UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Caiza Rodriguez Erik Andrés
Tutor/a:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador2024

APROBACIÓN DEL TUTOR

Yo, Msc. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: **Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure.**

Elaborado por: Erik Andrés Caiza Rodriguez, de C.I: 0202026357, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, Ph.D. Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: **Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure.**

Elaborado por: Erik Andrés Caiza Rodriguez, de C.I: 0202026357, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Erik Andrés Caiza Rodriguez con C.I: 0202026357, autor/a del proyecto de titulación denominado: **Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure**. Previo a la obtención del título de Magister en Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024

_____

Firma

TABLA DE CONTENIDOS

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Los proveedores de servicios en la nube (CSP) como AWS, Google Cloud y Microsoft Azure, son los principales responsables de desarrollar defensas contra los fallos de seguridad, cuyos usuarios deben dar prioridad a las prácticas de uso seguras y a la configuración adecuada del servicio, aparte de escoger un proveedor consciente de la seguridad. Por lo tanto, los clientes deben asegurarse de que las redes y el hardware del usuario final estén adecuadamente protegidos (Patiño y Valencia, 2019).

En el ámbito administrativo, a raíz que se incrementan la cantidad de organizaciones que se trasladan de los sistemas locales a la nube, específicamente con la administración de datos, es fundamental reconsiderar las estrategias de seguridad, sobre todo en la normativa de cumplimiento y la gestión de datos. Además, los CSP suelen seguir un modelo de responsabilidad compartida, en la cual se define las tareas de seguridad pertenecientes al proveedor de servicios, siendo fundamental compilar una estrategia de protección de nube resiliente (Parra et al., 2023).

En ese sentido, se debe comprender que los proveedores de servicios son los responsables directos de la nube y de su infraestructura principal, mientras que los clientes o usuarios están en la obligación de proteger todo lo que se ejecute en la nube, como la administración de identidades, accesos, controles de redes, aplicaciones y datos.

Para Rivero y Guerra (2023) se ha convertido en una necesidad básica para todos los sectores que operan en el mundo digital. El sector educativo no ajeno a esta realidad, también se beneficia de esta transición, puesto que, al utilizar los CSP, los centros educativos pueden cumplir mejor sus requisitos de protección de datos y verificar la protección de la información del personal y los alumnos. Además, los CSP realizan inversiones relacionadas con la seguridad que dotan a su infraestructura en nube de un grado elemental de protección.

Por otra parte, la seguridad de la nube permite al sector educativo fomentar la productividad, debido a que se podrá almacenar y guardar a través de copias de seguridad todos los documentos para la formación de los estudiantes, cuyo acceso será exclusivo para personas autorizadas. Además, permite ejecutar labores administrativas optimizando tiempo y recursos, de esta forma se facilita la realización de tareas, el trabajo colaborativo, reducción de costes y el desempeño eficiente en todos los centros de educación (Alvarez, 2021).

En el ámbito tecnológico, la seguridad en la nube ha evolucionado de manera significativa, transformándose en un aspecto crítico para las organizaciones que dependen de soluciones digitales.

No obstante, a raíz que el ámbito tecnológico avanza, también lo hacen los desafíos y amenazas relacionados a los datos protegidos de la nube (Bazzara, 2021).

Actualmente, las empresas se enfrentan a diversos riesgos en constante cambio que requiere de estrategias efectivas y atención urgente, en donde las tecnologías más modernas permiten a las organizaciones avanzar en capacidades fuera de los límites de la infraestructura local, por ello, empresas modernas necesitan lograr un equilibrio adecuado para beneficiarse del uso de la tecnología de nube interconectadas, mientras las prácticas de seguridad en la nube se implementan de manera adecuada (Castañeda y Villegas, 2020).

Problema de investigación

Los problemas de seguridad en la nube han aumentado de forma drástica, cuyos ataques cibernéticos han expuesto los defectos que presenta la nube con respecto a los protocolos de seguridad. Según un estudio publicado por Cloud Native Security (2023) a nivel mundial, el 80% de las exposiciones de seguridad se producen en la nube, mientras que un 20% en los servidores locales, entre los sectores más afectados se encuentran el sector de transporte y logística, servicios financieros, alta tecnología, sanidad, ventas y educación.

Por otra parte, la Compañía Rusa Tecnológica Kaspersky Lab (2020) en un informe reveló que, 3 de 4 equipos que operan en los sistemas de la nube han sufrido diariamente más de diez eventualidades, debido a una configuración deficiente del sistema, además de vulneraciones de almacenamientos y políticas inadecuadas de acceso al sistema.

De acuerdo a un informe publicado por la compañía tecnológica Thales Group (2023) en Latinoamerica, la causa principal de filtraciones de datos es la negligencia humana, esto debido al desconocimiento de los usuarios frente a las posibles amenazas, además las redes abiertas y públicas se han consolidado cada vez más en la región, sin tomar en consideración protocolos eficientes de seguridad en la nube, lo cual permite el aumento del ataque cibernético.

En Ecuador, la protección de servicios en la nube ha crecido de manera significativa debido a la era digital, que ha sido impulsado por la escalabilidad y flexibilidad en el manejo de datos, no obstante, dicho avance viene acompañado de diversos desafíos en la seguridad de información, tales como; falta de capacitación y conciencia en amenazas cibernéticas, siendo indispensable una atención crítica para que las empresas ecuatorianas puedan enfrentar el reto de proteger sus datos sensibles, en un ambiente cada vez más sofisticado por parte de los peligros cibernéticos (Novoa, 2020).

Según Ortiz et al. (2024) los recursos basados en la nube se alimentan de infraestructuras de terceros situadas fuera de la red de la empresa, lo cual significa que las tecnologías típicas de

visibilidad de red no son apropiadas para entornos en la nube, lo que dificulta la supervisión de todos los recursos en la nube, incluido aquellos usuarios que pueden acceder a los mismos.

Para Zúñiga et al. (2021) actualmente, las principales amenazas de seguridad en la nube son las organizaciones empresariales de remoto acceso, puesto que carecen de controles y configuración convincente, además la formación final de los usuarios hacia la ingeniería social debe ser necesaria, debido a que puede existir hurto de credenciales a través de métodos engañosos, así mismo, los usuarios no poseen suficientemente las capacidades para que la seguridad personal sea configurada.

Si bien es cierto que el objetivo de los servicios basados en la nube es facilitar el intercambio de datos y el acceso a los mismos, una mala configuración de la seguridad en la nube es una de las principales causas de las violaciones de la seguridad de los datos en los sistemas en la nube, por ello, es posible que muchas empresas no sepan cómo proteger la infraestructura de la nube, lo cual puede crear errores de configuración, como el uso de contraseñas por defecto, el olvido de activar el cifrado de datos o la gestión inadecuada de los controles de permisos (Ríos et al., 2023).

Objetivo general

- Desarrollar un análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre los protocolos de seguridad en diferentes plataformas de nube como, AWS, Google Cloud y Azure.
- Determinar la situación actual sobre el tratamiento de seguridad que ofrecen las plataformas de nube (AWS, Google Cloud y Microsoft Azure).
- Comparar los protocolos de seguridad que ofrecen las plataformas de nube (AWS, Google Cloud y Microsoft Azure) a través de una revisión sistemática.
- Valorar a través del criterio de especialistas los protocolos de seguridad que ofrecen las plataformas de nube (AWS, Google Cloud y Microsoft Azure).

Justificación

El estudio se lo realiza porque, actualmente, las empresas se enfrentan a diversos riesgos en constante cambio que requiere de estrategias efectivas y atención urgente, en donde las tecnologías más modernas permiten a las organizaciones avanzar en capacidades fuera de los límites de la infraestructura local, por ello, se necesita lograr un equilibrio adecuado para beneficiarse del uso de la tecnología de nube interconectadas, mientras las prácticas de seguridad en la nube se implementan de manera adecuada.

Es necesario desarrollar el presente estudio, ya que los problemas de seguridad en la nube han aumentado de forma drástica, cuyos ataques cibernéticos han expuesto los defectos que presenta la nube con respecto a los protocolos de seguridad. Según un estudio publicado por Cloud Native Security (2023) a nivel mundial, el 80% de las exposiciones de seguridad se producen en la nube, mientras que un 20% en los servidores locales, entre los sectores más afectados se encuentran el sector de transporte y logística, servicios financieros, alta tecnología, sanidad, ventas y educación.

El estudio es importante, ya que la seguridad en la nube desempeña un papel vital para garantizar la confidencialidad, la integridad y la disponibilidad de los datos sensibles almacenados en la misma. Por ende, es uno de los aspectos que las empresas u organizaciones deben abordar si deciden realizar, aunque sea una mínima parte de sus actividades en la nube, o mantener sus datos dentro de ella, ya que, si no lo efectúan, se arriesgan no solo a perder datos o a interrumpir sus operaciones empresariales, sino también a sufrir daños financieros y de reputación.

Es factible, puesto que se dispone de toda la información bibliográfica necesaria para realizar al análisis comparativo de las plataformas; AWS, Google Académico y Google Cloud. Además, se cuenta con el apoyo y la apertura de los especialistas de sistemas cloud y seguridad informática de cloud para la participación en el presente estudio, con la finalidad de contribuir con su criterio en relación a los protocolos de seguridad que ofrecen dichas plataformas.

Con esto la colectividad se podrá beneficiar, ya que podrán disponer de un artículo en donde se establece las mejores plataformas de seguridad, para que los usuarios puedan analizar y hacer uso del mismo, ya que una seguridad adecuada en la nube permitirá proteger los datos, controles de red virtual, aplicaciones, acceso de usuarios y sistema operativo.

Por lo tanto, tendrá un impacto positivo dentro de la sociedad, debido a que podrán beneficiarse al conocer la mejor plataforma en la nube para proteger el procesamiento, almacenamiento y red física, incluido la configuración y parches, protegiendo a su vez el acceso a los usuarios, protección de datos y aplicaciones. Por consiguiente, los beneficiarios directos, serán todos los usuarios que se

dedican a utilizar las tecnologías de la información, en donde es fundamental disponer de una plataforma adecuada de seguridad informática.

Cabe mencionar que, los protocolos de seguridad son un conjunto de normas, políticas, procedimientos o reglas que tiene por finalidad evitar que los usuarios no autorizados obtengan datos confidenciales o puedan modificarlos o eliminarlos. Dicho de otra manera, estas reglas buscan garantizar la integridad, confidencialidad y disponibilidad de la información, por tanto, la aplicación de estos protocolos permite tener una conexión segura para compartir información confidencial a través de la red, en general, estos protocolos disponen de tres componentes que les permiten garantizar la ciberseguridad de un sistema informático, estos son; la autenticación de los usuarios, cifrado de datos y organización de los datos.

Alcance del estudio

El presente estudio tiene la finalidad de Desarrollar un análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure, ya que, los problemas de seguridad en la nube han aumentado de forma drástica, cuyos ataques cibernéticos han expuesto los defectos que presenta la nube con respecto a los protocolos de seguridad.

Para realizar el análisis comparativo fue necesario efectuar una revisión bibliográfica de artículos científicos que tengan relación con el tema de investigación, para conocer los principales hallazgos entorno a los protocolos de seguridad tanto de, AWS, Microsoft Azure y Google Cloud, además, se desarrolló una encuesta que fue dirigida a 25 especialistas de sistemas cloud y seguridad informática, cuyo propósito se enfocó en obtener su criterio sobre la seguridad que ofrecen dichas plataformas.

En ese sentido, el estudio se enfocó en desarrollar una revisión bibliográfica mediante buscadores científicos, como Scielo, Scopus, Google Academic y Science Direct, en la cual se incluyó un total de 10 artículos, que posteriormente se sometieron a un análisis para realizar la respectiva comparación, tomando en consideración diversos parámetros; lista de controles de seguridad, usabilidad de administración del sistema, transparencia, manejo de Backups, tipos de servicio de despliegue y transmisión de datos además, El alcance del estudio se limita a escoger 25 especialistas a través de una encuesta que estuvo estructurada de 13 preguntas, cuyo enfoque se basó en las características, ventajas, deficiencias, vulnerabilidad y fortalezas que poseen las plataformas AWS, Google Cloud y Microsoft Azure.

Cabe mencionar que, el estudio se limita exclusivamente hacia una referencia bibliográfica, además, para complementar los resultados de la investigación, se efectuó encuestas a especialistas en el área para fundamentar los hallazgos del estudio, por tanto, las futuras investigaciones se pueden centrar en realizar una propuesta, en base a los problemas encontrados, con la finalidad de dar una

solución y reforzar los protocolos de seguridad en la nube de las plataformas, AWS, Google Cloud y Microsoft Azure.

Vinculación con la sociedad y beneficiarios directos:

El presente estudio pretende comparar los protocolos de seguridad en diferentes plataformas de la nube (AWS, Google Cloud y Microsoft Azure), cuya vinculación con la colectividad se dará a través de la valoración del criterio de los profesionales, con la finalidad de obtener una perspectiva técnica con respecto a los protocolos de seguridad que ofrecen dichas plataformas.

Con esto la colectividad se podrá beneficiar, ya que podrán disponer de un artículo en donde se establece las mejores plataformas de seguridad, para que los usuarios puedan analizar y hacer uso del mismo, ya que una seguridad adecuada en la nube permitirá proteger los datos, controles de red virtual, aplicaciones, acceso de usuarios y sistema operativo.

Por lo tanto, tendrá un impacto positivo dentro de la sociedad, debido a que podrán beneficiarse al conocer la mejor plataforma en la nube para proteger el procesamiento, almacenamiento y red física, incluido la configuración y parches, protegiendo a su vez el acceso a los usuarios, protección de datos y aplicaciones. Por consiguiente, los beneficiarios directos, serán todos los usuarios que se dedican a utilizar las tecnologías de la información, en donde es fundamental disponer de una plataforma adecuada de seguridad informática.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1 Contextualización general del estado del arte

1.1.1 Seguridad en la Nube

Las normas, mejores prácticas, controles y tecnologías utilizadas en los entornos de nube para salvaguardar los datos, las aplicaciones y la infraestructura se denominan en conjunto seguridad en la nube, cuyo objetivo es ofrecer gestión del acceso, cumplimiento de la normativa y gestión de datos, almacenamiento y protección de la red frente a amenazas externas e internas (Ortíz et al., 2024).

La seguridad en la nube se centra principalmente en cómo integrar políticas, procedimientos y herramientas tecnológicas para garantizar la protección de datos, facilitar su desempeño y dar a los usuarios y dispositivos control sobre la privacidad, el acceso y la autenticación.

1.1.2 Función de la Seguridad en la Nube

Los proveedores de servicios en nube (CSP) suelen operar bajo un paradigma de responsabilidad compartida, lo que significa que la seguridad de la computación en nube es implementada tanto por el CSP como por el cliente. Este marco de responsabilidades establece qué tareas de seguridad pertenecen al proveedor de servicios en nube y cuáles al cliente. Por ello, saber dónde terminan las obligaciones de seguridad del proveedor y del cliente es crucial para crear un sólido plan de seguridad en la nube (Castillo, 2020).

1.1.3 Importancia de la seguridad en la Nube

La seguridad es mucho más compleja que simplemente mantener a la gente fuera de su red, lamentablemente, muchas empresas dan prioridad a la transformación digital sobre la seguridad, a menudo ignorando las mejores prácticas en el proceso. Como resultado, los atacantes están cambiando sus estrategias para aprovechar los puntos débiles, ya que ven los objetivos basados en la nube como un camino potencialmente sencillo para obtener importantes beneficios económicos (Lezcano et al., 2023).

1.1.4 Ventajas e Inconvenientes de la Seguridad en la Nube

Las defensas de tipo perimetral dejan de funcionar cuando se eliminan recursos de la red, por lo que hay que reconsiderar las mejores formas de fomentar la productividad de los usuarios, detectar problemas de seguridad, reducir vulnerabilidades, detener el malware y evitar la pérdida de datos (Orozco, 2021).

Por lo tanto, es importante la seguridad en la nube, puesto que contribuye una gran cantidad de ventajas, tales como; escalabilidad, incremento de la visibilidad y la seguridad, ahorra los costes,

permite una gestión centralizada y actualizaciones automáticas. Sin embargo, trae consigo algunos inconvenientes y riesgos potenciales, como riesgo de configuraciones erróneas, preocupaciones de cumplimiento, problemas de privacidad y soberanía de datos (Méndez, 2021).

1.1.5 Proveedores de Servicio en la Nube

AWS (Amazon Web Services), Google Cloud y Microsoft Azure, son los proveedores principales de servicio en la nube. A continuación, se describen cada uno de ellos:

AWS (Amazon Web Services). - Se trata de un proveedor de servicios en la nube que proporciona potencia de procesamiento, almacenamiento, bases de datos, aplicaciones móviles, recursos informáticos y un sinfín de otras funciones de movilidad de la computación en nube. Puede haber problemas de seguridad, aunque el procesamiento de datos en una infraestructura externa parezca una solución muy intrigante y asequible. Gracias a sus certificaciones y auditorías, que incluyen ISO 27001, auditoría SOC 2, HIPAA, FISMA Moderado, PCI DSS nivel 1 y FISMA, AWS es fiable. (Cerna et al., 2022).

Google Cloud. - La infraestructura y los servicios que utiliza Google de forma interna están ahora abiertos a cualquier organización, de modo que pueden utilizarse para una amplia gama de procesos empresariales, dicha plataforma se conoce como Google Cloud Platform. En comparación con otras soluciones, brinda todas las herramientas que se requieren para crear, probar y lanzar aplicaciones desde cloud con mucha mayor seguridad y escalabilidad (Llontop, 2020).

Microsoft Azure. - Puede crear, lanzar y gestionar fácilmente aplicaciones en una red global de centros de datos de Microsoft con esta nube pública de pago por uso. Si elige una plataforma IaaS (servicio como infraestructura), cuyos servicios de cifrado y encriptación están integrados con Microsoft Azure para los datos en tránsito y en reposo, su personal se encargará de actualizar los parches de seguridad y otros requisitos de software. Por el contrario, su proveedor mantendrá las actualizaciones de software por usted cuando utilice una PaaS (plataforma como servicio) (López, 2023).

1.1.6 Investigaciones Similares

El autor Quintero (2023) realizó un estudio en Colombia con la finalidad de evaluar la privacidad y seguridad de la nube en las plataformas de AWS, Microsoft Azure y Google Cloud, para lo cual aplicó un método descriptivo comparativo, a través de encuestas. De acuerdo a los resultados se evidenció que, la plataforma AWS posee una mayor privacidad y cumplimiento de políticas de seguridad, seguido de las plataformas Google Cloud y Microsoft Azure, el estudio concluye que dichos programas

podrían ser mejor en términos de seguridad si permitiera la configuración de un tenant único para evitar los riesgos por completo al momento de su compartición.

Por otra parte, Omaza (2020) efectuó un estudio en España con el propósito de obtener una visión global del estado de la seguridad de una empresa de compras online haciendo hincapié en el entorno tecnológico como es AWS, a través de un método descriptivo no experimental. Los hallazgos evidenciaron que, la información confidencial se almacena encriptada y cumple con su propio patrón de nomenclatura, facilitando el mantenimiento y gestión de los recursos de forma ágil, además de la protección de borrado en las bases de datos ante probables accidentes, lo cual permite garantizar la seguridad y disponibilidad de la información.

Los autores Chávez et al. (2023) desarrollaron un estudio con el objetivo de proporcionar una visión integral y actualizada de los servicios que ofrecen las plataformas Microsoft Azure y AWS, para lo cual aplicaron un método de revisión bibliográfica, incluyendo un total de 13 artículos relevantes. Los hallazgos evidenciaron que, dichas plataformas entorno a la seguridad, identidad y acceso facilita a los usuarios el acceso a los servicios ofreciendo protección y seguridad de los datos, lo cual permite administrar los roles y directivas de seguridad para trabajar con diversas cuentas, proporcionando a su vez servicios de dominio administrado como LDAP o autenticación Kerberos.

Por otro lado, Serrano (2021) efectuó una investigación en Colombia con el fin de analizar la plataforma AWS como mecanismo de recuperación ante incidentes tecnológicos en Pymes, cuya metodología se enfocó en dos fases, exploración teórica del servicio y análisis comparativo, a nivel de seguridad, costos y disponibilidad. Los resultados demostraron que, el servicio de seguridad que ofrece AWS es fundamental, puesto que la seguridad basada en la nube permite identificar problemas de forma temprana, monitoreando los datos de forma continua sin utilizar todos sus recursos restringidos. Además, solo se cancela por lo que utiliza mientras utiliza los servicios en la nube.

1.2 Proceso investigativo metodológico

El estudio posee un enfoque mixto cuali-cuantitativo:

Enfoque cualitativo. - Se utilizará el análisis cualitativo, en la cual se recolectarán datos de información mediante el análisis de contenido de revistas indexadas sobre los protocolos de seguridad de las plataformas AWS, Google Cloud y Microsoft Azure.

Enfoque cuantitativo. - Se utilizará un análisis cuantitativo, puesto que se aplicarán encuestas a los especialistas de sistemas cloud y seguridad informática, con la finalidad de valorar su criterio sobre los protocolos de seguridad que ofrecen dichas plataformas, por tanto, se cuantificará en términos numéricos la recolección de datos.

Método descriptivo. - Posee un nivel descriptivo, debido a que se realizará una encuesta que estará dirigida a profesionales de informática, efectuando un análisis e interpretación mediante gráficos estadísticos, permitiendo de esta manera valorar el criterio de dichos profesionales con respecto a los protocolos de seguridad que ofrecen las plataformas AWS, Google Cloud y Microsoft Azure.

Método transversal. - Durante el desarrollo de la investigación los datos serán recogidos en un momento dado y durante un periodo determinado, por tanto, el artículo se lo efectuará durante el mes de agosto hasta septiembre del 2024.

Investigación bibliográfica. - Será pertinente realizar una revisión bibliográfica a través de plataformas científicas como; Scielo, Scopus, Google académico entre otras, con el propósito de conocer los mejores protocolos de seguridad que ofrecen las plataformas AWS, Google Cloud y Microsoft Azure.

1.2.1 Diseño de la investigación

El estudio posee un diseño no experimental de corte transversal, puesto que no se manipula las variables en estudio, por consiguiente, se observará el fenómeno tal como ocurre en su entorno natural, para su posterior análisis, cuya recolección de datos se obtendrá en un lapso de tiempo determinado.

1.2.2 Población

El tamaño de la población consta de un total de 25 a especialistas de sistemas cloud y seguridad informática, por lo tanto, al ser un grupo pequeño, no fue necesario aplicar ningún tipo de muestra. En este sentido, se tomó en consideración a todo el tamaño de la población.

1.2.3 Técnicas e instrumentos

Para desarrollar los resultados será necesario realizar una revisión sistemática de diversos estudios científicos, en donde se pretende establecer los protocolos de seguridad que ofrecen las plataformas de nube (AWS, Google Cloud y Microsoft Azure), para posteriormente realizar un análisis de comparación para establecer cuál es la plataforma que brinda el mejor servicio de seguridad y privacidad. Además, se aplicará encuestas a especialistas de sistemas cloud y seguridad informática que constará de 13 preguntas con respuestas de tipo Likert; Siempre, casi siempre, a veces, pocas veces y nunca.

1.2.4 Procesamiento y análisis de datos

Los datos serán procesados y analizados mediante el programa estadístico SPSS Statistics de IBM en español, lo cual permitirá establecer los gráficos para su respectivo análisis e interpretación, del mismo modo, el análisis comparativo será procesado en el programa Excel versión 2016.

1.3 Análisis de resultados

Tabla 1

Tabla resumen de los artículos científicos

Autor y año	Objetivo	Método de estudio	Hallazgos principales	Conclusiones
Cárdenas y Olarte (2022).	Examinar la seguridad entre microservicios con Amazon Web Service.	Presenta un método no exploratorio de enfoque cualitativo.	Los resultados evidenciaron que, la plataforma AWS cumple con los estándares de seguridad, debido a los métodos de cifrado Y encriptado como KMS, además de la forma segura de encriptar y desencriptar la información.	Se concluye que AWS posee un nivel suficientemente alto de seguridad para poderlo denominar hermético.
Omaza (2020)	Conseguir una visión general del estado de seguridad de una empresa haciendo referencia a la plataforma AWS.	Presenta un método de revisión documental de enfoque cualitativo.	Según los resultados se evidenció que, la empresa no utiliza herramientas para el monitorear el tráfico y la actividad en la infraestructura de AWS.	En caso de un incidente de seguridad e infraestructura no existe registros necesarios para identificar la causa y tomar medidas necesarias de seguridad.
(Caballero, C. y Jara, M, 2021)	Identificar el proveedor (AWS, Google Cloud e IBM Cloud más adecuado a nivel de la infraestructura como servicio (IaaS).	Presenta un método de revisión documental de enfoque cualitativo.	Tanto AWS como Google Cloud ofrecen un mejor servicio de seguridad con respecto a IBM Cloud, esto debido a que ofrecen Firewalls adicionales y políticas de IAM.	Respecto a la seguridad en la nube las dos plataformas (AWS y Google Cloud presentan mejores mecanismos de seguridad y protección.

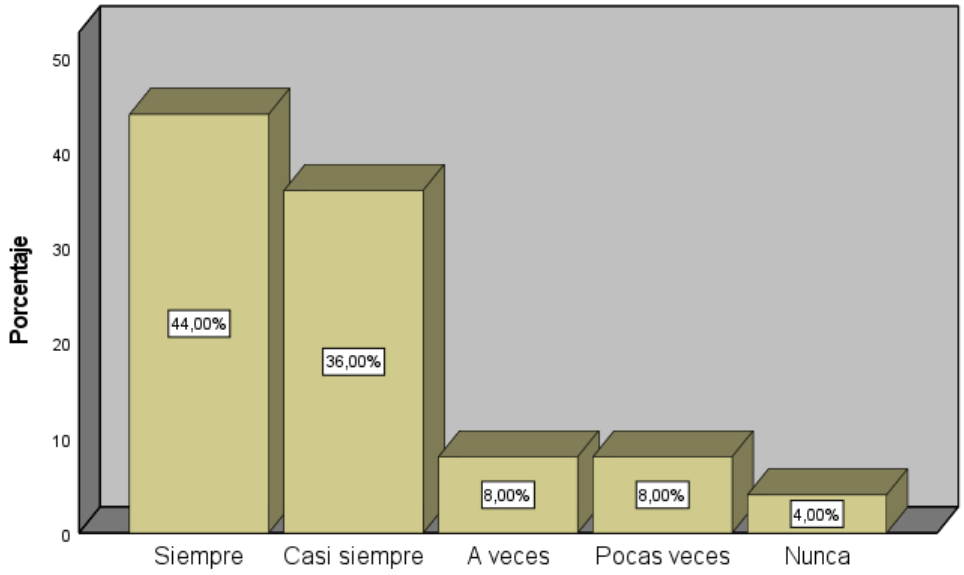
Landa y Lujan (2024)	Proporcionar una implementación que incluya una hoja de ruta detallada para la migración eficaz de un proyecto de aplicación on-premise basada en web a la nube de AWS.	Método descriptivo documental.	La integridad y confidencialidad de la información se garantizaron mediante la implantación de mecanismos de seguridad de infraestructuras y datos, incluidos el cifrado y la autenticación.	La migración de proyectos one premise a la nube AWS requirió de un enfoque minucioso a través de prácticas adecuadas de seguridad.
Almeida (2023)	Desarrollar un análisis comparativo de plataformas de virtualización en la nube para la dispersión de aplicaciones empresariales.	Método descriptivo comparativo.	La plataforma AWS ofrece una diversa gama de servicios empresariales debido a su flexibilidad y personalización, mientras que Azure posee una curva de aprendizaje más pronunciada para los usuarios	Es importante que las empresas se actualicen entorno a la infraestructura tecnológica, especialmente en sus protocolos de seguridad.
Gallego et al. (2023)	Estudiar la seguridad en la infraestructura de red implementada en la plataforma Microsoft Azure	Método descriptivo, no exploratorio de enfoque cuantitativo.	El análisis que efectúa esta herramienta se enfoca en características propias de la plataforma, sin embargo, implica mayores costos de operación para la infraestructura.	La implementación de la infraestructura en la nube de Microsoft Azure acarrea costos no planificados si no se efectúa una planificación segura y adecuada.
Guayas (2023)	Analizar cómo se utilizan plataformas AWS, Google Cloud y Azure Cloud.	El estudio posee un método descriptivo comparativo.	Las tres plataformas ofrecen diversos mecanismos de seguridad, sin embargo, la plataforma AWS ofrece más opciones para proteger los datos, que incluye firewalls, autenticación de usuarios, entre otros.	Las tres plataformas ofrecen una amplia gama de opciones de seguridad, sacando una ventaja la plataforma AWS, debido a sus diversas características de seguridad.

Quintero (2023)	Evaluar el nivel de seguridad que ofrecen las plataformas más populares de la nube (AWS, Google Cloud y Microsoft Azure).	El estudio presenta un método descriptivo con enfoque cuantitativo.	Los resultados mostraron que, la plataforma AWS ofrece una seguridad más alta, seguido de Microsoft Azure y Google Cloud, estas dos últimas presentan deficiencias tales como; falta de transparencia en políticas y multi-tenancy.	La plataforma AWS cumple con más características de seguridad tales como; controles de protección, transparencia, manejo seguro de copias de respaldo y usabilidad del sistema.
López (2023)	Implementar una serie de mecanismos para proteger y securizar la infraestructura y datos situados en Azure de una empresa genérica.	En el estudio se adopta una metodología Agile.	El uso de scripts en el lenguaje Powershell, usa una serie de módulos para gestionar los recursos de Azure completamente, permitiendo proteger la infraestructura a través de bloqueos de IPs en el cortafuegos.	Debido a los diversos servicios que se deben proteger y la constante actualización pueden presentarse limitaciones como claves SAS, dominios Kerberos de Active Directory.
Oliva (2019)	Describir los servicios que ofrece la plataforma Microsoft Azure entorno a la seguridad.	Método descriptivo documental.	La actualización y escaneo de datos en busca de amenazas que ofrece Azure de manera continua es una ventaja de seguridad que ofrece dicha plataforma, lo cual se vale de diversos protocolos de seguridad para que el intercambio de la información sea seguro.	Los acuerdos y contratos sobre la seguridad de Azure deben ser analizados completamente teniendo en consideración cualquier migración a la nube.

1.3.1 Encuestas aplicadas a especialistas de sistemas cloud y seguridad informática.

Figura 1

¿Considera usted que la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo?

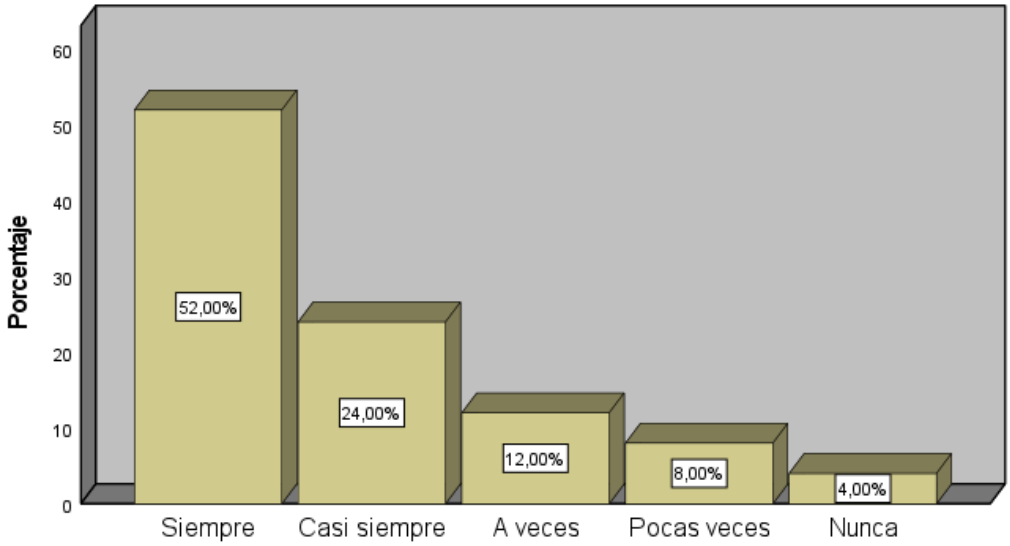


Análisis

Los resultados de la figura 1 muestran que, la mayoría de profesionales con el 44% consideran que la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo. Esto debido a que la plataforma cumple con una lista extensa de controles de seguridad, lo cual le permite manejar identidades, permisos, protección de infraestructura y redes, identificación y respuesta a amenazas demostrando el cumplimiento con logging, parches, auditoria, monitoreo, protección de datos y respuesta frente a incidentes.

Figura 2

¿Considera usted que la plataforma AWS posee más características de seguridad y privacidad a comparación de Google Cloud y Microsoft Azure?

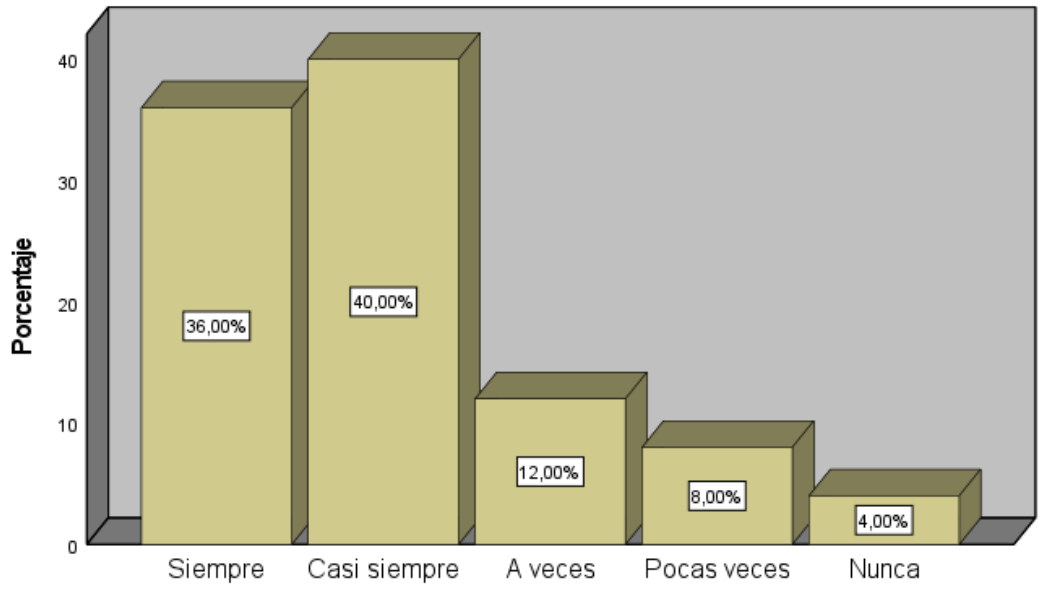


Análisis

La mayoría de encuestados con el 52% consideran que la plataforma AWS posee más características de seguridad y privacidad a diferencia de Google Cloud y Microsoft Azure. Esto debido a que el modelo de responsabilidad compartida permite a las empresas administrar los controles y políticas de seguridad de forma sencilla, además el servicio de administración de identidades y acceso (IAM) otorga permisos específicos evitando el riesgo y el ataque malicioso sobre datos confidenciales, así mismo dispone de una copia de datos confidenciales para su restauración en caso de un desastre.

Figura 3

¿Cree usted que la seguridad de AWS posee beneficios operativos y organizativos bien estructurados?

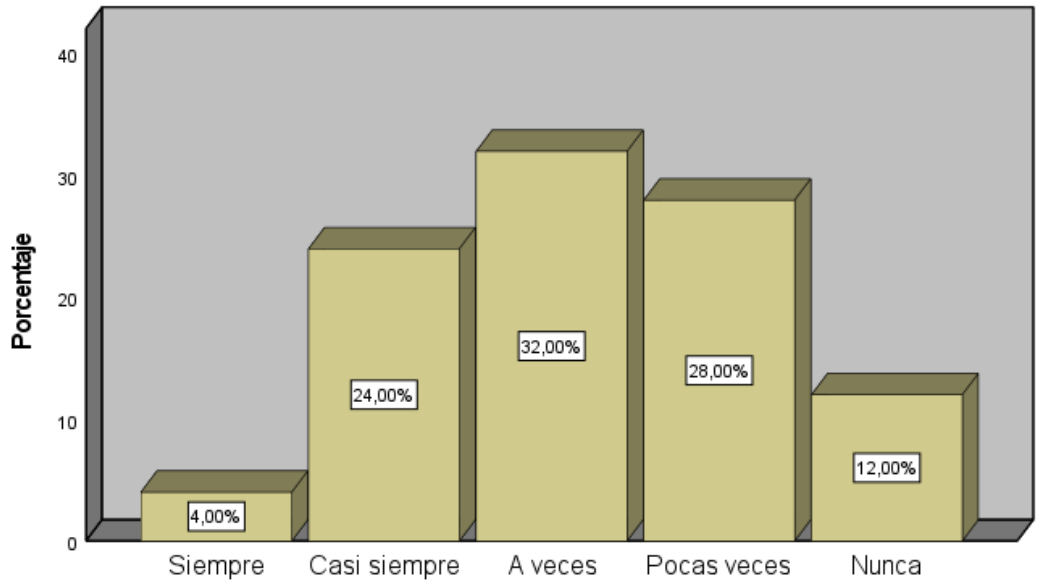


Análisis

La mayoría de encuestados con el 40% manifiestan que AWS posee beneficios operativos y organizativos bien estructurados, puesto que la plataforma se enfoca en proteger los datos, lo cual permite mejorar los procesos operativos, implementado una política de restricción de activos de información que permite a la organización garantizar la seguridad y protección de la misma.

Figura 4

¿Cree usted que la plataforma AWS presenta un grado mayor de desafío y riesgo de seguridad?

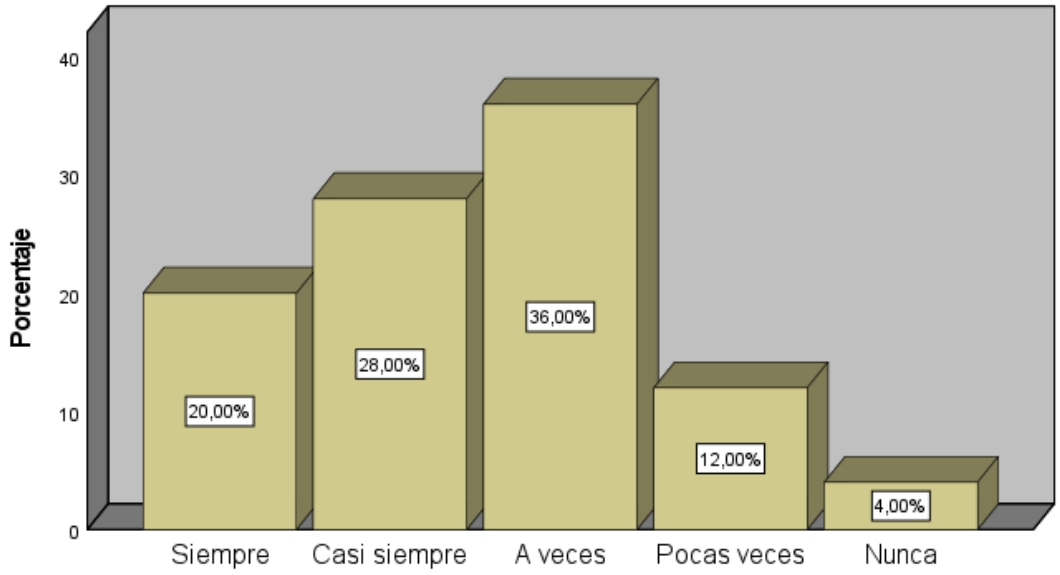


Análisis

Según la encuesta realizada a los profesionales, la mayoría con el 32% manifiestan que la plataforma no presenta un grado mayor de desafío y riesgo de seguridad, ya que ofrece servicios que ayudan a evitar el acceso no deseado a sus cuentas, datos y cargas de trabajo, por tanto, pa proteger los datos y cargas de trabajo, AWS Data Protection Services ofrece capacidades de cifrado, administración de claves y descubrimiento de datos confidenciales.

Figura 5

¿Considera usted que la responsabilidad de seguridad compartida que ofrece la plataforma Google Cloud es confiable y segura?

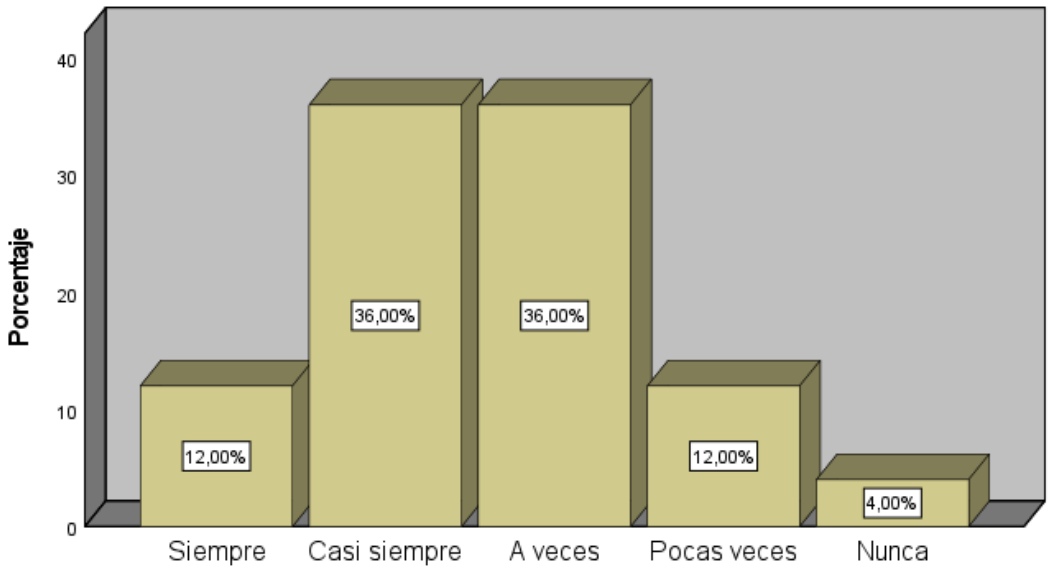


Análisis

La mayoría de encuestados con el 36% manifiestan que la responsabilidad compartida que ofrece plataforma Google Cloud no es segura y confiable, esto debido que los riesgos de seguridad asociados a la nube son comparables a los que se encuentran en los sistemas tradicionales, incluidos los ataques DDoS, phishing, malware, amenazas internas, pérdida de datos y brechas en la seguridad de los datos.

Figura 6

¿Considera usted que la plataforma Google Cloud posee más características de seguridad y privacidad a comparación de Microsoft Azure y AWS?

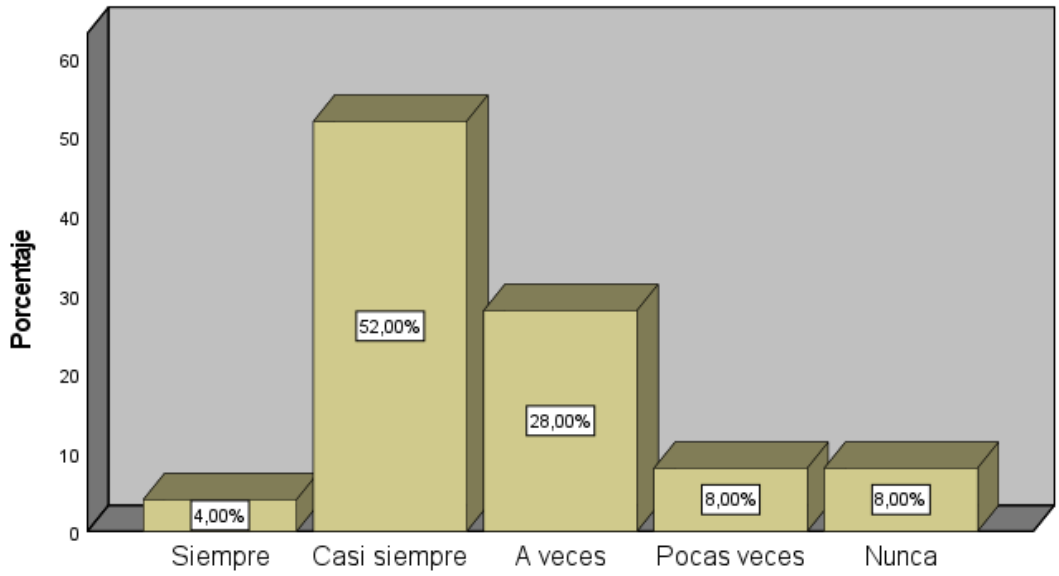


Análisis

La mayoría de encuestados con el 36% consideran que la plataforma Google Cloud posee menos características de seguridad a comparación de AWS y Microsoft Azure**,** ya que AWS posee el servicio de Identify and Access Management (IAM) mediante autenticación multi factor, asegurando el registro del usuario de forma verídica, mientras que Google Cloud no dispone de este servicio.

Figura 7

¿Cree usted que los sistemas de protección que dispone Google Cloud son suficientes para hacer frente a los Hacker e intrusos?

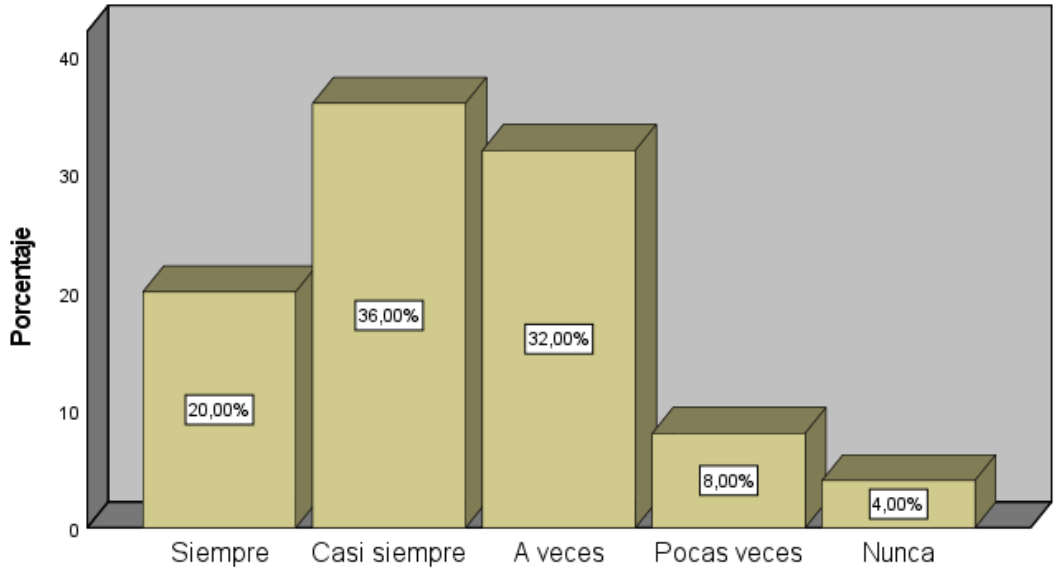


Análisis

La mayoría de encuestados con el 52% consideran que Google Cloud dispone de sistemas de protección suficientes para hacer frente a los hackers e intrusos, puesto que dispone de un hardware con diseño personalizado y un reforzado sistema operativo, además, los datos en tránsito de la plataforma y la empresa son cifrados en el servicio de Cloud Plataform, así mismo, la longitud de las claves de cifrado RSA se duplicó a 2048 bits, remplazando de forma continua dichas claves, con la finalidad de subir el listón del sector con respecto a la seguridad.

Figura 8

¿Considera usted que la plataforma Google Cloud cumple con los estándares de seguridad de primer nivel en todo el mundo?

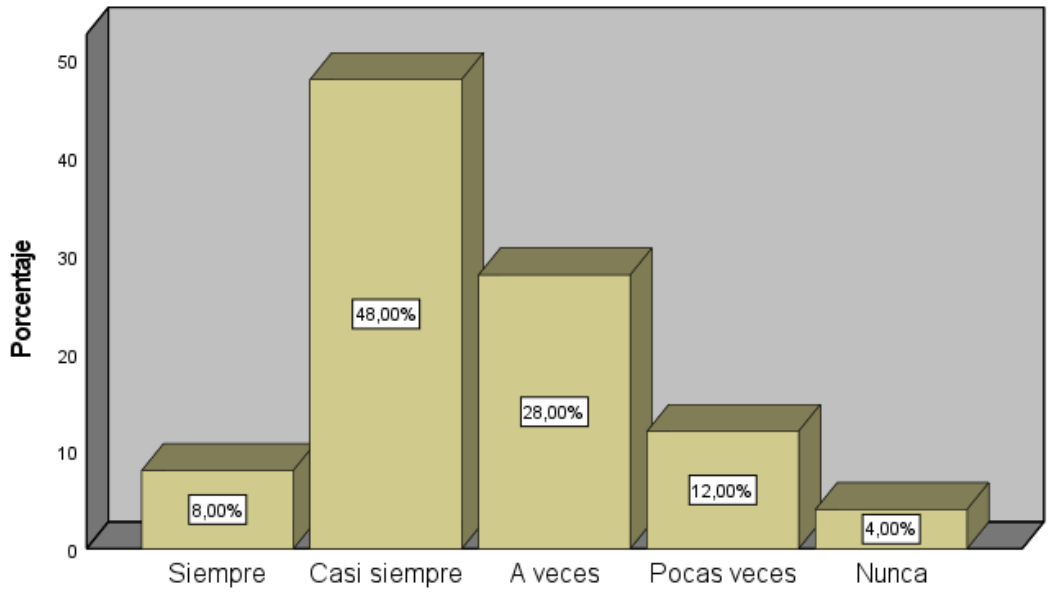


Análisis

La mayoría de encuestados con el 36% consideran que Google Cloud cumple con los estándares de seguridad de primer nivel en todo el mundo, ya que dicha plataforma también cumple con los estándares ISO 27001, lo cual permite evaluar de forma continua los nuevos riesgos. Además, la plataforma cumple con los estándares de seguridad HIPAA, permitiendo una gestión efectiva, acceso restringido, auditoria de información de salud protegida y cifrado.

Figura 9

¿Cree usted que la plataforma Google Cloud presenta un grado mayor de desafío y riesgo de seguridad?

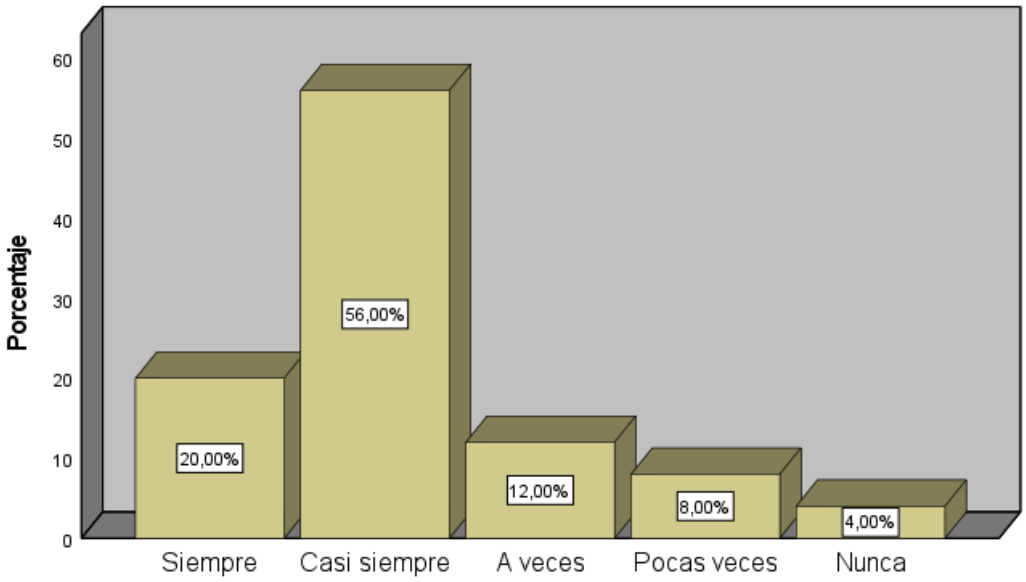


Análisis

Gran parte de los encuestados con un 48%, manifestaron que dicha plataforma presenta un mayor grado de desafíos y riesgos de seguridad, debido a que presenta inconvenientes como el riesgo de depender de los proveedores, la infraestructura subyacente presenta un control menos, además la integración con los sistemas actuales puede ser complejo.

Figura 10

¿Cree usted que la descripción general de la seguridad de Microsoft Azure se encuentra bien estructurada?

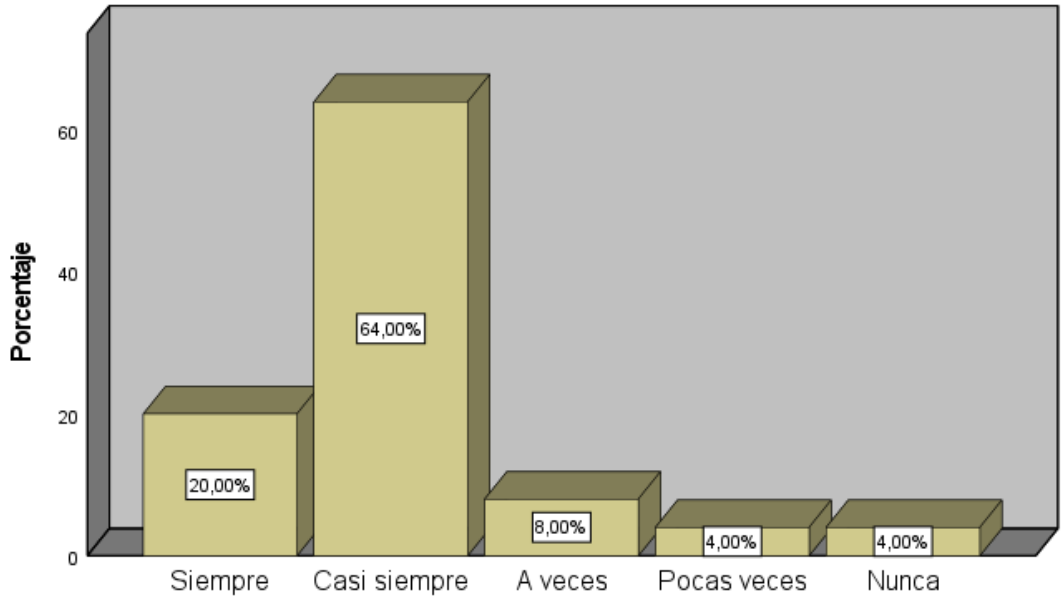


Análisis

Según el criterio de los profesionales, en su mayoría con el 56% consideran que Microsoft Azure se encuentra bien estructurado, ya que es la única empresa de computación en nube que ofrece infraestructura como servicio y una plataforma de aplicaciones segura y uniforme que permite a los equipos operar en la nube con distintos niveles de destreza y complejidad de proyecto. También ofrece servicios integrados de datos y análisis que permiten a los equipos encontrar inteligencia de datos en cualquier lugar.

Figura 11

¿Cree usted que la gestión de la postura de seguridad en la nube de Microsoft Azure es completa y eficiente?

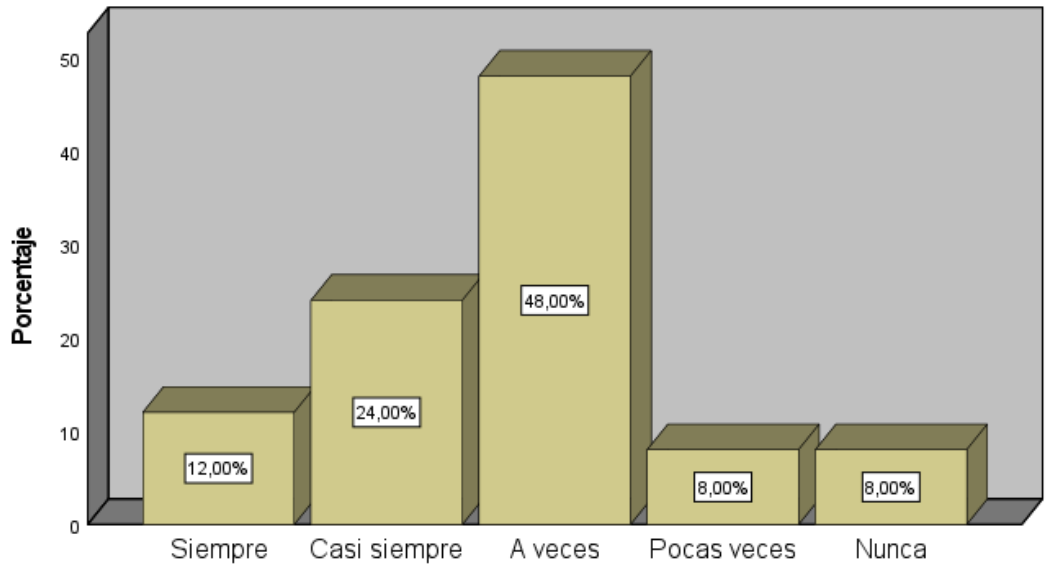


Análisis

En su mayoría, el 64% de encuestados manifiestan que la gestión de la postura de seguridad en la nube de Microsoft Azure es completa y eficiente, puesto que compara el entorno con una serie de medidas de seguridad prediseñadas, en donde la opción denominada puntuación segura del Centro de Seguridad, ayuda a cuantificar la postura de seguridad de su configuración, además, para aumentar su puntuación, el Centro de Seguridad ofrece recomendaciones prescriptivas si alguno de estos controles no se está utilizando o si hay alguna configuración errónea.

Figura 12

¿Considera usted que la plataforma Microsoft Azure posee más características de seguridad y privacidad a comparación de Google Cloud y AWS?

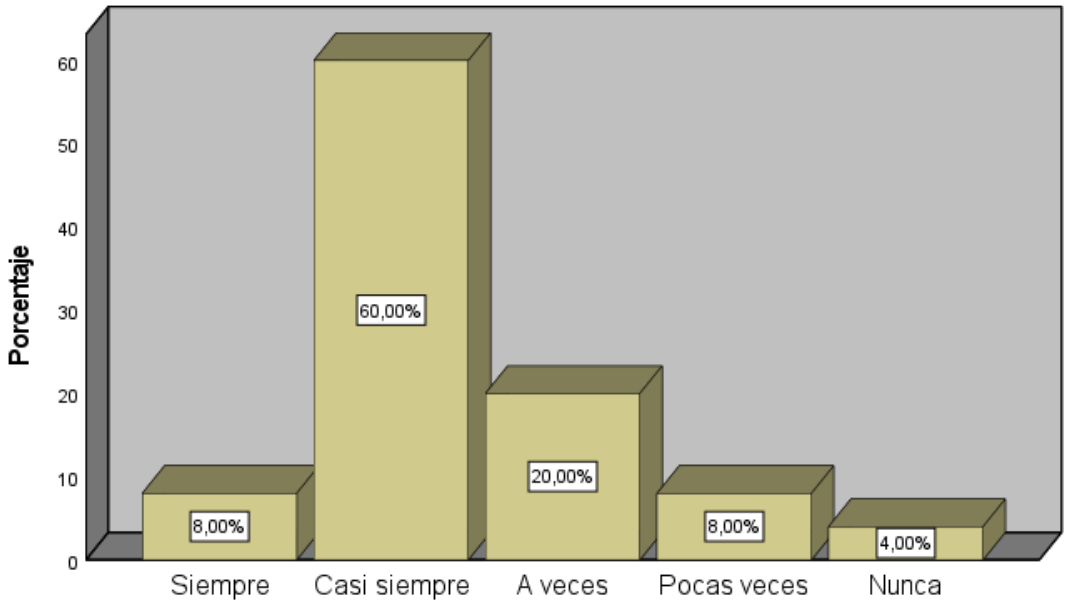


Análisis

La mayoría de encuestados con el 48% consideran que Azure posee menos características de seguridad y privacidad en comparación de Cloud y AWS, especificamente en los tipos de servicios de despliegue, debido a que la plataforma posee un aislamiento lógico, lo cual es compartido con diversos usuarios el mismo dispositivo, lo que supone un riesgo la política de responsabilidad compartida, con los usuarios que comparten espacio físico, generando brechas de seguridad.

Figura 13

¿Cree usted que la plataforma Microsoft Azure presenta un grado mayor de desafío y riesgo de seguridad?



Análisis

De acuerdo a los encuestado, la mayoría con el 60% consideran que Azure presenta un grado mayor de desafío. Sin embargo, Azure y AWS poseen un sistema más fiable y robusto, cuyas empresas ofrecen plataformas seguras, flexibles y resistentes a las amenazas, por ende, ninguna de las dos opciones es deficiente, por el contrario, ambas proporcionan conocimientos sobresalientes en este campo.

1.3.2 Discusión

De acuerdo a los resultados de la investigación, la plataforma AWS posee el modelo de responsabilidad compartida, lo cual permite tanto a la plataforma y a las empresas administrar los controles y las políticas de seguridad, siendo casi nulo el riesgo de perder datos sensibles, además, el servicio de administración de identidades y accesos (IAM) permite conceder permisos específicos en función de las responsabilidades. Dichos resultados se asimilan a los obtenidos por Cerna et al. (2022) en donde manifiesta que, las características de seguridad que posee AWS reduce el riesgo interno de intrusiones y ataques malintencionados a datos sensibles, garantizando un acceso único a los recursos que necesiten los miembros del equipo.

Las plataformas AWS, Microsoft Azure y Google Cloud cumplen con los requisitos necesarios para mantener la privacidad y seguridad de la plataforma. Así lo demuestra Quintero (2022) en su estudio

investigativo, cuyos resultados evidenciaron que, las tres plataformas en mención poseen una lista de controles de seguridad que cumplen con las exigencias necesarias para mantener la seguridad y privacidad en la nube.

Por otra parte, los resultados de la investigación evidenciaron que, la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo. Dichos resultados se asemejan a los obtenidos por Cárdenas y Olarte (2022) en donde el 75% de profesionales manifestaron que dicha plataforma cumple con una lista extensa de controles de seguridad, lo cual permite manejar identidades, permisos, protección de infraestructura y redes, identificación y respuesta a amenazas.

Así mismo, los hallazgos de la investigación demostraron que, la plataforma AWS posee más características de seguridad a diferencia de Google Cloud y Microsoft Azure. Estos resultados tienen relación con el estudio de Zúñiga et al. (2021) en donde evidenciaron que, el 66% de encuestados consideraban que dicha plataforma presenta características mayores de privacidad y seguridad, lo cual permite la implementación de un sistema robusto, de forma sencilla debido a la usabilidad en la administración del sistema con fácil documentación y gratuitos tutoriales.

Con respecto a Google Cloud, los hallazgos de la investigación evidenciaron que, dicha plataforma posee menos características de seguridad en comparación de AWS y Microsoft Azure. Estos resultados, se relacionan con los hallazgos de Rivero y Guerra (2023) en donde el 60% de encuestados manifestaron que la plataforma Google Cloud carece de un servicio de Identify and Access Management (IAM) mediante autenticación multi factor, lo cual no permite asegurar el registro del usuario de forma verídica.

En ese mismo contexto, los resultados de la investigación demostraron que, Google Cloud dispone de sistemas de protección suficientes para hacer frente a los hacker e intrusos. Tal como lo demuestra un estudio investigativo realizado por Coronel y Quirumbay (2022), cuyos resultados demostraron que, Google Cloud dispone de un hardware con diseño personalizado y un reforzado sistema operativo, además, los datos en tránsito de la plataforma y la empresa son cifrados en el servicio de Cloud Plataform, permitiendo de esta manera una plataforma segura frente a los hackers.

Según los resultados de la encuesta, Microsoft Azure se encuentra bien estructurada. Estos resultados se asimilan a los hallazgos de Cordero et al. (2020) en donde el 75% expresaron que dicha plataforma es la única empresa de computación en nube que ofrece infraestructura como servicio y una plataforma de aplicaciones segura y uniforme que permite a los equipos operar en la nube con distintos niveles de destreza y complejidad de proyecto.

Los resultados de la investigación, también evidenciaron que Azure posee menos características de seguridad y privacidad en comparación de Cloud y AWS. Así lo demuestra un estudio elaborado por

Gallego et al. (2023) en donde el 79% de encuestados manifestaron que, dicha plataforma posee menos características de seguridad, especificamente en los tipos de servicios de despliegue, debido a que la plataforma posee un aislamiento lógico, lo cual es compartido con diversos usuarios el mismo dispositivo, lo que supone un riesgo la política de responsabilidad compartida, con los usuarios que comparten espacio físico, generando brechas de seguridad.

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1 Resumen

El presente artículo se los realizó con la finalidad de desarrollar un análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure. Esto debido a que los problemas de seguridad en la nube han aumentado de forma drástica, cuyos ataques cibernéticos han expuesto los defectos que presenta la nube con respecto a los protocolos de seguridad. Para ello, se aplicó un método descriptivo, transversal y bibliográfico con un enfoque mixto cuali-cuantitativo a través de un diseño de investigación no experimental de corte transversal, siendo la revisión bibliográfica y las encuestas las principales técnicas de investigación. Los resultados de la investigación permitieron contextualizar los fundamentos teóricos, determinando la situación actual, además de comparar los protocolos de seguridad y valorar a través de criterios de especialistas, concluyendo que, las tres plataformas ofrecen altos niveles de seguridad, no obstante, AWS se posesiona como líder de la industria en términos de seguridad, seguido de Google Cloud y Microsoft Azure respectivamente.

Palabras clave: Protocolos de seguridad, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Políticas de privacidad, seguridad en la nube.

2.2 Abstract

The purpose of this article is to develop a comparative analysis of security protocols in different cloud platforms, such as AWS, Google Cloud and Microsoft Azure. This is due to the fact that security problems in the cloud have increased dramatically, whose cyber attacks have exposed the defects that the cloud presents with respect to security protocols. For this purpose, a descriptive, cross-sectional and bibliographic method was applied with a mixed quali-quantitative approach through a non-experimental cross-sectional research design, being the literature review and surveys the main research techniques. The results of the research allowed contextualizing the theoretical foundations, determining the current situation, in addition to comparing security protocols and assessing through the criteria of specialists, concluding that the three platforms offer high levels of security, however, AWS is positioned as the industry leader in terms of security, followed by Google Cloud and Microsoft Azure respectively.

Keywords: Security protocols, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, privacy policies, cloud security.

2.3 Introducción

Los problemas de seguridad en la nube han aumentado de forma drástica, cuyos ataques cibernéticos han expuesto los defectos que presenta la nube con respecto a los protocolos de seguridad. Según un estudio publicado por Cloud Native Security (2023) a nivel mundial, el 80% de las exposiciones de seguridad se producen en la nube, mientras que un 20% en los servidores locales, entre los sectores más afectados se encuentran el sector de transporte y logística, servicios financieros, alta tecnología, sanidad, ventas y educación.

Por otra parte, la Compañía Rusa Tecnológica Kaspersky Lab (2020) en un informe reveló que, 3 de 4 equipos que operan en los sistemas de la nube han sufrido diariamente más de diez eventualidades, debido a una configuración deficiente del sistema, además de vulneraciones de almacenamientos y políticas inadecuadas de acceso al sistema.

De acuerdo a un informe publicado por la compañía tecnológica Thales Group (2023) en Latinoamerica, la causa principal de filtraciones de datos es la negligencia humana, esto debido al desconocimiento de los usuarios frente a las posibles amenazas, además las redes abiertas y públicas se han consolidado cada vez más en la región, sin tomar en consideración protocolos eficientes de seguridad en la nube, lo cual permite el aumento del ataque cibernético.

En Ecuador, la protección de servicios en la nube ha crecido de manera significativa debido a la era digital, que ha sido impulsado por la escalabilidad y flexibilidad en el manejo de datos, no obstante, dicho avance viene acompañado de diversos desafíos en la seguridad de información, tales como; falta de capacitación y conciencia en amenazas cibernéticas, siendo indispensable una atención crítica para que las empresas ecuatorianas puedan enfrentar el reto de proteger sus datos sensibles, en un ambiente cada vez más sofisticado por parte de los peligros cibernéticos (Novoa, 2020).

Según Ortiz et al. (2024) los recursos basados en la nube se alimentan de infraestructuras de terceros situadas fuera de la red de la empresa, lo cual significa que las tecnologías típicas de visibilidad de red no son apropiadas para entornos en la nube, lo que dificulta la supervisión de todos los recursos en la nube, incluido aquellos usuarios que pueden acceder a los mismos.

Para Zúñiga et al. (2021) actualmente, las principales amenazas de seguridad en la nube son las organizaciones empresariales de remoto acceso, puesto que carecen de controles y configuración convincente, además la formación final de los usuarios hacia la ingeniería social debe ser necesaria, debido a que puede existir hurto de credenciales a través de métodos engañosos, así mismo, los usuarios no poseen suficientemente las capacidades para que la seguridad personal sea configurada.

En este sentido, el objetivo general de la investigación es Desarrollar un análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure. Para ello, se contextualizará los fundamentos teóricos, además de determinar la situación actual, para luego comparar los protocolos de seguridad que ofrecen dichas plataformas.

2.4 Metodología

2.4.1 Métodos de investigación

La metodología constó de varias fases; las cuales se detallan a continuación;

Primera fase. - En esta parte se realizó una revisión bibliográfica mediante artículos científicos que tengan relación con el tema de investigación, con la finalidad de conocer las características, mecanismos de seguridad y las falencias que poseen las plataformas de AWS, Google Cloud y Microsoft Azure, posteriormente, se elaboró una tabla resumen que constó de el autor y año, el objetivo, la metodología, los principales resultados y las conclusiones de cada artículo, siendo analizados un total de 10 artículos, que cumplieron con los criterios de inclusión.

Segunda fase. - En esta parte se realizó un análisis comparativo en base a los artículos analizados, cuyo análisis comparativo se realizó en base a los siguientes parámetros; Lista de controles de seguridad, usabilidad en la administración del sistema, transparencia, manejo de Backups, tipo de servicio de despliegue y transmisión de datos dependiente de la regulación. Cada uno de estos parámetros presentaron similitudes y diferencias en torno a la seguridad en la nube, tanto de AWS, Google Cloud y Microsoft Azure.

Tercera fase. – En esta fase se valoró el criterio de los especialistas de sistemas cloud y seguridad informática, para ello se utilizó 13 encuestas como instrumento principal, cuyas respuestas estuvieron estructuradas mediante la escala de Likert. Esto con la finalidad de contribuir al tema de investigación y fundamentar los protocolos de seguridad que poseen las plataformas AWS, Google Cloud y Microsoft Azure.

2.5 Resultados

2.5.1 Análisis Comparativo de las Plataformas AWS, Google Cloud y Microsoft Azure.

De acuerdo a los artículos analizados, se puede evidenciar que las plataformas en mención, poseen diversas características y mecanismos propios de seguridad que los diferencian entre sí. A continuación, se describe las características de cada plataforma tomando en consideración diversos parámetros.

Tabla 2

Análisis comparativo de las plataformas AWS, Google Cloud y Microsoft Azure.

	Aspectos a comparar						
Plataformas	Lista de controles de seguridad	Usabilidad en la administración del sistema	Transparencia	Manejo de Backups	Tipo de servicio de despliegue	Transmisión de datos dependiente de la regulación	Costos
AWS	De manera sencilla Amazon divide en cuatro categorías los servicios de seguridad; Identity and Access Management, detección, protección de redes y aplicaciones, protección de datos, respuesta frente a incidentes e inconformidad	Posee interfaces de fácil configuración para sus elementos básicos con tutoriales de despliegue en la misma página, también posee múltiples servicios de monitoreo para reforzar la seguridad.	En su página de legalidad proporciona toda la información necesaria y de fácil acceso en donde especifica el cumplimiento de los recursos.	Dispone de una solución efectiva de alta robustez, permitiendo la replicación cross región de manera automática de fácil monitoreo y Logs.	Ofrece tres tipos de despliegue; despliegue compartido, instancia dedicada que indica que corre en hardware de tenant único y host dedicado para el cliente.	Dispone de varias políticas de cumplimiento, según las normativas específicas de cada región, en donde no permite la creación de instancias en regiones donde no se disponga del permiso correspondiente	Generalmente AWS utiliza su plataforma Security Hub con respecto a la seguridad. Los costos varían según el tamaño de la organización: **Empresa pequeña:** 250 controles de seguridad x 1 cuenta= 0.25 ctv /mes. **Empresa grande:** 500 controles de seguridad x20 cuentas= 37.50 $/mes. **Empresa muy grande:** 1000 controles de seguridad x200 cuentas= 1.683 $/mes.
Google Cloud	Posee una cantidad enorme de servicios a cada uno de los clientes, los cuales incluyen	La configuración de interfaces los realiza mediante tutoriales de	También provee documentos de legalidad, sin embargo, son tediosos y amplios de leer,	Posee varias formas de generar replicación para recuperar información en caso de desastres, en	Dispone de de 2 o 3 tipos de tenancy de usuario único.	Posee diversas políticas de cumplimiento según las normas específicas de	La plataforma principal que utiliza Cloud entorno a la seguridad es Security Command Center, cuyo costo se basa en tres niveles, siendo el nivel

	analíticas y operaciones de seguridad, transformación acelerada, agilidad empresarial y maximización de cobertura en casos prácticos.	Microsoft Guard, además, la seguridad es reforzada con servicios múltiples de monitoreo.	lo cual ocasiona ciertas dificultades para entender los protocolos de seguridad.	donde todas sus plataformas cuentan con encriptación que se lo efectúa desde el formulario de la creación.		cada región, además cuando ocurre una infracción google deshabilita el recurso.	estándar sin costo alguno, mientras que el nivel Premium posee un precio promedio de 765$/mes mientras que el nivel Enterprise posee un promedio de 1.250 /mes.
Microsoft Azure	Construye y opera data centers en los que se controla de manera estricta los centros de datos con una protección multicapa, además adhiere a los controles de seguridad datos sensibles con autenticación multifactor para efectuar operaciones sensibles.	Las interfaces son configuradas mediante encriptación sencilla, así mismo, posee múltiples servicios de monitoreo para mayor protección.	Desde el primer momento entrega un documento completo de los términos, condiciones, auditorias, certificados, leyes y lineamientos indispensables para trabajar en la nube.	Posee varias formas de generar replicación para recuperar información en caso de desastres, en donde todas sus plataformas cuentan con encriptación que se lo efectúa por medio de diversos tipos de replicación cross región que garantiza la disponibilidad de datos.	Posee un aislamiento lógico, cuyo dispositivo es compartido con diversos usuarios, lo que supone un riesgo con la política de responsabilidad compartida.	Ofrece una variedad de políticas de cumplimiento según las normas específicas de cada región, en donde no permite la recopilación de datos entre regiones con regulaciones diversas.	Microsoft Azure ofrece planes de protección de forma segmentada, a diferencia de AWS que ofrece una lista amplia de controles de seguridad. Por ejemplo, Azure ofrece planes que van desde los 4$ hasta los 50.000 $/mes lo cual incluye planes para servidores, contenedores, base de datos, almacenamientos y API, además posee un paquete completo denominado Microsoft Defender For Cloud, cuyo precio varía según el nivel de protección, siendo el más bajo de 4.500$ /año hasta los 273.000 $/año con el nivel de seguridad más alto.

Análisis de la tabla comparativa

De acuerdo a los resultados de la investigación, se realiza un caso práctico en donde se demuestra las diferencias, falencias y ventajas que poseen tanto, la plataforma AWS, Google Cloud y Microsoft Azure. En este sentido, Cárdenas y Olarte (2022) en los resultados de su investigación evidenciaron que, la plataforma AWS cumple con todos los estándares de seguridad y con respecto a la transparencia. Sin embargo, Quintero (2023) en su estudio demostró que Microsoft Azure y Google Cloud presentan deficiencias con respecto a la transparencia en políticas y multi- tenancy, esto demuestra la ventaja que posee AWS en relación a las otras dos plataformas.

En ese mismo contexto, Oliva (2019) en su estudio investigativo evidenció que, la actualización y escaneo de datos en busca de amenazas que ofrece Azure de manera continua es una ventaja de seguridad que ofrece dicha plataforma, lo cual se vale de diversos protocolos de seguridad para que el intercambio de la información sea seguro. Sin embargo, Haro (2021) realizó un estudio para describir los servicios que ofrece la plataforma Microsoft Azure, en donde demostró que la actualización de datos no se realiza de manera continua, lo cual representa una deficiencia de los protocolos de seguridad para que sea seguro el intercambio de la información.

Por otro lado, Caballero y Jara (2021) en los resultados de su investigación mostraron que tanto AWS como Google Cloud ofrecen un mejor servicio de seguridad con respecto a IBM Cloud, esto debido a que ofrecen Firewalls adicionales y políticas de IAM. Lo cual se convierte en un aspecto positivo, ya que la seguridad en la nube las dos plataformas (AWS y Google Cloud) presentan mejores mecanismos de seguridad y protección.

De acuerdo a Gallego et al. (2023) en su estudio investigativo, evidenció que el análisis que efectúa Microsoft Azure enfoca en características propias de la plataforma, sin embargo, implica mayores costos de operación para la infraestructura. Esto lo convierte, en una desventaja al momento de adquirir dicha plataforma, por lo tanto, diversos usuarios optan por utilizar los servicios de seguridad que ofrece AWS y Google Cloud, para evitar gastos no planificados.

Los autores en mención, demuestran diversas características y mecanismos propios de seguridad que poseen las plataformas AWS, Google Cloud y Microsoft Azure, así lo demuestran especialistas de sistemas cloud y seguridad informática, cuyo criterio se obtuvo a través de encuestas realizadas a los mismos, en donde se evidencia que, según su perspectiva la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo. Dichos resultados lo respaldan investigaciones científicas, como Cárdenas y Olearte (2022), en donde demostraron que, el 75% de profesionales manifestaron que dicha plataforma cumple con una lista extensa de controles de

seguridad, lo cual permite manejar identidades, permisos, protección de infraestructura y redes, identificación y respuesta a amenazas.

Con respecto a Google Cloud, los hallazgos de la investigación evidenciaron que, dicha plataforma posee menos características de seguridad en comparación de AWS y Microsoft Azure. Cuyos resultados, se fundamentan en los hallazgos obtenidos por Rivero y Guerra (2023) en donde el 60% de encuestados manifestaron que la plataforma Google Cloud carece de un servicio de Identify and Access Management (IAM) mediante autenticación multi factor, lo cual no permite asegurar el registro del usuario de forma verídica.

Los especialista también mencionan que, Microsoft Azure se encuentra bien estructurada, cuya información lo respalda Cordero et al. (2020) en su investigación, en donde el 75% expresaron que dicha plataforma es la única empresa de computación en nube que ofrece infraestructura como servicio y una plataforma de aplicaciones segura y uniforme que permite a los equipos operar en la nube con distintos niveles de destreza y complejidad de proyecto.

Mediante este análisis práctico, se puede mencionar que, la amplia gama de controles disponibles en la plataforma de AWS asombra a los usuarios. Estos controles permiten el despliegue de un sistema fiable con una gestión del sistema fácil de usar, documentación clara y tutoriales gratuitos que ayudan a los usuarios a mantenerse al día con las frecuentes actualizaciones de la plataforma. AWS puede introducir mejoras en sus copias de seguridad manteniendo un alto nivel de seguridad, privacidad y conformidad mediante la introducción de métodos innovadores y la oferta de una gama más amplia de opciones.

Por otra parte, todas las soluciones de Microsoft Azure tienen un alto nivel de seguridad, pero la transparencia de la plataforma hace que todo sea más fácil de usar y más accesible para los usuarios, incluso a la hora de la implementación gracias a su documentación clara y sesiones de formación gratuitas. Muy al contrario; con un despliegue simplemente multi-tenancy, los clientes que no pueden permitirse los riesgos se ven disuadidos de compartir infraestructura física con otros clientes y corren el riesgo de sufrir una brecha de seguridad que podría afectar negativamente a su negocio.

Aunque los servicios que ofrece Google Cloud Platform parecen muy sólidos, la transparencia de la plataforma se resiente por el hecho de que el cliente no puede acceder fácilmente a la información legal que proporciona. En su lugar, el cliente debe investigar la normativa de cada una de las regiones en las que planea crear instancias y confirmar, mediante un examen minucioso de la documentación, si los servicios que decide utilizar se ajustan a las normas del sector.

¿En qué casos es conveniente utilizar AWS, Microsoft Azure y Google Cloud?

Con respecto a la lista de controles de seguridad, tanto la plataforma AWS, Microsoft Azure y Google Cloud son factibles para su utilización, puesto que dichas plataformas cumplen con los requisitos necesarios para mantener la privacidad y seguridad de los mismos. Con respecto a la usabilidad de la administración del sistema, las tres plataformas son adecuadas y convenientes para su uso, ya que poseen interfaces fácil configuración para sus elementos básicos con tutoriales de despliegue en la misma página, posee múltiples servicios de monitoreo para reforzar la seguridad.

Sin embargo, al hablar de transparencia, la plataforma AWS y Azure son los más convenientes debido a que en su página de legalidad proporcionan toda la información necesaria y de fácil acceso en donde especifica el cumplimiento de los recursos de forma sencilla y clara. Haciendo referencia al manejo de backs up, es aconsejable utilizar las plataformas Azure y Cloud, puesto que ofrecen formas más variadas de generar replicación para la recuperación en caso de desastres, por otro lado, AWS posee una solución efectiva de alta robustez, pero la cantidad de opciones que permite Azure y Cloud ofrecen más que una resiliencia cross-región sencilla.

Haciendo mención al tipo de servicio de despliegue, las tres plataformas tienen un servicio de despliegue de alta seguridad, sin embargo, en este caso es más conveniente utilizar AWS y Google Cloud, ya que permiten tener dos o tres tipos de tenancy, los cuales incluyen el tenancy de usuario único, mientras que Azure supone un riesgo con su política de responsabilidad compartida. Con respecto a la transmisión de datos dependiente de la regulación, se aconseja utilizar las tres plataformas, debido a que poseen varias políticas de cumplimiento bastantes variadas, en donde todas verifican que la transmisión de datos, replicación de datos y replicación de instancias sigan las normativas específicas de cada región, aunque tengan sistemas diferentes y el acercamiento dentro de cada plataforma sea distinto.

Finalmente, las tres plataformas ofrecen precios competitivos y modelos de facturación basados en el consumo. Aunque hay diferencias en cómo se tarifican los servicios, en general, los costes son comparables entre sí. **AWS** y **Google Cloud** ofrecen descuentos por uso prolongado, mientras que **Azure** brinda descuentos a los clientes que ya tienen licencias de Microsoft.

CONCLUSIONES

De acuerdo a los fundamentos teóricos, la plataforma AWS se posesiona como el líder de la industria en términos de seguridad, ya que ofrece una mejor lista de controles de seguridad, usabilidad de administración del sistema, transparencia, manejo de Backups, tipos de servicio de despliegue y transmisión de datos, seguido de Google Cloud y Microsoft Azure, que carecen en criterio de transparencia, riesgo con la política de seguridad compartida y riesgos con la entidad o usuario que utiliza los servicios de un proveedor de servicios en la nube.

La situación actual sobre la seguridad que ofrecen las plataformas AWS, Google Cloud y Microsoft Azure, son diversas, puesto que, existe una diferencia entorno a las características y mecanismos de seguridad. En este contexto, AWS se ubica como la plataforma más segura disponiendo de una amplia gama de controles de seguridad, seguido de la plataforma Microsoft Azure que, a pesar de ofrecer una seguridad sólida, presenta inconvenientes con el despliegue multi-tenancy, así mismo, Google Cloud aparentemente ofrece servicios de seguridad muy sólidos, no obstante, existe deficiencias con respecto a la transparencia de sus protocolos de seguridad.

Mediante del análisis comparativo, se determinó que la plataforma AWS posee una amplia gama de controles de seguridad, lo cual permite un despliegue de un sistema fiable, induciendo mejoras en las copias de seguridad, mientras que, la plataforma Google Cloud aparentemente ofrece servicios de seguridad muy sólidos, sin embargo, presenta deficiencias con la transparencia, cuya información legal no es de fácil acceso para los usuarios. Por último, la plataforma Azure también posee un alto nivel de seguridad, no obstante, el usuario puede sufrir riesgos al compartir la infraestructura física debido a que solamente posee un despliegue multi-tenancy.

De acuerdo a las encuestas realizadas a los especialistas, la mayoría con el 44% consideran que la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo, el 52% también consideran que posee más características de seguridad y privacidad. Por otra parte, el 36% consideran que la plataforma Google Cloud no presenta características suficientes de seguridad, además, un 48% consideran que dicha plataforma presenta un grado mayor de riesgo, con respecto a Microsoft Azure, el 48% consideran que no posee las características suficientes de privacidad y un 60% expresan que la plataforma presenta un grado mayor de desafío y riesgos entorno a la seguridad.

RECOMENDACIONES

A pesar que la plataforma AWS sorprende con su lista de controles gigantes que lo transforman en un sistema robusto, se puede mejorar en lo que respecta a las copias de respaldo a través de técnicas nuevas que permitan una diversidad más alta de soluciones para mantener de forma correcta la seguridad, el cumplimiento y la privacidad.

Las plataformas de Google Cloud y Microsoft Azure ofrecen altos niveles de seguridad, sin embargo, es recomendable que se mejore el criterio de transparencia para de esta forma se acerque a los usuarios de forma más agradable y darles a conocer a los clientes directamente los términos que se están aceptando al utilizar dichas plataformas.

Se recomienda que los resultados de la investigación sean socializados con la comunidad estudiantil, especialmente en el área de informática, para que puedan conocer las características y mecanismo de seguridad que ofrecen las plataformas AWS, Google Cloud y Microsoft Azure, de esta manera se incentiva a realizar investigaciones enfocadas a dar solución a las deficiencias que presentan dichas plataformas, para mejorar los servicios de seguridad.

De acuerdo a los problemas identificados, se recomienda que las futuras investigaciones se enfoquen en dar soluciones o implementar propuestas que permitan mejorar los protocolos de seguridad que ofrecen las plataformas AWS, Google Cloud y Microsoft Azure, de esta forma se contribuye a reforzar la seguridad en la nube, manteniendo la privacidad y la protección de las plataformas en mención.

BIBLIOGRAFÍA

Almeida, F. (2023). *Análisis comparativo de plataformas de virtualización en la nube para el despliegue de aplicaciones empresariales .* Obtenido de Proyecto de posgrado. Pontificia Universidad Católica del Ecuador : https://repositorio.puce.edu.ec/bitstreams/01dba843-9cb9-4dc3-922b-7af09fee6e2d/download

Alvarez, A. (2021). Uso crítico y seguro de tecnologías digitales de profesores universitarios. *Revista Formación universitaria, 14*(1), 35. doi:http://dx.doi.org/10.4067/S0718-50062021000100033

Bazzara, L. (2021). Datificación y streamificación de la cultura: Nubes, redes y algoritmos en el uso de las plataformas digitales. *Revista Inmediaciones de la Comunicación, 16*(2), 39. doi:https://doi.org/10.18861/ic.2021.16.2.3082

Caballero, C. y Jara, M. (2021). Obtenido de http://servicios.fpune.edu.py:83/fpunescientific/index.php/fpunescientific/article/view/210

Cárdenas, B. y Olarte, C. (2022). Análisis de seguridad entre microservicios con Amazon Web Service. *Revista Logos Ciencia & Tecnología, 14*(2), 42-52. doi:https://doi.org/10.22335/rlct.v14i2.1546

Castañeda, J y Villegas, G. (2020). *Recomendaciones y Estrategias para la Protección de Datos en la Nube.* Obtenido de https://dspace.tdea.edu.co/bitstream/handle/tdea/1393/Informe%20Protecci%C3%B3n%20datos.pdf?sequence=1&isAllowed=y

Castillo, R. (Noviembre de 2020). *Servicios de amazon en la nube: AWS.* Obtenido de https://repositorio.usam.ac.cr/xmlui/handle/11506/2118

Cerna, Y., Delgado, Y. y Salas, H. (2022). Cloud Computing y gestión documental en una empresa de servicios BPO, distrito de Magdalena del Mar (Lima-Perú), 2021. *Revista Industrial Data, 25*(1). doi:http://dx.doi.org/10.15381/idata.v25i1.21960

Chávez, L., Fernández, F. y Mendoza, A. (2023). Tendencias computacionales de los servicios de TI de nube pública aplicados en los negocios: Una revisión sistemática. *Revista Ingeniería Investiga, 5*(1), 1-6. doi:https://doi.org/10.47796/ing.v5i0.797

Cloud Native Security. (28 de Octubre de 2023). *El 80% de los riesgos de seguridad están presentes en los sistemas en la nube.* Obtenido de https://www.forbes.com.ec/today/declaran-emergencia-sector-energetico-ecuador-n57686

Cordero, X., Socorro, A., Soler, J., Hernández, H. y Guerra, P. (2020). Sistema estructurado de gestión del aprendizaje virtual de la Universidad Metropolitana del Ecuador. *Revista Universidad y Sociedad, 12*(5), 404-414, . Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202020000500404

Coronel, I. y Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE (RCTU), 9*(2), 97-109. doi:https://doi.org/https://doi.org/10.26423/rctu.v9i2.672

Gallego, J., Rubio, D. y Herrera, H. (2023). *Análisis de ciberseguridad a una infraestructura de red implementada en Microsoft Azure.* Obtenido de Estudio investigativo. Universidad los Libertadores : https://repository.libertadores.edu.co/bitstreams/511dfb24-98f7-48d5-8f47-baad80c06a9e/download

Gallego, J., Rubio. y Herrera, H. (2023). *Análisis de ciberseguridad a una infraestructura de red implementada en Microsoft Azure.* Obtenido de Estudio Investigativo. Universidad los Libertadores: https://repository.libertadores.edu.co/handle/11371/5949

Guayas, A. (2023). *Análisis comparativo de las plataformas Amazon Cloud, Google Cloud y Azure Cloud* . Obtenido de Proyecto de titulación. Universidad Técnica de Babahoyo : http://dspace.utb.edu.ec/handle/49000/14184

Kasperskay Lab. (2020). *Problemas y riesgos de la seguridad en la nube.* Obtenido de https://www.kaspersky.es/resource-center/preemptive-safety/cloud-security-issues-challenges

Landa, R. y Lujan, O. (08 de Julio de 2024). *Integración de servicios de AWS enfocado al uso de DevSecOps para mejorar el rendimiento y la seguridad en proyectos de Data & Analytics.* Obtenido de Proyecto de titulación. Universidad Peruana de Ciencias Aplicadas: https://repositorioacademico.upc.edu.pe/handle/10757/674691

Lezcano, A., Olivarez, P. y Mendoza, A. (2023). Principales medidas de seguridad para la protección de información y datos en la nube: una revisión sistemática. *Revista Ingeniería investiga, 5*(1), 3. doi:https://doi.org/10.47796/ing.v5i0.796

Llontop, R. (2020). *Implementación de una arquitectura escalable basada en Google Cloud Platform para mejorar la disponibilidad y escalabilidad de información de la empresa Smartbrands, Lima 2019.* Obtenido de Trabajo de Titulación. Universidad Católica Santo Toribio de Mogrovejo: https://tesis.usat.edu.pe/handle/20.500.12423/2921

López, S. (Enero de 2023). *Infraestructura de seguridad en la nube de Azure .* Obtenido de Proyecto investigativo. Universitat Oberta de Catalunya: https://openaccess.uoc.edu/handle/10609/147879

Méndez, M. (06 de Septiembre de 2021). *Planificación y diseño de un servicio seguro en la nube.* Obtenido de Trabajo de Fin de Máster. Universidad de Jaén: https://crea.ujaen.es/handle/10953.1/20347

Novoa. (2020). El derecho a la protección de datos de personales en la prestación de servicios de cloud computing. Una perspectiva ecuatoriana. *Revista de Derecho (Universidad Católica Dámaso A. Larrañaga, Facultad de Derecho), 22*(1), 66. doi:https://doi.org/10.22235/rd.vi22.2239

Oliva, S. (Mayo de 2019). *Microsoft Azure, un nuevo alcance para servicios de IT en la nube.* Obtenido de Proyecto de grado. Universidad San Carlos de Guatemala: http://www.repositorio.usac.edu.gt/14105/

Omaza, K. (2020). *Arquitectura de seguridad en la nube: Revisión de la implementación AWS.* Obtenido de https://oa.upm.es/58279/1/TFG_KIYOSHI_JOSE_OMAZA_SALDANA.pdf

Orozco, C. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático.* Obtenido de Trabajo de titulación. Universidad Politécnica Salesiana: https://dspace.ups.edu.ec/bitstream/123456789/20933/1/UPS-GT003374.pdf

Ortíz, E., Villacorta, C. y Mendoza, A. (2024). Seguridad de la Información en la Nube: Una revisión sistemática. *Revista Científica Ciencias Ingenieriles, 4*(1), 71. doi:https://doi.org/10.54943/ricci.v4i1.383

Patiño, A y Valencia, D. (2019). Modelo para la Adopción de Cloud Computing en las Pequeñas y Medianas Empresas del Sector Servicios en Medellín, Colombia. *Revista Información tecnológica, 30*(6), 159. doi:http://dx.doi.org/10.4067/S0718-07642019000600157

Quintero, A. (16 de Enero de 2023). *Seguridad y privacidad en la Nube, fortalezas y vulnerabilidades: Recomendaciones para tener en cuenta con los proveedores de servicios de la nube.* Obtenido de https://repositorio.uniandes.edu.co/entities/publication/f4c9eca3-aa99-4720-a18c-93e372ee46d8

Quintero, N. (16 de Enero de 2023). *Seguridad y privacidad en la Nube, fortalezas y vulnerabilidades: Recomendaciones para tener en cuenta con los proveedores de servicios de la nube.* Obtenido de Proyecto de grado. Universidad de los Ándes de Colombia: https://repositorio.uniandes.edu.co/flip/?pdf=/bitstreams/32ab7069-1a56-4a2a-9dc6-a5207954a1ea/download

Ríos, J., Vásquez, R. y Mendoza, A. (2023). Métodos emergentes de auditoría en integridad de datos en la nube: Una revisión sistemática de las últimas tendencias. *Revista Investigación & Desarrollo, 23*(1), 109. doi:https://doi.org/10.23881/idupbo.023.1-8i

Rivero, D. y Guerra, L. (2023). Seguridad y componentes nativos en una aplicación híbrida. *Revista Científica UISRAEL, 10*(1), 133. doi:https://doi.org/10.35290/rcui.v10n1.2023.748

Serrano, Y. (2021). Aws S3 como mecanismo de recuperación ante desastres tecnológicos en pymes. Obtenido de https://preprints.scielo.org/index.php/scielo/preprint/download/325/411/400

Thales Group . (17 de Septiembre de 2023). *La principal causa de filtración de datos en empresas de Latinoamérica no son hackers.* Obtenido de https://www.larepublica.co/empresas/principal-causa-de-filtracion-de-datos-en-empresas-de-latinoamerica-no-son-los-hackers-3706619

Zúñiga, A., Jalón, E., Andrade, M. y Giler, J. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. *Revista Universidad y Sociedad, 13*(3), 455. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000300454

ANEXOS

ANEXO 1: FORMATO DE ENCUESTA

Preguntas	Respuestas				
	Siempre	**Casi siempre**	**A veces**	**Pocas veces**	**Nunca**
1. ¿Considera usted que la plataforma AWS cumple con los estándares de seguridad de primer nivel en todo el mundo?					
2. ¿Considera usted que la plataforma AWS posee más características de seguridad y privacidad, a comparación de Google Cloud y Microsoft Azure?					
3. ¿Cree usted que la seguridad de AWS posee beneficios operativos y organizativos bien estructurados?					
4. ¿Cree usted que la plataforma AWS presenta un grado mayor desafío y riesgo de seguridad?					
5. ¿Considera usted que la responsabilidad de seguridad compartida que ofrece la plataforma Google Cloud es confiable y segura?					
6. ¿Considera usted que la plataforma Google Cloud posee más características de seguridad y privacidad, a comparación de Microsoft Azure y AWS?					
7. ¿Cree usted que los sistemas de protección que dispone Google Cloud son suficientes para hacer frente a los Hackers e intrusos?					
8. ¿Considera usted que la plataforma Google Cloud cumple con los estándares de seguridad de primer nivel en todo mundo?					

9. ¿Cree usted que la plataforma Google Cloud presenta un grado mayor desafío y riesgo de seguridad?					
10. ¿Cree usted que la descripción general de la seguridad de Microsoft Azure se encuentra bien estructurada?					
11. ¿Cree usted que la gestión de la postura de seguridad en la nube de Microsoft Azure es completa y eficiente?					
12. ¿Considera usted que la plataforma Microsoft Azure posee más características de seguridad y privacidad, a comparación de Google Cloud y AWS?					
13. ¿Cree usted que la plataforma Microsoft Azure presenta un grado mayor desafío y riesgo de seguridad?					

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".** Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Wilmer Enrique Ortiz Gavilánez
Título obtenido: Ingeniero en Sistemas Computacionales
C.I.: 0201561412
E-mail: wilmer.ortiz@gmail.com
Institución de Trabajo: Cooperativa de Ahorro y Crédito Guaranda Ltda.
Cargo: Analista Programador
Años de experiencia en el área: 12

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.

- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad	**X**				
Novedad	**X**				
Fundamentación pedagógica	**X**				
Fundamentación tecnológica	**X**				
Indicaciones para su uso	**X**				
TOTAL	**35**				

Observaciones:……

……

……

Recomendaciones:……

……

……

Lugar, fecha de validación: Guaranda, 30 de agosto de año 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firmado electrónicamente por:
WILMER ENRIQUE ORTIZ GAVILANEZ

Firma del especialista
Wilmer Ortiz

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".** Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Wilson Fernando Freire Sandoval
Título obtenido: Magister en Telecomunicaciones
C.I.: 1716310725
E-mail: wilsonfreire_ldu@hotmail.com
Institución de Trabajo: Puntonet
Cargo: Jefe Nacional de Cloud y Datacenter
Años de experiencia en el área: 15

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad		**X**			
Novedad		**X**			
Fundamentación pedagógica		**X**			
Fundamentación tecnológica	**X**				
Indicaciones para su uso		**X**			
TOTAL	**15**	**16**			

Observaciones: Hacer un análisis de la responsabilidad compartida entre el usuario y el proveedor de servicio

Recomendaciones: Hacer un análisis financiero entre las soluciones de nube profundizar en análisis de nube hibrida.

Lugar, fecha de validación: Quito, 30 de agosto de año 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista
Wilson Freire

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".** Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Darwin Mora
Título obtenido: Master Administración Estratégica de Telecomunicaciones
C.I.: 0401105598
E-mail: darwin.mora@puntonet.ec
Institución de Trabajo: Puntonet
Cargo: Gerente Nacional de Infraestructura
Años de experiencia en el área: 25

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Análisis comparativo de protocolos de seguridad en diferentes plataformas de nube, como AWS, Google Cloud y Microsoft Azure".

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad			**X**		
Novedad		**X**			
Fundamentación pedagógica		**X**			
Fundamentación tecnológica	**X**				
Indicaciones para su uso		**X**			
TOTAL	**15**	**12**	**3**		

Observaciones:……

……

……

Recomendaciones: Llevarlo a la practica

……

……

……

Lugar, fecha de validación: Quito, 30 de agosto de año 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista
Darwin Mora

Turnitin_Erik_Caiza_Protocolos

INFORME DE ORIGINALIDAD

3%	3%	0%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad TecMilenio Trabajo del estudiante	1%
2	repositorio.uisrael.edu.ec Fuente de Internet	1%
3	aws.amazon.com Fuente de Internet	1%
4	www.ceste.es Fuente de Internet	1%