan frustración cuando enfrentan tiempos de respuesta lentos o cuando no pueden acceder al servicio debido a problemas de disponibilidad. Esto puede generar insatisfacción entre los clientes y, en última instancia, provocar la pérdida de los mismos. (Xu, Goteng, He 2021)

Amron, Ibrahim y Chuprat (2017) explican los modelos de servicios. IaaS procesa y almacena data en la nube, además de ofrecer recursos como servicios. En general, se provee con máquinas virtuales, almacenamiento, configuración de redes, hardware aislado, etc. PaaS permite a los clientes, en la aplicación del cloud provider, administrar y configurar su infraestructura. Los clientes tienen dominio total sobre sus aplicaciones y servicios desplegados. SaaS permite al usuario, acceder a los sistemas alojados en la nube. El usuario, mediante un acceso a internet, se conecta a estos sistemas e interactúa como

usuario final. (Amron, Ibrahim, Chuprat 2017)

Para Song, Pan y Liu (2022) IaaS es responsable de proveer la infraestructura, mientras que los proveedores SaaS pueden utilizar esta infraestructura para construir, desplegar y rentar su propio software como un servicio". De alguna manera, una de las mayores ventajas de rentar servicios en la nube implica no tener la necesidad de adquirir sus propios centros de datos y mantener el hardware. (Song, Pan, Liu 2022)

Según Wu, Ping, Ge, Wang y Fu (2010) ofrecen una rápida introducción al almacenamiento en la nube. Abarca las tecnologías clave de la computación y almacenamiento en la nube, varios tipos diferentes de servicios en nube, y describe las ventajas y los retos del almacenamiento en nube tras la introducción del modelo de referencia del almacenamiento en nube. (Wu et al. 2010)

De acuerdo con Ardagna, Asal, Damiani, Dimitrakos, Ioini y Pahl (2021), para garantizar la flexibilidad y estabilidad, los sistemas se diseñan y despliegan en un entorno en la nube, independientemente del modelo de servicio en la nube. Una de las ventajas que se tiene con la computación en la nube, es poder utilizar recursos físicos, alquilándolos como recursos virtuales. En relación a ello, las empresas pequeñas, medianas y grandes pueden tener el acceso a estos servicios y ajustarse teniendo en cuenta las necesidades del negocio y tránsito en sus aplicaciones. (Ardagna et al. 2021)

Del mismo modo, Ivanova, Borovska y Zahov (2018) determinan que se puede desarrollar una infraestructura en la nube a través de la infraestructura como código (IaC) para el software médico de análisis de imágenes, es más factible en cuanto facilidad, seguridad, velocidad, y óptimo con Terraform. (Ivanova, Borovska, Zahov 2018)

Rodríguez de la Cruz (2020) indica que Terraform siendo un software que permite desplegar infraestructura en la nube como código en un lenguaje de

alto nivel, agiliza al desarrollo de una infraestructura y gestiona sus despliegues. Además de que se reduce el esfuerzo y aumenta la productividad del desarrollo de los productos. Por último, la finalidad de utilizar infraestructura como código, permite abordar necesidades genéricas reutilizando componentes con código. (Rodríguez de la Cruz 2020)

Kumari y Singh (2021) Para identificar problemas de seguridad en softwares alojados en la nube, se puede lograr a través de la criptografía y algoritmos genéricos. Por otro lado, para asegurar los datos en la nube, se puede aplicar herramientas o técnicas como Multi-tenancy, Autenticación (MFA) e identificación de los usuarios (Gestionar cuáles usuarios se utilizan o no), encriptación de datos y aplicar Frameworks de seguridad. (Kumari, singh 2021)

Para Zhang (2020) las arquitecturas cloud, en efecto, pueden tener un impacto en el rendimiento de los servidores y/o servicios asociados, y que pueden ser testeados cuidadosamente para identificar las fallas y lo que lo ocasiona. Por otro lado, la arquitectura e infraestructura debería ser evaluada periódicamente cuán segura es y cómo aporta con cumplir las metas de la empresa. Tales pruebas se pueden realizar con herramientas como AppDynamics o DynaTrace u otras herramientas semejantes. (Zhang 2020)

Por otra parte, Abdalla y Varol (2019) en su investigación analizan el concepto de almacenamiento como servicio (StaaS), que permite a los usuarios o clientes utilizar el almacenamiento en la nube para guardar datos proporcionándoles espacio sin que tengan que utilizar el almacenamiento físico. (Abdalla, Varol 2019)

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El presente trabajo se desarrolló siendo de tipo de investigación aplicada ya que el propósito fundamental es solucionar un problema concreto o mejorar una situación existente en la vida real, utilizando los conocimientos y teorías disponibles dentro de un ámbito específico.

El enfoque cuantitativo es un método de investigación que se enfoca en medir variables y recolectar datos numéricos que pueden ser analizados utilizando técnicas estadísticas. Se utilizó principalmente un análisis numérico y estadístico para medir y analizar la variable de estudio. En este tipo de investigación, se busca medir y cuantificar datos objetivos y precisos, y las conclusiones se basan en la interpretación de los datos recopilados. El enfoque cuantitativo implica la recolección y análisis de datos numéricos y estadísticas para entender y explicar el fenómeno estudiado" (Babbie, 2013, p. 302)

El diseño del estudio aplicado es no experimental de nivel descriptivo. Se utilizó la propuesta planteada utilizando buenas prácticas en la implementación y seguridad de una infraestructura que se consideran al construir entornos de producción y pruebas para una aplicación.

La investigación al ser con diseño de estudio aplicado, no experimental y de nivel descriptivo, se centró en la descripción y caracterización de un fenómeno o situación en su entorno natural, sin manipulación de la variable de estudio ni control de las condiciones de la investigación, con la intención de aplicar los conocimientos y teorías existentes para resolver problemas prácticos.

3.2. Variables y operacionalización

La variable de estudio que se utilizó para la presente investigación es **Infraestructura en la nube**. Esta se define como la recopilación de elementos de hardware y software necesarios para hacer posible la informática de nube. Incluye capacidad de procesamiento, red y almacenamiento, así como una

consola administrativa para acceder a los recursos. Esta variable presenta tres dimensiones: Seguridad; Complejidad y Rendimiento.

La dimensión **Seguridad** tiene como único indicador el **Nivel de cumplimiento del control de la norma ISO 27017:2015**.

La dimensión **Complejidad** tiene como único indicador el **Tiempo de diseño e implementación (días)**.

Por último, la dimensión **Rendimiento** tiene como indicadores el P**orcentaje de utilización del recurso virtualizado**, el **Tiempo de actividad del servicio** y los **Tiempos de respuesta**. Los cinco indicadores presentan la razón como escala de medición.

3.3. Población, muestra y muestreo

Según los autores (Arias-Gómez, Villasís-Keever, Miranda-Novales 2016) indican que la población es un grupo de personas, expedientes, animales, entidades entre otros, los cuales se rigen por características que posteriormente pasarán a ser estudiadas como parte de una investigación.

Se tomó como población cierta parte del catálogo de servicios virtualizados ejecutándose, específicamente los relacionados a servidores, redes, almacenamiento y seguridad que presenta el catálogo de servicios de Amazon Web Services.

El proyecto de investigación se desarrolló como marco de referencia para cualquier tipo de entidad que esté inclinado en adquirir e implementar estas tecnologías.

3.4. Técnicas e instrumentos de recolección de datos

Según (Arias Gonzales 2021) define a la técnica de recolección de datos como el medio que utiliza un investigador con el propósito de obtener la información. Esta debe tener una relación con el tipo de estudio de la investigación que se realiza. Asimismo, se utiliza como criterio a la población.

Se aplicó la técnica de la observación como técnica de recolección de datos. En esta, se ejecutó la observación no experimental, dado que no se manipuló la variable de estudio y solo se limitó a observar los hechos en su naturaleza sin intervenir en el suceso del entorno.

El instrumento de recolección de datos permite ejecutar actividades, medidas y secuencias que ayudan al investigador a lograr su objetivo de obtener la información necesaria para satisfacer las incógnitas del proyecto. (Mendoza y Ávila, 2020).

Se utilizó como primer instrumento de recolección de datos, la ficha de observación, siendo un total de tres fichas para el registro. De la misma manera, según Arias, Jesús (2017) menciona que la ficha de observación mide y analiza en relación a un su incógnita o indicador, por lo que se emplea para medir las situaciones de personas, animales, entidades entre otros.

La primera ficha se realizó adecuadamente con el fin de medir el indicador de Nivel de cumplimiento del control de la norma ISO 27017:2015. En esta ficha, se midió el nivel de cumplimiento, donde se evalúa los siguientes niveles: **Totalmente en desacuerdo**, **En desacuerdo**, **Neutral**, **De acuerdo** y **Totalmente de acuerdo**.

La segunda ficha se aplicó para medir el indicador de **Tiempo de diseño e implementación (días)**. Por último, en la tercera ficha se evaluó para medir los indicadores de **Porcentaje de utilización del recurso virtualizado**, **Tiempo de actividad del servicio** y los **Tiempos de respuesta**.

Por otro lado, se utilizó como segundo la revisión documental y según Quintana, Alberto (2006) enuncia a la revisión documental como una revisión sostenida y de manera relativa a la literatura relacionada, constituyéndose como un marco único e interpretado y analizado por el investigador.

3.5. Procedimientos

Con respecto a la ficha de observación, se utilizó la información respecto al desarrollo y aplicación de la guía metodológica propuesta. Ello se realizó teniendo los indicadores mencionados anteriormente y posteriormente ingresados a sus fichas correspondientes.

Para obtener los datos del estudio, se solicitó el consentimiento y la autorización a las empresas y/o instituciones, con el fin de aplicar la guía metodológica propuesta en resultado del proyecto de investigación, siendo el documento brindado por el investigador.

En dos empresas, se realizó el diseño e implementación de estos servicios en la nube. En las dos empresas se utilizó a Amazon Web Services como proveedor de servicios en la nube.

Tabla 1. *Guía de implementación de servicios en la nube*

Cloud service customer	Cloud service provider
Tedregal E.I.R.L.	Amazon Web Services
Plataformas y Soluciones Digitales S.A.C.	

Fuente: ISO/IEC 27017:2015

En Amazon Web Services, se aprovisionaron los servicios de Route53, CloudFront, Certificate Manager, Simple Storage Service, Instancias EC2, Relational Database Service. Además, se configuraron otros servicios como IAM, CloudWatch, ECS, etc. con el fin de aplicar las recomendaciones establecidas por la ISO 27017:2015.

Se obtuvieron los controles aplicables para ambas empresas, el tiempo utilizado para cada configuración de los servicios, el rendimiento y disponibilidad de estos. Asimismo, la configuración respectiva se puede verificar en el anexo 21.

3.6. Método de análisis de datos

Se decidió asignar un peso a cada respuesta del primer instrumento utilizado para medir el indicador "Nivel de cumplimiento del control de la norma ISO 27017:2015" al utilizar una escala de Likert y necesitar cuantificar el resultado final en la dimensión "Seguridad". Se evaluó el indicador en una escala de Likert de 5 puntos, donde se asignó un valor del 1 al 5 para cada nivel.

Tabla 2*. Ponderación de respuestas correspondientes al indicador Seguridad*

Totalmente de acuerdo	**5**
De acuerdo	**4**
Neutral	**3**
En desacuerdo	**2**
Totalmente en desacuerdo	**1**

Fuente: elaboración propia

- **Totalmente de acuerdo**: Se cumple plenamente con todos los requisitos de la norma ISO y se demuestra un alto nivel de cumplimiento.
- **De acuerdo**: Se cumple en gran medida con la mayoría de los requisitos de la norma ISO, pero aún hay algunos aspectos que pueden mejorarse.
- **Neutral**: Se cumple parcialmente con la mayoría de los requisitos de la norma ISO, pero aún hay áreas de mejora.
- **En desacuerdo**: Se cumple con algunos requisitos de la norma ISO, pero hay áreas significativas de incumplimiento.
- **Totalmente en desacuerdo**: No se cumple con ninguno de los requisitos de la norma ISO.

Para el proceso y manipulación de los datos, se utilizó el software estadístico IBM SPSS Statistics para el análisis del contenido de cada una de las fichas de registro, permitiendo obtener los resultados para el proyecto de investigación.

Según IBM (2014) describe a SPSS Statistics como un software estadístico que tiene reconocimiento a nivel mundial en empresas, instituciones educativas de nivel académico superior entre otros cuando se necesita manipular los datos mediante una herramienta para su análisis y su facilidad para su uso, teniendo en cuenta a usuarios como investigadores, analistas y estadísticos.

3.7. Aspectos éticos

El proyecto de investigación estableció a la confidencialidad al uso de la información que fue utilizada y obtenida en el transcurso del desarrollo del proyecto, asimismo como la información de los centros donde se aplicó el proyecto de investigación.

También se mantuvo el consentimiento y autorización de parte del centro u organización para el desarrollo del proyecto y su confidencialidad, integridad, resguardo de la información proporcionada.

Finalmente, se garantizó la originalidad del proyecto de investigación que se llevó a cabo y los datos obtenidos son de fuente propia hecha por el investigador, permitiendo realizar la sustentación del proyecto.

IV. RESULTADOS

El presente trabajo utilizó estadística inferencial a fin de analizar los resultados obtenidos por medio de su ejecución. Se comparó los resultados de la ejecución de la guía metodológica de las muestras a través de los indicadores establecidos. A partir de instrumentos aplicados, se logró obtener la información.

Variable: Infraestructura en la nube

Con el fin de evaluar los indicadores de esta variable, se aplicaron métodos descriptivos y se evaluaron por medio una ficha de observación. Los instrumentos se aplicaron en dos muestras diferentes, donde cada una es una empresa diferente.

Con el análisis y normalización de los datos, se aplicó la prueba de Shapiro-Wilk debido a que el tamaño de la muestra es menor de 50.

OE1: Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento.

Indicador: Nivel de cumplimiento del control de la norma ISO 27017:2015.

Los datos se obtuvieron a través de una ficha de observación, la cual se aplicó a dos empresas diferentes, obteniendo el nivel de cumplimiento de los controles de la norma ISO 27017:2015 para determinar la diferencia en ambas muestras.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN

Si $p < 0.05$, se rechaza la Ho y se acepta la Ha.

Si $p >= 0.05$, se rechaza la Ha y se acepta la Ho.

Tabla 3. *Prueba de normalidad de indicador Nivel de cumplimiento del control de la norma ISO 27017:2015*

Shapiro-Wilk			
Muestras	**Estadístico**	**gl**	**Sig.**
Muestra 1	0.904	15	0.110
Muestra 2	0.880	15	0.047

Fuente: Elaboración propia

Como se obtuvo una significancia inferior al 0.05, los datos no se ajustan a una distribución normal, por lo que se acepta la hipótesis alternativa. Al trabajar con dos muestras independientes, la prueba estadística no paramétrica a utilizar es la prueba de U Mann-Whitney.

HIPÓTESIS PARA PRUEBA U MANN WHITNEY (PRUEBA NO PARAMÉTRICA)

Ho: No existe una diferencia en el nivel de cumplimiento de los controles de seguridad de la norma ISO 27017:2015 en AWS entre las dos empresas evaluadas.

Ha: Existe una diferencia en el nivel de cumplimiento de los controles de seguridad de la norma ISO 27017:2015 en AWS entre las dos empresas evaluadas.

CRITERIOS DE DECISIÓN:

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 4. *Prueba de U MANN-Whitney para el indicador Nivel de cumplimiento del control de la norma ISO 27017:2015*

Prueba U de Mann-Whitney		
	Z	**Sig. Asin. (Bilateral)**
Muestra	-0.521	0.602

Fuente: Elaboración propia

Dado que el valor de la significancia asintótica es mayor que 0.05, no se rechazaría la hipótesis nula a ese nivel de significancia. El nivel de cumplimiento no se ve afectado por ser de dos muestras distintas. Esto implica que no existe una diferencia en el nivel de cumplimiento de los controles de seguridad de la norma ISO 27017:2015 en AWS entre las dos empresas evaluadas y por lo tanto no hay suficiente evidencia para afirmar que el resultado observado es estadísticamente significativo. Aunque no se encontró una diferencia estadísticamente significativa en el nivel de cumplimiento de los controles de seguridad de la norma ISO 27017:2015 en AWS entre las empresas evaluadas, es crucial tener en cuenta las limitaciones y considerar otros factores que podrían influir en los resultados, como el tamaño de la muestra, las políticas internas de seguridad, las limitaciones en cuanto a cuántos servicios en la nube pueden aplicar, etc.

OE2: Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube.

Indicador: Tiempo de diseño e implementación (días).

Los datos se obtuvieron a través de una ficha de observación, la cual se aplicó a dos empresas diferentes, obteniendo el tiempo de diseño e implementación para determinar la diferencia en ambas muestras.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 5. *Prueba de normalidad de indicador Tiempo de diseño e implementación (días)*

	Shapiro-Wilk		
Muestras	**Estadístico**	**gl**	**Sig.**
Muestra 1	0.674	12	0.000
Muestra 2	0.536	9	0.000

Fuente: Elaboración propia

Como se obtuvo una significancia inferior al 0.05, los datos no presentan una distribución normal y se acepta la hipótesis alternativa. Al trabajar con dos muestras independientes, la prueba estadística no paramétrica a utilizar es la prueba de U Mann-Whitney

HIPÓTESIS PARA PRUEBA U MANN WHITNEY (PRUEBA NO PARAMÉTRICA)

Ho: Los factores clave que influyen en el tiempo necesario para diseñar e implementar servicios en la nube no se relacionan entre las dos empresas evaluadas.

Ha: Los factores clave que influyen en el tiempo necesario para diseñar e implementar servicios en la nube se relacionan entre las dos empresas evaluadas.

CRITERIOS DE DECISIÓN:

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 6. *Prueba de U MANN-Whitney para el indicador Tiempo de diseño e implementación (días)*

Prueba U de Mann-Whitney		
	Z	**Sig. Asin. (Bilateral)**
Muestra	-0.630	0.529

Fuente: Elaboración propia

Dado que el valor de la significancia asintótica es mayor que 0.05, se acepta la hipótesis nula a ese nivel de significancia. Por lo tanto, se concluye que los factores clave que influyen en el tiempo necesario para diseñar e implementar servicios en la nube no se relacionan en las dos empresas evaluadas. En base a los datos y análisis realizados, no se puede concluir que los factores clave tengan un impacto significativo en el tiempo necesario para el diseño e implementación de servicios en la nube en las dos empresas evaluadas. Sin embargo, es importante considerar algunas limitaciones, como que otros factores no considerados en este estudio y podrían influir en el tiempo requerido para el diseño e implementación de servicios en la nube. Además, la muestra evaluada puede no ser completamente representativa de todas las empresas y

contextos relacionados con la implementación de servicios en la nube. Por lo tanto, se debe tener precaución al generalizar estos resultados a otras situaciones.

Por otro lado, se muestra los estadísticos descriptivos en relación al objetivo.

Tabla 7. *Estadísticos descriptivos de Tiempo de diseño e implementación (días)*

	Total	**Mínimo**	**Máximo**	**Media**
Muestra 1	12	1	3	1.42
Muestra 2	9	1	2	1.22

Fuente: Elaboración propia

En la Muestra 1, se registraron datos de 12 observaciones, lo cual representa un tamaño de muestra mayor en comparación con la Muestra 2, que cuenta con 9 observaciones. En cuanto a los valores mínimos y máximos, ambas muestras tienen un valor mínimo de 1 día, sin embargo, la Muestra 1 presenta un valor máximo de 3 días, mientras que en la Muestra 2 el valor máximo es de 2 días. Esto demuestra que en la Muestra 1 se tuvo un caso en el que la implementación tomó más tiempo en comparación con la Muestra 2. Al analizar las medias de ambas muestras, se tiene que la Muestra 1 tiene una media de 1.42 días, mientras que la Muestra 2 tiene una media de 1.22 días. Esto indica que, en promedio, los servicios implementados en la Muestra 1 requirieron un poco más de tiempo en comparación con la Muestra 2, por lo que puede ser atribuido a diversos factores, como la complejidad de los servicios, el tamaño de los recursos utilizados, etc.

OE3: Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta.

Indicador: Porcentaje de utilización del recurso virtualizado.

Los datos se obtuvieron a través de una ficha de observación, la cual se aplicó a dos empresas diferentes, obteniendo el porcentaje de utilización del recurso virtualizado para determinar la diferencia en ambas muestras.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 8. *Prueba de normalidad de indicador Porcentaje de utilización del recurso virtualizado*

	Shapiro-Wilk		
Muestras	**Estadístico**	**gl**	**Sig.**
Muestra 1	0.897	6	0.357
Muestra 2	0.688	6	0.005

Fuente: Elaboración propia

Se aplicó la prueba de Shapiro-Wilk, debido a que el tamaño de la muestra es menor de 50. Como se obtuvo una significancia inferior al 0.05, los datos no se ajustan a una distribución normal y se acepta la hipótesis alternativa.

Al trabajar con dos muestras independientes, la prueba estadística no paramétrica a utilizar es la prueba de U Mann-Whitney.

HIPÓTESIS PARA PRUEBA U MANN WHITNEY (PRUEBA NO PARAMÉTRICA)

Ho: El porcentaje de utilización del recurso virtualizado entre el software utilizado por la Empresa A no presenta una diferencia significativa relacionada con el software utilizado por la Empresa B.

Ha: El porcentaje de utilización del recurso virtualizado entre el software utilizado por la Empresa A presenta una diferencia significativa relacionada con el software utilizado por la Empresa B.

Siendo, empresa “A” (Tedregal E.I.R.L.) y empresa “B” (Plataformas y Soluciones Digitales S.A.C.).

CRITERIOS DE DECISIÓN:

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 9. *Prueba de U MANN-Whitney para el indicador Porcentaje de utilización del recurso virtualizado*

Prueba U de Mann-Whitney		
	Z	**Sig. Asin. (Bilateral)**
Muestra	-2.887	0.004

Fuente: Elaboración propia

Dado que el valor de la significancia asintótica es menor que 0.05, se acepta la hipótesis alternativa de acuerdo al nivel significancia obtenido. Por lo tanto, el porcentaje de utilización del recurso virtualizado entre el software utilizado por la Empresa A presenta una diferencia significativa relacionada con el software utilizado por la Empresa B. Esto implica que hay una diferencia notable en el uso de recursos virtualizados entre ambos softwares de las empresas, posiblemente debido a diferencias en los sistemas, las prácticas de gestión utilizadas, etc.

Con respecto a los estadísticos descriptivos, se tiene.

Tabla 10. *Estadísticos descriptivos del indicador Porcentaje de utilización del recurso virtualizado*

	Total	**Mínimo**	**Máximo**	**Media**	**Desviación estándar**
Muestra 1	6	8.47	66.9	34.05	22.45
Muestra 2	6	0.74	5.52	2.38	2.35

Fuente: Elaboración propia

Ambas muestras muestran diferencias significativas en términos de los porcentajes de utilización del recurso virtualizado. La Muestra 1 presenta una mayor variabilidad en los valores de utilización, con un rango más amplio y una desviación estándar más alta. En contraste, la Muestra 2 muestra una variabilidad mucho menor y niveles generalmente bajos de utilización del recurso virtualizado.

Indicador: Tiempo de actividad del servicio.

Los datos se obtuvieron a través de una ficha de observación, la cual se aplicó a dos empresas diferentes, obteniendo el tiempo de actividad del servicio para determinar la diferencia en ambas muestras.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 11*. Prueba de normalidad de indicador Tiempo de actividad del servicio*

	Shapiro-Wilk		
Muestras	**Estadístico**	**gl**	**Sig.**
Muestra 1	0.008	6	0.003
Muestra 2	0.496	6	0.000

Fuente: Elaboración propia

Con el análisis y normalización de los datos, se aplicó la prueba de Shapiro-Wilk debido a que el tamaño de la muestra es menor de 50. Como se obtuvo una significancia inferior al 0.05, los datos no se ajustan a una distribución normal y se acepta la hipótesis alternativa.

Al trabajar con dos muestras independientes, la prueba estadística no paramétrica a utilizar es la prueba de U Mann-Whitney.

HIPÓTESIS PARA PRUEBA U MANN WHITNEY (PRUEBA NO PARAMÉTRICA)

Ho: El tiempo de actividad de los servicios utilizados la Empresa A no presenta una diferencia significativa relacionada el tiempo de actividad de los servicios por la Empresa B.

Ha: El tiempo de actividad de los servicios utilizados la Empresa A presenta una diferencia significativa relacionada el tiempo de actividad de los servicios por la Empresa B.

Siendo, empresa “A” (Tedregal E.I.R.L.) y empresa “B” (Plataformas y Soluciones Digitales S.A.C.).

CRITERIOS DE DECISIÓN:

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 12. *Prueba de U MANN-Whitney para el indicador Tiempo de actividad del servicio*

Prueba U de Mann-Whitney		
	Z	**Sig. Asin. (Bilateral)**
Muestra	-3.144	0.002

Fuente: Elaboración propia

Dado que el valor de la significancia asintótica es menor que 0.05, se acepta la hipótesis alternativa de acuerdo al nivel significancia obtenido. Por lo tanto, el tiempo de actividad de los servicios utilizados la Empresa A presenta una diferencia significativa relacionada el tiempo de actividad de los servicios por la Empresa B. El resultado implica que la Empresa A muestra una mayor disponibilidad de servicios en comparación con la Empresa B, lo que podría deberse a una mejor gestión, infraestructura tecnológica y la implementación de políticas y prácticas más efectivas para garantizar un tiempo de actividad más alto.

Los estadísticos descriptivos para este indicador son los siguientes.

Tabla 13. *Estadísticos descriptivos del indicador Tiempo de actividad del servicio*

	Total	Mínimo	Máximo	Media	Desviación estándar
Muestra 1	6	12	48	20	14.53
Muestra 2	6	1	2	1.17	0.40

Fuente: Elaboración propia

La Muestra 1 presenta una mayor variabilidad en los tiempos de actividad del servicio, con algunos servicios teniendo períodos más cortos y otros con períodos más largos. En contraste, la Muestra 2 muestra una variabilidad mucho menor y períodos de actividad más consistentes y cortos. Esta disparidad se causada por diferentes características de los servicios en cada muestra, como su estabilidad, configuración o demanda.

Indicador: Tiempos de respuesta.

Los datos se obtuvieron a través de una ficha de observación, la cual se aplicó a dos empresas diferentes, obteniendo los tiempos de respuesta para determinar la diferencia en ambas muestras.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 14. *Prueba de normalidad de indicador Tiempos de respuesta*

Shapiro-Wilk			
Muestras	**Estadístico**	**gl**	**Sig.**
Muestra 1	0.604	6	0.001
Muestra 2	0.848	6	0.152

Fuente: Elaboración propia

Con el análisis y normalización de los datos, se aplicó la prueba de Shapiro-Wilk con una muestra menor de 50 y con lo obtenido se acepta la hipótesis alternativa.

Al trabajar con dos muestras independientes, la prueba estadística no paramétrica a utilizar es la prueba de U Mann-Whitney.

HIPÓTESIS PARA PRUEBA U MANN WHITNEY (PRUEBA NO PARAMÉTRICA)

Ho: El software desplegado en el servidor de la Empresa A no tiene tiempos de respuesta similares al software desplegado en el servidor de la Empresa B.

Ha: El software desplegado en el servidor de la Empresa A tiene tiempos de respuesta similares al software desplegado en el servidor de la Empresa B.

Siendo, empresa “A” (Tedregal E.I.R.L.) y empresa “B” (Plataformas y Soluciones Digitales S.A.C.).

CRITERIOS DE DECISIÓN:

Si p < 0.05, se rechaza la Ho y se acepta la Ha.

Si p >= 0.05, se rechaza la Ha y se acepta la Ho.

Tabla 15. *Prueba de U MANN-Whitney para el indicador Tiempos de respuesta*

Prueba U de Mann-Whitney		
	Z	**Sig. Asin. (Bilateral)**
Muestra	-1.925	0.054

Fuente: Elaboración propia

Dado que el valor de la significancia asintótica es mayor que 0.05, se acepta la hipótesis nula de acuerdo al nivel significancia obtenido. Por lo tanto, el software desplegado en el servidor de la Empresa A no tiene tiempos de respuesta similares al software desplegado en el servidor de la Empresa B. El resultado implica que el software de ambas empresas presenta cargas de trabajo diferentes, existen problemas en su infraestructura, sus servicios tienen diferentes recursos, etc., lo que puede indicar un rendimiento deficiente.

Por último, se presenta los siguientes estadísticos descriptivos.

Tabla 16. *Estadísticos descriptivos del indicador Tiempos de respuesta*

	Total	**Mínimo**	**Máximo**	**Media**	**Desviación estándar**
Muestra 1	6	120	706	248.50	225.53
Muestra 2	6	301	353	320.83	22.35

Fuente: Elaboración propia

Las muestras presentan diferencias notables en los tiempos de respuesta. En la Muestra 1, se observa una mayor variabilidad con tiempos mínimos de 120

milisegundos y máximos de 706 milisegundos, mientras que la Muestra 2 muestra una variabilidad más reducida, con tiempos mínimos de 301 milisegundos y máximos de 353 milisegundos. Además, la media de tiempos de respuesta es de 248.50 milisegundos en la Muestra 1 y de 320.83 milisegundos en la Muestra 2.

V. DISCUSIÓN

Se tuvo como finalidad proponer una guía metodológica para la implementación de una infraestructura en la nube. Asimismo, se establecieron objetivos específicos con el fin de demostrar dicha finalidad. Entre estos, son: Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento; Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube y Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta.

Con el propósito de lograrlo, se seleccionaron dos empresas y se recopilaron datos a través de tres fichas de observación. Los datos obtenidos de cada muestra, revelaron una distribución que no seguía una distribución normal. Por ello, se utilizó la prueba no paramétrica de U de Mann-Whitney, además de que se utilizó dos muestras independientes.

La hipótesis que se planteó es “Una guía metodológica basada en Amazon Web Services (AWS) facilita la selección, implementación y despliegue de servicios y aplicaciones en la nube”. Los resultados obtenidos permitirían determinar si se debía aceptar o rechazar dicha hipótesis a través de los servicios en la nube que se aprovisionaron aplicando la norma ISO 27017:2015, el tiempo que demandó realizar ello y, el rendimiento y la disponibilidad de estos. La hipótesis se acepta utilizando los indicadores mencionados, ya que no se ve afectada. Al realizar la prueba no paramétrica de U Mann Whitney, se puede observar que no hay diferencias entre las dos muestras independientes.

En lo que respecta a determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento radica en asegurar el nivel de cumplimiento en las empresas ya que norma proporciona directrices para la seguridad de la información en la nube, abordando la gestión de riesgos y la protección de datos. Los resultados de la investigación señalaron la frecuencia de uso de estas normas como lo es la ISO

27017:2015 siguiendo las recomendaciones de NIST tal como lo indica (Mell, Grance 2011), en relación a los estándares de seguridad para los servicios en la nube.

Con respecto a la frecuencia de uso de los controles de seguridad de la norma ISO 27017:2015, en la aplicación de la mayoría de sus controles, la primera empresa presentó un nivel de acuerdo a lo establecido en el indicador, esto significa que se cumplen en gran medida la mayoría de los requisitos de la norma ISO, sin embargo, todavía existen algunos aspectos que pueden ser mejorados. Mientras que en la segunda empresa, su frecuencia de uso fue de un nivel neutral, esto significa que existen algunas deficiencias en el cumplimiento de los requisitos de la norma ISO, con áreas que requieren mejoras. En ambas también se denotó que no se implementaron controles criptográficos y de seguridad, y al ser empresas que almacenan datos puede causar violaciones de seguridad, filtraciones de datos, pérdida de confianza de los clientes e interrupciones en los servicios, lo que resulta en un déficit económico. La implementación de controles es crucial para proteger los datos almacenados en la nube de AWS, según las investigaciones de (Bagaeen et al. 2019; Kamaruddin et al. 2020; Bhardwaj et al. 2016; Kumari, singh 2021). Estos estudios enfatizan la importancia de dichos controles, ya que señalan que la falta de implementación puede dejar los datos vulnerables a ataques y accesos no autorizados.

La importancia de estos estándares se acredita con la investigación de (Zeadally, Das, Sklavos 2021) acerca de tecnologías criptográficas y estándares de protocolo para el Internet de las Cosas que también ejecuta la norma ISO 27017 ya que es crucial para las empresas fabricantes de dispositivos y electrodomésticos de IoT. Además, se contrasta la aplicabilidad de estas normas con lo que indica el artículo de (Ali et al. 2020; Kim et al. 2020) donde el propósito de estas certificaciones es establecer estándares que aseguren la seguridad y protección de la información, con el fin de fomentar una adopción segura y responsable de la tecnología en la nube.

Continuando con los resultados, en lo que concierne a identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube, se utilizó el indicador “Tiempo de diseño e implementación” y se obtuvo que en la primera empresa tomó 17 días para diseñar e implementar los servicios en nube, mientras que en la segunda empresa fue de 11 días. Se tiene que comprender los requisitos específicos de cada cliente (o empresa) para adaptar los servicios en la nube según sus necesidades individuales. Esto incluye considerar aspectos como capacidad de almacenamiento, rendimiento, seguridad y cumplimiento normativo. Además, se deben abordar los desafíos relacionados con la integración de sistemas existentes en la infraestructura del cliente.

El tiempo que se empleó ya sea en la primera o segunda empresa, se relaciona con la investigación de (Peralta Trejo, Laura Ochoa 2019) donde se empleó dieciséis días en lo que respecta a implementar los servicios en la nube y se demuestra cómo además de la complejidad de la implementación de servicios en la nube, se implica considerar aspectos como capacidad de almacenamiento, rendimiento, seguridad y cumplimiento normativo. Asimismo, hay que tener en cuenta la complejidad de la arquitectura en cuanto al tipo de aplicación. Por ejemplo, el tiempo necesario para aprovisionar una arquitectura de una aplicación web difiere considerablemente del requerido para una relacionada con ciencias médicas en el caso del trabajo de (Avula et al. 2012). En lo que respecta a una aplicación web, el enfoque se centra en la disponibilidad, escalabilidad y seguridad de los datos, lo que permite un proceso de aprovisionamiento más rápido. Por otro lado, las aplicaciones médicas deben considerar aspectos como la privacidad de los datos, regulaciones específicas, interoperabilidad y seguridad avanzada, lo que implica un análisis exhaustivo y pruebas rigurosas. También, se contrasta con las investigaciones de (Bahrami 2015; Garay Gómez 2016; Figueroa Lozano 2019) donde en cada investigación, el tiempo de diseño y/o de implementación va en relación con la complejidad del software.

En cuanto al evaluar el rendimiento y la disponibilidad de servicios en la nube, se utilizaron los indicadores “Porcentaje de utilización del recurso virtualizado”, “Tiempo de actividad del servicio” y “Tiempos de respuesta”, cuando se compara los conjuntos de datos de cada muestra, se pueden observar diferencias significativas en las métricas de rendimiento de los servicios en la nube. El software de la primera muestra, tanto para EC2 como para RDS, se registra un porcentaje de utilización más bajo en comparación con el software de la segunda muestra. El tiempo de actividad se mantiene constante en 1 unidad para ambos servicios en este conjunto, mientras que los tiempos de respuesta varían dentro de un rango específico. También, se observa un aumento considerable en el porcentaje de utilización para EC2, indicando un mayor nivel de carga de trabajo o tráfico en el sistema en comparación con el primer conjunto. Además, el tiempo de actividad se incrementa en diferentes intervalos de tiempo, lo que sugiere un monitoreo más prolongado, tal como lo realiza (Zhang 2020) con herramientas de monitoreo de manera constante. Los tiempos de respuesta en EC2 muestran una mayor variabilidad, con algunas mediciones más altas que podrían indicar períodos de mayor demanda y otros más bajos que indicarían un rendimiento más eficiente. También, como lo indican (Lin, Pan, Liu 2022; Büyüközkan, Uztürk, Maden 2023; Ardagna et al. 2021) en su investigación, al evaluar el rendimiento de los servicios en la nube, es importante considerar todas las medidas detectadas para tomar decisiones más eficientes y rápidas. Lo anterior también se respalda con la investigación de (Xu, Goteng, He 2021) la cual se demuestra que una baja latencia y alta disponibilidad en los servicios en la nube correctamente configurados, brindan un mayor tiempo de respuesta y garantizan estabilidad en las solicitudes que realizan los usuarios en las aplicaciones, reflejando un mayor nivel de usabilidad y confiabilidad de los servicios en la nube.

El presente estudio se consideró relevante debido al uso de la emergente tecnología en la nube y sus grandes beneficios y variedades que se han ido

desarrollando, teniendo como fundamento la investigación de (Wu et al. 2010) e investigaciones actuales como la de (Kewate 2022).

Por otro lado, se enfocó en la implementación de una infraestructura en la nube y su evaluación en cuanto a su rendimiento, seguridad y tiempo de implementación. Mientras que investigaciones previas han abordado aspectos similares pero con enfoques diferentes como es el caso de la investigación de (Bora, Ahmed 2013) donde se ejecuta en instituciones educativas y utilizan tecnología cloud de vanguardia relacionada en lo que respecta a seguridad, privacidad, etc. También con las investigaciones de (Amron, Ibrahim, Chuprat 2017; Abdalla, Varol 2019) donde lo realizan a través de otros modelos de servicios como IaaS y StaaS haciendo uso principalmente del almacenamiento. Por último, con las investigaciones de (Ivanova, Borovska, Zahov 2018; Rodríguez de la Cruz 2020) donde se reducen los tiempos de implementación a través de la infraestructura como código, ejecutándolo de manera automatizada.

Finalmente se destacó la importancia de cumplir con los controles de seguridad de la norma ISO 27017:2015 y se contrastaron los resultados obtenidos con investigaciones anteriores que respaldan la relevancia de las certificaciones en la seguridad de la información en la nube. Además, se compararon los tiempos de implementación encontrados con investigaciones anteriores que también han destacado la complejidad y los desafíos relacionados con el diseño e implementación de servicios en la nube.

VI. CONCLUSIONES

1. Con respecto al objetivo general se concluyó que sí es posible proponer una guía metodológica ya que se ha fundamentado en la comprensión de los controles de seguridad, la consideración de factores como los costos, la tecnología y la complejidad, y la evaluación del rendimiento y la disponibilidad de los servicios en la nube. Estos aspectos son fundamentales para garantizar la seguridad, eficiencia y continuidad en el uso de la infraestructura en la nube por parte de las empresas.

2. En relación al primer objetivo específico, se concluye la importancia de comprender y determinar los controles de seguridad establecidos por la norma ISO 27017:2015 y evaluar su aplicabilidad en el entorno de AWS para asegurar el cumplimiento de estos controles en las empresas debido a lo esencial que es para garantizar la seguridad y protección de los datos y evitar riesgos como la pérdida, divulgación o alteración no autorizada de los datos. La evaluación del nivel de cumplimiento en relación con esta norma resulta esencial para asegurar la implementación de los controles adecuados y el seguimiento de las mejores prácticas en la protección de datos en la nube. Asimismo se concluye que la evaluación del nivel de cumplimiento de la norma ISO 27017:2015 brinda una visión clara de posibles brechas de seguridad y áreas que requieren mejoras, permitiendo la adopción de medidas correctivas y el establecimiento de una sólida estrategia de gestión de riesgos de los servicios en la nube.

3. Con el segundo objetivo específico, el tiempo necesario para diseñar e implementar servicios en la nube varía entre empresas debido a factores como los costos, la tecnología, la complejidad y el software específico de cada organización. Los costos tuvieron un papel importante en el tiempo requerido para implementar servicios en la nube, ya que cada empresa tiene un presupuesto único y debe evaluar cuidadosamente los gastos

asociados. Esto se pudo comprobar debido a que los servicios implementados por la primera empresa fueron mayores a los de la segunda empresa y fue por el criterio económico. Además, con la influencia económica, la elección de la tecnología también influye en el tiempo necesario, ya que las empresas pueden optar por soluciones consolidadas y rápidas o tecnologías emergentes que requieren más tiempo de configuración. La complejidad del software para cada empresa también fue otro factor a considerar, ya que cada empresa tiene su propia arquitectura tecnológica que debe integrarse en la nube.

4. Por último, con el tercer objetivo específico se concluye que la evaluación del rendimiento y la disponibilidad de servicios en la nube es esencial para cualquier aplicación, ya sea una aplicación móvil como para una aplicación web, estas alojadas en AWS. Al evaluar el rendimiento, es importante considerar aspectos como la latencia, la capacidad de respuesta y la eficiencia en el uso de recursos por lo que esta evaluación permite anticipar a futuros desafíos y garantizar la escalabilidad y el crecimiento adecuado de la aplicación. Al identificar posibles cuellos de botella y limitaciones en el rendimiento, se puede tomar medidas proactivas para escalar y adaptar la infraestructura en la nube según sea necesario. Con la respectiva evaluación del rendimiento y la disponibilidad de los servicios en la nube que se configuraron, fue esencial para garantizar un correcto funcionamiento en las aplicaciones ambas. Al analizarlas, se observaron diferencias en el porcentaje de utilización, el tiempo de actividad y los tiempos de respuesta. Mientras que en la primera muestra, hubo una alta carga en los recursos utilizados, lo que requiere optimizar el rendimiento para una experiencia de usuario satisfactoria. En la segunda muestra, la carga fue menor, pero aún se deben mejorar los tiempos de respuesta. Esto depende por parte de la debida configuración de los servicios en la nube, el tiempo de las consultas hacia el servidor o las consultas hacia la base de datos.

También al software por sí mismo dado que es posible que no esté lo mejor optimizado posible.

VII. RECOMENDACIONES

Existen áreas adicionales en las que se puede profundizar, como los procedimientos de administración y despliegue de infraestructuras en la nube, los factores clave asociados al tiempo de diseño e implementación, y la evaluación del rendimiento y la disponibilidad de los servicios en la nube.

La investigación no incluyó el uso de infraestructura como código, donde en lugar de configurar manualmente los recursos de infraestructura, se utilizan scripts y archivos de configuración que permiten crear y mantener la infraestructura de manera automatizada y reproducible. Para futuras investigaciones, sería recomendable explorar cómo la infraestructura como código puede ser aplicada y optimizada en el contexto específico de la implementación de una infraestructura en la nube y el cumplimiento de los controles de seguridad. Esto podría incluir el diseño y desarrollo de modelos de infraestructura reutilizables, la evaluación de herramientas y prácticas recomendadas, y la comparación de enfoques tradicionales de gestión de infraestructura con la metodología de infraestructura como código.

En el proyecto de investigación, el criterio de inclusión se definió de manera específica y limitada. Por ello, se recomienda ampliar el criterio de inclusión en futuras investigaciones para abordar una mayor diversidad de variables y participantes, lo que permitiría obtener conclusiones más sólidas y representativas.

Se recomienda dedicar más tiempo y esfuerzo a estudiar exhaustivamente el estado del arte de la investigación relacionada. Esto permitirá obtener una visión completa de las teorías, metodologías y hallazgos más recientes para comparar los estudios de los años previos. Al comparar los enfoques y resultados de diferentes investigaciones previas, permitirá comprender cómo ha avanzado el conocimiento sobre el tema de la investigación. Es por ello que el instrumento utilizado esté actualizado y sea capaz de capturar dichos elementos adicionales. Esto puede implicar la incorporación de nuevas preguntas, un

tamaño de muestra mayor, escalas o ítems al instrumento existente, o incluso el desarrollo de un nuevo instrumento en su totalidad.

Se recomienda la incorporación de proveedores de servicios en la nube adicionales ya que el utilizar otros proveedores de servicios en la nube, ofrece beneficios como diversificación, redundancia, optimización de costos, acceso a características especializadas y mayor flexibilidad. Sin embargo, es importante tener en cuenta que otros proveedores pueden ofrecer tecnologías diferentes o semejantes a las de AWS, y que no fueron estudiadas previamente debido a la falta de exploración para observar los resultados de la investigación.

Finalmente, se recomienda realizar un diseño preexperimental en el estudio para evaluar el impacto de la implementación en los controles de la norma ISO 27017:2015, el tiempo de demanda y el monitoreo del rendimiento de las aplicaciones. Este diseño permite establecer una línea base de medición antes de la intervención y comparar los resultados con las mediciones posteriores.

REFERENCIAS

SYNERGY RESEARCH GROUP, 2022. Q2 Cloud Market Grows by 29% Despite Strong Currency Headwinds; Amazon Increases its Share. en línea. 28 julio 2022. Recuperado a partir de : https://www.srgresearch.com/articles/q2-cloud-market-grows-by-29-despite-strong-currency-headwinds-amazon-increases-its-share

ABDALLA, Peshraw Ahmed y VAROL, Asaf, 2019. Advantages to Disadvantages of Cloud Computing for Small-Sized Business. En: 2019 7th International Symposium on Digital Forensics and Security (ISDFS). junio 2019. pp. 1-6. DOI 10.1109/ISDFS.2019.8757549.

AMRON, Mohd Talmizie, IBRAHIM, Roslina y CHUPRAT, Suriayati, 2017. A Review on Cloud Computing Acceptance Factors. Procedia Computer Science. 1 enero 2017. Vol. 124, pp. 639-646. DOI 10.1016/j.procs.2017.12.200.

ARDAGNA, C.A., ASAL, R., DAMIANI, E., DIMITRAKOS, T., IOINI, N.E. y PAHL, C., 2021. Certification-Based Cloud Adaptation. IEEE Transactions on Services Computing. 2021. Vol. 14, no. 1, pp. 82-96. DOI 10.1109/TSC.2018.2793268. Scopus

ZEADALLY, Sherali, DAS, Ashok Kumar y SKLAVOS, Nicolas, 2021. Cryptographic technologies and protocol standards for Internet of Things. Internet of Things. Vol. 14, p. 100075. DOI 10.1016/j.iot.2019.100075.

KIM, Hyunmin et al., 2020. The role of fifth-generation mobile technology in prehospital emergency care: An opportunity to support paramedics. Health Policy and Technology. Vol. 9, número 1, pp. 109-114. DOI 10.1016/j.hlpt.2020.01.002.

ALI, Omar et al., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly. Vol. 37, número 1, p. 101419. DOI 10.1016/j.giq.2019.101419.

AVULA, Tejaswi, NELA, Manoj Kumar, GUDAPATI, Radhika y VELAGAPUDI, Sreenivas, 2012. Efficient Use of Cloud Computing in Medical Science. American Journal of Computational Mathematics. 2012. Vol. 02, no. 03, pp. 240-243. DOI 10.4236/ajcm.2012.23032.

BAGAEEN, Aroba, AL-ZOUBI, Sawsan, AL-SAYYED, Rizik y RODAN, Ali, 2019. Storage as a Service (STaaS) Security Challenges and Solutions in Cloud Computing Environment: An Evaluation Review. En: 2019 Sixth HCT Information Technology Trends (ITT). noviembre 2019. pp. 208-213. DOI 10.1109/ITT48889.2019.9075097.

KAMARUDDIN, Ahada, MOHAMED, Ibrahim, JARNO, Ahmad y DAUD, Maslina, 2020. CLOUD SECURITY PRE-ASSESSMENT MODEL FOR CLOUD SERVICE PROVIDER BASED ON ISO/IEC 27017:2015 ADDITIONAL CONTROL. *International Journal of Innovation and Industrial Revolution*. 1 diciembre 2020. Vol. 2, pp. 01-17. DOI 10.35631/IJIREV.25001.

XU, Peng, GOTENG, Gokop L. y HE, Yu, 2021. Modelling cloud service latency and availability using a deep learning strategy. *Expert Systems with Applications*. Vol. 182, p. 115121. DOI 10.1016/j.eswa.2021.115121.

BAHRAMI, Mehdi, 2015. Cloud Computing for Emerging Mobile Cloud Apps. En: 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. marzo 2015. pp. 4-5. DOI 10.1109/MobileCloud.2015.40.

Benefits of Cloud Computing, 2022. en línea. [Accedido 5 octubre 2022]. Recuperado a partir de: https://www.ibm.com/cloud/learn/benefits-of-cloud-computing

BHARDWAJ, Akashdeep, SUBRAHMANYAM, G. V. B., AVASTHI, Vinay y SASTRY, Hanumat, 2016. Security Algorithms for Cloud Computing. Procedia

Computer Science. 1 enero 2016. Vol. 85, pp. 535-542. DOI 10.1016/j.procs.2016.05.215.

BORA, Utpal Jyoti y AHMED, Majidul, 2013. E-Learning using Cloud Computing. en línea. Vol. 1, número 2. Disponible en: https://www.ijisme.org/wp-content/uploads/papers/v1i2/B0111011213.pdf

BÜYÜKÖZKAN, Gülçin, UZTÜRK, Deniz y MADEN, Ayça, 2023. Influential factor analysis for cloud computing technology service provider. *Technological Forecasting and Social Change*. Vol. 192, p. 122531. DOI 10.1016/j.techfore.2023.122531.

LIN, L., PAN, L. y LIU, S., 2022. Methods for improving the availability of spot instances: A survey. Computers in Industry. 2022. Vol. 141. DOI 10.1016/j.compind.2022.103718. Scopus

SONG, X., PAN, L. y LIU, S., 2022. An online algorithm for optimally releasing multiple on-demand instances in IaaS clouds. Future Generation Computer Systems. 2022. Vol. 136, pp. 311-321. DOI 10.1016/j.future.2022.06.014. Scopus

WU, Jiyi, PING, Lingdi, GE, Xiaoping, WANG, Ya y FU, Jianqing, 2010. Cloud Storage as the Infrastructure of Cloud Computing. En: 2010 International Conference on Intelligent Computing and Cognitive Informatics. junio 2010. pp. 380-383. DOI 10.1109/ICICCI.2010.119.

FIGUEROA LOZANO, Jean Pierre, 2019. Definición y aplicación de una metodología de gestión de riesgos de seguridad de la información para la implementación de una plataforma web alojado en el modelo de servicio IaaS de Cloud Computing. Universidad Tecnológica del Perú. en línea. 2019. [Accedido 6 octubre 2022]. Recuperado a partir de: http://repositorio.utp.edu.pe/handle/20.500.12867/2818Accepted: 2020-03-01T00:31:18Z

GARAY GÓMEZ, Kramer Silverio, 2016. Buenas prácticas de seguridad para la migración del ambiente de desarrollo/pruebas de un centro de datos on premise hacia una nube pública. Universidad Tecnológica del Perú. en línea. 2016. [Accedido 6 octubre 2022]. Recuperado a partir de: http://repositorio.utp.edu.pe/handle/20.500.12867/3523Accepted: 2021-01-08T22:13:26Z

PERALTA TREJO, Gustavo Alonso y LAURA OCHOA, Víctor, 2019. Propuesta de plan de migración de cloud para los sistemas de información del instituto nacional de estadística e informática. Universidad Tecnológica del Perú. en línea. 2019. [Accedido 6 octubre 2022]. Recuperado a partir de: http://repositorio.utp.edu.pe/handle/20.500.12867/2929Accepted: 2020-07-08T17:53:17Z

IVANOVA, Desislava, BOROVSKA, Plamenka y ZAHOV, Stefan, 2018. Development of PaaS using AWS and Terraform for medical imaging analytics. AIP Conference Proceedings. 10 diciembre 2018. Vol. 2048, no. 1, pp. 060018. DOI 10.1063/1.5082133.

KEWATE, Neha, 2022. A Review on AWS - Cloud Computing Technology. *International Journal for Research in Applied Science and Engineering Technology*. 31 enero 2022. Vol. 10, no. 1, pp. 258-263. DOI 10.22214/ijraset.2022.39802.

KUMARI, Poonam y SINGH, Meeta, 2021. A Review: Different Challenges in Energy-Efficient Cloud Security. IOP Conference Series: Earth and Environmental Science. junio 2021. Vol. 785, no. 1, pp. 012002. DOI 10.1088/1755-1315/785/1/012002.

MELL, Peter y GRANCE, Timothy, 2011. The NIST Definition of Cloud Computing. 2011. pp. 7.

RODRÍGUEZ DE LA CRUZ, Alberto, 2020. Herramienta para despliegue y gestión de plataformas en la nube. en línea. 2020. [Accedido 13 octubre 2022].

Recuperado a partir de: https://idus.us.es/handle/11441/108955Accepted: 2021-05-12T17:10:45Z.

ZHANG, Ruidong, 2020. The impacts of cloud computing architecture on cloud service performance. Journal of Computer Information Systems. 3 marzo 2020. Vol. 60, no. 2, pp. 166-174. DOI 10.1080/08874417.2018.1429957.

ARIAS-GÓMEZ, Jesús, VILLASÍS-KEEVER, Miguel y MIRANDA-NOVALES, María, 2016. El protocolo de investigación III: la población de estudio. Revista Alergia México. 11 mayo 2016. Vol. 63, pp. 201. DOI 10.29262/ram.v63i2.181.

Babbie, E. R. (2013). The basics of social research (6th ed.). Wadsworth, Cengage Learning.

ARIAS GONZALES, Jose, 2021. TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN CIENTÍIFICA.

HERNÁNDEZ MENDOZA, Sandra Luz y Danae DUANA AVILA. Técnicas e instrumentos de recolección de datos. Revista científica [en línea]. 2020, 9(17), 53. ISSN 2007-4913 [consultado el 5 de mayo de 2022]. Disponible en: https://repository.uaeh.edu.mx/revistas/index.php/icea/article/download/6019/7678

QUINTANA PEÑA, Alberto, 2006. Metodología de Investigación Científica Cualitativa. Investigación cualitativa. pp. 38.

IBM (2014). ¿Por qué elegir IBM SPSS Statistics? Recuperado de http://www01.ibm.com/software/mx/analytics/spss/products/statistics/ IBM SPSS Statistics (Edition 22) [Software de computación]. Chicago, IL, EE.UU.

ANEXOS

Anexo 1: Matriz De Consistencia

Título	Pregunta General	Objetivo General	Preguntas Específicas	Objetivos Específicos	Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala De medición	Diseño Metodológico
Metodología basada en la implementación de una infraestructura en la nube	¿Cuál es la aplicabilidad de los controles de seguridad de la norma ISO 27017:2015 en la implementación de servicios en la nube?	Proponer una guía metodológica para la implementación de una infraestructura en la nube	¿Cuáles son los procedimientos para poder administrar y desplegar una correcta infraestructura en la nube?	Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento	Infraestructura en la nube	La infraestructura de nube es la recopilación de elementos de hardware y software necesarios para hacer posible la informática de nube. Incluye capacidad de procesamiento, red y almacenamiento, así como una interfaz para que los usuarios accedan a sus recursos virtualizados.	Estas tecnologías conforman una arquitectura informática de nube en la que se pueden ejecutar las aplicaciones, lo que brinda a los usuarios finales la capacidad de aprovechar el potencial de los recursos de la nube.	Seguridad	Nivel de cumplimiento del control de la norma ISO 27017:2015	Ordinal	Descriptivo
				Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube				Complejidad	Tiempo de diseño e implementación (días)	Razón	
				Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta				Rendimiento	Porcentaje de utilización del recurso virtualizado		
									Tiempo de actividad del servicio		
									Tiempos de respuesta		

Fuente: Elaboración propia del autor.

Anexo 2: Indicadores de variables

OBJETIVO ESPECÍFICO	INDICADOR	DESCRIPCIÓN	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento	Nivel de cumplimiento del control de la norma ISO 27017:2015	Medida en que una organización ha implementado los controles de seguridad de la información específicos establecidos en la norma por parte del investigador para garantizar la seguridad de sus servicios en la nube.	Observación/Ficha de observación	2 semanas	Evaluación según el criterio del investigador. Se mide en una escala de Likert que va desde Totalmente en desacuerdo, En desacuerdo, Neutral, De acuerdo y Totalmente de acuerdo
Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube	Tiempo de diseño e implementación (días)	Cantidad de días que se estima que tomará completar el proceso de diseño y aprovisionamiento de los servicios.		3 semanas	Evaluación según el criterio del investigador
Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta	Porcentaje de utilización del recurso virtualizado	Medida o cuantificación de utilización del recurso virtualizado (CPU, RAM, red, etc.) durante una carga de trabajo.		1 semana	Obtenidos a través de la consola de administración en la nube.
	Tiempo de actividad del servicio	Cuantificación del tiempo durante el cual el servicio se mantiene ejecutándose.		3 semanas	

	Tiempos de respuesta	Cuantificación de la velocidad/resultado del servicio ejecutándose con el fin de medir su velocidad y estabilidad en condiciones de trabajo.		1 semana	Obtenidos a través de las herramientas de desarrollo para pruebas de conectividad.

Fuente: Elaboración propia del autor.

Anexo 3. Matriz de operacionalización de variables

VARIABLE DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN	COMO MEDIRLO	TÉCNICA/ INSTRUMENTO
Infraestructura en la nube	La infraestructura de nube es la recopilación de elementos de hardware y software necesarios para hacer posible la informática de nube. Incluye capacidad de procesamiento, red y almacenamiento, así como una interfaz para que los usuarios accedan a sus recursos virtualizados.	Estas tecnologías conforman una arquitectura informática de nube en la que se pueden ejecutar las aplicaciones, lo que brinda a los usuarios finales la capacidad de aprovechar el potencial de los recursos de la nube.	Seguridad	Nivel de cumplimiento del control de la norma ISO 27017:2015	Ordinal	Escala de Likert	Observación/Ficha de observación
			Complejidad	Tiempo de diseño e implementación (días)	Razón	Escala numérica	
			Rendimiento	Porcentaje de utilización del recurso virtualizado			
				Tiempo de actividad del servicio			
				Tiempos de respuesta			

Fuente: Elaboración propia del autor.

Anexo 4: Instrumento de recolección de datos – Ficha de observación - I

Ficha de observación				
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva
Empresa / Institución				
Objetivo específico	Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento			
Dimensión de estudio	Seguridad			
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023	

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Nivel de cumplimiento del control de la norma ISO 27017:2015	Nivel de cumplimiento

No de iteración	**Fecha de revisión**	**Control de la norma ISO**	**Nivel de cumplimiento**
1			
2			
3			
4			
5			

Fuente: Elaboración propia del autor.

Anexo 5: Instrumento de recolección de datos – Ficha de observación - II

Ficha de observación				
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva
Empresa / Institución				
Dimensión de estudio	Complejidad			
Objetivo específico	Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube			
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023	

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Tiempo de diseño e implementación (días)	Días

No de iteración	**Fecha de revisión**	**Nombre del recurso**	**Tiempo (días)**
1			
2			
3			
4			
5			

Fuente: Elaboración propia del autor.

Anexo 6: Instrumento de recolección de datos – Ficha de observación III

Ficha de observación						
Investigador	Carlos Gabriel Masias Ordinola			**Tipo de prueba**	Descriptiva	
Empresa / Institución						
Dimensión de estudio	Rendimiento					
Objetivo específico	Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta					
Fecha de inicio	01/06/2023		**Fecha final**	05/07/2023		

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Porcentaje de utilización del recurso virtualizado	Tasa porcentual
	Tiempo de actividad del servicio	Horas
	Tiempos de respuesta	Milisegundos

No de iteración	**Fecha de revisión**	**Tipo de recurso**	**Nombre del servicio**	**Porcentaje de utilización**	**Tiempo de actividad**	**Tiempos de respuesta**
1						
2						
3						
4						
5						

Fuente: Elaboración propia del autor.

Anexo 7: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad – I

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Silva Cumpa Gustavo Porfirio
Título y/o Grado Académico:	Maestria en Ingenieria de Sistemas

Doctor ( ) Magister (X) Ingeniero ( ) Licenciado ( ) Otro ().....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.					81
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					83
ORGANIZACION	Existe una organización lógica.					81
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					82
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					82
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					84
COHERENCIA	En los datos respecto al indicador.					81
METODOLOGIA	Responde al propósito de investigación.					90
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					82
	TOTAL					91

Anexo 8: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad – II

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Macalupú Masias Max Leo Junior
Título y/o Grado Académico:	Ingeniero informático

Doctor ( ) Magister () Ingeniero (X) Licenciado ( ) Otro ().....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					83
OBJETIVIDAD	Esta expresado en conducta observable.					83
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					83
ORGANIZACION	Existe una organización lógica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					82
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					85
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					86
COHERENCIA	En los datos respecto al indicador.					90
METODOLOGIA	Responde al propósito de investigación.					95
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					87
	TOTAL					85

Anexo 9: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad – III

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Seguridad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Huapaya Silupú Luis Fernando
Título y/o Grado Académico:	Bachiller en Ingenieria de Sistemas

Doctor ( ) Magister (_) Ingeniero ( ) Licenciado ( ) Otro (X).....

Universidad que labora:	
Fecha:	10/04/2023

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					81
OBJETIVIDAD	Esta expresado en conducta observable.					81
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					82
ORGANIZACION	Existe una organización lógica.					82
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					82
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					81
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					83
COHERENCIA	En los datos respecto al indicador.					81
METODOLOGIA	Responde al propósito de investigación.					82
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					81
	TOTAL					82

Anexo 10: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad – I

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Silva Cumpa Gustavo Porfirio
Título y/o Grado Académico:	Maestria en Ingenieria de Sistemas

Doctor ( ) Magister (X) Ingeniero ( ) Licenciado ( ) Otro ().....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					82
ORGANIZACION	Existe una organización lógica.					83
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					81
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					81
COHERENCIA	En los datos respecto al indicador.					83
METODOLOGIA	Responde al propósito de investigación.					82
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					81
	TOTAL					81

Anexo 11: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad – II

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Macalupú Masias Max Leo Junior
Título y/o Grado Académico:	Ingeniero informático

Doctor ( ) Magister (_) Ingeniero (X) Licenciado ( ) Otro ().....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					90
OBJETIVIDAD	Esta expresado en conducta observable.					98
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					85
ORGANIZACION	Existe una organización lógica.					95
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					91
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					92
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					90
COHERENCIA	En los datos respecto al indicador.					100
METODOLOGIA	Responde al propósito de investigación.					95
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					95
	TOTAL					93

Anexo 12: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad – III

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Complejidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Huapaya Silupú Luis Fernando
Título y/o Grado Académico:	Bachiller en Ingenieria de Sistemas

Doctor ( ) Magister (_) Ingeniero ( ) Licenciado ( ) Otro (X).....

Universidad que labora:	
Fecha:	**10/04/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					82
OBJETIVIDAD	Esta expresado en conducta observable.					82
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					81
ORGANIZACION	Existe una organización lógica.					81
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					82
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					82
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					81
COHERENCIA	En los datos respecto al indicador.					81
METODOLOGIA	Responde al propósito de investigación.					82
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					82
	TOTAL					82

Anexo 14: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento – I

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Silva Cumpa Gustavo Porfirio
Título y/o Grado Académico:	Maestria en Ingenieria de Sistemas

Doctor ( ) Magister (X) Ingeniero ( ) Licenciado ( ) Otro () .....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					90
OBJETIVIDAD	Esta expresado en conducta observable.					98
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					85
ORGANIZACION	Existe una organización lógica.					95
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					91
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					92
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					90
COHERENCIA	En los datos respecto al indicador.					100
METODOLOGIA	Responde al propósito de investigación.					95
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					95
	TOTAL					93

Anexo 15: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento – II

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Macalupú Masias Max Leo Junior
Título y/o Grado Académico:	Ingeniero informático

Doctor ( ) Magister ( ) Ingeniero (X) Licenciado ( ) Otro ( ) .....

Universidad que labora:	Universidad César Vallejo - Piura
Fecha:	**18/05/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					82
ORGANIZACIO N	Existe una organización lógica.					83
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					81
INTENCIONALI DAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCI A	Está basado en aspectos teóricos y científicos.					81
COHERENCIA	En los datos respecto al indicador.					83
METODOLOGI A	Responde al propósito de investigación.					82
PERTENENCI A	El instrumento es adecuado al tipo de investigación.					81
	TOTAL					81

Anexo 16: TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento – III

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Rendimiento.

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Huapaya Silupú Luis Fernando
Título y/o Grado Académico:	Bachiller en Ingenieria de Sistemas

Doctor ( ) Magister (_) Ingeniero ( ) Licenciado ( ) Otro (X) .....

Universidad que labora:	
Fecha:	**10/04/2023**

TESIS: METODOLOGÍA BASADA EN LA IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA EN LA NUBE

Autor: Masias Ordinola, Carlos Gabriel

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.					82
OBJETIVIDAD	Esta expresado en conducta observable.					82
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					82
ORGANIZACION	Existe una organización lógica.					81
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					82
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					81
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					82
COHERENCIA	En los datos respecto al indicador.					82
METODOLOGIA	Responde al propósito de investigación.					81
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					81
	TOTAL					82

Anexo 17: Carta de autorización – I

CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Tedregal

Yo MAX LEO JUNIOR MACALUPU MASIAS, identificado con DNI 46257001, en mi calidad de GERENTE GENERAL de la empresa **TEDREGAL EIRL** con R.U.C N° 20605744843, ubicada en la ciudad de Lima.

OTORGO LA AUTORIZACIÓN,

Al señor CARLOS GABRIEL MASIAS ORDINOLA, identificado con DNI N° 77132031, estudiante del décimo semestre de la Carrera profesional de Ingeniería de sistemas de la universidad César Vallejo filial Piura, para que utilice la siguiente información necesaria de la empresa con la finalidad de que pueda desarrollar su Trabajo de Investigación para optar al grado de Bachiller.

CONFIDENCIAL

_____

Firma y sello del Representante Legal o Representante del área

El Egresado/Bachiller declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos.

CONFIDENCIAL

_____

Firma del Egresado

Lima, 17 de octubre del 2022

Anexo 18: Carta de autorización – II

CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Yo SEGUIN RUÍZ ENRIQUE EMPERADOR, identificado con DNI N° XXXXXXXX, en mi calidad de REPRESENTANTE LEGAL de la empresa **PLATAFORMAS Y SOLUCIONES DIGITALES S.A.C.** con R.U.C N° 20610695257, ubicada en la ciudad de Piura.

OTORGO LA AUTORIZACIÓN,

Al señor CARLOS GABRIEL MASIAS ORDINOLA, identificado con DNI N° XXXXXXXX, estudiante del décimo semestre de la Carrera profesional de Ingeniería de sistemas de la universidad César Vallejo filial Piura, para que utilice la siguiente información necesaria de la empresa con la finalidad de que pueda desarrollar su Trabajo de Investigación para optar al grado de Bachiller.

CONFIDENCIAL

_____

Firma y sello del Representante Legal o Representante del área

El Egresado/Bachiller declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos.

CONFIDENCIAL

_____

Firma del Egresado

Piura, 17 de abril del 2023

Anexo 19: Contrato de confidencialidad – I

CONTRATO DE CONFIDENCIALIDAD, TRATAMIENTO Y PROTECCIÓN DE DATOS

Este Contrato de Confidencialidad, Tratamiento y Protección de Datos (en adelante, el "**Contrato**") se realiza entre:

Carlos Gabriel Masias Ordinola identificado con DNI XXXXXXXX, estudiante del último semestre de la carrera profesional de Ingeniería de Sistemas en la universidad César Vallejo filial Piura (en adelante, "**El Investigador**"), por una parte; y la empresa **TEDREGAL EIRL** con R.U.C N° 20605744843, (en adelante, "**La Empresa**"), por otra parte.

Ambas partes, conjuntamente conocidas como "**Las Partes**".

CONSIDERANDO:

1. El Investigador está llevando a cabo una tesis de investigación que implica la utilización de instrumentos y metodologías desarrolladas por él/ella misma en La Empresa.
2. La Empresa posee información y datos de carácter confidencial relacionados con su actividad y operaciones comerciales, que deben ser protegidos adecuadamente.
3. Las Partes desean establecer los términos y condiciones para garantizar la confidencialidad, tratamiento y protección de los datos y la información relevante en relación con la ejecución de la tesis en La Empresa.

Por lo tanto, ambas partes acuerdan lo siguiente:

1. Confidencialidad de la Información
    a. El Investigador se compromete a mantener en estricta confidencialidad toda la información y datos proporcionados por La Empresa, ya sea verbalmente, por escrito, electrónicamente o en cualquier otro formato, que sean considerados como confidenciales.
    b. El Investigador utilizará dicha información y datos exclusivamente para los fines de la ejecución de la tesis y se compromete a no

Anexo 20: Contrato de confidencialidad – II

CONTRATO DE CONFIDENCIALIDAD, TRATAMIENTO Y PROTECCIÓN DE DATOS

Este Contrato de Confidencialidad, Tratamiento y Protección de Datos (en adelante, el "**Contrato**") se realiza entre:

Carlos Gabriel Masias Ordinola identificado con DNI XXXXXXXX, estudiante del último semestre de la carrera profesional de Ingeniería de Sistemas en la universidad César Vallejo filial Piura (en adelante, "**El Investigador**"), por una parte; y la empresa **PLATAFORMAS Y SOLUCIONES DIGITALES S.A.C.** con R.U.C N° 20610695257, (en adelante, "**La Empresa**"), por otra parte.

Ambas partes, conjuntamente conocidas como "**Las Partes**".

CONSIDERANDO:

1. El Investigador está llevando a cabo una tesis de investigación que implica la utilización de instrumentos y metodologías desarrolladas por él/ella misma en La Empresa.
2. La Empresa posee información y datos de carácter confidencial relacionados con su actividad y operaciones comerciales, que deben ser protegidos adecuadamente.
3. Las Partes desean establecer los términos y condiciones para garantizar la confidencialidad, tratamiento y protección de los datos y la información relevante en relación con la ejecución de la tesis en La Empresa.

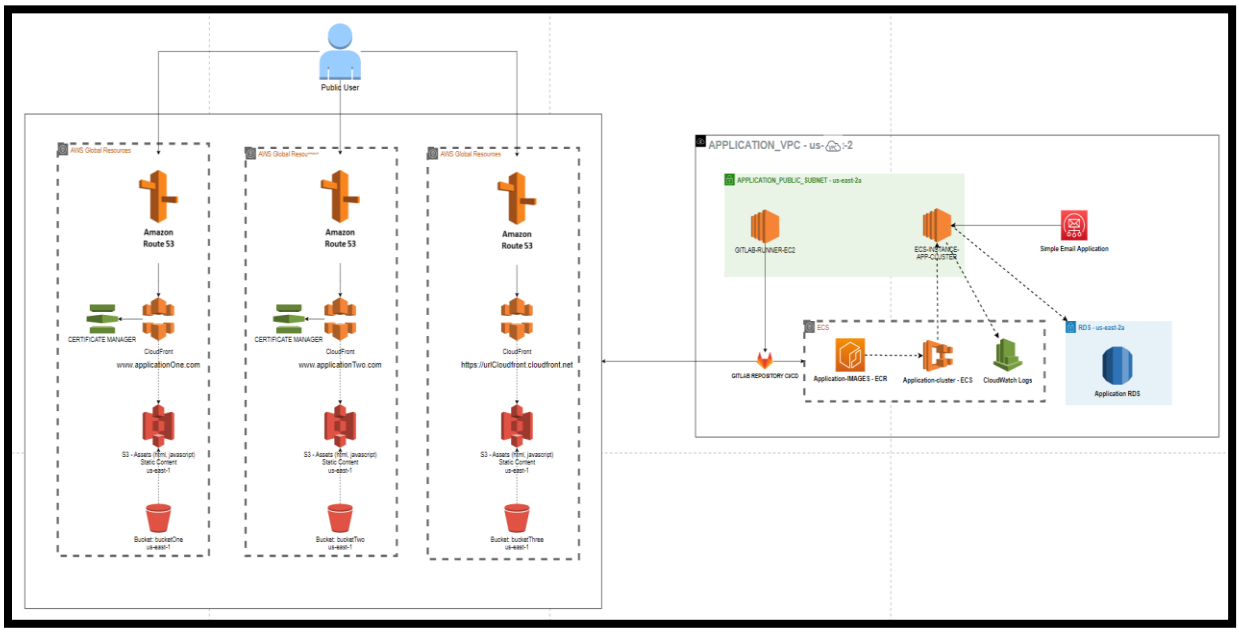
Por lo tanto, ambas partes acuerdan lo siguiente:

1. Confidencialidad de la Información
    a. El Investigador se compromete a mantener en estricta confidencialidad toda la información y datos proporcionados por La Empresa, ya sea verbalmente, por escrito, electrónicamente o en cualquier otro formato, que sean considerados como confidenciales.

Anexo 21: Desarrollo del proyecto

En el siguiente diagrama se detalla la arquitectura planteada para la empresa Tedregal E.I.R.L. y se analiza lo siguiente:

Figura 26. Diagrama de infraestructura en AWS de Tedregal E.I.R.L.



Fuente: Elaboración propia

- En el lado izquierdo del diagrama, se encuentra una red CDN. Los servicios que se muestran en ese lado del diagrama incluyen **Amazon Route 53**, **Amazon CloudFront**, **AWS Certificate Manager** y **Amazon Simple Storage Service (S3)**.

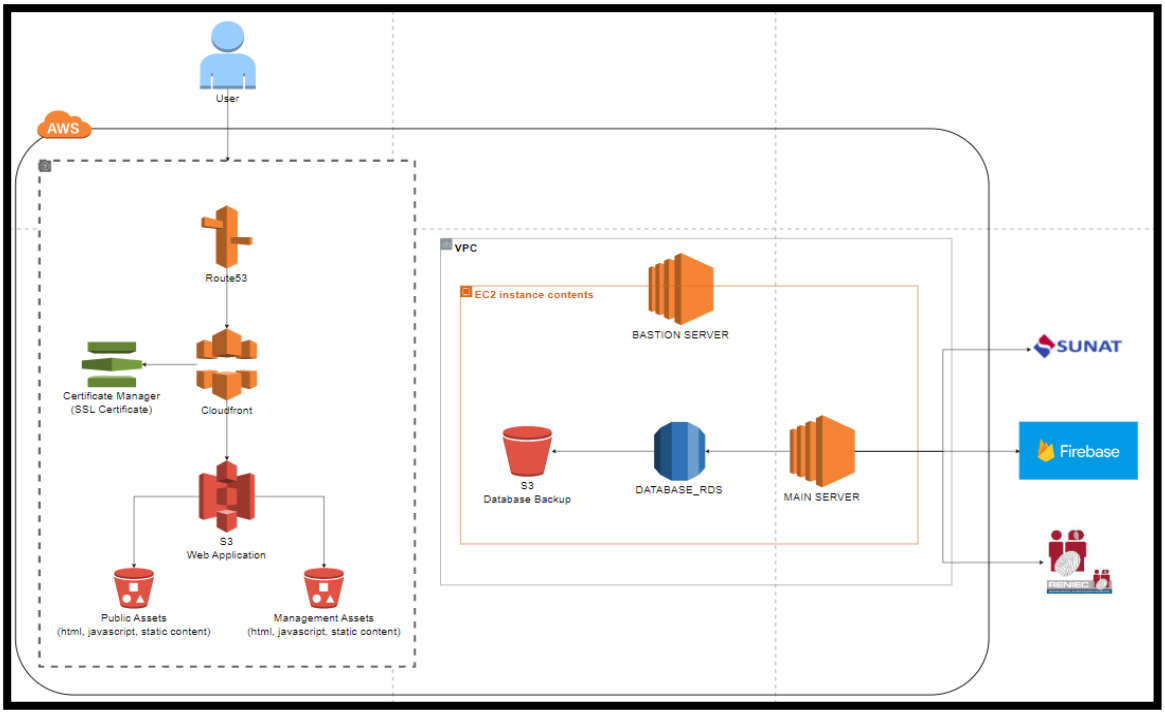
- Cada zona hospedada apunta a una distribución CloudFront. En las dos primeras distribuciones CloudFront se configuró para que tenga los certificados SSL, el punto de origen (nombre de dominio) y el Bucket junto a la ubicación donde se encuentra la aplicación web (contenido estático). Con respecto a la última distribución CloudFront, no se estableció un certificado SSL, puesto que se utiliza como entorno de pruebas.

- En el lado derecho del diagrama, se encuentran servidores para sus distintos usos, así como una base de datos, alarmas, repositorio de imágenes de

Docker, una aplicación de envío de correos y una integración hacia Gitlab para realizar integración y entrega continua. Una instancia EC2 (**Elastic Compute Cloud**), **Elastic Container Registry**, ECS (**Elastic Container Service**), **CloudWatch**, RDS (**Relational Database Service**) y **Amazon Simple Email Service** (SES).

Para el siguiente diagrama, se detalla la arquitectura planteada para la empresa Plataformas y Soluciones Digitales S.A.C. y se analiza lo siguiente:

Figura 41. Diagrama de infraestructura en AWS de Plataformas y Soluciones Digitales S.A.C.



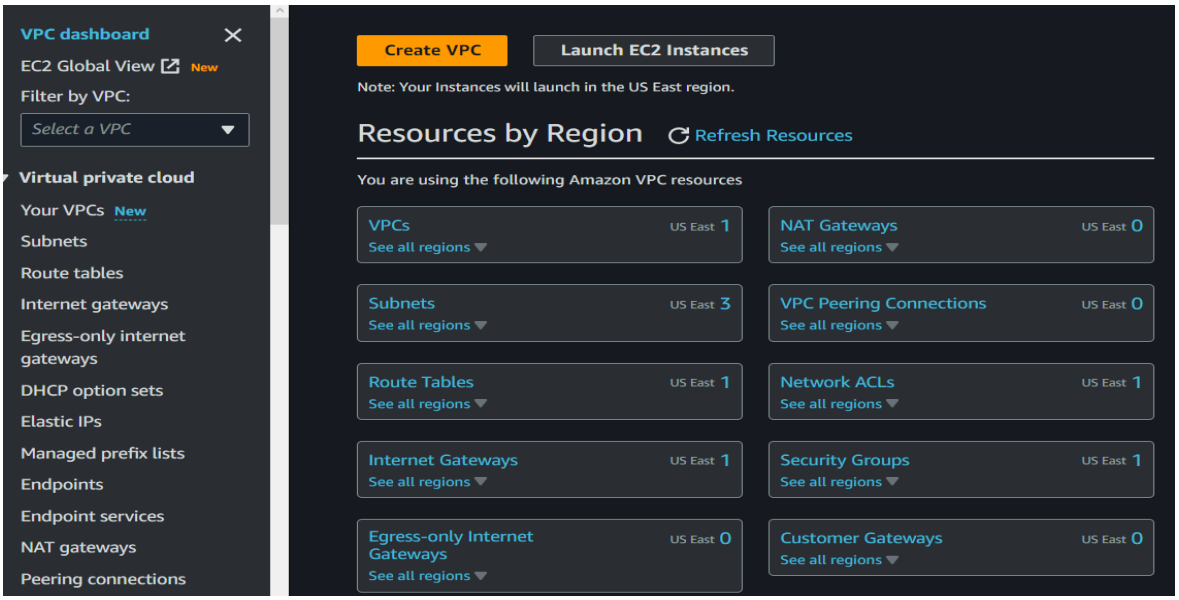
Fuente: Elaboración propia

- En el lado izquierdo del diagrama de la segunda empra, hay una red de entrega de contenido (Content Delivery Network). Los servicios de AWS que se muestran en ese lado del diagrama incluyen **Amazon Route 53**, **Amazon CloudFront**, **AWS Certificate Manager** y **Amazon Simple Storage Service**.

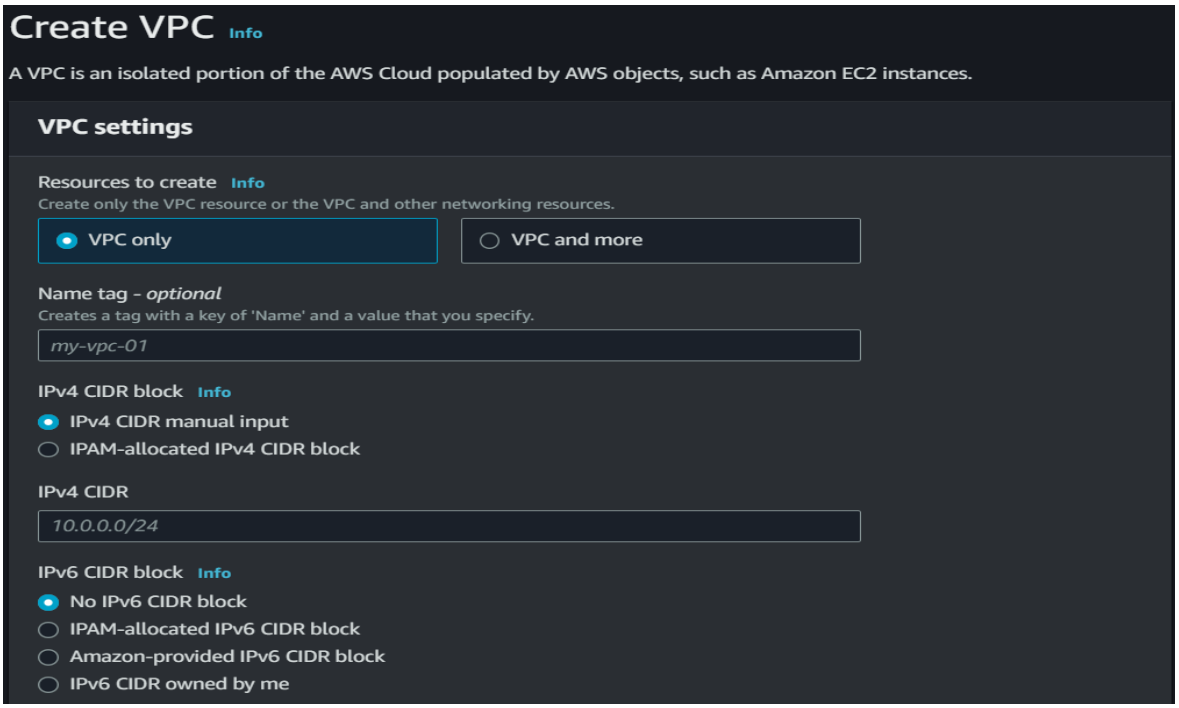
- La zona hospedada apunta a una distribución CloudFront. CloudFront se configuró para utilice el certificado SSL, el punto de origen (nombre de dominio) y el Bucket junto a la ubicación donde se encuentra la aplicación web (contenido estático).

- En el lado derecho del diagrama, se encuentran servidores para sus distintos usos. Dos instancias EC2 (**Elastic Compute Cloud**), la primera funciona como servidor Bastion y la segunda tiene el rol del servidor principal. RDS (**Relational Database Service**) donde se aloja la base de datos y **Amazon Simple Storage Service (S3)** donde se almacenan los Backups generados por la base de datos y del servidor.

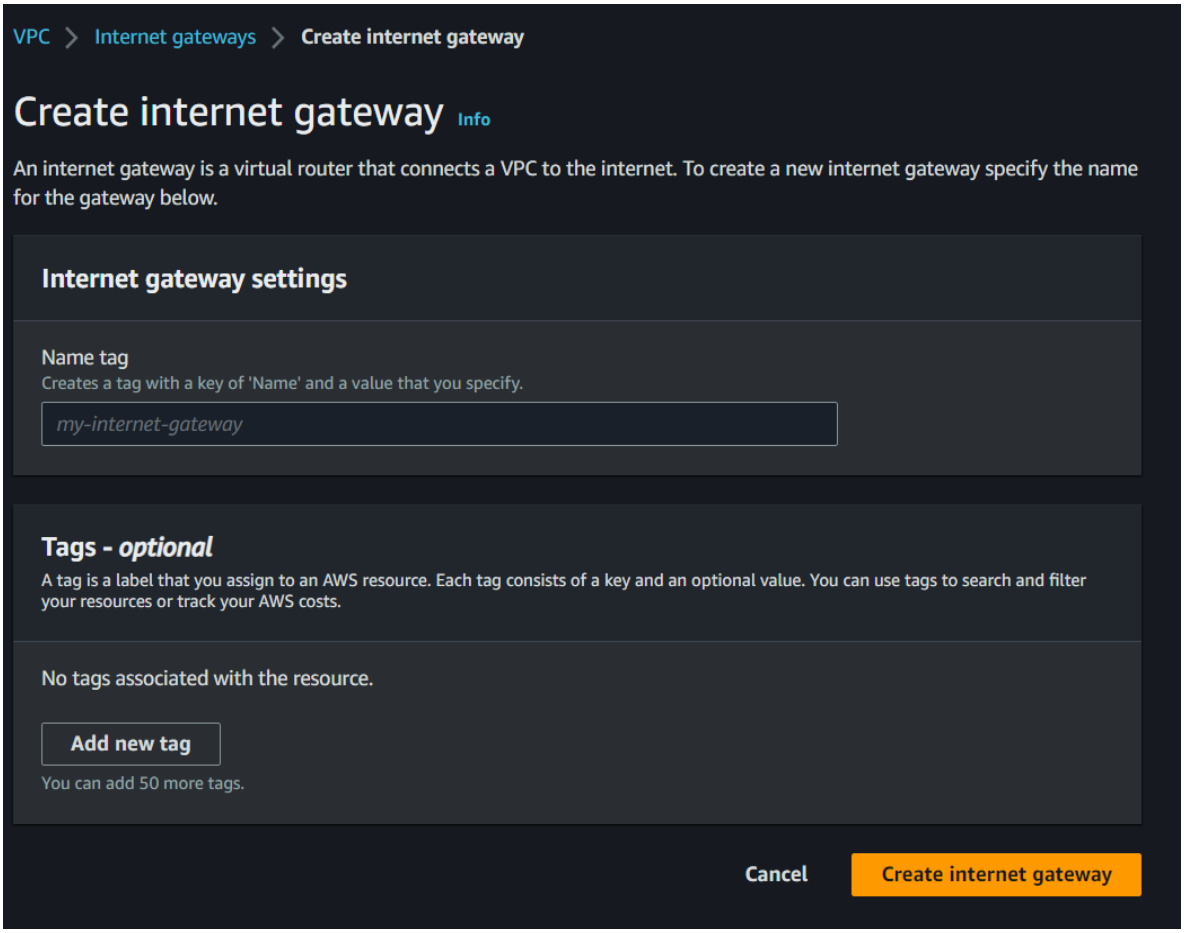
Para la configuración de los servicios en AWS se empieza, por ejemplo, si se implementarán servidores, por crear una Virtual Private Network (VPC) en caso de que no se utilice tecnología **Serverless**.

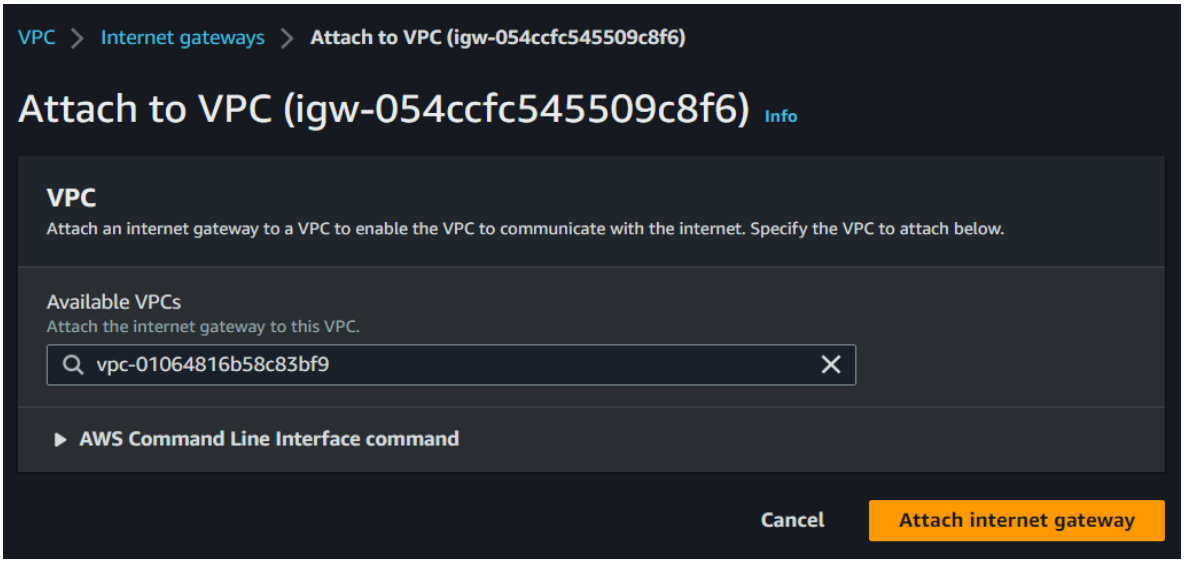


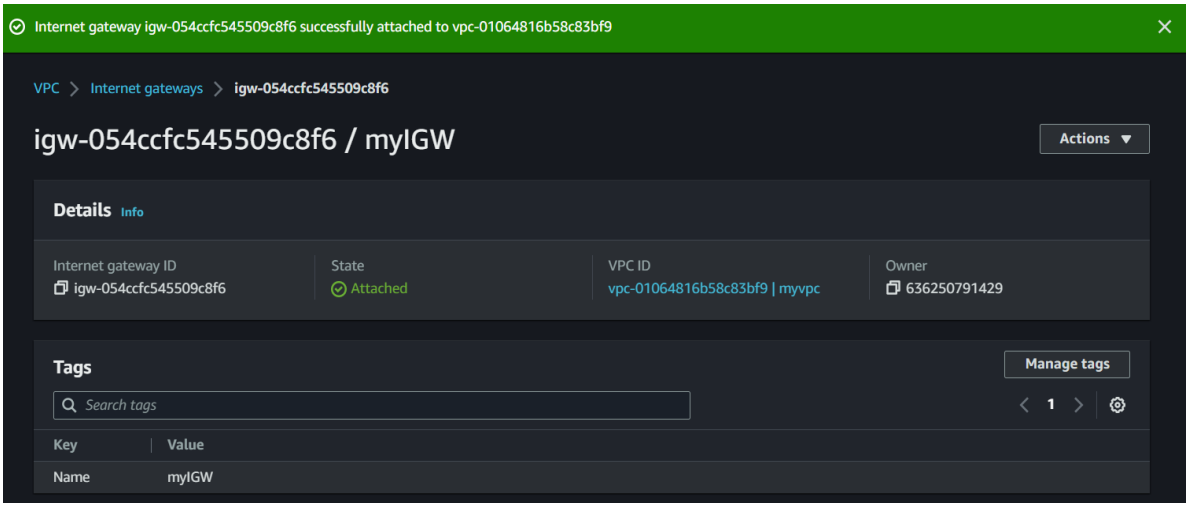
Al crear una red virtual aislada para proteger y controlar el acceso a los recursos. Donde se proporciona un control total sobre la configuración de la red, incluyendo direcciones IP, enrutamiento y Gateways. Por último, permite establecer conexiones seguras entre tu infraestructura local y los recursos en la nube.



El Internet Gateway (IGW) en AWS es esencial para permitir la conexión a Internet en una VPC. Se puede definir como una puerta de entrada y salida para las solicitudes de red entre la VPC y la Internet pública.







Las subredes en AWS dividen una VPC en segmentos más pequeños y fáciles de gestionar. Cada subred es una parte de las direcciones IP de la VPC y se configura en una zona de disponibilidad. La creación de subredes públicas y privadas en AWS se fundamenta en la seguridad y control de la arquitectura de la red.

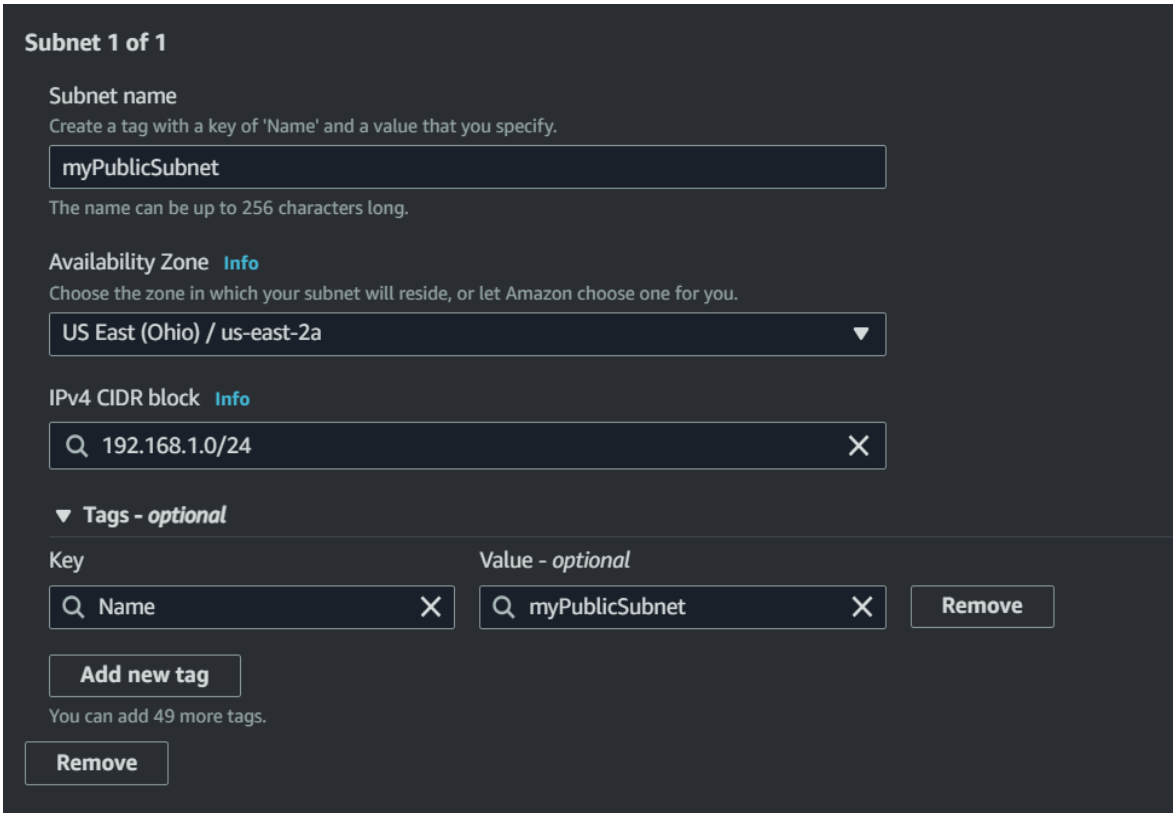
Las subredes públicas se configuran con una conexión directa a Internet a través de un Internet Gateway. Esto es útil para permitir que recursos específicos, como servidores web o API, sean accesibles desde Internet. Al ubicar estos recursos en una subred pública, es posible controlar y restringir el acceso utilizando herramientas como políticas de acceso y grupos de seguridad.

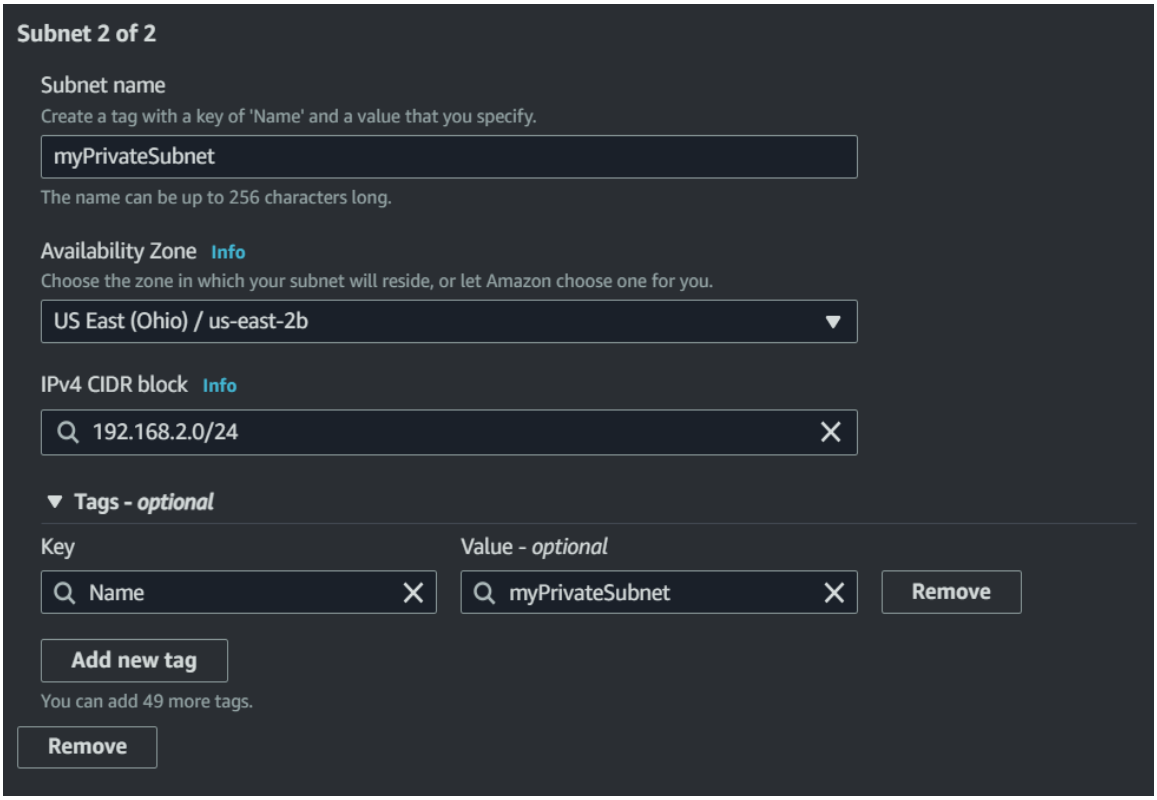
Al crear subredes privadas en AWS, los recursos alojados en esas subredes no tienen una conexión directa a Internet. Esto brinda mayor seguridad al ocultar los recursos de la VPC detrás de direcciones IP públicas. Los recursos en subredes privadas solo pueden ser accedidos a través de conexiones internas dentro de la VPC o mediante conexiones híbridas con la infraestructura local a través de servicios como AWS Direct Connect o VPN.

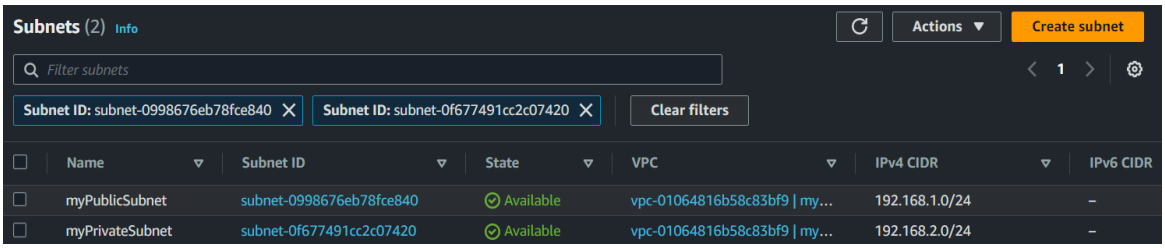
Las subredes en AWS generalmente utilizan una máscara de /24, lo que proporciona suficientes direcciones IP (hasta 256) para alojar diversos recursos. Esta elección ofrece flexibilidad, escalabilidad y sigue prácticas comunes en redes. Además, simplifica la gestión y cumple con los estándares de compatibilidad. En

resumen, la máscara de /24 es ampliamente utilizada debido a su equilibrio entre disponibilidad de direcciones y eficiencia en la gestión de la red.

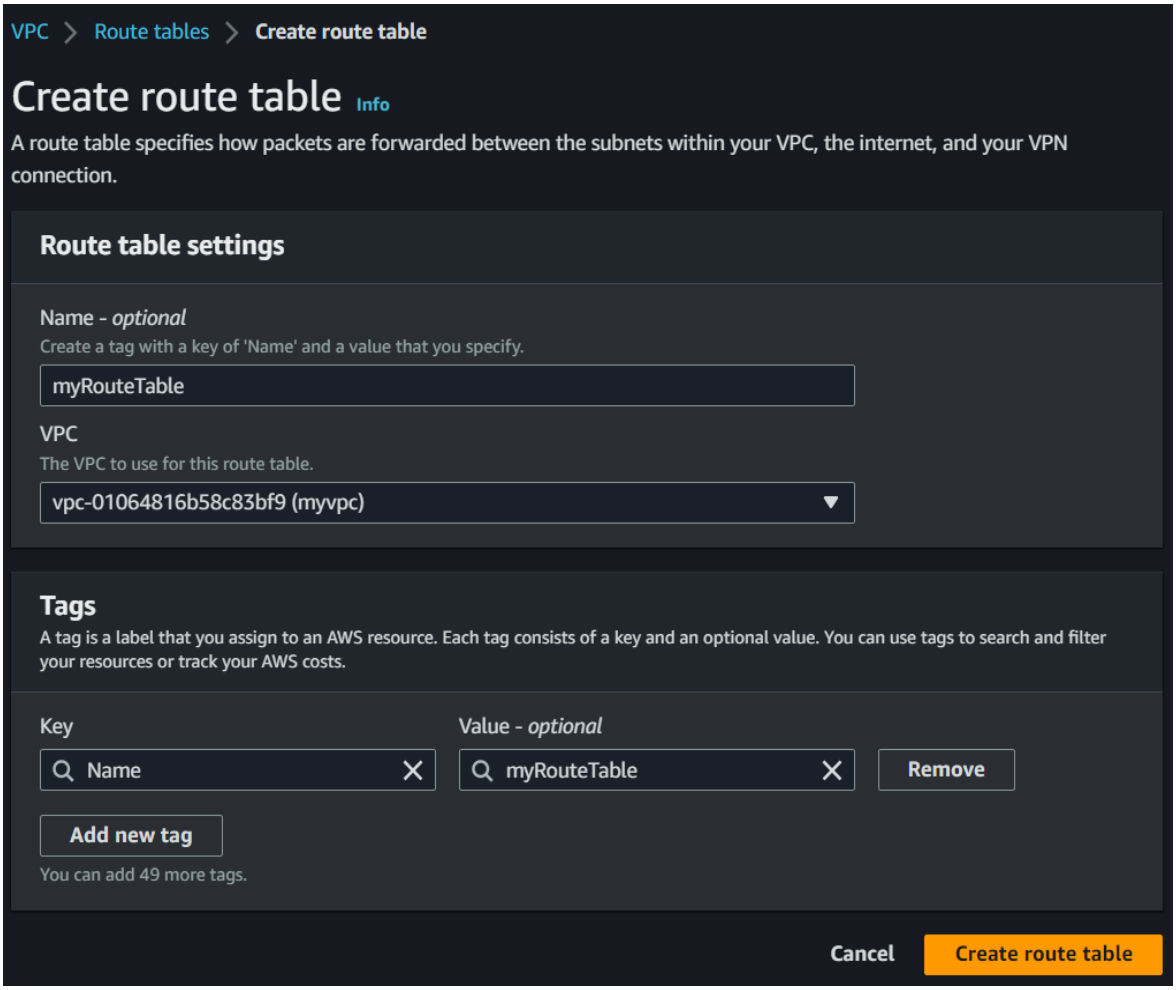
Una Availability Zone (AZ) es una unidad de infraestructura físicamente separada dentro de una región de AWS. Cada AZ funciona de manera independiente, con su propia infraestructura de energía, refrigeración y red. Las AZs brindan resiliencia y alta disponibilidad a los servicios en la nube al permitir la distribución estratégica de recursos. Son fundamentales para garantizar la tolerancia a fallos y mejorar la continuidad del servicio.



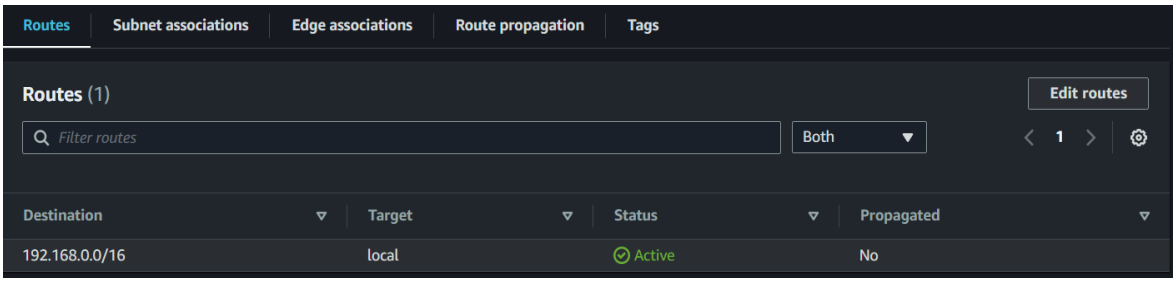


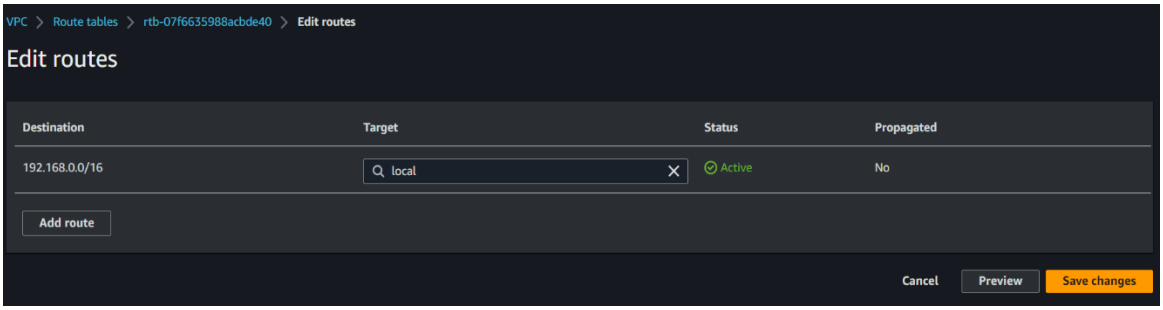


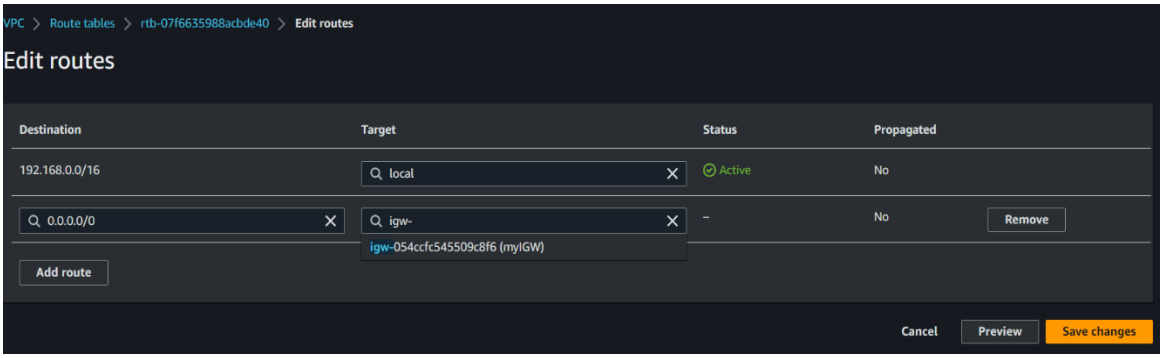
Un Route Table en AWS es una tabla de enrutamiento que controla el flujo de tráfico dentro y fuera de una VPC. Define cómo se deben enviar los datos entre las subredes y los destinos dentro y fuera de la VPC. Permite la comunicación interna de las subredes, el acceso a Internet, la conexión con redes externas y el control del tráfico mediante reglas y rutas específicas.

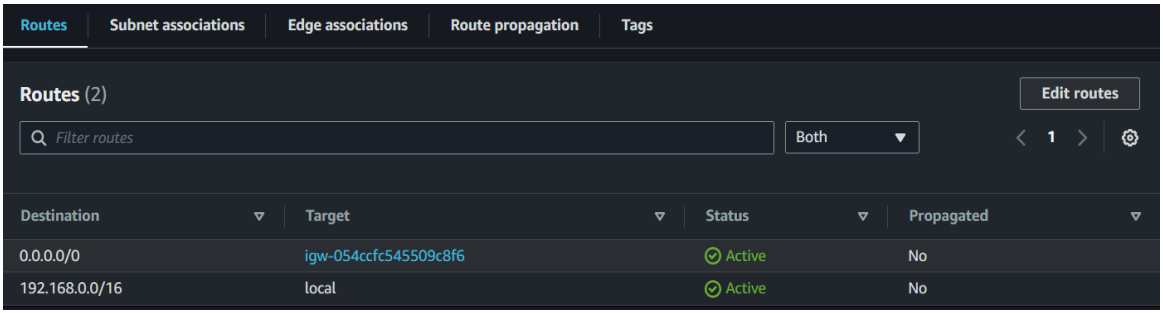


Dentro de un Route Table, las "**routes**" (rutas) son las configuraciones que indican cómo se debe enviar el tráfico de red. Cada ruta tiene un destino y un destino siguiente que especifican a dónde debe dirigirse el tráfico. Las rutas se utilizan para controlar el flujo del tráfico dentro de la VPC y hacia destinos externos.

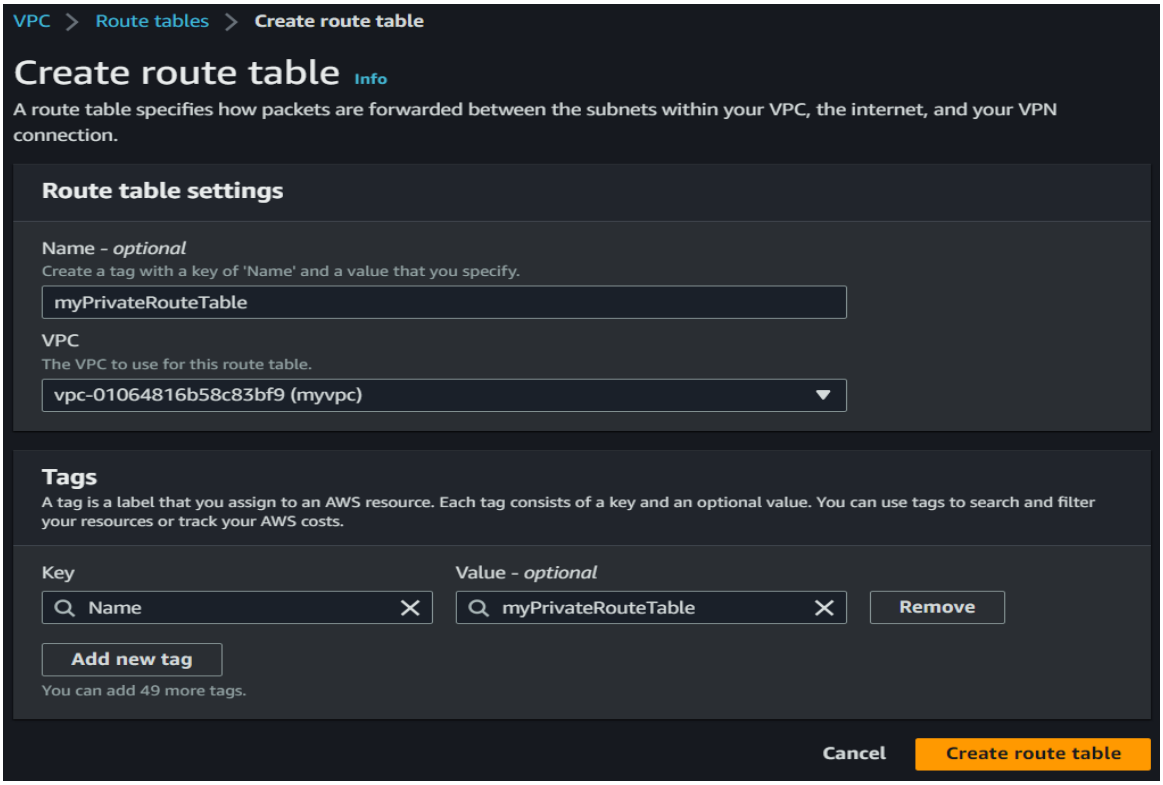




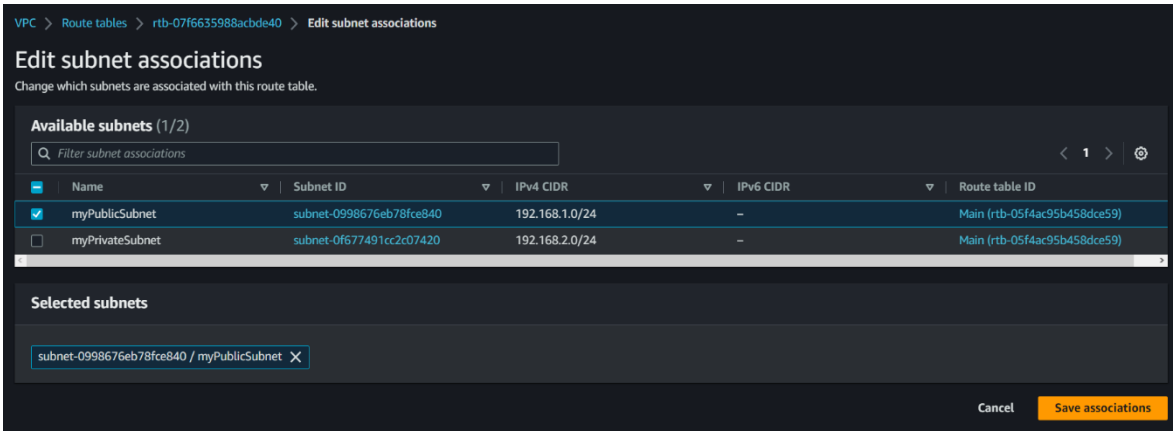


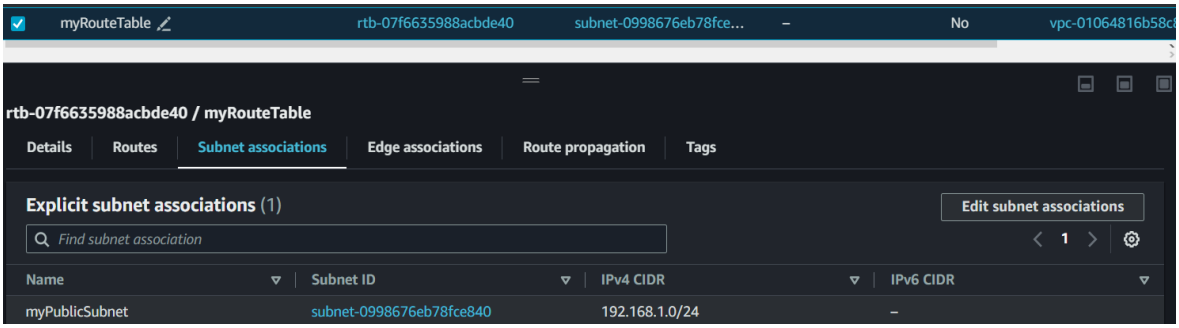


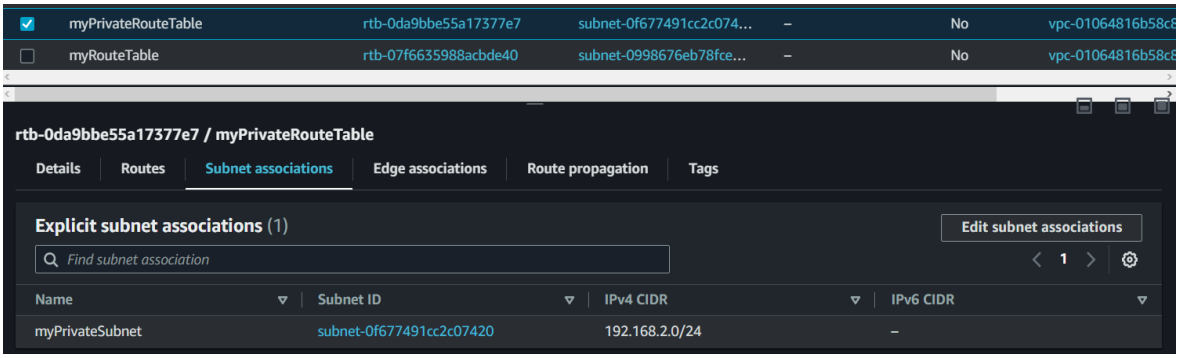
Es necesario crear un Route Table para Subnets privadas en AWS. Aunque estas Subnets no tienen acceso directo a Internet, el Route Table se utiliza para establecer las rutas de comunicación interna dentro de la VPC y para conexiones con recursos externos. El Route Table asegura que las Subnets privadas puedan comunicarse con otras Subnets y servicios externos a través de conexiones internas o híbridas.



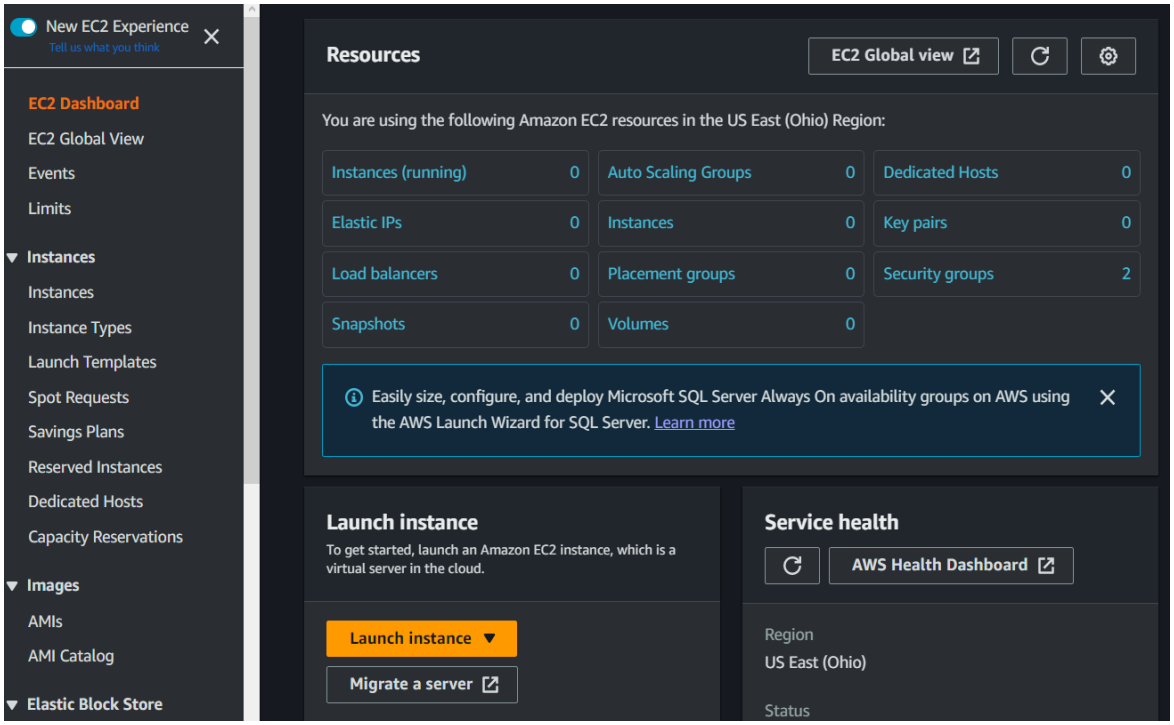
Las "**subnet associations**" (asociaciones de subred) en un Route Table se refieren a la vinculación de subredes específicas con un Route Table en particular. Estas asociaciones determinan cómo se dirige el tráfico dentro de cada subred. Son configuraciones flexibles que permiten controlar y personalizar el enrutamiento de la red según las necesidades específicas.

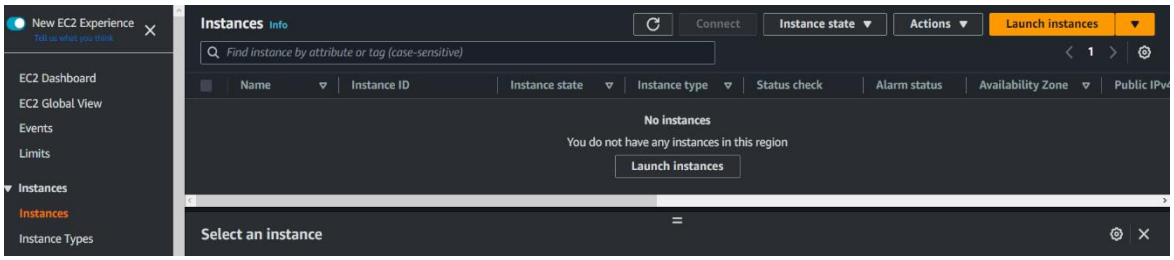




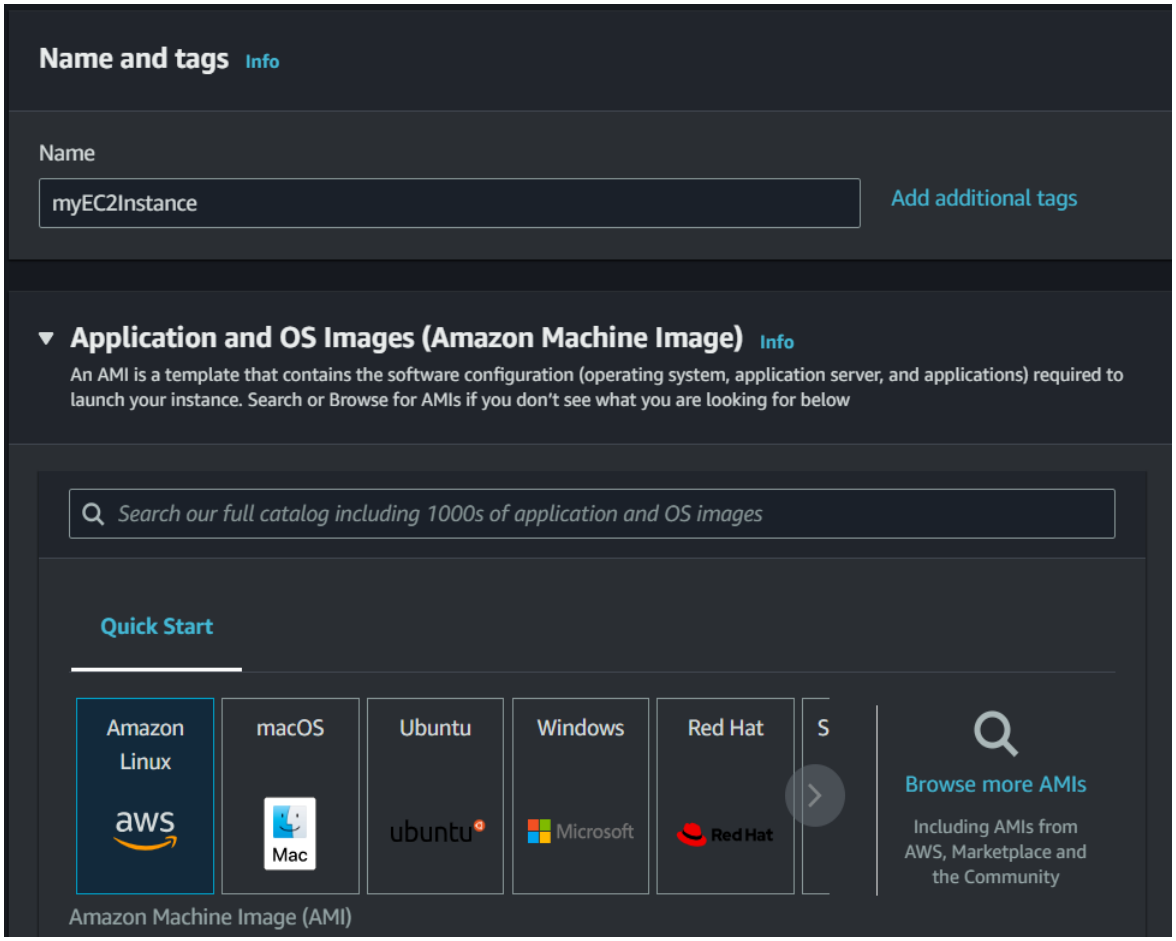


Para crear servidores o máquinas virtuales, Elastic Compute Cloud (EC2) implementa y ejecuta máquinas virtuales (instancias). Se utiliza para alojar aplicaciones, desarrollar y probar software, procesar datos, almacenar información, implementar aplicaciones empresariales y lograr escalabilidad y alta disponibilidad.



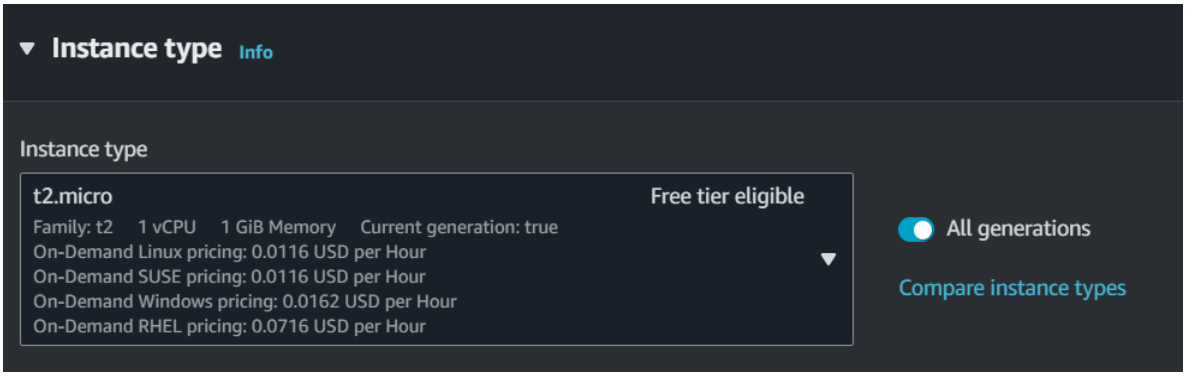


EC2 de AWS ofrece diversos tipos de instancias optimizadas para diferentes necesidades, como propósito general, cómputo, memoria, almacenamiento, GPU e inferencia de IA, con capacidades mejoradas en términos de cómputo, memoria y almacenamiento para cargas de trabajo específicas.

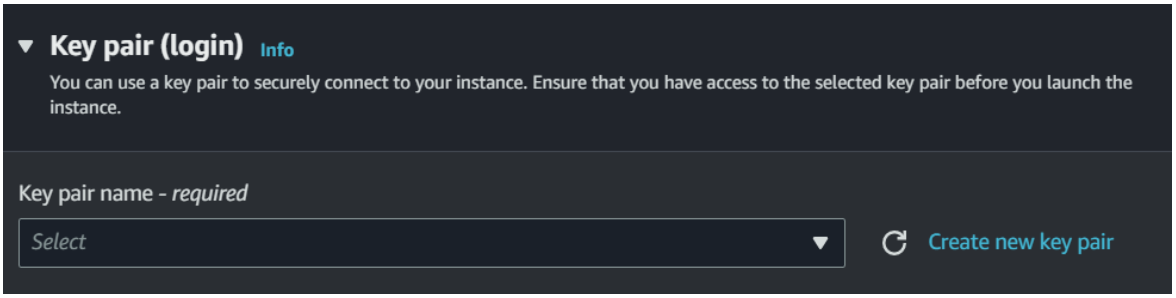


Una Amazon Machine Image (AMI) es una plantilla que incluye una configuración predefinida de un sistema operativo y software necesario para iniciar instancias en EC2. Es una instantánea que sirve como base para crear y replicar entornos de computación en la nube de manera rápida y consistente. Las AMIs permiten el despliegue ágil de instancias con la misma configuración y software preinstalado. Se puede utilizar AMIs con macOS, Ubuntu, Windows, Red Hat, etc.

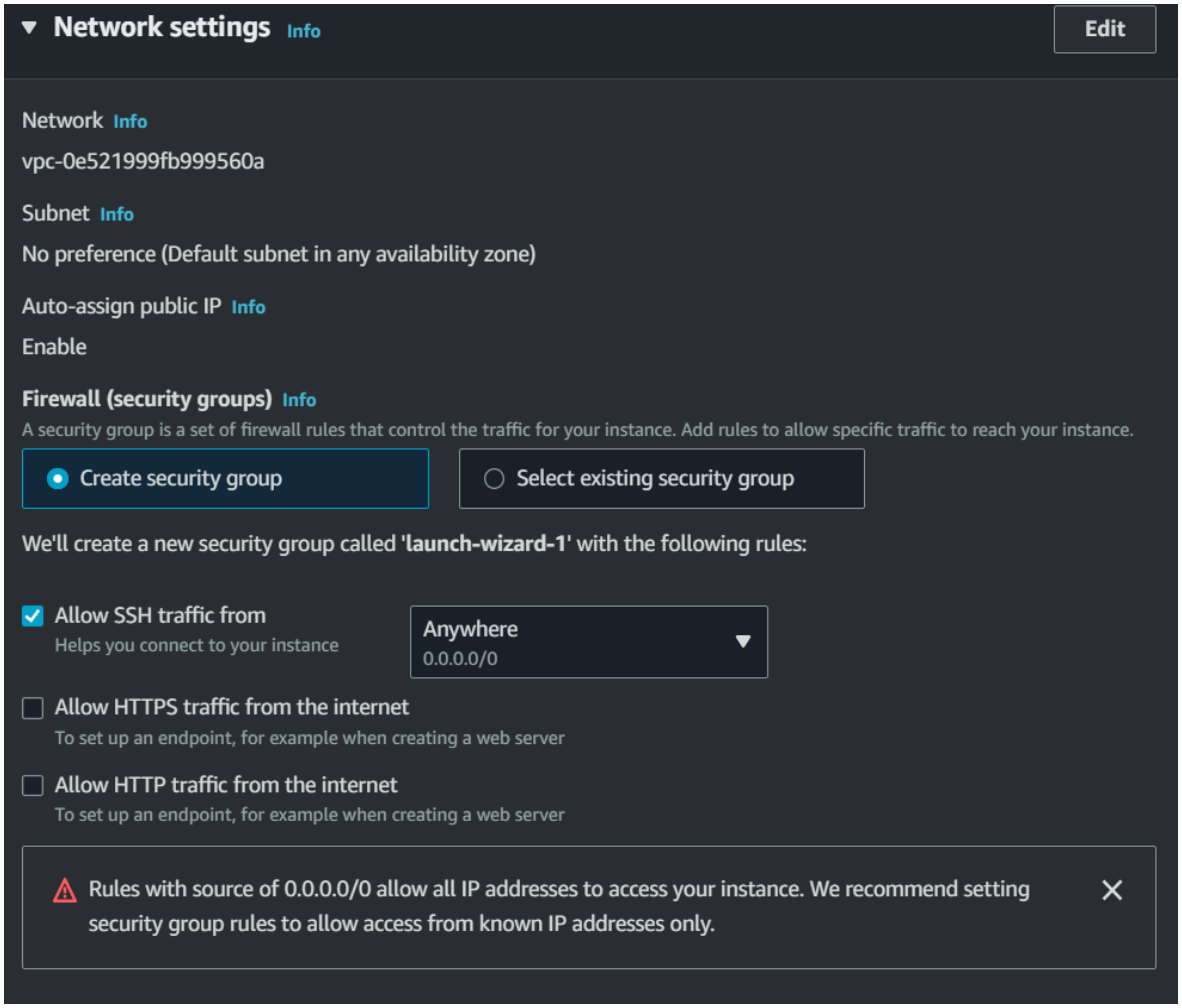
Un tipo de instancia en EC2 se refiere a la configuración de recursos y capacidades de hardware asignados a una instancia virtual. Cada tipo de instancia tiene diferentes características, como CPU, memoria RAM, almacenamiento y rendimiento de red. Los tipos de instancia están clasificados en categorías según su propósito y características.



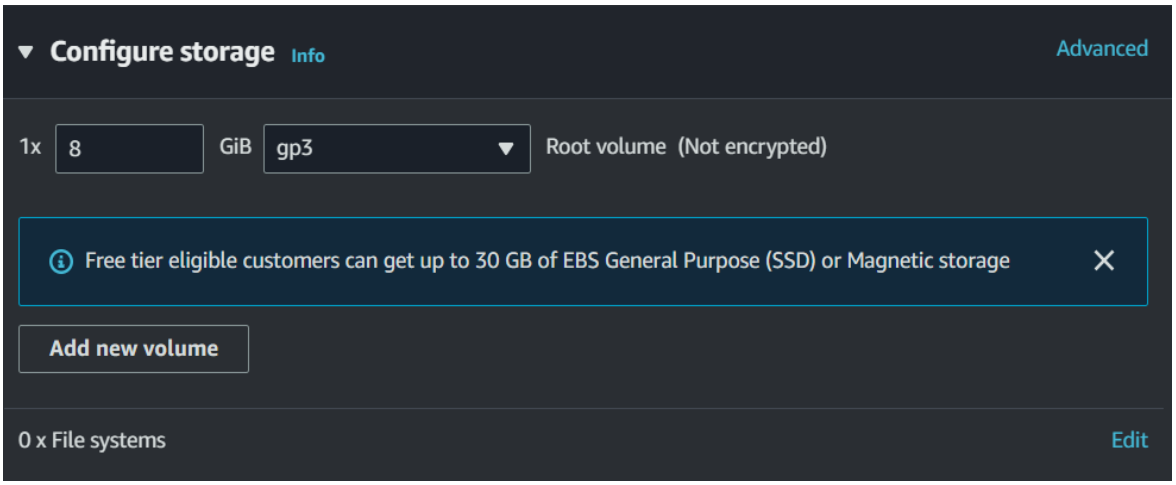
Un Key Pair (login) en AWS son llaves criptográficas, llave pública y privada. Se utiliza para autenticarse y acceder de forma segura a las instancias de EC2. La llave pública se asocia con la instancia y se utiliza para cifrar los datos, mientras que la llave privada se guarda en el dispositivo del usuario y se utiliza para descifrar los datos en la instancia. Al proporcionar el Key Pair correspondiente al conectarse a una instancia, se garantiza la autenticidad y confidencialidad de la conexión.



Además, se realiza las configuraciones de red con la VPC creada anteriormente. Asimismo, se habilita un *Security group*, siendo este un sistema de seguridad virtual que facilita el control del flujo de datos en una red. hacia y desde las instancias EC2, donde se determinan qué tráfico está permitido y qué tráfico está bloqueado en función de direcciones IP, puertos y protocolos

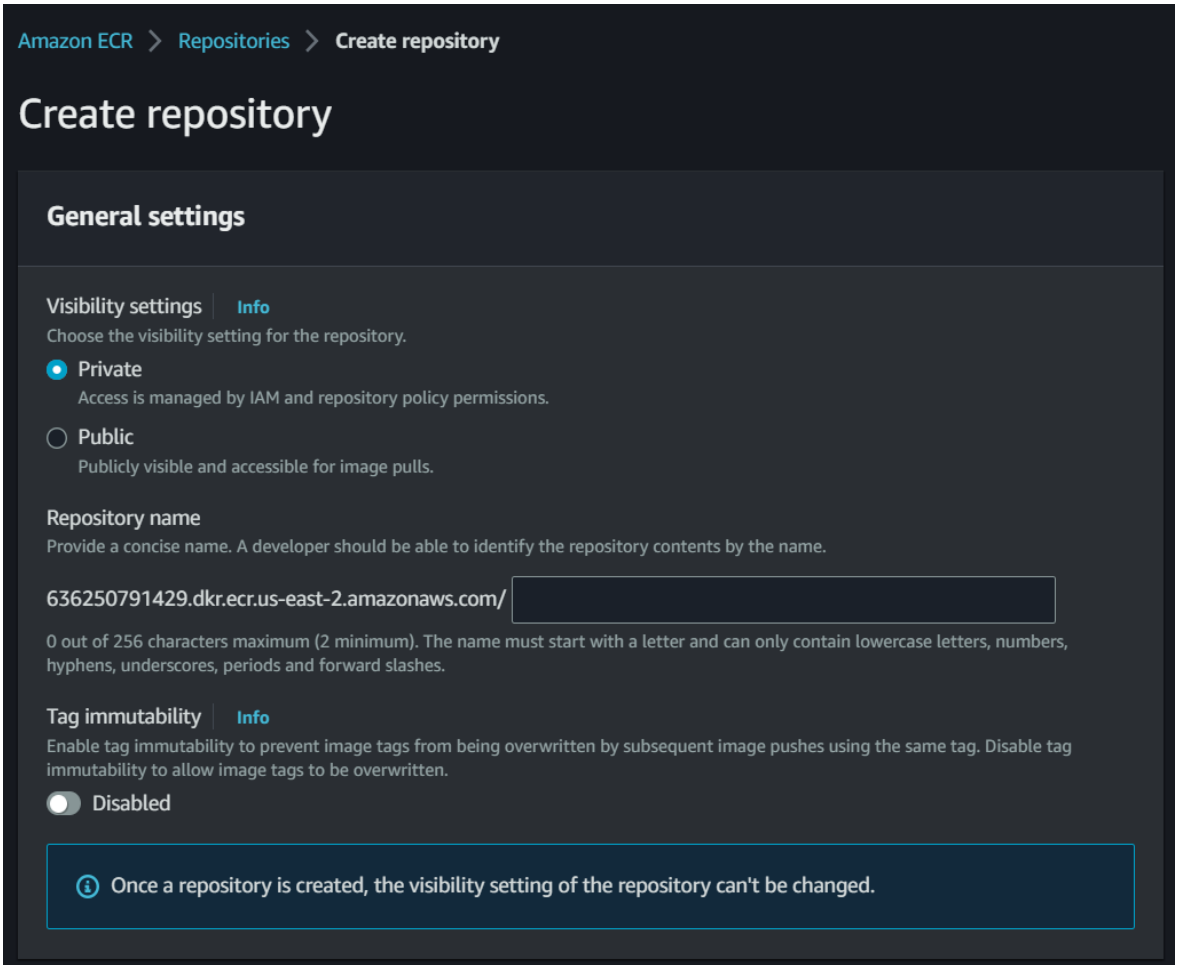


También se define el almacenamiento de la instancia.

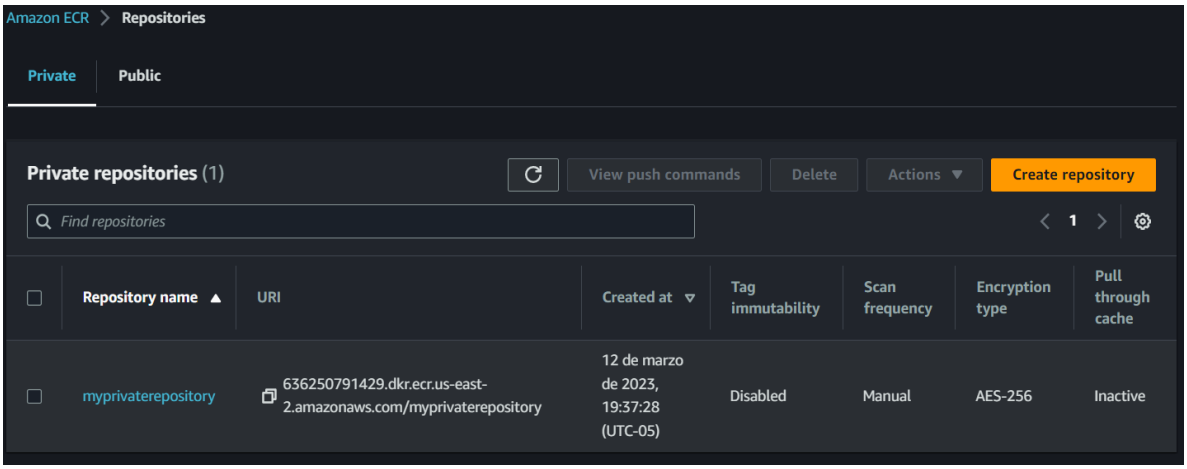


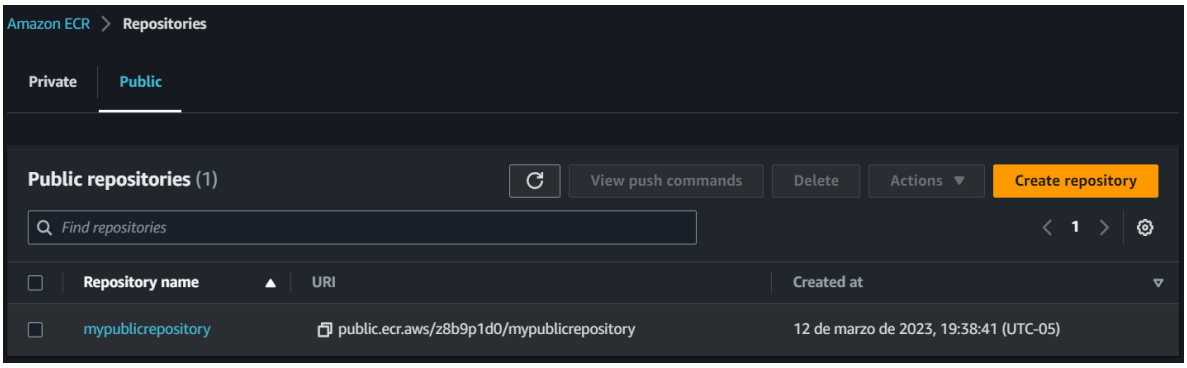
En el caso de aprovisionar el servicio de *ECS*, el cual permite ejecutar y administrar aplicaciones en contenedores Docker de manera eficiente, se debe trabajar con el servicio de Elastic Container Registry (ECR) ya que son servicios complementarios de AWS para la gestión de contenedores. ECS se encarga de ejecutar y administrar contenedores, mientras que ECR es un registro seguro para almacenar imágenes de contenedor. En conjunto, ECS utiliza ECR como fuente de imágenes para desplegar aplicaciones en contenedores.

Se puede configurar repositorios públicos y privados dentro de ECR. Los repositorios públicos permiten compartir imágenes de contenedor de forma abierta, mientras que los repositorios privados restringen el acceso a las imágenes a usuarios autorizados.



Para crear un repositorio privado en ECR, se escoge la opción privada, se asigna un nombre y, opcionalmente, se agrega etiquetas. Después de crear el repositorio, puedes cargar imágenes de contenedor y configurar los permisos de acceso. Los repositorios privados en ECR aseguran la privacidad y la seguridad de las imágenes almacenadas. A diferencia de un repositorio público, se realizan los mismos pasos a excepción de que se puede cargar imágenes de contenedor y compartirlas abiertamente sin requerir autenticación.

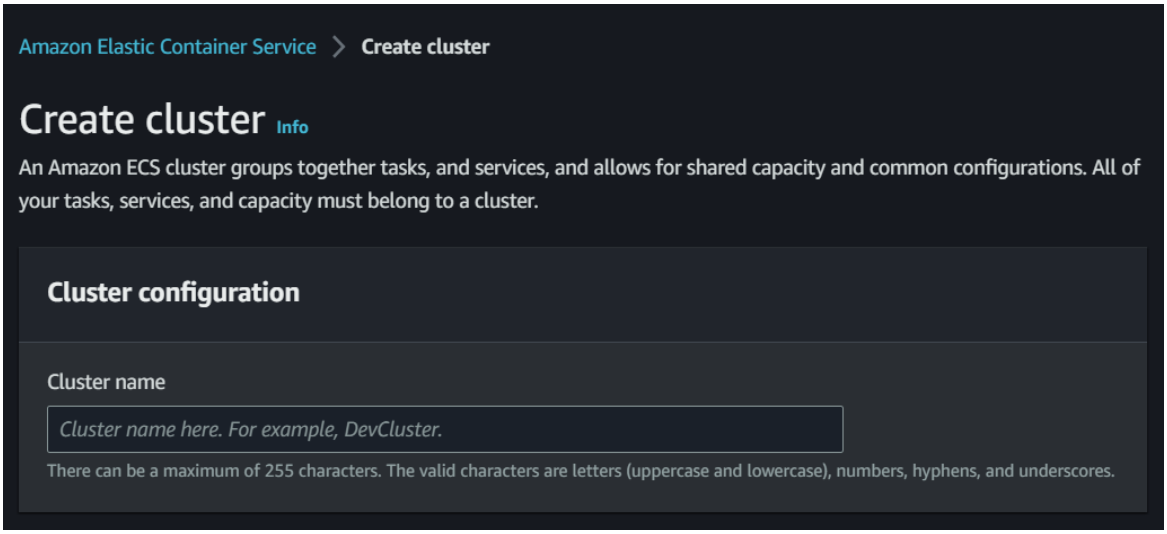




Una gran ayuda de crear un repositorio ya sea público o privado, es que cuenta con una guía para la subida de una imagen al repositorio.

Una vez configurado los repositorios con las imágenes, se procede a crear el clúster. Un clúster es un conjunto de recursos de cómputo donde se ejecutan y

gestionan contenedores. Actúa como un entorno que organiza y administra las instancias EC2 o servicios de AWS Fargate utilizados para ejecutar tareas y servicios de contenedores. El clúster permite la asignación eficiente de recursos, la carga equilibrada de contenedores y ofrece características adicionales como la auto escalabilidad y la programación de tareas.



Crear un clúster implica los siguientes pasos:

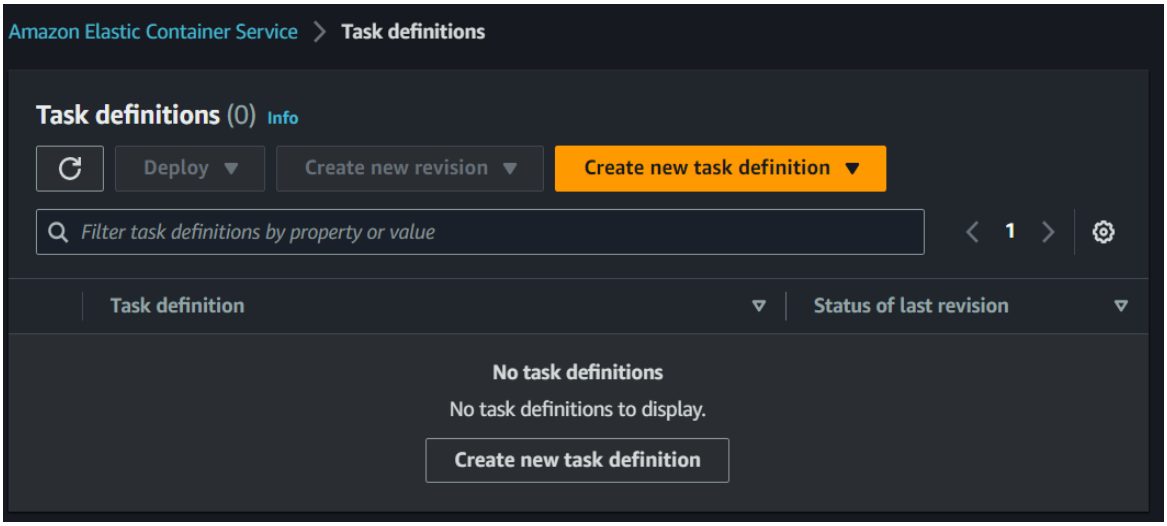
- Se ingresa un nombre para el clúster.
- Se configura la red VPC. Por defecto, las tareas y servicios se ejecutan en las subredes predeterminadas para una VPC predeterminada. Para utilizar la VPC no predeterminada, se especifica la VPC y las subredes.
- El clúster se configura automáticamente para utilizar AWS Fargate, un servicio

sin servidor, con dos proveedores de capacidad. Si se desea, se puede añadir instancias de Amazon EC2 o instancias externas utilizando ECS Anywhere.

- De manera opcional, se configura el servicio de monitoreo con Container Insights. Este está desactivado por defecto. Cuando se utiliza Container Insights, hay un costo adicional.
- Por último, se agregan etiquetas de manera opcional.

Una vez creado, el clúster se utiliza para ejecutar y administrar contenedores. Siempre es recomendable consultar la documentación oficial de AWS para obtener instrucciones actualizadas y detalladas.

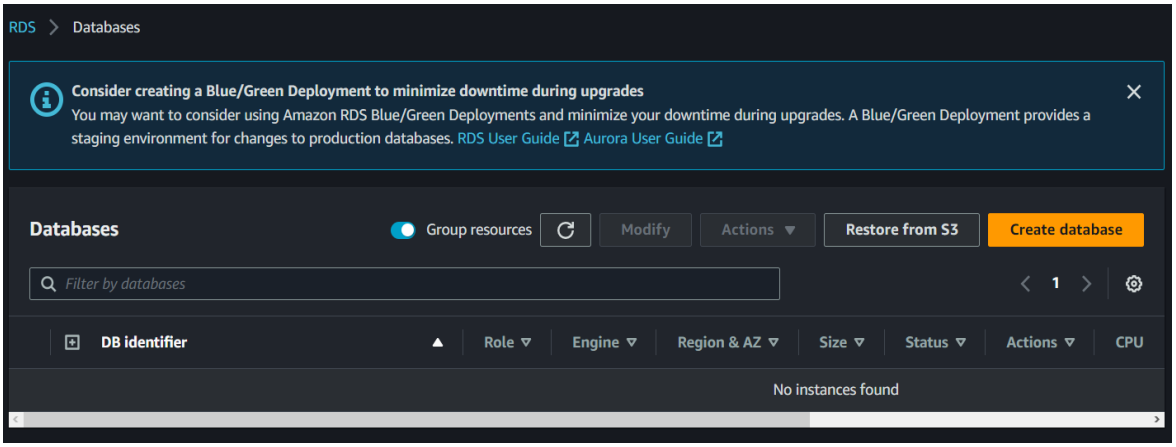
Una definición de tarea (Task Definition) es requerido para ejecutar contenedores Docker en ECS. En esta se describe cómo se ejecutan y se gestionan un conjunto de contenedores en un clúster, contiene información esencial sobre los contenedores, su configuración y las políticas asociadas. Especifica los detalles necesarios, como imágenes de contenedor, puertos expuestos, variables de entorno y asignación de recursos. También permite establecer estrategias de despliegue y gestionar volúmenes de almacenamiento. Es en esta configuración donde se utiliza el repositorio creado en ECR.



Al crear un servicio en ECS, se siguen los siguientes pasos después de crear un archivo de definición de tarea: se crea un clúster, se configura el servicio especificando la definición de tarea y el número de tareas, se puede configurar un balanceador de carga y se revisa y confirma la configuración antes de crear el servicio.

Una vez que se crea el servicio, ECS se encarga de aprovisionar las tareas en las instancias y ejecutar el código de la aplicación. El servicio se puede gestionar y monitorear a través de la consola de AWS. Se pueden realizar actualizaciones y cambios en la aplicación modificando la definición de tarea y actualizando el servicio.

La instalación de RDS (Relational Database Service) es un paso esencial para aprovechar las ventajas de este servicio. Con este servicio, se puede ejecutar y administrar bases de datos sin necesidad de construir la infraestructura por detrás. Con RDS, se puede automatizar, tener alta disponibilidad y seguridad avanzada, donde se utilizan herramientas de monitoreo y métricas para garantizar un rendimiento óptimo.



Asimismo, se puede realizar los siguientes pasos para configurar una instancia RDS, ya sea en PostgreSQL o MySQL.

1. Seleccionar el motor de base de datos en "Crear base de datos" y se elige el motor de base de datos que se desea utilizar, ya sea PostgreSQL o

MySQL.

2. Seleccionar la opción de base de datos estándar en "Creación estándar" para configurar una instancia de base de datos desde cero.
3. Configurar las opciones de base de datos. Se debe proporcionar la siguiente información:
    a. Motor de base de datos y versión: Seleccionar la versión deseada del motor de base de datos PostgreSQL o MySQL.
    b. Plantilla de inicio: Elegir una plantilla de configuración que se ajuste a las necesidades o personalizar las opciones avanzadas según los requisitos específicos.
    c. Configuración de instancia: Definir el tamaño de la instancia, la capacidad de almacenamiento y otras opciones relacionadas con el rendimiento.
    d. Configuración de identificación: Establecer un nombre para la instancia de base de datos y las credenciales para un usuario.
    e. Configuración de red: Seleccionar las opciones de conectividad, como la red virtual (VPC), las subredes y los grupos de seguridad.
    f. Configuración de acceso público: Decidir si la instancia de base de datos debe tener acceso público a través de Internet o no.
    g. Opciones adicionales: Se configura características adicionales como copias de seguridad automáticas, monitoreo y notificaciones, entre otros. Tener en cuenta que esto puede generar costos adicionales.
4. Revisar y lanzar la instancia. Se verifica todas las configuraciones y se lanzar base de datos, donde se creará la instancia RDS.
5. Se espera a que se complete la creación. La creación de la instancia puede llevar varios minutos. Durante este tiempo, AWS aprovisionará y configurará la infraestructura necesaria.

Una vez se complete la creación de la instancia de RDS, se puede conectar a esta utilizando la dirección de conexión proporcionada por AWS, con el Endpoint.

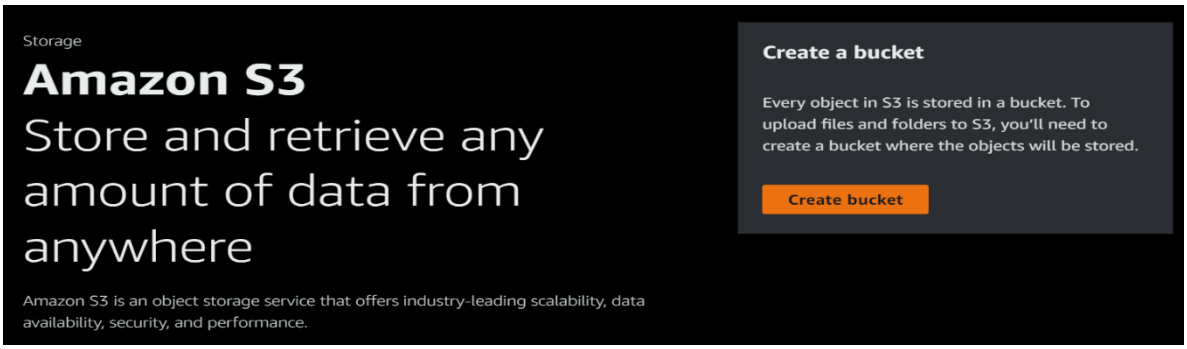
Configurar adecuadamente las reglas de seguridad y de acceso para permitir la conectividad desde aplicaciones o herramientas de administración de bases de datos.

Un bucket de S3 proporciona una forma segura y escalable de almacenar y acceder a datos en la nube. Se puede utilizar para almacenar y compartir archivos, realizar copias de seguridad, distribuir contenido y alojar sitios web estáticos. También se puede configurar reglas y políticas para controlar el acceso y la seguridad de los datos.

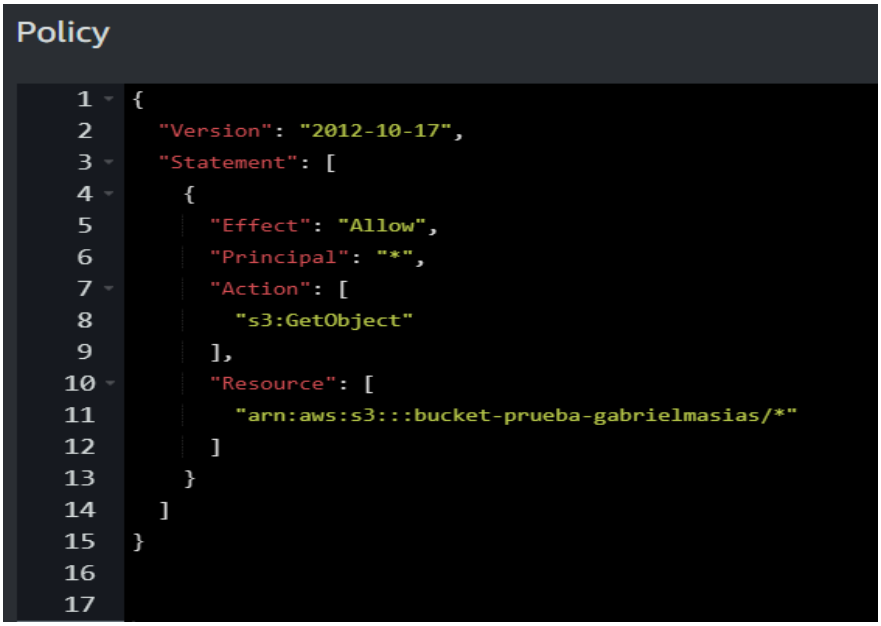
A continuación, se puede realizar los siguientes pasos para crear un bucket S3.

1. Crear un nuevo bucket en "Crear bucket" y proporcionar un nombre único para tu bucket de S3.
    a. El nombre del bucket debe ser único en todo el servicio de AWS S3. No puede haber otro bucket con el mismo nombre, independientemente de la cuenta o región.
    b. Los nombres de los buckets pueden contener solo caracteres alfanuméricos (letras y números) y deben estar en minúsculas. Los caracteres especiales y las mayúsculas no están permitidos.
    c. El nombre del bucket debe tener entre 3 y 63 caracteres. No puede contener guiones seguidos ni puntos seguidos, ni puede comenzar ni terminar con un guion.
    d. Además de ser único en todo AWS S3, el nombre del bucket también debe ser único dentro de tu propia cuenta de AWS. No puedes tener dos buckets con el mismo nombre dentro de tu cuenta.
2. Configurar las opciones del bucket:
    a. Se elige la región geográfica donde se desea almacenar el bucket.
    b. Se puede habilitar el control de bloqueo de objetos para evitar su eliminación accidental.
    c. Se puede habilitar el control de versiones para mantener un historial de cambios en los objetos almacenados en el bucket.

3. Configurar las reglas del bucket:
    a. Si el bucket será accesible públicamente, se selecciona la opción correspondiente y hay que tener en cuenta los riesgos asociados. Si no, se desmarca esta opción para mantener el acceso restringido.
    b. Se puede configurar políticas de bucket para controlar el acceso y los permisos de los usuarios y roles en relación con el bucket.
4. Revisar y crear el bucket.



Ejemplo de una política de un bucket que permite el acceso público a los objetos.



En este ejemplo, la política permite a cualquier usuario o entidad ("Principal": "*"), a nivel global, realizar la acción "s3:GetObject", que es obtener un objeto del

bucket. La propiedad "Resource" especifica el recurso en el cual se aplica la política, en este caso, todos los objetos dentro del bucket llamado "prueba-gabrielmasias".

Es importante tener en cuenta que la configuración de acceso público a nivel global debe utilizarse con precaución, ya que puede permitir acceso no deseado a los objetos del bucket. Si se requiere acceso controlado, es recomendable establecer políticas más específicas y restringidas utilizando identidades y grupos de usuarios autorizados.

Dentro de la norma ISO 27017:2015 se incluyen controles importantes, como políticas de seguridad de la información, específicamente diseñadas para la computación en la nube. Estas políticas deben ser establecidas por los clientes de servicios en la nube para garantizar la protección de su información y otros activos en línea con los niveles aceptables de riesgo de seguridad.

La norma establece medidas de seguridad específicas para servicios en la nube, asegurando la protección de la información almacenada, procesada y transmitida en dichos servicios. Esta se puede tomar en cuenta como una extensión de la norma ISO/IEC 27001, ya que se enfoca en los controles de seguridad específicos de los servicios en la nube, pero sigue utilizando el mismo enfoque basado en riesgos que se encuentra en la norma ISO/IEC 27001.

La ISO 27017:2015 tiene dominios enfocados en lo siguiente:

1. Conceptos específicos del sector de la nube
2. Políticas de seguridad de la información
3. Organización de la seguridad de la información
4. Seguridad de los recursos humanos
5. Gestión de activos
6. Control de acceso
7. Criptografía
8. Seguridad física y ambiental
9. Seguridad operativa

10. Seguridad de las comunicaciones
11. Adquisición, desarrollo y mantenimiento de sistemas
12. Relaciones con proveedores
13. Gestión de incidentes de seguridad de la información
14. Aspectos de seguridad de la información de la gestión de la continuidad del negocio
15. Cumplimiento

En el desarrollo de esta investigación, se explicará la aplicabilidad de los siguientes dominios en los controles y objetivos, según el criterio del investigador:

1. Políticas de seguridad de la información

1.1. Dirección de la seguridad de la información

1.1.1. Políticas de seguridad de la información

- Evaluación de riesgos

  Realizar una evaluación de riesgos es beneficioso puesto que detecta posibles amenazas y peligros que podrían afectar la seguridad de la información en tu entorno de AWS.

- Acceso y autenticación

  Con AWS Identity and Access Management (IAM) se gestiona el acceso a los recursos y datos, además de configurar políticas de acceso basadas en el principio de "menos privilegios".

- Monitorización y registro de eventos

  AWS CloudTrail y Amazon CloudWatch son necesarios cuando se supervisa y registran eventos relacionados con la seguridad en la cuenta de AWS. Esto permitirá identificar y responder rápidamente a incidentes de seguridad.

- Respaldo y recuperación de datos

  Se puede configurar el respaldo y recuperación de datos

con Amazon S3 y/o Amazon Glacier. Por otro lado, se pueden realizar Backups periódicas y probar regularmente la capacidad de recuperación de los datos.

- Gestión de vulnerabilidades

  Con AWS Inspector se identifica y corrige vulnerabilidades en las instancias EC2 (Elastic Compute Cloud). Además, se mantienen actualizados los sistemas operativos y aplicaciones, aplicando parches de seguridad de manera regular.

2. Organización de la seguridad de la información

2.1. Organización interna

2.1.1. Roles y responsabilidades de la seguridad de la información

- Responsabilidad de la alta dirección de una organización

  La alta dirección de una organización tiene la responsabilidad de establecer una política que abarque los requisitos específicos de la computación en la nube y se alinee con las metas y objetivos de la organización.

- Responsabilidad de los proveedores de servicios en la nube (CSP)

  Los proveedores de servicios tienen el deber de ofrecer a sus clientes una plataforma segura y de confianza. Esto implica garantizar la seguridad de la infraestructura física, administrar identidades y accesos, separar los datos de manera adecuada y cumplir con las leyes y regulaciones correspondientes.

- Responsabilidad compartida

  En un entorno de AWS, la protección de la información es una tarea compartida entre el cliente y AWS. AWS asume la responsabilidad de asegurar la seguridad de la infraestructura, mientras que el cliente es responsable de salvaguardar la seguridad dentro de su nube. Esto significa que el cliente debe implementar las configuraciones de seguridad pertinentes, como la administración de identidades y accesos, el cifrado de datos, el monitoreo y la gestión de incidentes.

- Gestión de riesgos

  Tanto el proveedor de servicios en la nube como el cliente deben adoptar un enfoque de gestión de riesgos para detectar, evaluar y abordar los riesgos relacionados con la seguridad de la información. Esto implica llevar a cabo

evaluaciones de riesgos, implementar controles de seguridad adecuados y realizar un monitoreo constante del entorno para identificar posibles amenazas y vulnerabilidades.

Algunos servicios de AWS que se pueden utilizar para implementar controles de seguridad de la información incluyen IAM, CloudTrail y KMS.

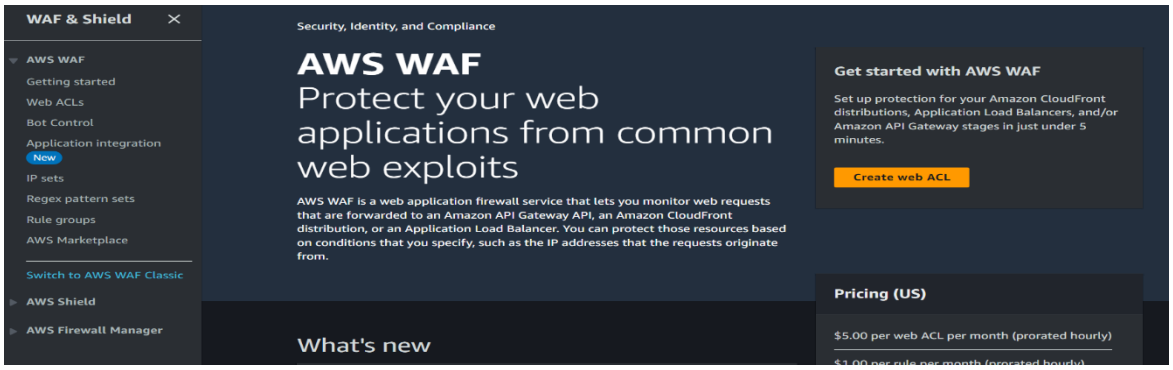
3. Gestión de activos

3.1. Responsabilidad por los activos

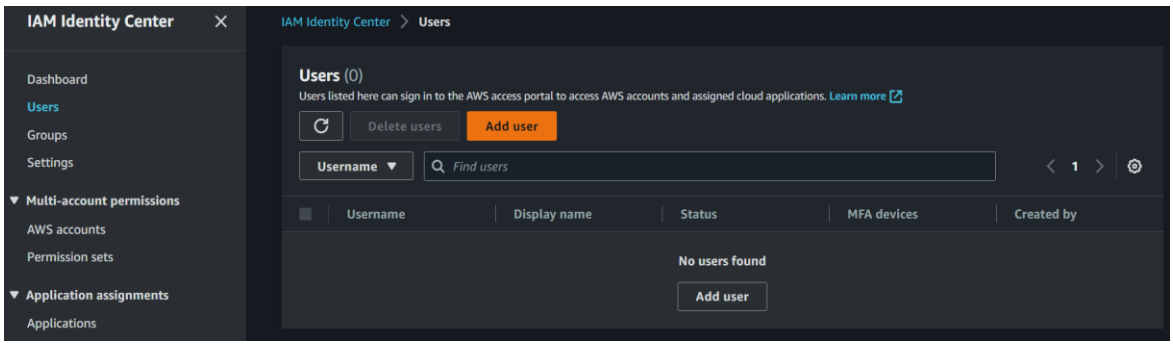
3.1.1. Responsabilidad por los activos

Los activos son responsables por parte del proveedor y del cliente. El cliente únicamente protege sus datos y aplicaciones. Esto incluye el cifrado y protección contra accesos no autorizados.

- El cliente es responsable de configurar las políticas de seguridad de acceso a la nube y de configurar los cortafuegos adecuados para proteger sus aplicaciones. Se puede configurar con **Web Application Firewall** (WAF).



El cliente es responsable de gestionar su propia identidad y acceso, esto incluye la creación y gestión de las cuentas de usuario y la definición de políticas de acceso a la nube donde se puede ejecutar en el servicio de **Identity Access Management** (IAM) y en **IAM Identity Center**.



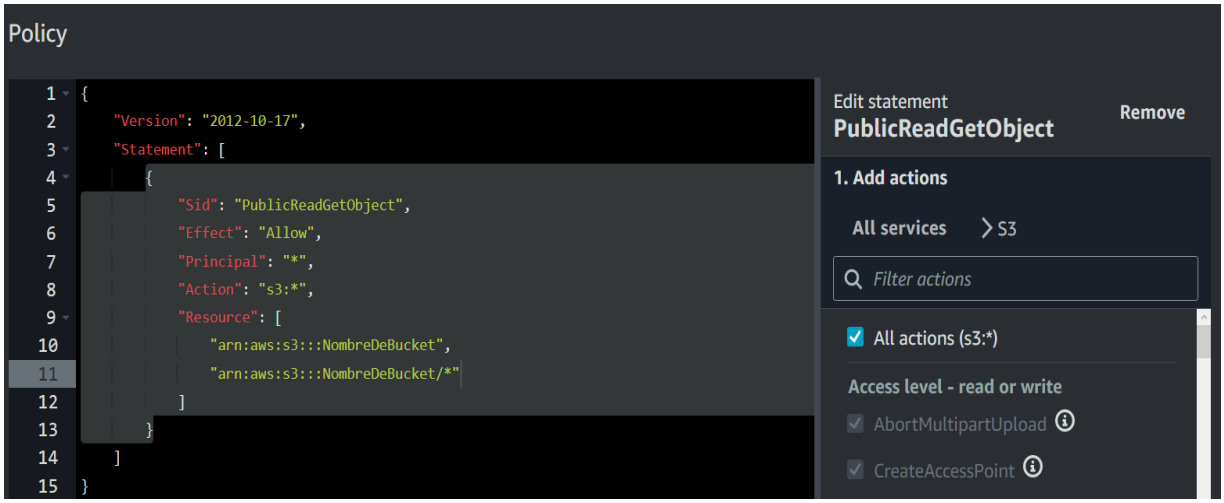
4. Control de acceso

4.1. Requisitos comerciales de control de acceso

4.1.1. Política de control de acceso

En la gestión de acceso, se utilizan políticas para controlar el acceso a los recursos. Al realizar una operación, se deben especificar la acción, el recurso, la entidad principal (usuario o rol), la cuenta principal y otra información relevante. Esto permite definir permisos y restricciones precisos, asegurando la seguridad y eficiencia en la administración de permisos en AWS. AWS verifica la autenticación y autorización de la entidad antes de autorizar la acción solicitada en el recurso mediante el análisis de las políticas correspondientes. Por ejemplo, al acceder a un Bucket de S3, se puede configurar la accesibilidad restringiendo la visualización del Bucket y también se puede ejercer un control más específico sobre las acciones relacionadas con este recurso. A continuación se presenta un ejemplo de una política en formato JSON que otorga todos los permisos al Bucket y a su contenido en general.

Así como se puede asignar políticas a un recurso, es posible realizarlo a nivel de permisos de usuarios y su acceso a los servicios.

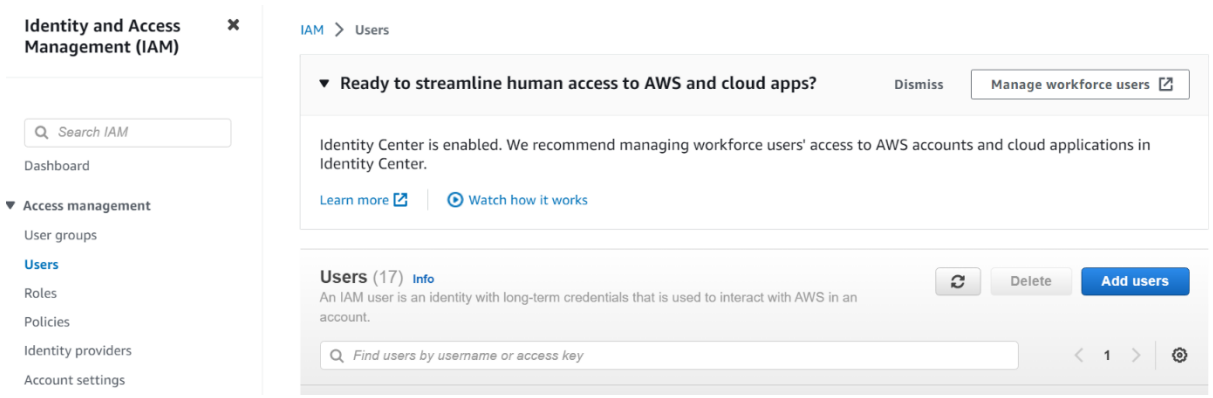


4.2. Gestión de acceso de usuarios

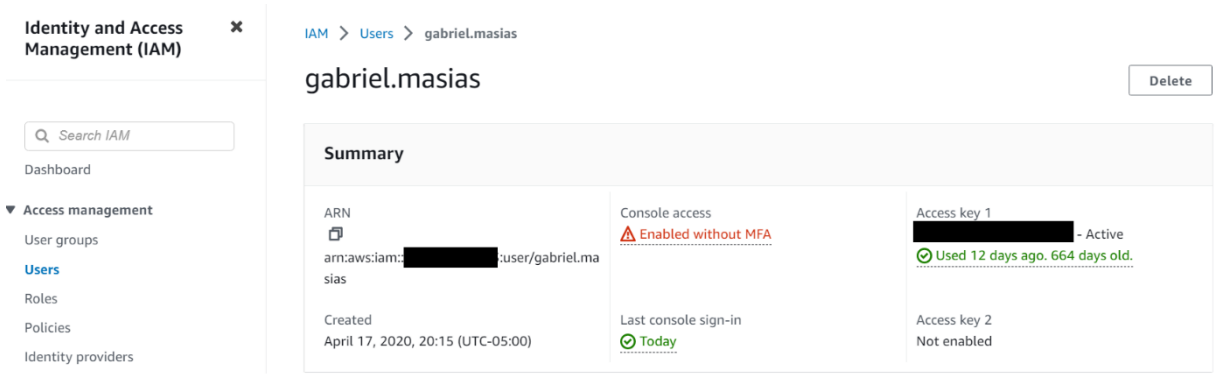
4.2.1. Alta y baja de usuarios

Para crear y/o darle de baja a usuarios, se realiza desde el servicio de **IAM**.

En caso se quiera crear un usuario, se proporcionará un nombre de usuario, acceso a la consola administrativa de AWS y/o vía AWS CLI, una contraseña específica o autogenerada que le solicitará crear una nueva en su próximo inicio de sesión, los permisos correspondientes del usuario (acceso a la consola, acceso a servicios, lectura y escritura de activos, etc.) y alguna etiqueta, pero puede ser opcional.

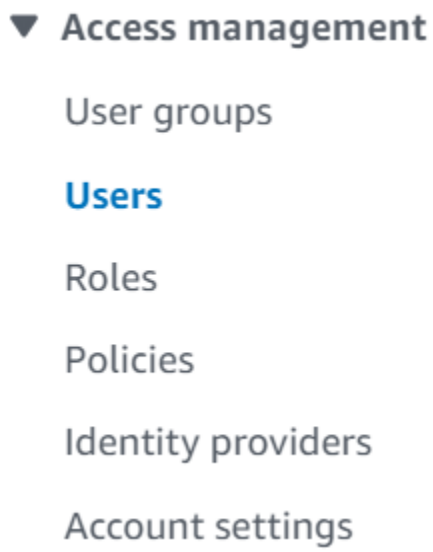


Además, si se desea eliminar un usuario, se ingresa a este desde la lista de usuarios, y se procede a eliminar.

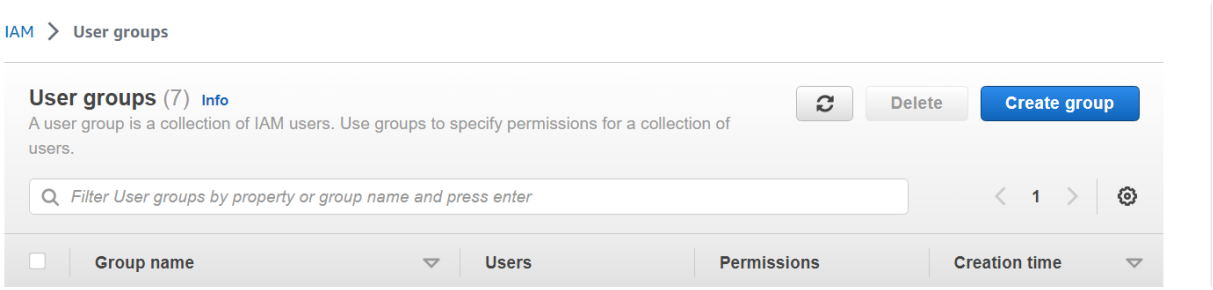


4.2.2. Provisión de acceso de usuarios

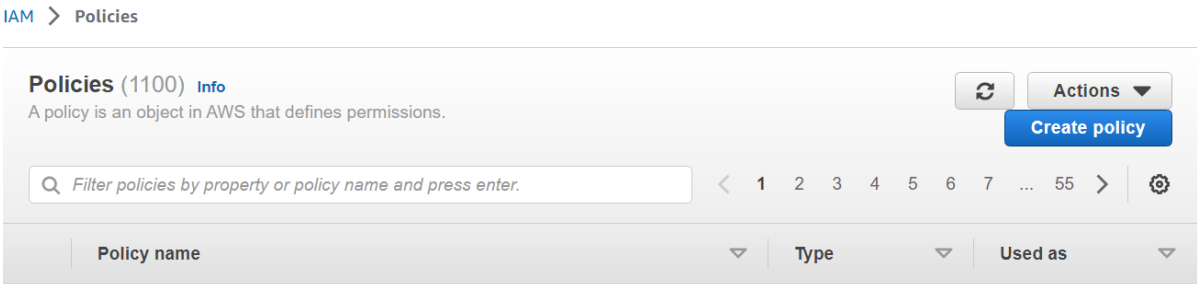
El acceso a usuarios se puede realizar desde **User groups**, y **Policies** dentro de **Access Management**.



Dentro de **User groups**, se crean los grupos donde cada usuario puede estar. Cada usuario puede estar en varios grupos a la vez, sin embargo, tendrá las políticas de este y se compartirá con los demás usuarios.



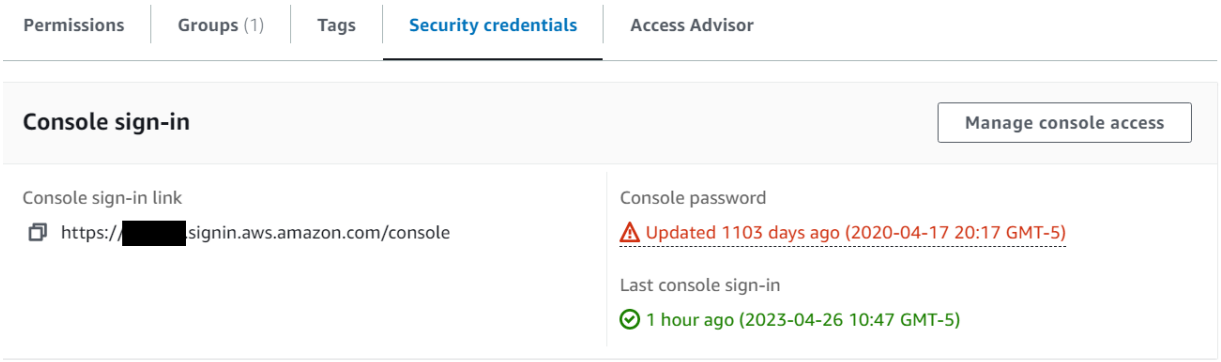
Por otro lado, se puede conceder acceso al usuario con solo políticas sin necesidad de estar en un grupo.



De igual manera, estas políticas se pueden adjuntar al usuario cuando se crea, también, se pueden editar luego de crearlo.

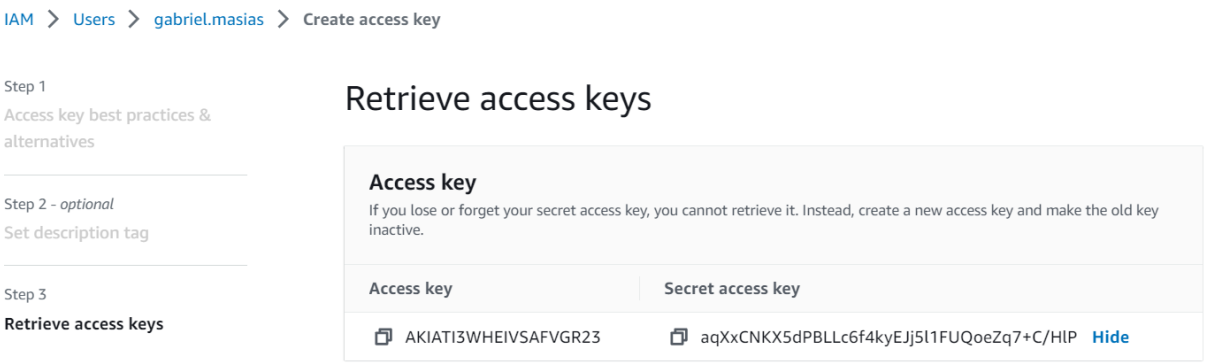
4.2.3. Gestión de la información secreta de autenticación de los usuarios

Un usuario puede acceder a los servicios de AWS vía la consola administrativa y/o AWS CLI. Dentro del perfil de usuario en **IAM**, está la opción de **Security Credentials**, donde se puede visualizar el estado de la contraseña (tiempo desde que se creó por última vez) y su último inicio de sesión.



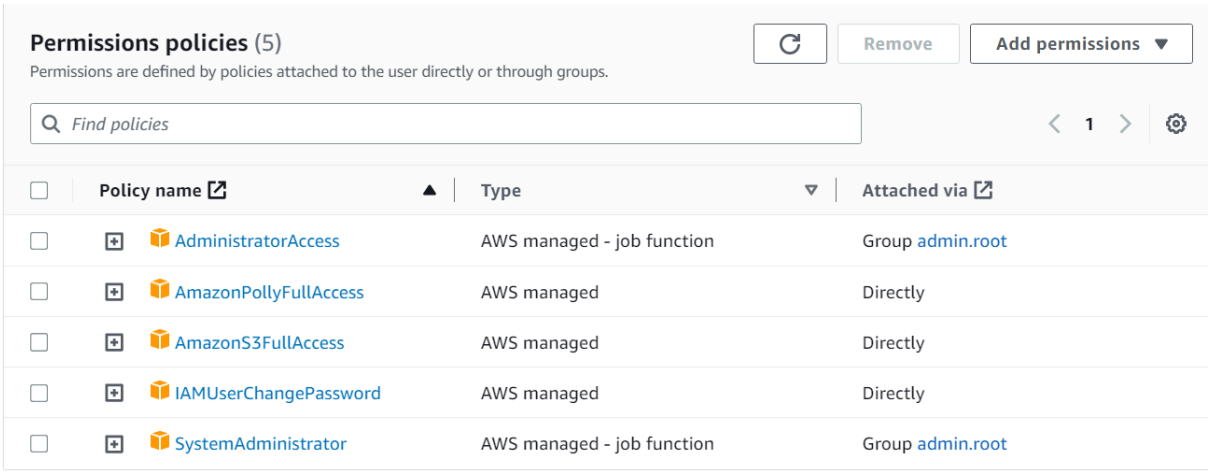
Por otro lado, para el acceso a los servicios de AWS vía CLI se gestiona mediante dos llaves de acceso, llave de acceso y llave de acceso secreta. Como aplicación de buenas prácticas, se realiza lo siguiente:

- Nunca almacenar la clave de acceso en texto plano, en un repositorio de código o en código.
- Desactivar o eliminar la clave de acceso cuando ya no se necesite.
- Activar los permisos de privilegio mínimos.
- Cambiar regularmente las llaves de acceso

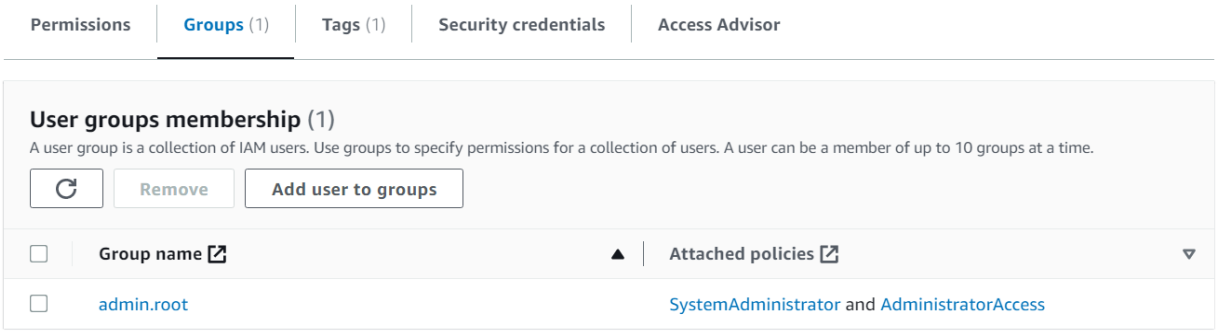


4.2.4. Revisión de los derechos de acceso de los usuarios

Para regularizar los derechos de acceso a un usuario, se revisan sus políticas, grupo(s) y permisos. Estos se pueden añadir o revocar cuando se necesite.



Un grupo tiene políticas adjuntadas directamente, por lo que, si se revoca una política, esto afectará a cada usuario perteneciente al grupo. En cambio, si se revocan políticas adjuntadas directamente al usuario, solo le afectarán a este mas no a los demás.



4.2.5. Supresión o ajuste de los derechos de acceso

Los usuarios deben tener habilitado y deshabilitado sus distintos accesos mediante las políticas, roles y grupos. Sin embargo, esto es un término muy general, ya que AWS ofrece distintos modos de acceder, ya sea a la consola administrativa, CLI, recursos, etc. Estos siempre se trabajan con un formato JSON, que afectan al servicio en sí para habilitar o restringir el acceso a los recursos y activos dentro de la infraestructura. Por ejemplo, con **IAM**, las políticas de los servicios, el rol de usuario, etc.

4.3. Responsabilidades del usuario

4.3.1. Uso de información secreta de autenticación

El uso de información secreta de autenticación en AWS es crucial para garantizar la seguridad de los recursos y datos almacenados en la nube. A continuación, se presentan algunas buenas prácticas que se recomiendan seguir:

- Utilizar **IAM**.
- Utilizar credenciales de acceso seguras: Se utiliza claves de acceso de AWS o credenciales de seguridad basadas en roles para autenticar a los usuarios y aplicaciones que acceden a los recursos de AWS. Establezca políticas de contraseña sólidas y rotación periódica de claves para garantizar la seguridad.
- **KMS**: Con el propósito de crear y gestionar claves de

cifrado y autenticación. Asegúrese de que las claves estén protegidas por controles de acceso y cifrado, y que solo los usuarios autorizados tengan acceso a ellas.

- Registre y supervise las actividades: Se utiliza AWS **CloudTrail** para registrar todas las actividades realizadas en su cuenta de AWS, incluyendo el acceso a los recursos y la administración de las claves de acceso. Configure alertas para detectar actividad sospechosa y revise regularmente los registros de actividad.

4.4. Control de acceso a sistemas y aplicaciones

4.4.1 Restricción del acceso a la información

La restricción del acceso a la información en AWS es fundamental para garantizar la seguridad de los datos. Para lograrlo, es importante seguir algunas mejores prácticas:

- Utilizar grupos de seguridad para definir las reglas de entrada y salida del tráfico de red.
- Utilizar Amazon **Virtual Private Cloud** (VPC) para limitar el acceso a los recursos de AWS desde la red.
- Usar **IAM**.
- Utilizar AWS **Organizations** para administrar y controlar el acceso a las cuentas de AWS en la organización.
- Utilizar **KMS**.
- Capacitar a los usuarios sobre las mejores prácticas de seguridad y cómo identificar y responder a las amenazas de seguridad en AWS.
- Configurar y proteger los accesos a los servidores que se implementen. Se puede configurar un servidor bastión para acceder a los demás recursos.

4.4.2. Procedimientos seguros de inicio de sesión

El inicio de sesión debe estar protegido con medidas y procedimientos que garanticen el ingreso seguro a los

servicios de AWS.

- Utilizar una contraseña segura: Se debe utilizar una contraseña fuerte, con una combinación de letras, números y símbolos. Además, evitar usar la misma contraseña para varias cuentas y cambiar la contraseña periódicamente. Según la norma ISO 27001:2013, una contraseña muy segura debe cumplir con los siguientes criterios:
    - Longitud: la longitud mínima de 8 caracteres, aunque se recomienda que sea de al menos 12 caracteres.
    - Complejidad: utilizar caracteres alfanuméricos y especiales.
    - Cambio frecuente: se recomienda cambiar las contraseñas regularmente, al menos cada 90 días.
    - No reutilizar contraseñas: cada cuenta en línea debe tener su propia contraseña única y no se deben reutilizar contraseñas en varias cuentas.
    - Restricciones de reintentos: se deben implementar restricciones en los intentos de inicio de sesión para evitar ataques de fuerza bruta.
    - Almacenamiento seguro: las contraseñas deben almacenarse de forma segura, utilizando técnicas como el hash de contraseñas.
    - Gestión de contraseñas: se debe implementar una política de gestión de contraseñas que incluya la creación, el almacenamiento y el cambio de contraseñas.
- Usar autenticación multifactor (MFA): La autenticación multifactor (MFA) en AWS exige el uso de varias formas de autenticación, como contraseña y código generado

por una app móvil como Google Authenticator, para garantizar una mayor seguridad en las cuentas y servicios.

4.4.3. Sistema de gestión de contraseñas

Amazon Web Services (AWS) ofrece un servicio llamado AWS **Secrets Manager** que se utiliza para gestionar y proteger contraseñas, claves de API y otros datos confidenciales. Este servicio proporciona una forma segura de almacenar y recuperar estos datos confidenciales, lo que facilita la administración y el acceso a ellos desde cualquier lugar.

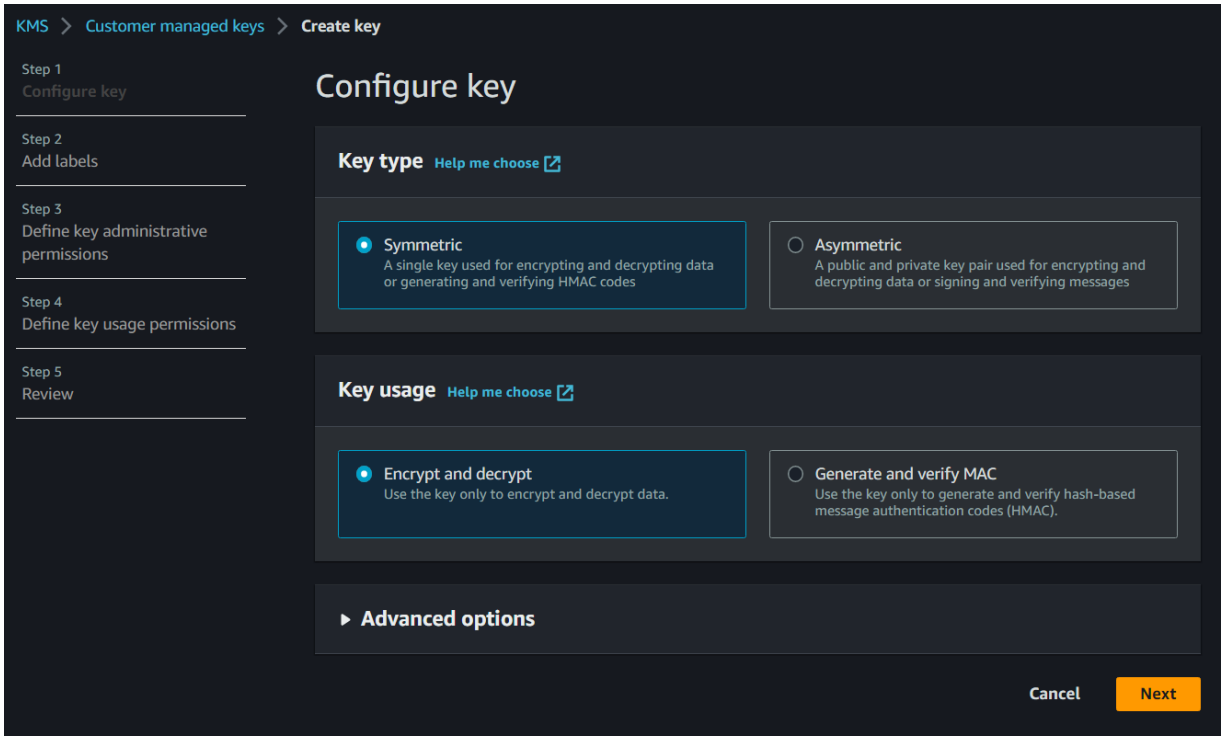
5. Criptografía

5.1. Controles criptográficos

5.1.1. Gestión de claves

La gestión de claves se lleva a cabo a través **KMS** y esto permite a los usuarios generar y administrar claves de cifrado de forma centralizada y utilizarlas para proteger datos almacenados en diferentes servicios de AWS, como Amazon **S3**, Amazon **EBS**, Amazon **RDS** y Amazon **Redshift**. Para controlar el acceso a las claves de cifrado, se utilizan políticas de control de acceso que permiten especificar qué usuarios o roles pueden utilizar las claves de cifrado y qué acciones pueden realizar con ellas.

Por ejemplo, para crear una clave criptográfica, se tiene en cuenta los dos tipos de claves que ofrece **KMS**:



- Clave simétrica: esta clave criptográfica se emplea tanto para cifrar como para descifrar datos, lo que significa que la misma clave es utilizada para ambas acciones. Es una

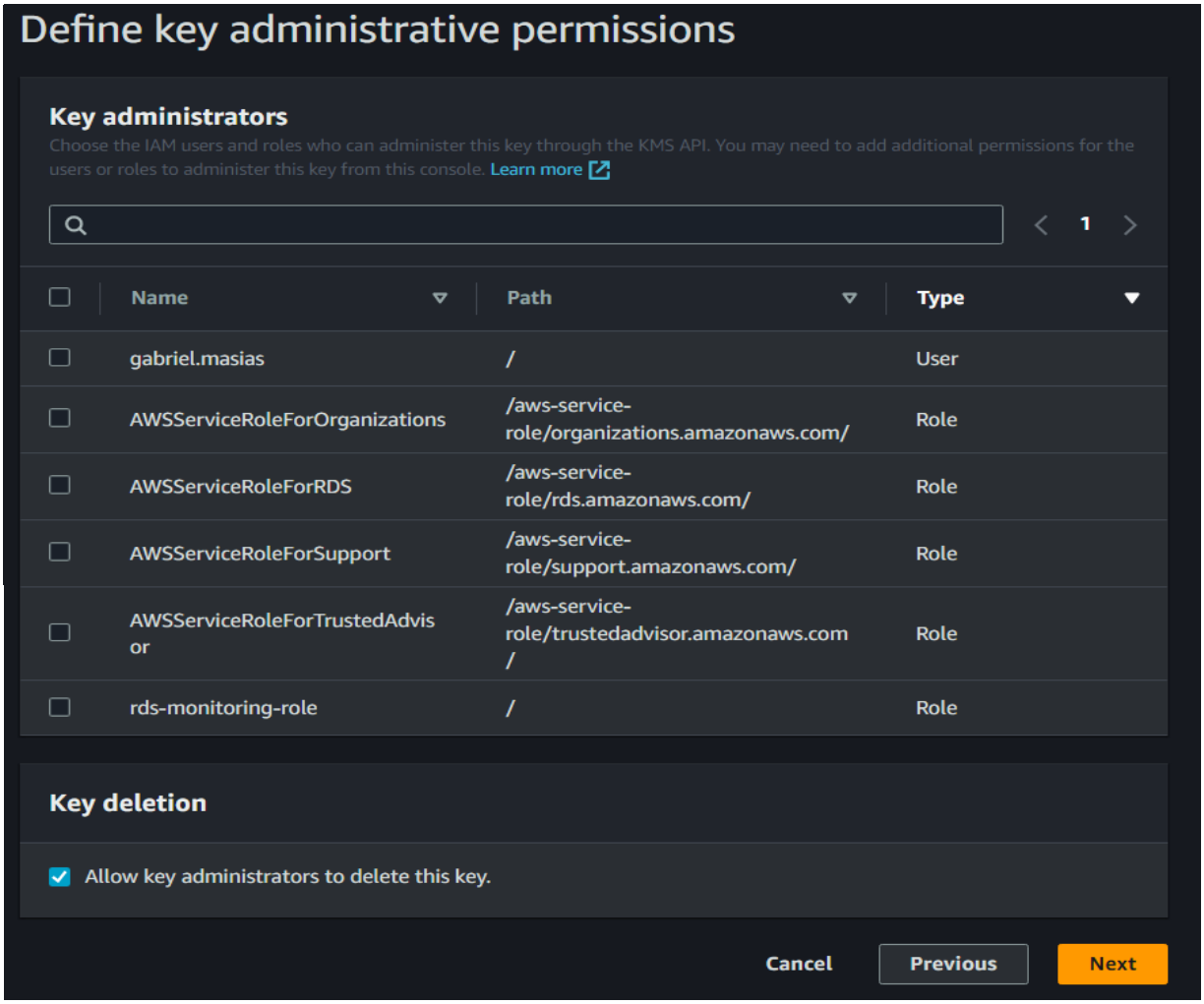
solución ideal para cifrar grandes cantidades de datos en poco tiempo y con alta eficiencia, por ejemplo, para cifrar bases de datos o archivos de gran tamaño.

- Clave asimétrica: también conocida como clave pública, esta clave criptográfica se utiliza para cifrar datos, pero no para descifrarlos. En su lugar, se utiliza una clave privada correspondiente para descifrar los datos cifrados. Las claves asimétricas se utilizan comúnmente para establecer comunicaciones seguras entre dos partes, como en el intercambio de claves de sesión en SSL/TLS. Las claves asimétricas también se utilizan para firmar digitalmente datos y garantizar su integridad.

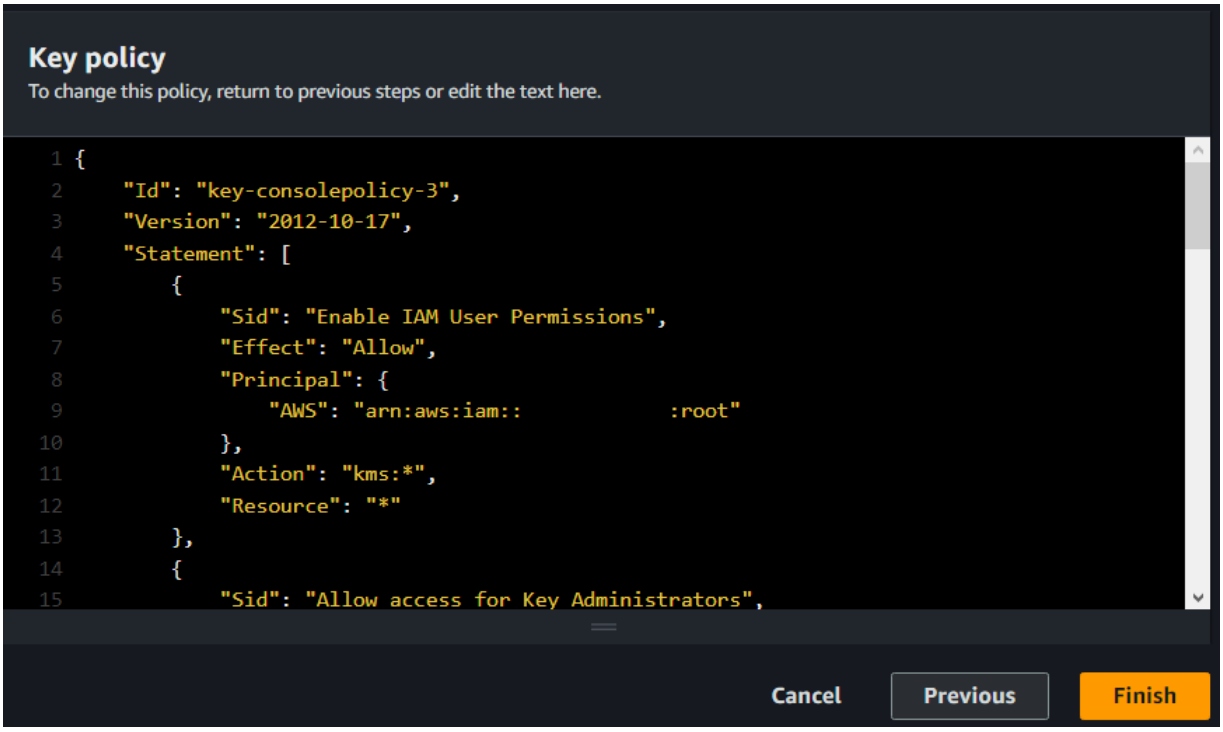
Además, hay dos tipos de **Key Usage** disponibles en KMS:

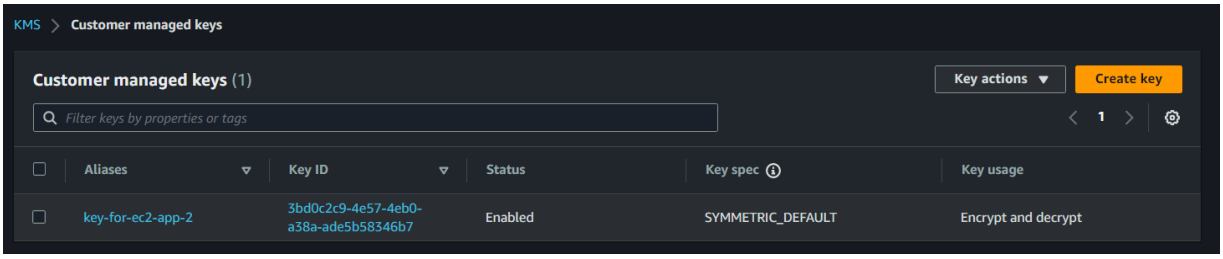
- Cifrado/Descifrado (**ENCRYPT/DECRYPT**): Las claves criptográficas con Key Usage "ENCRYPT/DECRYPT" se utilizan para cifrar y descifrar datos. Estas claves son adecuadas para aplicaciones que requieren protección de datos confidenciales, como el cifrado de bases de datos, el cifrado de archivos, el cifrado de datos de red y el cifrado de mensajes.
- Firmado/Verificación (**SIGN/VERIFY**): Las claves criptográficas con Key Usage "SIGN/VERIFY" se utilizan para firmar y verificar digitalmente datos. Estas claves son adecuadas para aplicaciones que requieren garantizar la integridad y autenticidad de los datos, como la firma digital de documentos, la verificación de la autenticidad de los datos y la validación de las identidades.

Se agrega el Alias para la clave criptográfica y una breve descripción de esta.



Se elije los usuarios y roles IAM que pueden administrar esta clave a través de la API KMS. Es posible que tenga que añadir permisos adicionales para los usuarios o roles para administrar esta clave desde esta consola. Además, se selecciona los usuarios y roles IAM que pueden utilizar la clave KMS en operaciones criptográficas. Finalmente, antes de crear la clave, se muestra un resumen, y en este, se detalla las políticas y acceso mediante formato JSON.





Esta clave se puede utilizar para proteger y cifrar una variedad de recursos en AWS, como, **EC2**, **EBS**, **S3**, etc.

6. Seguridad operativa

6.1. Procedimientos operativos y responsabilidades

6.1.1. Gestión de la capacidad

La capacidad se refiere a la cantidad de recursos de computación, almacenamiento y redes necesarios para satisfacer la demanda de los clientes y usuarios finales. AWS ofrece varios servicios y herramientas para ayudar en la gestión de la capacidad, incluyendo:

- Elastic Load Balancing: Este servicio balancea tráfico entrante hacia múltiples instancias, lo que permite manejar grandes volúmenes de tráfico. También proporciona escalado automático y monitoreo.
- Amazon EC2 Auto Scaling: Este servicio permite escalar automáticamente la capacidad de la instancia de EC2 en función de la demanda de carga de trabajo. EC2 Auto Scaling monitorea continuamente la carga de trabajo y ajusta automáticamente el número de instancias de EC2 en función de las métricas predefinidas, como la utilización de la CPU, la memoria y el tráfico de red. Se puede configurar políticas de escalado automático para ajustar automáticamente la capacidad de instancias de Amazon EC2 en función de la demanda.
- Amazon CloudWatch: Este servicio permite monitorear la capacidad y el rendimiento de los recursos en AWS. Se pueden configurar alarmas para alertar cuando se alcance un umbral específico de capacidad o rendimiento.
- Amazon RDS Auto Scaling: Similar a EC2 Auto Scaling, este servicio ajusta automáticamente el tamaño de la base de datos de Amazon RDS en función de la demanda. La capacidad se puede ajustar verticalmente (cambiar el tamaño de la instancia de base de datos) o horizontalmente

(agregar más instancias de base de datos).

6.1.2. Separación de los entornos de desarrollo, pruebas y operativo

La separación de los entornos es una práctica recomendada para garantizar la calidad y estabilidad de las aplicaciones en AWS. Esto implica crear entornos separados para el desarrollo, pruebas y producción de las aplicaciones, y asegurarse de que las pruebas se realicen en el entorno de pruebas antes de implementar en producción.

AWS ofrece varios servicios que se pueden utilizar para implementar esta práctica recomendada. A continuación, se describen algunos de estos servicios y ejemplos de cómo se pueden utilizar:

- EC2 es un servicio que permite crear y administrar instancias de servidores virtuales en la nube. Los entornos de desarrollo, pruebas y operativo se pueden crear en instancias de EC2 separadas. Por ejemplo, se puede crear una instancia de EC2 para el entorno de desarrollo y otra para el entorno de pruebas. Esto permite a los desarrolladores realizar pruebas y experimentar sin afectar el entorno de producción.
- ECS es un servicio que permite ejecutar aplicaciones en contenedores de Docker en AWS. Puede utilizarse para crear clústeres de contenedores separados para los entornos de desarrollo, pruebas y operativo.
- EKS es un servicio de orquestación de contenedores basado en Kubernetes que permite ejecutar aplicaciones en contenedores en AWS. Al igual que ECS, se puede utilizar para crear clústeres de contenedores separados para cada entorno.

- RDS es un servicio de bases de datos relacional en la nube. Se puede crear una instancia de Amazon RDS para cada entorno (desarrollo, pruebas y operativo) para mantener las bases de datos separadas. Esto garantiza que los datos de producción no se vean afectados por cambios realizados en los entornos de desarrollo o pruebas.
- S3 es un servicio de almacenamiento de objetos en la nube que permite almacenar y recuperar datos de forma segura y escalable. Puede utilizarse para almacenar y compartir datos y artefactos entre entornos.

6.2. Copia de seguridad

6.2.1. Copia de seguridad de la información

Se pueden utilizar estrategias para una copia de seguridad eficaz y cumplir con los requisitos de la ISO 27017:2015. Algunos de estos servicios son:

- Amazon S3.
- Amazon EBS.

6.3. Registro y monitoreo

La ISO 27017:2015 establece que los proveedores de servicios en la nube deben implementar sistemas de registro y eventos que permitan el seguimiento de actividades relevantes relacionadas con la seguridad de la información. El objetivo principal es mantener un registro de eventos para fines de auditoría, análisis forense y detección de incidentes de seguridad. Algunos de los eventos que se pueden registrar incluyen el acceso a los servicios en la nube, cambios en la configuración, intentos de autenticación fallidos y acciones realizadas por los usuarios.

6.3.1. Registro de eventos

- AWS CloudTrail: Es un servicio que registra eventos de API para todas las cuentas de AWS en tu organización. Se puede utilizar para auditar y monitorear las acciones

realizadas en la cuenta de AWS, lo que incluye el seguimiento de eventos relacionados con la seguridad.

- AWS CloudWatch Logs: Este servicio permite almacenar, monitorear y acceder a los registros generados por las aplicaciones y recursos de AWS. Se puede configurar CloudWatch Logs para recibir y analizar registros de diferentes fuentes, incluidos los registros de eventos generados por otros servicios de AWS.
- Amazon GuardDuty: Proporciona detección de amenazas en tiempo real y análisis de seguridad para ayudar a proteger las cargas de trabajo en AWS. Puede ayudar a identificar eventos de seguridad y actividades sospechosas.

6.3.2. Protección de la información de registro

- Almacenamiento seguro de registros: AWS ofrece servicios como Amazon CloudWatch Logs y Amazon S3 (Simple Storage Service) que permiten almacenar y gestionar los registros de eventos de las aplicaciones y sistemas de manera segura. Se puede aplicar cifrado a los datos almacenados y configurar permisos adecuados para el acceso.
- Monitorización de eventos de seguridad: Se configura alertas y notificaciones en AWS CloudWatch para detectar eventos de seguridad específicos en registros, como intentos de acceso no autorizado o cambios en la configuración de recursos. Esto permite tomar medidas rápidas en caso de actividades sospechosas o anómalas.
- Respaldo y recuperación: Realiza copias de seguridad regulares de registros y establecer un plan de recuperación ante desastres. AWS ofrece servicios como AWS Backup y Amazon S3 Glacier para realizar respaldos seguros y

almacenar datos a largo plazo.

- Monitoreo y registros: AWS CloudTrail audita y registra eventos de actividad en la cuenta de AWS. Esto permite realizar un seguimiento de las acciones realizadas en un entorno y mantener registros de auditoría para fines de cumplimiento. AWS CloudTrail también proporciona registros de auditoría para los recursos de Amazon S3.
- Protección de datos: KMS.
- Control de acceso: AWS Identity and Access Management (IAM).
- Protección de la red: Amazon VPC crea una red virtual aislada y controlada donde se puede lanzar recursos. Se puede utilizar VPC para segmentar y proteger los recursos en la nube.
- Evaluación de riesgos: AWS Trusted Advisor es una herramienta que ayuda a identificar posibles problemas de seguridad, optimizar la configuración de los recursos y mejorar el rendimiento de la infraestructura en la nube.
- Continuidad del negocio: AWS ofrece servicios como AWS Backup y AWS Disaster Recovery que te permiten crear y administrar copias de seguridad de tus datos, así como implementar planes de recuperación ante desastres.

6.2.3. Registros de administrador y operador

- AWS CloudTrail: Se utiliza para auditar y registrar las acciones realizadas por los administradores en la cuenta de AWS. Esto incluye acciones como la creación, modificación o eliminación de recursos, cambios en la configuración de seguridad, y acceso a servicios y datos sensibles. Los registros de CloudTrail permiten rastrear las actividades de administración y proporcionan evidencia para fines de auditoría y cumplimiento normativo.

- CloudWatch Logs y Amazon CloudWatch Events: Se puede capturar y almacenar los registros de eventos y métricas relacionados con las operaciones en un entorno de AWS. Se puede configurar alertas basadas en eventos específicos para detectar anomalías o comportamientos sospechosos.
- AWS Systems Manager y AWS Security Hub: Permiten gestionar y responder a incidentes de seguridad de manera efectiva. Estas herramientas ayudan a registrar y documentar los eventos relacionados con incidentes y a tomar medidas correctivas y preventivas adecuadas.

6.3. Gestión de vulnerabilidades técnicas

- AWS Inspector: Es un servicio de evaluación de seguridad automatizado que ayuda a mejorar la seguridad y el cumplimiento de los recursos de AWS. Inspector analiza los recursos de AWS en busca de vulnerabilidades, violaciones de políticas y desviaciones de mejores prácticas de seguridad.
- Amazon GuardDuty: Permite detectar amenazas para analizar el tráfico de red y las actividades de los usuarios en AWS. GuardDuty puede ayudar a identificar posibles amenazas de seguridad, incluyendo vulnerabilidades técnicas y ataques maliciosos.

7. Relaciones con los proveedores

7.1. Seguridad de la información en las relaciones con los proveedores

7.1.1. Política de seguridad de la información para las relaciones con los proveedores

Es fundamental llevar a cabo una evaluación completa de seguridad antes de elegir un proveedor de servicios en la nube como AWS. Esta evaluación abarca aspectos como examinar sus medidas de seguridad, certificaciones y cumplimiento normativo, así como su historial de confiabilidad y seguridad.

AWS ofrece acuerdos de nivel de servicio exhaustivos que establecen los compromisos de la plataforma en términos de disponibilidad, rendimiento y seguridad de sus servicios en la nube. Es importante revisar y comprender los SLA (Service Level Agreements) de AWS para garantizar que se ajusten a tus requisitos de seguridad.

El conjunto de servicios de AWS, como Amazon EC2, Amazon S3 y Amazon RDS, cuenta con acuerdos de nivel de servicio específicos para cada uno. Estos acuerdos son herramientas clave para establecer expectativas claras y garantizar el cumplimiento en relación con el rendimiento y la disponibilidad de cada servicio.

8. Gestión de incidentes de seguridad de la información

8.1. Gestión de incidentes y mejoras en la seguridad de la información

8.1.1. Responsabilidades y procedimientos

- Evaluación de riesgos y tratamiento: La norma establece la obligación de realizar una evaluación de riesgos y aplicar medidas apropiadas para abordar los riesgos identificados. En el contexto de AWS, esto implica evaluar los riesgos relacionados con la utilización de los servicios de AWS y tomar acciones para mitigarlos. Por ejemplo, implementar medidas de control de acceso adecuadas, configurar de manera apropiada las políticas de seguridad de AWS Identity and Access Management (IAM) y utilizar la encriptación de datos.
- Seguridad de la información: La seguridad de la información es de vital importancia en el entorno de la nube. Es posible aplicar los servicios y características de seguridad proporcionados por la plataforma para cumplir con estos controles. Por ejemplo, se configurar grupos de seguridad para controlar el tráfico de red, AWS CloudTrail para el registro y seguimiento de eventos, y AWS Shield para protegerse contra ataques de denegación de servicio (DDoS).
- Gestión de identidades y accesos: El uso de IAM es aplicable en este caso.

8.1.2. Notificación de incidentes relacionados con la seguridad de la información

- Responsabilidades del proveedor de servicios en la nube (AWS)
  - Detección de incidentes

    AWS cuenta con sistemas y servicios dedicados a la detección oportuna de incidentes de seguridad de la

información. Un ejemplo de ello es Amazon GuardDuty, que detecta amenazas y realiza un monitoreo constante de las actividades y eventos de la cuenta de AWS, buscando comportamientos sospechosos o maliciosos.

- Notificación a los clientes

  Si ocurre un incidente que afecte la seguridad de la información de los clientes, AWS asume la responsabilidad de informar a los clientes afectados. Esta notificación puede abarcar información detallada sobre el incidente, su posible impacto y las medidas recomendadas para reducir el riesgo.

- Colaboración con los clientes

  AWS y los clientes colaboran de manera cercana para abordar los incidentes de seguridad de forma efectiva. Esta colaboración implica la coordinación de esfuerzos en la investigación del incidente, implementación de medidas correctivas e intercambio de información pertinente sobre las amenazas o vulnerabilidades identificadas.

❖ Responsabilidades del cliente (customer) de los servicios de AWS

- Reporte de incidentes

  Es responsabilidad de los usuarios de los servicios de AWS notificar a la plataforma sobre cualquier incidente de seguridad de la información que impacte en sus datos o recursos en la nube. Esta acción permite que AWS tome las medidas pertinentes para investigar y abordar el incidente de manera oportuna.

- Utilización de servicios de notificación

  AWS ofrece servicios como Amazon CloudWatch, los cuales brindan a los usuarios la posibilidad de configurar

alarmas y notificaciones personalizadas para supervisar y recibir alertas sobre eventos y métricas relacionadas con la seguridad de la información. Los usuarios pueden aprovechar estas funcionalidades para recibir notificaciones en tiempo real acerca de posibles incidentes de seguridad.

- Implementación de medidas de respuesta y mitigación

  Es importante que los usuarios de los servicios de AWS consideren la implementación de planes de respuesta a incidentes y medidas de mitigación para abordar los incidentes de seguridad de manera eficiente. Estas medidas pueden comprender la activación de copias de seguridad de datos, la restauración de sistemas o la aplicación de parches de seguridad.

8.1.3. Notificación de deficiencias en la seguridad de la información

- ❖ Responsabilidades del proveedor de servicios en la nube (AWS)
  - Identificación y evaluación de deficiencias

    AWS asume la responsabilidad de detectar y evaluar cualquier deficiencia en la seguridad de la información que pueda surgir en sus servicios. Para lograr esto, se llevan a cabo evaluaciones periódicas de seguridad, auditorías internas y pruebas de penetración, con el objetivo de identificar posibles vulnerabilidades o áreas que requieran mejoras.
  - Notificación a los clientes

    Si se detectan deficiencias que puedan impactar la seguridad de la información de los clientes, AWS asume la responsabilidad de informar a los clientes afectados. Esta notificación puede contener información detallada acerca de la naturaleza de la deficiencia, su posible

impacto y las acciones recomendadas para solucionarla.

- Acciones correctivas y mejoras

  AWS está obligado a tomar acciones correctivas y fortalecer la seguridad de la información en sus servicios en base a las deficiencias detectadas. Estas medidas pueden comprender la aplicación de parches de seguridad, actualizaciones de software, mejoras en los controles de acceso y otras acciones necesarias para abordar y mitigar los riesgos identificados.

❖ Responsabilidades del cliente (customer) de los servicios de AWS

- Reporte de deficiencias

  Los clientes de AWS tienen la responsabilidad de reportar cualquier deficiencia en la seguridad de la información que puedan detectar en sus sistemas o en los servicios de AWS que utilizan. Al informar de estas deficiencias a AWS, se les brinda la oportunidad de tomar medidas correctivas y mejorar la seguridad de sus servicios en general. De esta manera, los usuarios también contribuyen a la seguridad de la nube de AWS y a la protección de sus datos.

- Utilización de canales de comunicación designados

  AWS pone a disposición de los usuarios canales específicos para reportar deficiencias en la seguridad, tales como el AWS Support Center. Es importante que los usuarios utilicen estos canales designados para garantizar una comunicación eficiente y efectiva con el equipo de seguridad de AWS. De esta manera, las deficiencias reportadas pueden ser atendidas y abordadas adecuadamente.

- Colaboración en la resolución de deficiencias

  Es necesario que los usuarios colaboren con AWS en la resolución de las deficiencias identificadas. Esto implica brindar información adicional, cooperar en la implementación de medidas correctivas y participar en auditorías o revisiones de seguridad solicitadas por AWS. Trabajar de forma conjunta y cooperativa con AWS es fundamental para abordar y solucionar eficazmente las deficiencias de seguridad.

En la ejecución de los instrumentos en la primera empresa, se obtuvieron los siguientes datos. El primer instrumento se utilizó para la dimensión **Seguridad**.

Ficha de observación			
Investigador	Carlos Gabriel Masias Ordinola	**Tipo de prueba**	Descriptiva
Empresa / Institución	Tedregal E.I.R.L.		
Objetivo específico	Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento		
Dimensión de estudio	Seguridad		
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Nivel de cumplimiento del control de la norma ISO 27017:2015	Nivel de cumplimiento
No de iteración	**Control de la norma ISO**	**Nivel de cumplimiento**
	Políticas de seguridad de la información	
1	Políticas de seguridad de la información	En desacuerdo
	Organización de la seguridad de la información	
2	Roles y responsabilidades de la seguridad de la información	Neutral
	Gestión de activos	
3	Responsabilidad por los activos	De acuerdo
	Control de acceso	
4	Requisitos comerciales de control de acceso	De acuerdo
5	Gestión de acceso de usuarios	Totalmente de acuerdo
6	Responsabilidades del usuario	Neutral
7	Control de acceso a sistemas y aplicaciones	Neutral
	Criptografía	
8	Controles criptográficos	En desacuerdo

	Seguridad operativa	
9	Procedimientos operativos y responsabilidades	De acuerdo
10	Copia de seguridad	De acuerdo
11	Registro y monitoreo	De acuerdo
12	Gestión de vulnerabilidades técnicas	Totalmente en desacuerdo
	Seguridad de las comunicaciones	
13	Gestión de la seguridad de la red	Neutral
	Relaciones con los proveedores	
14	Seguridad de la información en las relaciones con los proveedores	De acuerdo
	Gestión de incidentes de seguridad de la información	
15	Gestión de incidentes y mejoras en la seguridad de la información	Neutral

El segundo instrumento fue aplicado para la dimensión **Complejidad**.

Ficha de observación				
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva
Empresa / Institución	Tedregal E.I.R.L.			
Dimensión de estudio	Complejidad			
Objetivo específico	Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube			
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023	

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Tiempo de diseño e implementación (días)	Días

No de iteración	**Fecha de revisión**	**Nombre del recurso**	**Tiempo (días)**
1	07/04/23	Route53	1
2	08/04/23	CloudFront	1
3	09/04/23	Bucket S3	1
4	10/04/23	Certificate Manager	1
5	11/04/23	Instancia EC2	1
6	12/04/23	Elastic Container Registry	1
7	13/04/23	Elastic Container Service	2
8	15/04/23	CloudWatch	1
9	16/04/23	Identity Access Management	3
10	19/04/23	Relational Database Service	1
11	20/04/23	CloudTrail	2
12	22/04/23	Key Management Service	2

El tercer instrumento se ejecutó para la dimensión de **Rendimiento**. Se realizó en dos servicios específicos, EC2 (propio del ECS) y RDS.

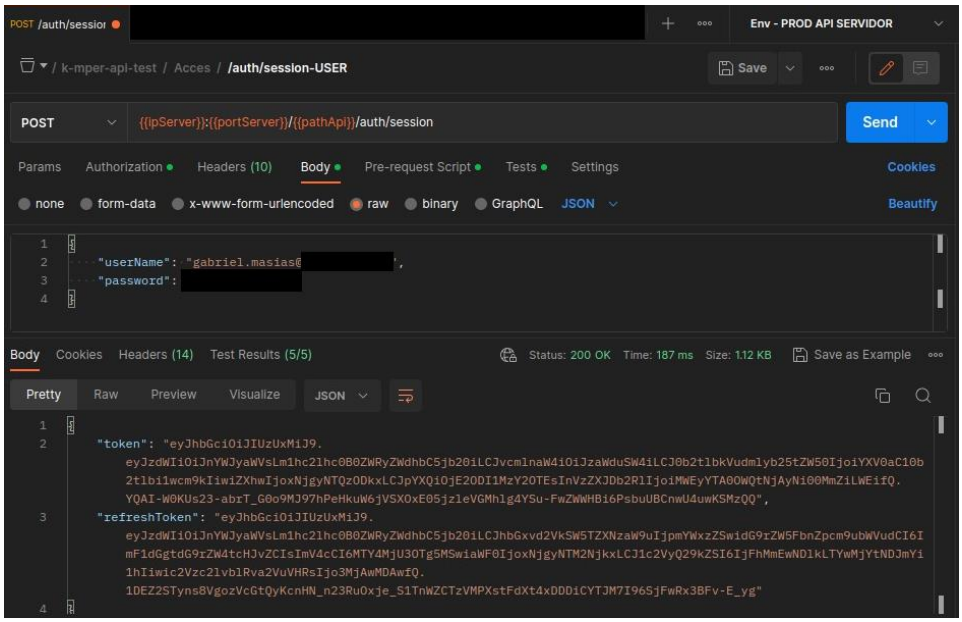
Ficha de observación				
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva
Empresa / Institución	Tedregal E.I.R.L.			
Dimensión de estudio	Rendimiento			
Objetivo específico	Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta			
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023	

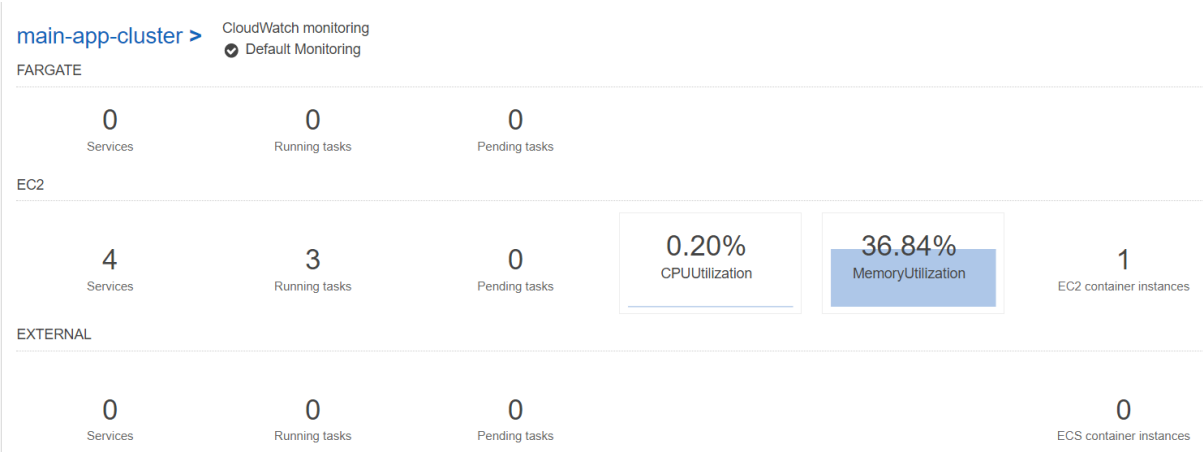
Variable	**Indicador**	**Medida**
Infraestructura en la nube	Porcentaje de utilización del recurso virtualizado	Tasa porcentual
	Tiempo de actividad del servicio	Horas
	Tiempos de respuesta	Milisegundos

No de iteración	**Nombre del servicio**	**Porcentaje de utilización**	**Tiempo de actividad**	**Tiempos de respuesta**
1	EC2	36.84%	12	187
2	EC2	42.57%	12	706
3	EC2	40.99%	24	166
4	EC2	66.99%	48	176
5	RDS	8.48%	12	120
6	RDS	8.47%	12	136

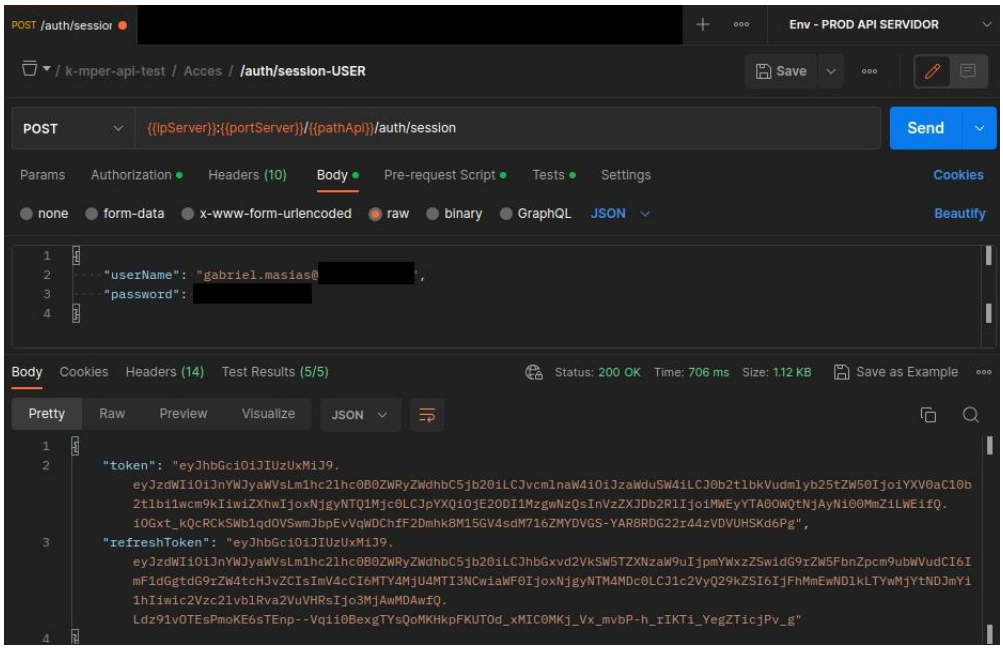
Los datos se consiguieron por medio de la consola administrativa de AWS y el uso de la herramienta Postman.

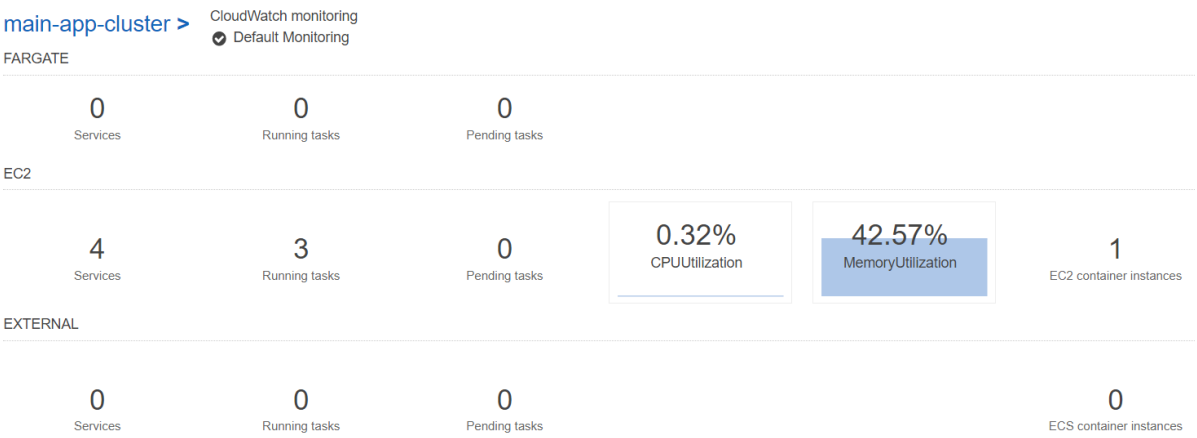
Se ejecutó cuatro veces una solicitud POST donde corre una aplicación en EC2. En la primera iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 187 milisegundos. La utilización de memoria fue de 36.84%. El tiempo de actividad fue de 12 horas.



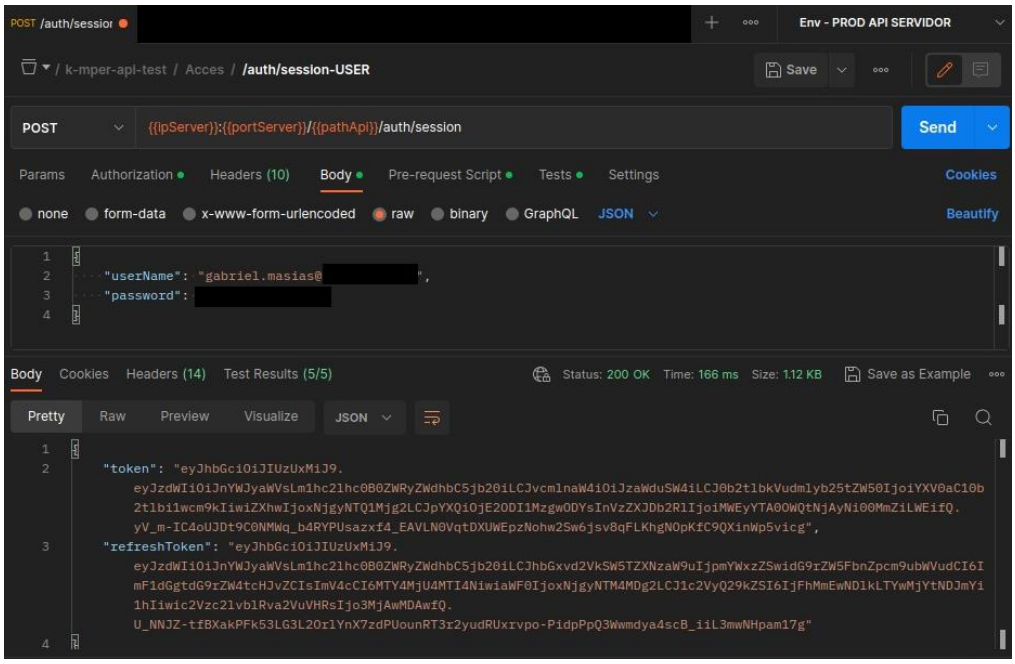


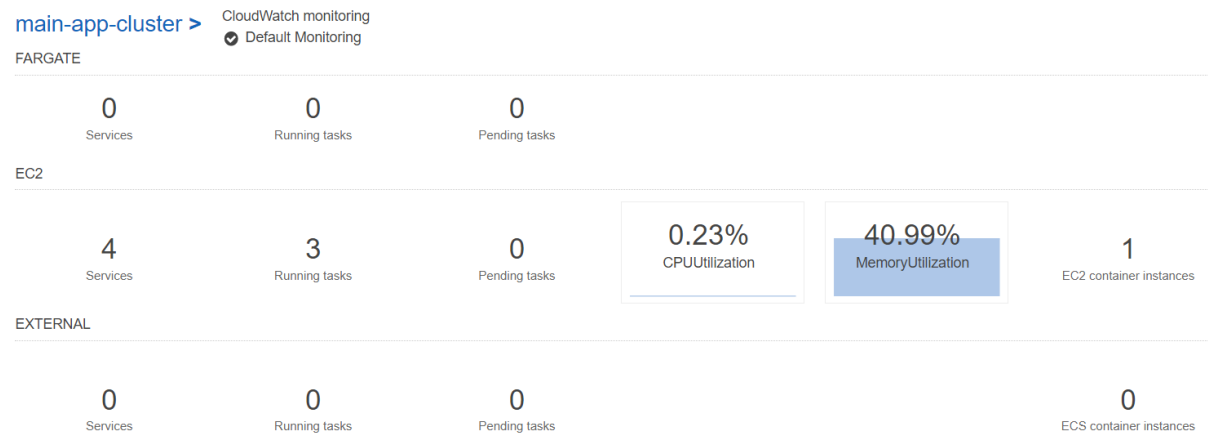
En la segunda iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 706 milisegundos. La utilización de memoria era de 42.57%. El tiempo de actividad fue de 12 horas.



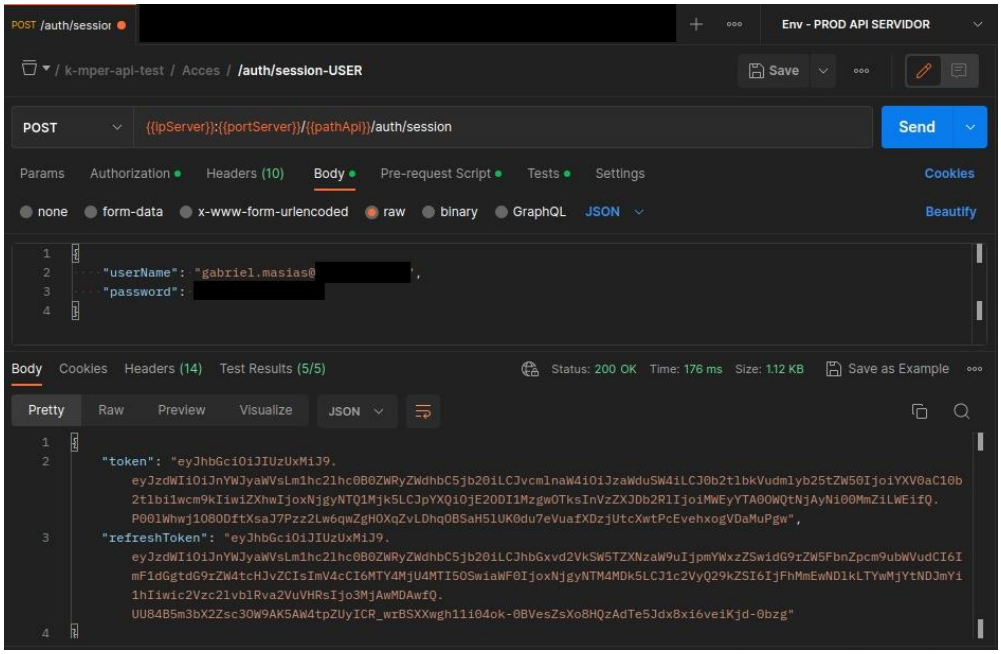


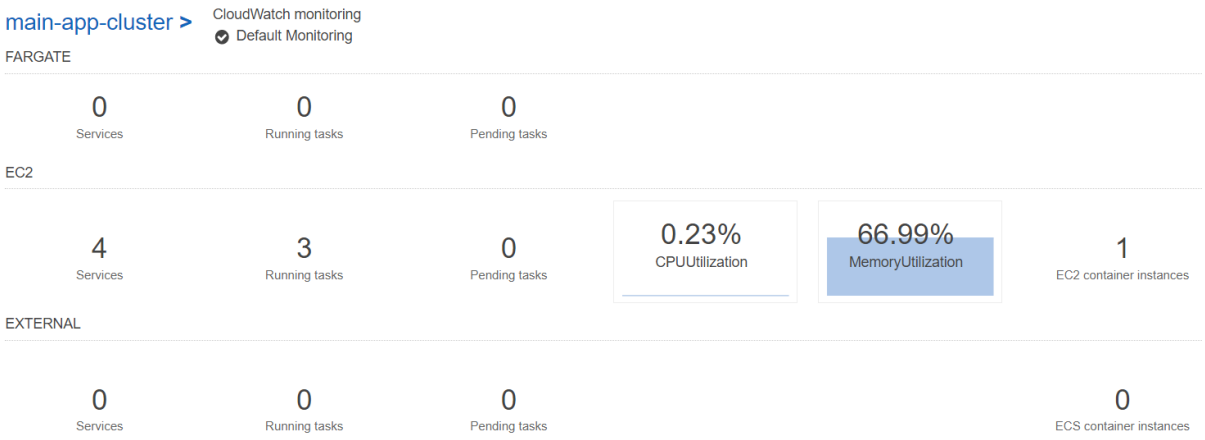
En la tercera iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 166 milisegundos. La utilización de memoria era de 40.99%. El tiempo de actividad fue de 24 horas.



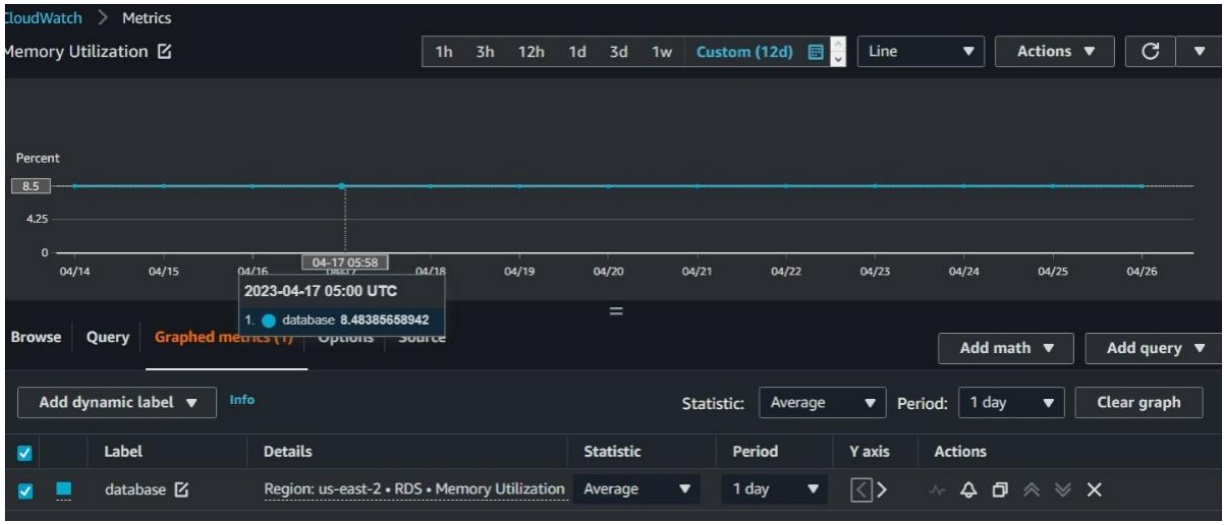


Por último, en la cuarta iteración aplicada en EC2, se obtuvo un Status Code de 200 y un tiempo de respuesta de 176 milisegundos. La utilización de memoria era de 66.99%. El tiempo de actividad fue de 48 horas.

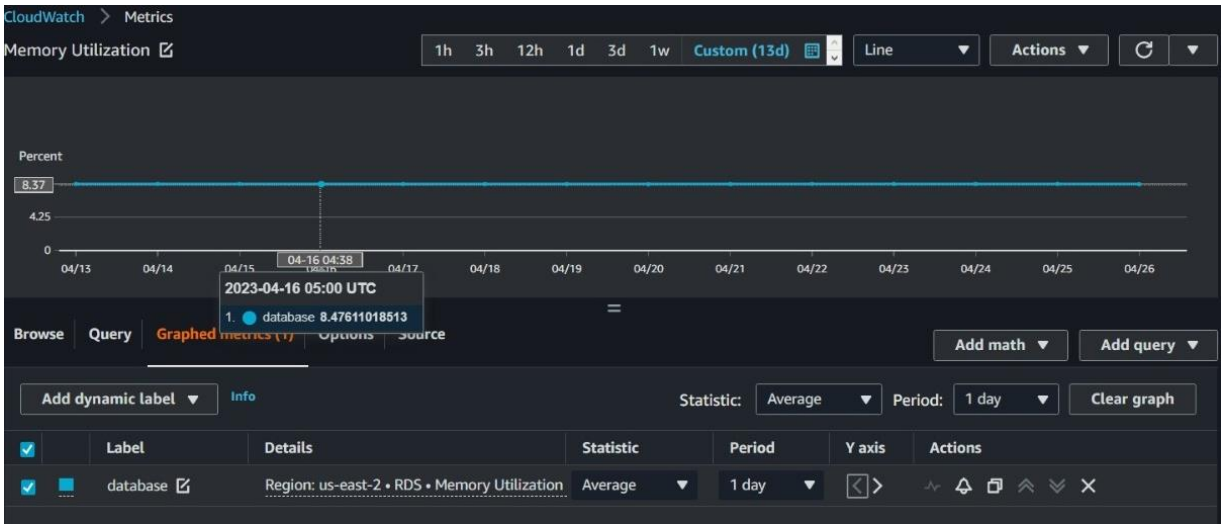




En la quinta iteración, se obtuvo un valor de 8.48%, donde el tiempo de actividad fue de 12 horas.



En la segunda iteración, se obtuvo un valor de 8.47% de utilización de memoria y el tiempo de actividad fue de 12 horas.



Para la segunda empresa, se obtuvo en el primer instrumento:

Ficha de observación			
Investigador	Carlos Gabriel Masias Ordinola	**Tipo de prueba**	Descriptiva
Empresa / Institución	Plataformas y Soluciones Digitales S.A.C.		
Objetivo específico	Determinar los controles de seguridad de la norma ISO 27017:2015 y su aplicabilidad a AWS para evaluar su nivel cumplimiento		
Dimensión de estudio	Seguridad		
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Nivel de cumplimiento del control de la norma ISO 27017:2015	Nivel de cumplimiento
No de iteración	**Control de la norma ISO**	**Nivel de cumplimiento**
	Políticas de seguridad de la información	
1	Políticas de seguridad de la información	En desacuerdo
	Organización de la seguridad de la información	
2	Roles y responsabilidades de la seguridad de la información	Neutral
	Gestión de activos	
3	Responsabilidad por los activos	De acuerdo
	Control de acceso	
4	Requisitos comerciales de control de acceso	De acuerdo
5	Gestión de acceso de usuarios	Totalmente de acuerdo
6	Responsabilidades del usuario	Neutral
7	Control de acceso a sistemas y aplicaciones	Neutral
	Criptografía	
8	Controles criptográficos	Totalmente en desacuerdo

	Seguridad operativa	
9	Procedimientos operativos y responsabilidades	De acuerdo
10	Copia de seguridad	Neutral
11	Registro y monitoreo	De acuerdo
12	Gestión de vulnerabilidades técnicas	Totalmente en desacuerdo
	Seguridad de las comunicaciones	
13	Gestión de la seguridad de la red	Totalmente en desacuerdo
	Relaciones con los proveedores	
14	Seguridad de la información en las relaciones con los proveedores	De acuerdo
	Gestión de incidentes de seguridad de la información	
15	Gestión de incidentes y mejoras en la seguridad de la información	Neutral

En el segundo instrumento se obtuvo:

Ficha de observación					
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva	
Empresa / Institución	Plataformas y Soluciones Digitales S.A.C.				
Dimensión de estudio	Complejidad				
Objetivo específico	Identificar los factores clave que se asocian en el tiempo de diseño e implementación de servicios en la nube				
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023		
Variable	**Indicador**		**Medida**		
Infraestructura en la nube	Tiempo de diseño e implementación (días)		Días		
No de iteración	**Fecha de revisión**	**Nombre del recurso**	**Tiempo (días)**		
1	05/05/23	Route53	1		
2	06/05/23	CloudFront	1		
3	07/05/23	Bucket S3	1		
4	08/05/23	Certificate Manager	1		
5	09/05/23	Instancia EC2 N° 1	1		
6	10/05/23	Instancia EC2 N° 2	2		
7	12/05/23	Base de datos - RDS	1		
8	13/05/23	CloudWatch	1		
9	14/05/23	Identity Access Management	2		

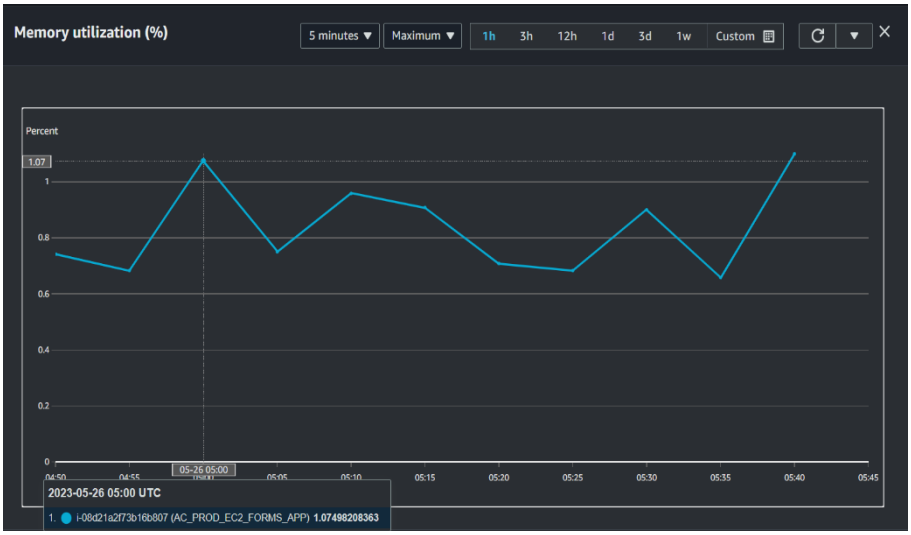
Finalmente, en el tercer instrumento se obtuvieron los siguientes resultados.

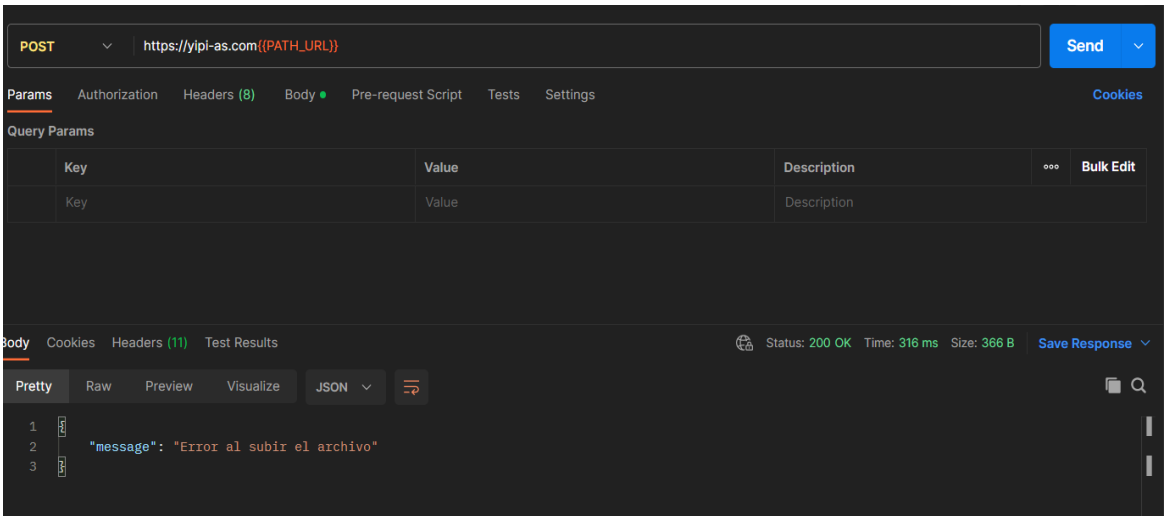
Ficha de observación				
Investigador	Carlos Gabriel Masias Ordinola		**Tipo de prueba**	Descriptiva
Empresa / Institución	Plataformas y Soluciones Digitales S.A.C.			
Dimensión de estudio	Rendimiento			
Objetivo específico	Evaluar el rendimiento y la disponibilidad de servicios en la nube utilizando métricas de recursos, tiempo de actividad y tiempos de respuesta			
Fecha de inicio	01/06/2023	**Fecha final**	05/07/2023	

Variable	**Indicador**	**Medida**
Infraestructura en la nube	Porcentaje de utilización del recurso virtualizado	Tasa porcentual
	Tiempo de actividad del servicio	Horas
	Tiempos de respuesta	Milisegundos

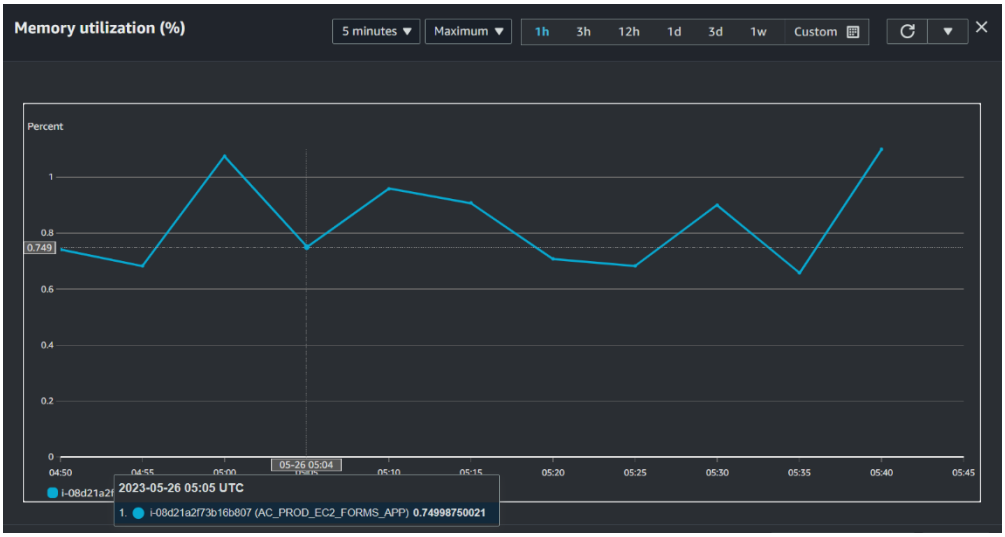
No de iteración	**Nombre del servicio**	**Porcentaje de utilización**	**Tiempo de actividad**	**Tiempos de respuesta**
1	EC2	1.07%	1	316
2	EC2	0.74%	1	301
3	EC2	0.74%	1	344
4	EC2	0.90%	1	301
5	RDS	5.52%	1	353
6	RDS	5.32%	1	310

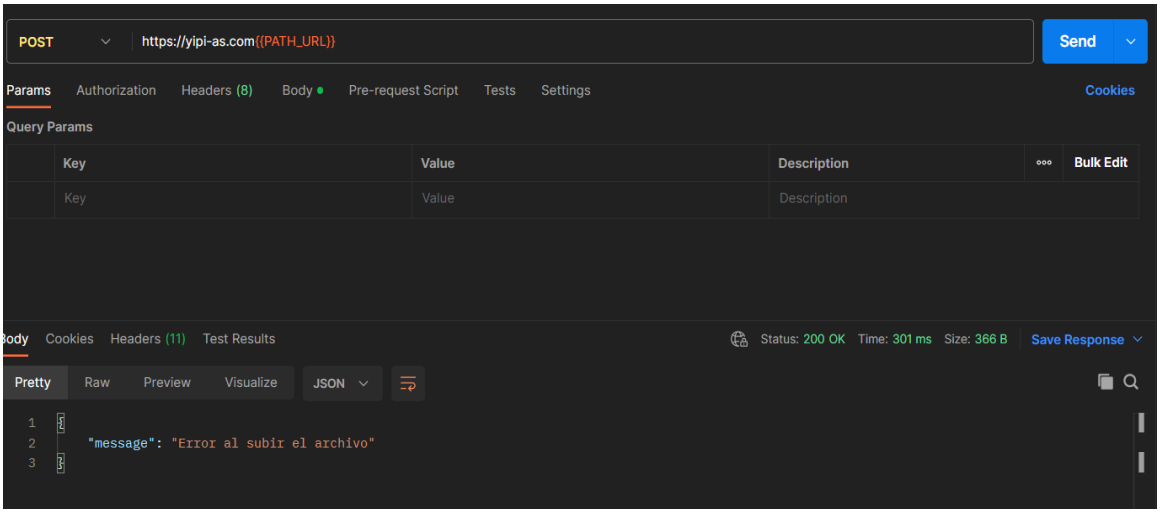
Se ejecutó cuatro veces una solicitud POST donde corre una aplicación en EC2. En la primera iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 316 milisegundos. La utilización de memoria fue de 1.07%. El tiempo de actividad fue de 1 hora.



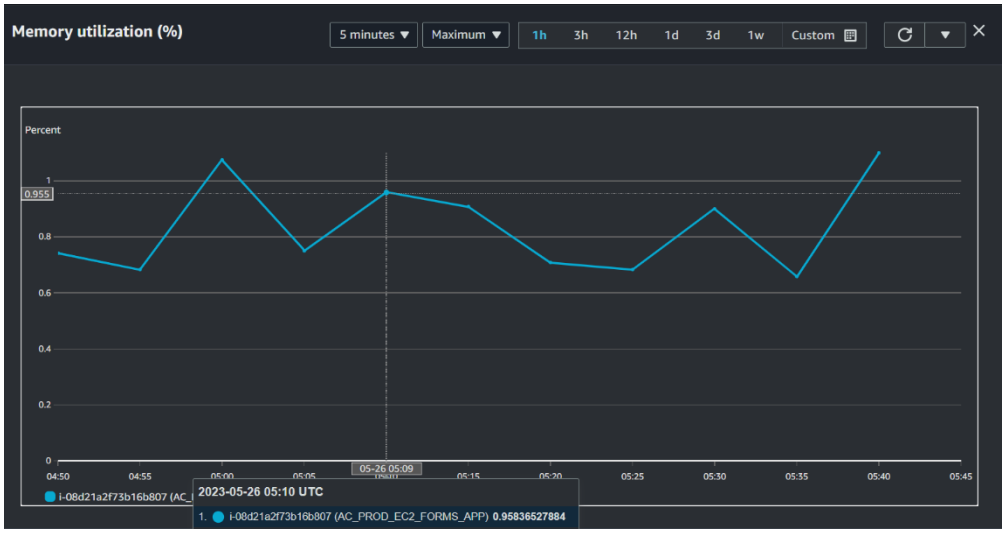


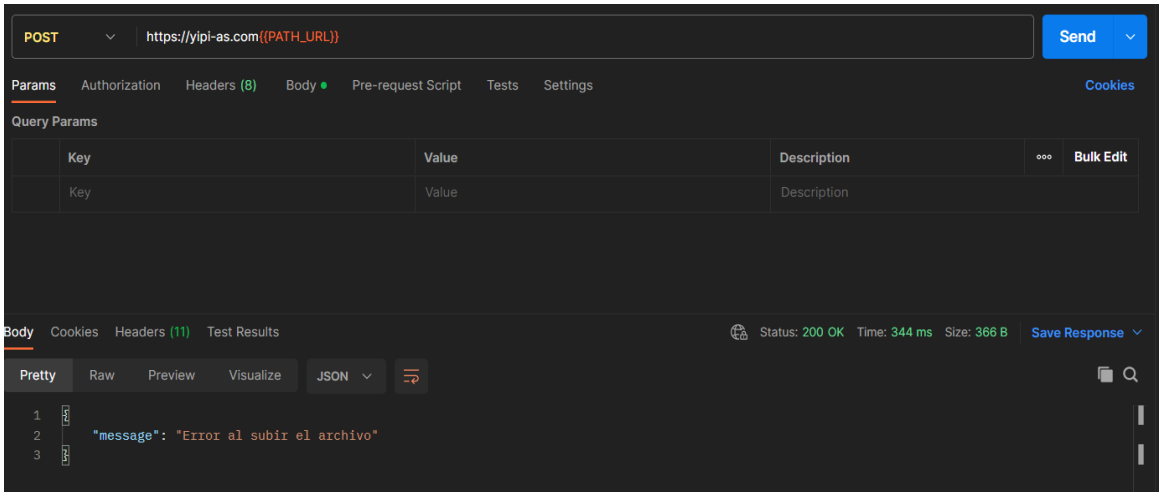
En la segunda iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 301 milisegundos. La utilización de memoria fue de 0.74%. El tiempo de actividad fue de 1 hora.



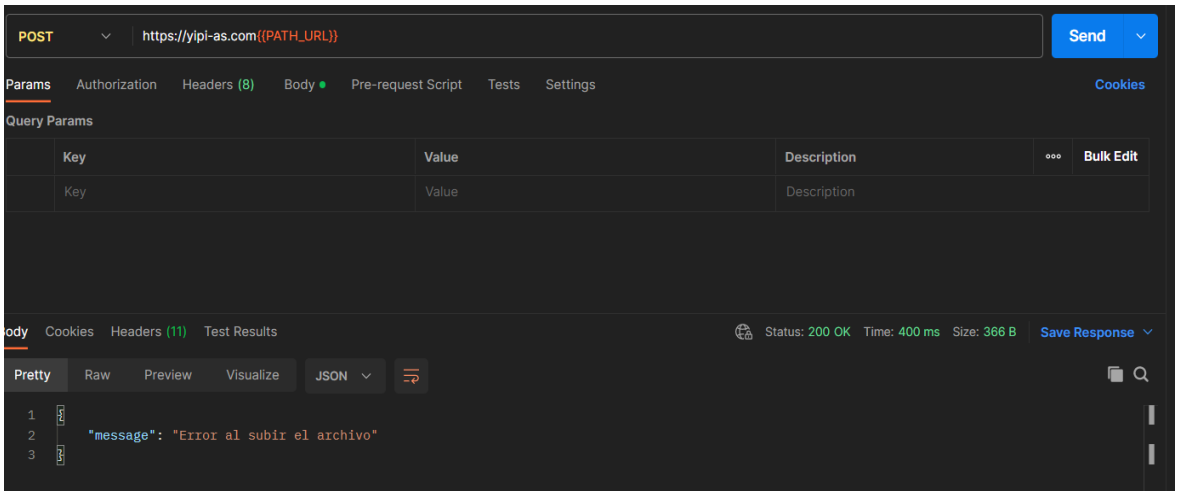


En la tercera iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 344 milisegundos. La utilización de memoria fue de 0.74%. El tiempo de actividad fue de 1 hora.

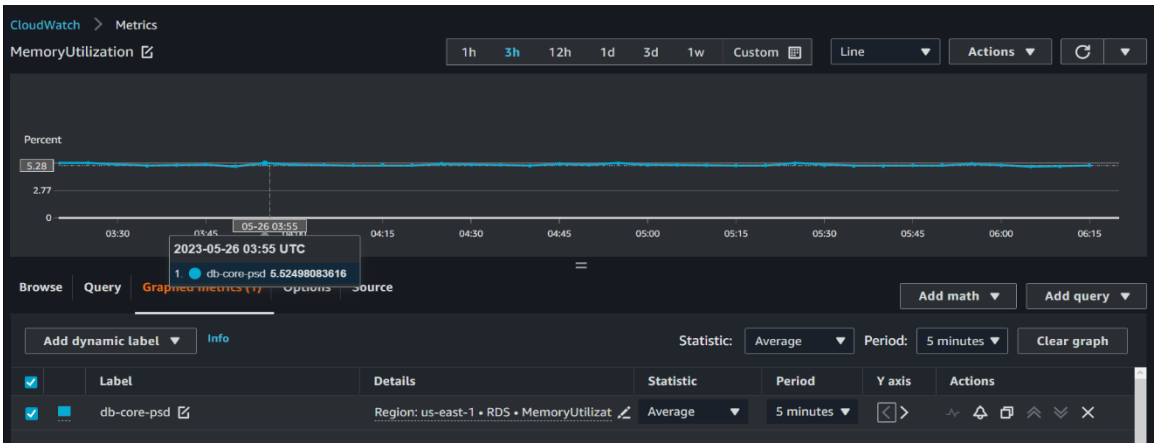




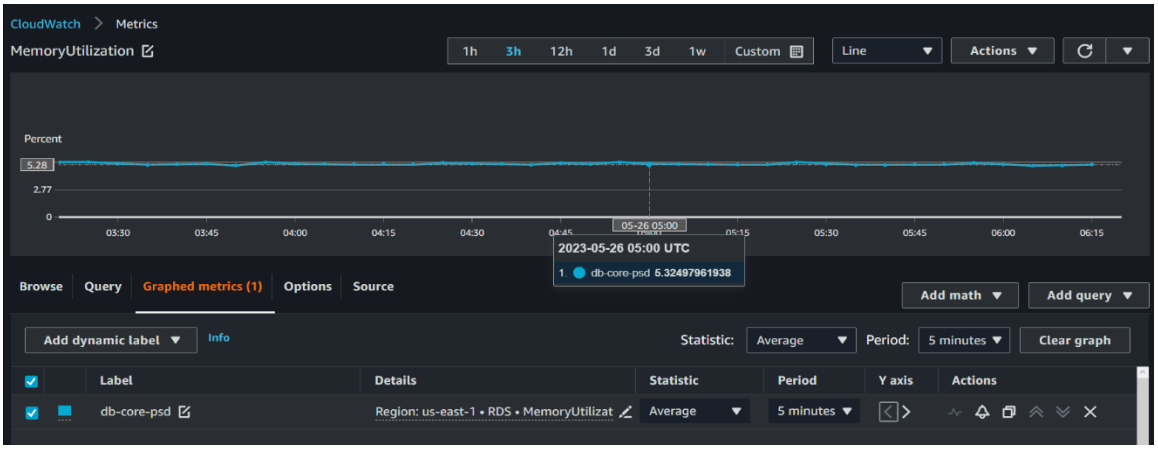
En la cuarta iteración, se obtuvo un Status Code de 200 y un tiempo de respuesta de 301 milisegundos. La utilización de memoria fue de 0.90%. El tiempo de actividad fue de 1 hora



En la quinta iteración, se obtuvo un valor de 5.52%, donde el tiempo de actividad fue de 1 hora.



En la sexta iteración, se obtuvo un valor de 5.32%, donde el tiempo de actividad fue de 1 hora.



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, TAVARA RAMOS ANTHONY PAUL, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Metodología basada en la implementación de una infraestructura en la nube", cuyo autor es MASIAS ORDINOLA CARLOS GABRIEL, constato que la investigación tiene un índice de similitud de 18.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 26 de Junio del 2023

Apellidos y Nombres del Asesor:	**Firma**
TAVARA RAMOS ANTHONY PAUL **DNI:** 40784283 **ORCID:** 0000-0002-4159-930X	Firmado electrónicamente por: ATAVARAR el 09-07-2023 18:06:57

Código documento Trilce: TRI - 0551693

INVESTIGA UCV