Revista Científica Ciencias Ingenieriles (2024)

Vol. 4, Núm. 1, pp. 69 – 78

https://doi.org/10.54943/ricci.v4i1.383

ISSN: 2961-2357**(En línea)**
ISSN: 2961-2446**(Impreso)**

ARTÍCULO DE REVISIÓN

Seguridad de la Información en la Nube: Una revisión sistemática.

Information Security in the Cloud: A Systematic Review.

• Elvis Ortiz [1] • Cristhian Villacorta [2] • Alberto Mendoza [3]

[1] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t023300220@unitru.edu.pe
ORCID: https://orcid.org/0009-0001-6369-2919
[2] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: t013300620@unitru.edu.pe
ORCID: https://orcid.org/0009-0008-2504-7354
[3] Universidad Nacional de Trujillo, Trujillo, Perú.
Correo electrónico: amendozad@unitru.edu.pe
ORCID: https://orcid.org/0000-0002-0469-915X

Recibido: 05 octubre del 2023 / **Revisado**: 31 octubre del 2023 / **Aprobado:** 07 diciembre del 2023 / **Publicado:** 22 de Enero del 2023

RESUMEN

En un contexto de creciente adopción de tecnologías en la nube, la seguridad de la información se ha convertido en un aspecto crítico. Este artículo se enfoca en identificar, analizar y abordar los desafíos en la seguridad de la información en entornos de nube, al mismo tiempo que resalta las mejores prácticas recomendadas para garantizar la integridad, confidencialidad y disponibilidad de los datos. Empleando la metodología PRISMA se busca responder ¿Cuáles son los desafíos y mejores prácticas de la seguridad de la información en entornos de nube? A partir de esta base, se exploran los desafíos clave, incluyendo el almacenamiento seguro de información confidencial y la protección de la privacidad de los datos. Se subraya la importancia de cumplir con las regulaciones y leyes de protección de datos, como el GDPR (Reglamento General de Protección de Datos), especialmente en un entorno de nube que opera en diferentes ubicaciones geográficas. Para abordar estos desafíos, se presentan mejores prácticas esenciales. La encriptación se destaca como una medida fundamental para asegurar la confidencialidad de los datos, mientras que el control de acceso basado en roles se menciona como una estrategia clave para gestionar quién tiene acceso a la información en la nube. Además, se enfatiza la necesidad de realizar evaluaciones de riesgos continuas y de contar con un sólido plan de respuesta a incidentes para proteger eficazmente la información en entornos digitales cada vez más vulnerables.

Palabras clave: Computación en la nube; seguridad de información; desafíos; prácticas.

ABSTRACT

In a context of increasing adoption of cloud technologies, information security has become a critical issue. This article focuses on identifying, analyzing and addressing information security challenges in cloud environments, while highlighting recommended best practices to ensure data integrity, confidentiality and availability. Using the PRISMA methodology, we seek to answer What are the challenges and best practices of information security in cloud environments? From this base, key challenges are explored, including the secure storage of confidential information and the protection of data privacy. The importance of complying with data protection regulations and laws, such as GDPR (General Data Protection Regulation), is highlighted, especially in a cloud environment operating in different geographic locations. To address these challenges, essential best practices are presented. Encryption is highlighted as a key measure to ensure data confidentiality, while role-based access control is mentioned as a key strategy for managing who has access to information in the cloud. In addition, the need for ongoing risk assessments and a robust incident response plan to effectively protect information in increasingly vulnerable digital environments is emphasized.

Keywords: Cloud computing; information security; challenges; practices

1. INTRODUCCIÓN

La rápida evolución tecnológica ha transformado la manera en que las organizaciones gestionan y almacenan datos cruciales. La creciente adopción de la computación en la nube ha sido un impulsor fundamental de este cambio, brindando flexibilidad asimismo acceso global a recursos informáticos esenciales. No obstante, esta revolución tecnológica ha planteado nuevos interrogantes y desafíos, particularmente en lo que concierne a la seguridad de la información.

Este artículo se propone abordar dos objetivos cruciales. En primer lugar, se enfocará en la identificación y análisis de los desafíos inherentes a la seguridad de la información en el entorno de la nube. Esto abarca una evaluación exhaustiva de las amenazas tanto internas como externas, considerará la privacidad de los datos, abordará cuestiones de cumplimiento normativo y explorará otros aspectos críticos que pueden afectar la integridad de la información almacenada en la nube.

En este contexto, el primer punto a tratar se basa en las observaciones de (Abdullayeva, 2023), quien identificó varios desafíos relacionados con la seguridad de la información en la nube. Estos desafíos proporcionan una base sólida para comprender la complejidad de la seguridad en la nube, asimismo esto permitirá a las organizaciones anticipar y abordar de manera efectiva las amenazas además de las preocupaciones que pueden surgir en el entorno digital en constante evolución.

En segundo lugar, se destacarán las mejores prácticas recomendadas para mitigar estos desafíos, lo que se busca es lograr determinar los desafíos que presenta la nube en términos de seguridad de la información asimismo señalar las mejores prácticas de seguridad de la información en un entorno de nube considerando esto como objetivos.

En este sentido, el segundo punto de enfoque se basa en las investigaciones de (Prasad, 2023), quien destaca que la seguridad en la nube no solo es un conjunto de desafíos, sino también una oportunidad para implementar estrategias efectivas que fortalezcan la protección de los datos y la integridad de la información en un entorno digital en constante cambio.

2. METODOLOGÍA

Al realizar este estudió se optó por un método de revisión sistemática. El período de recopilación de la literatura estuvo limitado entre 2019 y 2023. Dicha decisión cronológica se tomó luego de explorar en Google Trends el término de búsqueda “Information security” (ver Fig. 1) y “Computación en la nube” (ver Fig. 2). Las búsquedas de interés relacionadas con computación en la nube iniciaron en 2004 y se establecieron a cierta medida en 2016, pero empezaron a aumentar a fines del año 2019. Por otro lado, las búsquedas relacionadas con information security se mantuvieron en una media desde 2012 hasta inicios de 2019 que hubo mayor interés entre los buscadores. Asimismo, se consideró dicha limitación de tiempo con el fin de asegurar que la información y evidencia utilizada esté actualizada y refleje el estado más reciente de la investigación en el campo. Esto ayudó a tener una visión más precisa y relevante de las tendencias, avances y cambios en el conocimiento científico, lo que mejora la calidad y aplicabilidad de la revisión

.

Figura 1

Análisis de tendencias de Google sobre 'Information security'

Figura 2
Análisis de tendencias de Google sobre 'computación en la nube'.

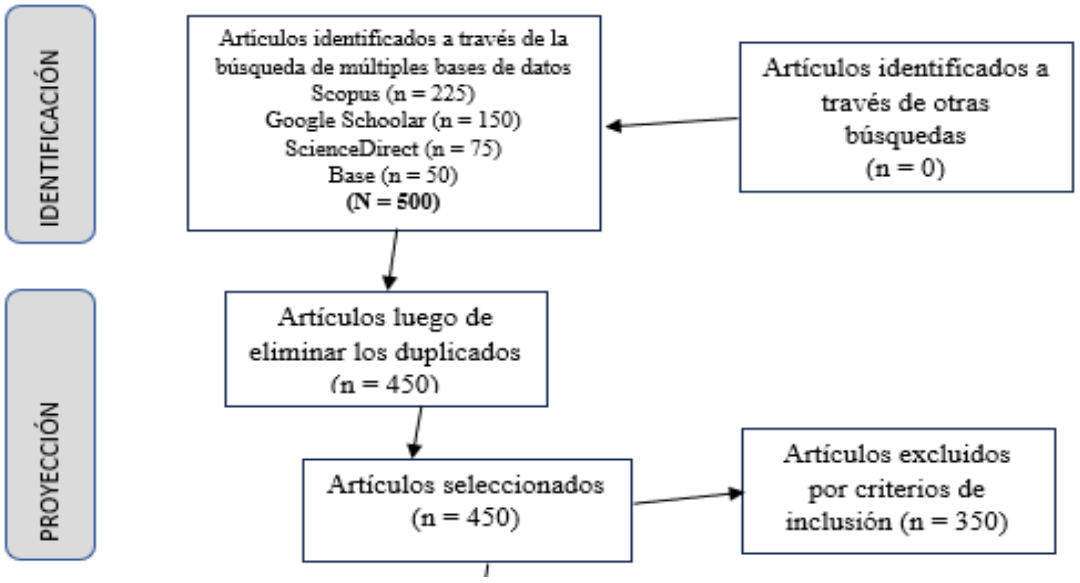
Los artículos relevantes se extrajeron de bases de datos de publicaciones académicas. Para reducir el sesgo y para la validez de la calidad de la investigación, durante el proceso de revisión, se utilizó un conjunto de directrices de elementos de informe preferidos de revisiones sistemáticas y metaanálisis (PRISMA). La figura 3 contiene el diagrama de flujo de PRISMA que incluye la identificación, selección, elegibilidad e inclusión del estudio.

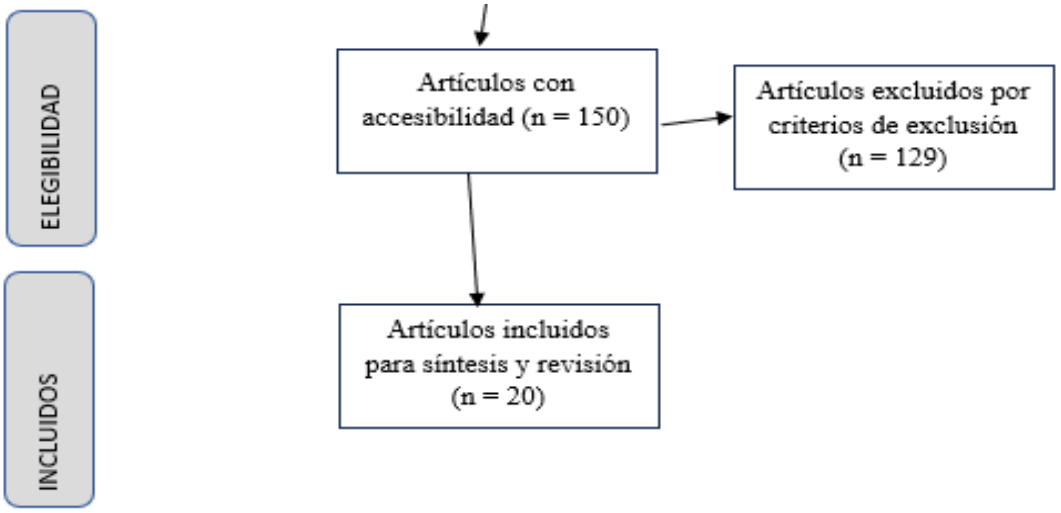
La pregunta de investigación en la que se basó el proceso metodológico es la siguiente: ¿Cuáles son los desafíos y mejores prácticas de la seguridad de la información en entornos de nube?

De acuerdo con lo mencionado por Carmen P. (2012), en julio de 2009 se lanzó la declaración PRISMA, que representa una actualización diseñada con fines educativos para complementar la lista de verificación. Esta declaración respalda los 27 componentes de la lista de verificación y también incluye 7 tablas que detallan aspectos esenciales de la metodología. Además, es importante destacar que PRISMA no solo se limita a los metaanálisis de ensayos clínicos, sino que se puede adaptar a una variedad de revisiones sistemáticas. Según la autora, PRISMA se concibe como una herramienta beneficiosa para mejorar los estudios en términos de contextos, intervenciones y otros aspectos relevantes.

Teniendo en cuenta estas definiciones, a continuación, se describirán las fases posteriores del proceso de investigación, que comprenden la formulación de la estrategia de búsqueda, la selección de la literatura pertinente, el registro de los hallazgos y, finalmente, la interpretación de los resultados obtenidos.

Figura 3
Diagrama de flujo PRISMA





Para un abordaje más integral, se consultaron e incluyeron en la colección publicaciones de las bases de datos de Google Scholar, Scopus, ScienceDirect y Base. Las cuales fueron seleccionadas debido a su prestigio en el ámbito académico y la riqueza del contenido implícito que pueden proporcionar para enriquecer nuestra investigación. Asimismo, se empleó gestores de referencias bibliográficas como Mendeley y IEEE Xplore para obtener las fuentes bibliográficas.

Tabla 1

Base de datos con los términos de búsqueda empleados correspondientemente.

Base de datos	Terminos de busqueda
Scopus	"Cloud computing", "Information security", "Better practices", "Challenges", "Threats"
Google Scholar	"Computación en la nube", "Seguridad de la información","Prácticas", "Desafíos", "Amenazas"
ScienceDirect	"Cloud computing", "Information security", "cloud security", "Cloud threats", "Cloud challenges"
Base	"Cloud computing", "Cloud challenges", "Desafíos", "Amenazas"

Tabla 2

Criterios de inclusión y exclusión considerados.

	Criterios de inclusión	Criterios de exclusión
Título	Incluir cualquiera de los términos de búsqueda	No incluir alguno de los terminos de búsqueda
Fecha de publicación	2019 - 2023	Antes 2019
Publicación	Revistas, artículos	Tesis
Objetivos del estudio	Artículos centrados en el funcionamiento de la nube y cómo es gestionada la seguridad de la información, asimismo los distintos desafíos y prácticas que presenta.	Artículos que no se centran en la nube, ni mucho menos en seguridad de la información.
Metodología	Investigación primaria que incluye experimental, cuasi experimental, investigación cualitativa, estudios o revisiones sistemáticas	Artículos que carecen de una explicación clara de metodología.

3. DESARROLLO

La creciente adopción de tecnologías en la nube ha transformado la forma en que las organizaciones gestionan y almacenan datos e información crítica. Sin embargo, esta evolución tecnológica ha planteado nuevos desafíos en lo que respecta a la seguridad de la información. En un mundo cada vez más dependiente de la nube, es esencial comprender los desafíos y las mejores prácticas asociadas con la seguridad de la información en estos entornos. En este artículo, exploramos a fondo los desafíos clave que enfrentan las organizaciones y examinaremos las estrategias y prácticas recomendadas para garantizar la integridad, la confidencialidad y la disponibilidad de los datos en la nube.

3.1. Definición de la seguridad de la información en la nube.

En la era digital en la que vivimos, es relevante conocer donde se almacenan los datos, documentos, aplicaciones y más, y cabe destacar que se puede acceder desde cualquier lugar del mundo, hacemos referencia a la nube. De acuerdo a lo mencionado por (Al-Ghuwairi et., 2023) en el área de la tecnología de la información, nube hace referencia a los diversos recursos informáticos los cuales se comparten en internet entre ellos se encuentran servidores, servicios de almacenamiento, estaciones de trabajo virtuales esto representa un sector el cual está en un constante crecimiento debido a la demanda actual.

Sin embargo, el tener acceso desde cualquier lugar es crucial hablar de seguridad de la información que se maneja al hablar de nube, tal como menciona (Rodriguez et al, 2020) al estar en desarrollo y constante avance la nube, es de suma trascendencia avalar la seguridad de toda información, al mismo tiempo lograr su afable oportuna. En relación a lo mencionado se debe tener en cuenta tres aspectos: la confidencialidad, la integridad y la disponibilidad. Confidencialidad cuando deseas que nadie más que tú pueda visualizar tu información, integridad es asegurar que tu información no sea alterada y por último, pero no menos importante disponibilidad hace referencia a que tu información debe estar disponible cuando lo desees.

3.2. Descripción de los modelos de servicio en la nube (SaaS, PaaS, IaaS).

(Blanco et al., 2023) Señala que los avances tecnológicos en tecnologías de la información tales como los servicios SaaS, PaaS, IaaS en la computación en la nube tienen gran relevancia, lo cual involucra la exploración de cómo la tecnología de la nube aborda cuestiones como flexibilidad, dinamismo.

3.2.1. SaaS

Se refiere a la oportunidad de utilizar aplicaciones proporcionadas por un proveedor. Los usuarios pueden acceder a estas aplicaciones a través de una interfaz de aplicación web, como un navegador web o una interfaz de aplicación específica. En el caso de SaaS, el cliente no se encarga de administrar y monitorear la infraestructura de la nube mencionada (Mohammed et al., 2020). Es por ello que es de suma importancia evaluar los servicios de SaaS, es esencial considerar la accesibilidad de la interfaz de usuario para una amplia variedad de usuarios y abordar adecuadamente la cuestión de la propiedad de los datos para garantizar que los derechos de los clientes se protejan de manera efectiva. Estos dos aspectos son fundamentales para evaluar la calidad y la seguridad de los servicios de SaaS mencionados en (Nadeem, 2022).

3.2.2. PaaS

Es un modelo de servicio en la nube que proporciona a los desarrolladores de software un entorno completo para crear, desplegar y gestionar aplicaciones en línea. Tal como indica (Mohammed et al., 2020) los clientes pueden alquilar servidores y recursos definidos por software para ejecutar sus aplicaciones, sin necesidad de contar el hardware necesario, a pesar de que todo es gestionado por el proveedor, el control lo tiene el cliente.

3.2.3. IaaS

Es un modelo de servicio en la nube que proporciona a las organizaciones acceso a recursos de infraestructura de TI a través de Internet. Tal como señala (Mohammed et al., 2020) Infrastructure as a Service, en el contexto de nube hace referencia a el poder de un cliente de acceder a servicios informáticos, los cuales van desde instalar sistemas operativos a gestionar máquinas virtuales sin necesidad de tener infraestructura, a un costo variable lo que significa que se paga por lo que se consume.

3.3. Amenazas en la nube.

No se puede discutir los numerosos beneficios que ha traído la nube a los diversos clientes en todo el mundo, no obstante, también ha dado lugar a una serie de amenazas en términos de seguridad de la información. Tal como señala (Alshayeji et al., 2022) las amenazas internas son una gran amenaza para la computación en la nube, dichas amenazas se basan principalmente en errores humanos, no intencionales. Estos errores pueden ser costosos y potencialmente dañinos para una organización. Sin embargo, en cuanto a las amenazas internas, (Alshayeji et al., 2022) afirma que aún persisten porque los contenidos se almacenan en la nube sin ser cifrados, es decir los enfoques AES-GCM y AES-CBC128 no protegen la confidencialidad, integridad o privacidad del usuario frente a amenazas internas (solo de los extraños).

Asimismo, también se presentan amenazas asociadas a redes físicas tradicionales, tomando como referente un contexto VNF (Funciones de red virtual) las cuales pueden afectar al sistema mencionado en (Abu-Alhaija et al., 2022).

A su vez (Tahirkheli et al., 2021) resalta que los flujos de información han aumentado drásticamente, lo que a su vez ha dado lugar a mayores amenazas, específicamente las ciudades inteligentes han planteado troyanos, malware.

Por su parte (Goyal et al., 2022) señala amenazas en entornos de nube tales como: Sybil consiste en un atacante controla múltiples nodos o identidades falsas en una red o sistema para obtener una ventaja indebida, Whitewashing hace referencia a la práctica de ocultar o encubrir una actividad maliciosa, generalmente en registros o registros de auditoría.

Por otro lado, Soveizi et al. (2023) menciona que la pérdida de control se produce cuando un flujo de trabajo se externaliza en la nube, lo que resulta en que el sistema de gestión de flujos de trabajo pierda el control sobre las tareas. Esta situación puede aumentar significativamente los riesgos de seguridad y dejar los flujos de trabajo expuestos a posibles ataques maliciosos.

Asimismo, es relevante destacar que, según las observaciones de (Prasad, 2023), la fuga de datos representa una preocupación de gran envergadura en el ámbito de la computación en la nube. Esta inquietud surge debido a la variedad de factores que pueden propiciarla, tales como configuraciones inadecuadas, vulnerabilidades de seguridad que pueden ser explotadas por actores maliciosos, y en ocasiones, acciones inadvertidas por parte de los propios usuarios.

Además, es importante destacar que según (ThiBac & Minh, 2022), los ataques de denegación de servicio (DDoS) tienen como objetivo abrumar deliberadamente los servidores en la nube mediante un flujo constante de tráfico malicioso. Este proceso conlleva la consecuencia de interrumpir la disponibilidad de los servicios ofrecidos en dichos servidores, lo que afecta negativamente a los usuarios que dependen de ellos. Esta práctica, que se ha vuelto cada vez más común en el entorno digital actual, pone de manifiesto la importancia de contar con estrategias eficaces para prevenir este tipo de ataques, con el fin de garantizar un acceso seguro y continuo a los recursos en la nube.

3.4. Desafíos en la Seguridad de la Información en la Nube

La computación en la nube ha revolucionado la forma en que almacenamos, gestionamos y accedemos a datos y servicios. Sin embargo, esta innovación tecnológica no está exenta de desafíos significativos en términos de seguridad, privacidad y rendimiento. A medida que las organizaciones y usuarios adoptan la nube, es crucial comprender y abordar estos desafíos para garantizar un uso seguro y eficiente de esta tecnología.

Tal como señala (Agapito et al., 2023) uno de los desafíos principales es el almacenamiento seguro de información confidencial en la nube, tomando como referencia a la salud médica en el que un paciente acude a un establecimiento de salud con la confianza de que todo proceso se lleva de manera confidencial y no se está divulgando.

Sumado a esto en el ambiente educativo la nube debe cumplir con las necesidades de usuarios en el ámbito de gestión de identidad y acceso, asegurando un control de identidad para evitar vulnerabilidades señala (Malkawi et al., 2023).

(Sandhu, 2022) señala que la protección de la privacidad de los datos es esencial,

especialmente en entornos de nube donde los datos pueden residir en servidores compartidos.
Además, según (Soveizi et al. 2023), la mejora en la automatización del modelado de requisitos de seguridad en los flujos de trabajo en la nube no solo simplifica la comprensión y el uso del sistema, sino que también beneficia a los especialistas sin experiencia en seguridad. Esto se evidencia en su capacidad para realizar análisis de conflictos, reutilizar componentes del modelo y validar el sistema de manera más efectiva.

Por otro lado, (Abdullayeva, 2023) identifica varios desafíos adicionales relacionados con la seguridad de la información en la nube: Amenazas cibernéticas: La nube está expuesta a diversas amenazas digitales, como ataques de hackers, malware, phishing y robo de datos, que pueden comprometer la confidencialidad e integridad de la información almacenada. Privacidad de los datos: La transferencia y almacenamiento de datos en la nube generan inquietudes acerca de la privacidad de la información. Los usuarios deben confiar en que los proveedores de servicios en la nube protejan de manera adecuada sus datos y prevengan el acceso no autorizado. Cumplimiento normativo: El uso de servicios en la nube exige que las organizaciones cumplan con regulaciones y leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, lo que puede ser desafiante debido a la dispersión geográfica de los datos. Resiliencia cibernética: La resiliencia cibernética se refiere a la capacidad de un sistema para resistir, adaptarse y recuperarse de ataques cibernéticos. En el contexto de la computación en la nube, es fundamental que esta pueda resistir y recuperarse de ataques para garantizar la continuidad del servicio.

3.5. Mejores Prácticas

La seguridad de la información en la nube es una preocupación fundamental en la era digital actual. A medida que las organizaciones y los individuos confían cada vez más en servicios en la nube para almacenar y gestionar sus datos, la implementación de las mejores prácticas de seguridad se convierte en una prioridad esencial.

La encriptación se utiliza para convertir los datos del usuario en un formato cifrado que solo el receptor autorizado puede descifrar, asegurando así la confidencialidad de la información durante la transmisión de datos y las comunicaciones señaladas en (Suganya et al., 2023) dicha encriptación es esencial para convertir la información en un formato ilegible para terceros durante su transmisión y almacenamiento en la nube. Esta práctica garantiza la confidencialidad de los datos, lo que se alinea con la importancia de la criptografía mencionada en el texto.

A su vez (Amardeep & Amandeep, 2023) resalta que el acceso a los servicios de la nube se controla mediante un firewall que establece políticas de control de acceso. Estas políticas determinan qué acciones y operaciones pueden realizar los usuarios legítimos en los recursos disponibles. En particular, se hace hincapié en el modelo de control de acceso basado en roles, donde el acceso a los recursos se basa en la función o rol de un usuario en la empresa.

En adición (Bhamare et al., 2017) indica que la necesidad de probar y mejorar constantemente los modelos de aprendizaje automático en diversos entornos operativos para garantizar su eficacia en la seguridad en la nube hace referencia a una evaluación y mejora continua de la seguridad en la nube como una práctica relevante. Dicha práctica implica una evaluación constante de las soluciones de seguridad en la nube y la adaptación a las cambiantes amenazas y entornos.

Por otro lado, (Abdullayeva, 2023) señala que una sólida gestión de identidad y acceso desempeña un papel fundamental en el fortalecimiento del control sobre los recursos en la nube. Además, la implementación de autenticación de múltiples factores y la aplicación de políticas de acceso basadas en roles aseguran la seguridad al verificar la identidad de la persona autorizada de manera efectiva.

Adicionalmente, llevar a cabo evaluaciones periódicas de riesgos se revela como una estrategia esencial para identificar posibles vulnerabilidades y amenazas en el entorno de la nube. Esto, a su vez, permite tomar medidas proactivas para mitigar los riesgos que puedan surgir.

Sumado a esto (Prasad, 2023) enfatiza que, es fundamental llevar a cabo una vigilancia y auditoría constante de los accesos. Además, es esencial contar con un sólido plan de acción para responder eficazmente a

posibles incidentes en caso de una infracción de la integridad de la información. Esta preparación proactiva es esencial para salvaguardar la información crítica en entornos digitales cada vez más vulnerables.

La revisión sistemática nos brindó una definición de aquello que implica nube tal como menciona (Al-Ghuwairi et al., 2023) asimismo reforzando dicha idea es reforzada por (Blanco et al., 2023) quién indica que nube no solo queda en un concepto, sino que involucra diferentes servicios que son empleados por los clientes. Cuando hablamos de administrar y monitorear la infraestructura (Mohammed et al., 2021) indica que es de suma importancia evaluar los servicios de SaaS, es esencial considerar la accesibilidad de la interfaz y a su vez (Nadeem, 2022) señala la garantía que debe existir de manera tal que se asegure la protección de manera efectiva de los datos.

En la ardua labor de asegurar dicha seguridad de la información (Alshayeji et al., 2022) asegura que hay una amenaza importante para la computación en la nube, que consiste en errores humanos, no intencionales, y todo surge de manera interna, no obstante (Abu-Alhaija et al., 2022) manifiesta que existen amenazas asociadas a redes físicas tradicionales, a su vez Sybil, Whitewashing, son amenazas de entorno de nube indica (Tahirkheli., 2021).

Antes tales amenazas se presentan desafíos tales como almacenamiento seguro de información confidencial señala (Agapito et al., 2023), dicha afirmación la refuerza (Malkawi et al., 2023) cuando menciona que es necesario llevar un control de identidad y acceso con el fin de salvaguardar la información, no obstante (Sandhu, 2022) comparte el mismo sentir indicando que la protección de la privacidad de los datos es esencial, dicha idea la comparte (Abdullayeva, 2023) al mencionar que la transferencia y almacenamiento de datos en la nube generan inquietudes acerca de la privacidad de la información.

A su vez para asegurar dicha protección de datos, es necesario asegurar diversas prácticas las cuales consisten en una encriptación para convertir la información en un formato ilegible para terceros indica (Suganya & Sasipraba, 2023), no obstante llevar un control mediante un firewall y una resaltante es realizar una evaluación constante de las soluciones de seguridad en la nube y la adaptación a las cambiantes amenazas y entornos, así también se desea resaltar (Abdullayeva, 2023) señala que una sólida gestión de identidad y acceso desempeña un papel fundamental en el fortalecimiento del control sobre los recursos en la nube, no obstante Prasad, 2023) refuerza la idea mencionando que, es fundamental llevar a cabo una vigilancia y auditoría constante de los accesos.

4. CONCLUSION

La seguridad de la información se basa en proteger los datos y sistemas de información contra amenazas y riesgos, como el acceso no autorizado, la pérdida, el robo o la manipulación de datos. Partiendo de este enunciado es vital la seguridad de la información en la nube debido a la gran cantidad de información que se maneja.
Por ende, se concluye que los desafíos que se presentan en la nube en términos de seguridad de la información son lograr un almacenamiento seguro de la información, mantener un control de identidad y acceso para evitar vulnerabilidades y asegurar la privacidad de los datos de terceros. Asimismo, se logró determinar las prácticas, la cuales comprenden encriptar la información de manera tal que solo el receptor autorizado puede descifrar, asegurando así la confidencialidad de la esta, establecer un acceso mediante un firewall que establece políticas de control de acceso, y evaluación y mejora continua de la seguridad en la nube debido a las nuevas amenazas que aparecen día a día.
Esta revisión sistemática es de suma importancia a las personas interesadas en tomar en cuenta aquello que implica seguridad de la información en la nube, asimismo se anima a nuevos investigadores de acuerdo a lo expuesto lograr determinar técnicas de aprendizaje automático para la detección de amenazas en la nube con el fin de salvaguardar la información, la cuál es importante para cualquier empresa.

5. REFERENCIA BIBLIOGRÁFICA

Abu-Alhaija, M., Turab, N. M., & Hamza, A. R. (2022). *Extensive study of cloud computing technologies, threats and solutions prospective. Computer Systems Science and Engineering*, 41(1), 225–240. https://doi.org/10.32604/csse.2022.019547

Abdullayeva, F. J. (2023). *Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization*, 12, 100268. https://doi.org/10.1016/j.rico.2023.100268

Agapito, G., & Cannataro, M. (2023, June 1). *An Overview on the Challenges and Limitations Using Cloud Computing in Healthcare Corporations. Big Data and Cognitive Computing*. MDPI. https://doi.org/10.3390/bdcc7020068

Al-Ghuwairi, AR., Sharrab, Y., Al-Fraihat, D. *et al. Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. J Cloud Comp 12, 127 (2023).* https://doi.org/10.1186/s13677-023-00491-x

Alshayeji, M. H., & Abed, S. (2022). *Enhanced video-on-demand security in cloud computing against insider and outsider threats. International Journal of Security and Networks*, 17(1), 48–55. https://doi.org/10.1504/IJSN.2022.122550.

Amardeep Kaur, Amandeep Verma (2023). *Adaptive Access Control Mechanism (AACM) for Enterprise Cloud Computing. Journal of Electrical and Computer Engineering*, https://doi.org/10.1155/2023/3922393.

Blanco, D. F., Le Mouel, F., Lin, T., & Escudie, M. P. (2023). *A Comprehensive Survey on Software as a Service (SaaS) Transformation for the Automotive Systems*. IEEE Access, 11, 73688–73753. https://doi.org/10.1109/ACCESS.2023.3294256.

Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2017). *Feasibility of Supervised Machine Learning for Cloud Security. In ICISS 2016 - 2016 International Conference on Information Science and Security. Institute of Electrical and Electronics Engineers Inc*. https://doi.org/10.1109/ICISSEC.2016.7885853.

Carmen Pérez Rodrigo (2012*). "Las revisiones sistemáticas: declaración PRISMA"*. Consultado de https://renc.es/imagenes/auxiliar/files/Nutr_1-2012%20Taller%20escritura.pdf.

F. Nadeem, *"Evaluating and Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non-Functional Key Performance Indicators,"* in IEEE Access, vol. 10, pp. 63245-63257, 2022, doi: 10.1109/ACCESS.2022.3182688.

Goyal, P., & Deora, S. S. (2022). *Trust Management Techniques and their Challenges in Cloud Computing: A Review. International Journal of Computer Networks and Applications*, 9(6), 761–774. https://doi.org/10.22247/ijcna/2022/217708.

Malkawi, A. R., Bakar, M. S. A., & Dahlin, Z. M. (2023). *Cloud computing virtual learning environment: issues and challenges. Indonesian Journal of Electrical Engineering and Computer Science*, 30(3), 1707–1712. https://doi.org/10.11591/ijeecs.v30.i3.pp1707-1712.

Mohammed, S., Nanthini, S., Krishna, N. B., Srinivas, I., Rajagopal, M., & Kumar, M. A. (2023). *A new lightweight data security system for data security in the cloud computing*. Measurement: Sensors, 29, 100856. https://doi.org/10.1016/j.measen.2023.100856.

Mohammed, C. M., & Zeebaree, S. R. (2021). *Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS*: A review. International Journal of Science and Business, 5(2), 17-30.

Mustafa Mohammed, C., & M Zeebaree, S. R. (2021). *Sufficient Comparison Among Cloud Computing Services: IaaS, PaaS, and SaaS*: A Review. International Journal of Science and Business, 5(2), 17–30.

Prasad, S. N., & Rekha, C. (2023). *Block chain based IAS protocol to enhance security and privacy in cloud computing*. Measurement: Sensors, 28, 100813. https://doi.org/10.1016/j.measen.2023.100813.

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Diaz, M. A. A. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana*. Propósitos y Representaciones, 8(3).

Sandhu, A. K. (2022). *Big Data with Cloud Computing: Discussions and Challenges*. Big Data Mining and Analytics, 5(1). https://doi.org/10.26599/BDMA.2021.9020016.

Soveizi, N., Türkmen, F., & Karastoyanova, D. (2023b). *Security and privacy concerns in cloud-based scientific and business workflows*: A Systematic review. Future Generation Computer Systems, 148, 184-

200. https://doi.org/10.1016/j.future.2023.05.015.

Suganya, M., & Sasipraba, T. (2023). *Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment*. Journal of Cloud Computing, 12(1). https://doi.org/10.1186/s13677-023-00442-6.

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., … Kim, K. I. (2021). *A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures and challenges*. Electronics (Switzerland), 10(15). https://doi.org/10.3390/electronics10151811.

ThiBac, D., & Minh, N. H. (2022b). *Design of network security storage system based on under cloud computing technology*. Computers & Electrical Engineering, 103, 108334. https://doi.org/10.1016/j.compeleceng.2022.108334.