INGENIERÍA INVESTIGA

Vol. 5, e796, año 2023
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v5i0.796

Artículo de revisión

Principales medidas de seguridad para la protección de información y datos en la nube: una revisión sistemática

Main security measures for the protection of information and data in the cloud: a systematic review

Alfredo José Lezcano Gil[1]
https://orcid.org/0000-0002-8318-0996

Percy Olivarez Geronimo Dionicio[2]
https://orcid.org/0009-0003-6248-7440

Alberto Carlos Mendoza De Los Santos[3]
https://orcid.org/ 0000-0002-0469-915X

Recibido: 27/03/2023
Aceptado: 28/06/2023
Publicado: 10/07/2023

[1,2,3]Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La Libertad, Perú

E-mail: [1]t533300220@unitru.edu.pe, [2]t1063300120@unitru.edu.pe, [3]amendozad@unitru.edu.pe

Facultad de Ingeniería
Publicación Oficial

Resumen

La revisión sistemática realizada se enfoca en identificar las principales medidas de seguridad para proteger la información y los datos en entornos de computación en la nube. El objetivo fue resaltar la importancia de implementar medidas sólidas de seguridad y explorar su aplicabilidad práctica. Mediante la metodología PRISMA, se seleccionaron artículos relevantes y se analizaron sus resultados. Los hallazgos destacan la importancia de políticas de contraseñas sólidas, control de acceso, la autenticación biométrica, multifactorial y el uso de cortafuegos. Además, se analizaron soluciones específicas como la gestión de claves SSH en AWS y la adopción del CASB para fortalecer la seguridad en la nube. Finalmente se determinó que el cifrado de datos, el control de acceso y la autenticación multifactorial son medidas cruciales para proteger la información en la nube. Estas medidas previenen violaciones de seguridad y garantizan la privacidad de los usuarios. Las aplicaciones prácticas incluyen políticas de contraseñas robustas, autenticación multifactorial y cifrado de datos.

Palabras clave: medidas de seguridad; computación en la nube; seguridad de la información; información en la nube; seguridad cibernética.

Abstract

The systematic review conducted focuses on identifying the main security measures to protect information and data in cloud computing environments. The objective was to highlight the importance of implementing robust security measures and explore their practical applicability. Relevant articles were selected and their results were analyzed through the PRISMA methodology. The findings emphasize the importance of strong password policies, access control, biometric and multifactor authentication, and the use of firewalls. In addition, specific solutions such as SSH key management in AWS and the adoption of CASB to strengthen cloud security were examined. Finally, it was determined that data encryption, access control, and biometric and multifactor authentication are crucial measures to protect information in the cloud. These measures prevent security breaches and ensure user privacy. Practical applications include robust password policies, multifactor authentication, and data encryption.

Keywords: security measures, cloud computing, information security, information in the cloud, cyber security.

1. Introducción

En los últimos años, la creciente implementación de sistemas de computación basados en la nube como modelo de entrega de servicios informáticos ha traído consigo numerosos beneficios para las organizaciones, como la reducción de costos, la escalabilidad y la flexibilidad en el acceso a recursos tecnológicos. No obstante, la seguridad de la información y los datos almacenados en la nube sigue siendo una preocupación importante, ya que cualquier tipo de acceso no autorizado podría poner en riesgo los datos confidenciales de una empresa (Castillo, 2015).

De acuerdo con Amazon Web Services (AWS), la seguridad en el entorno de la nube presenta similitudes con la seguridad en los centros de datos locales, con la excepción de no incurrir en los costos asociados al mantenimiento de instalaciones físicas y hardware. En lugar de gestionar servidores físicos y dispositivos de almacenamiento, en la nube se emplean herramientas de seguridad basadas en software para supervisar y salvaguardar el flujo de información que circula hacia y desde los recursos alojados en la nube. Por consiguiente, la seguridad en la nube constituye una responsabilidad compartida entre el cliente y la compañía proveedora de servicios.

Según estudio de Joyanes (2022) las razones para la adopción del modelo multinube son: una mayor seguridad, acceso fácil y rápido por parte del usuario a una variedad de contenidos, reducción de tareas internas relacionadas con infraestructuras, disminución en los gastos asociados a licencias para facilitar la adaptación a las regulaciones de distintos países.

Cisco (s.f.) destaca que en un mundo multinube, la conectividad es práctico, pero administrar los distintos entornos puede complicarse rápidamente. La implementación de soluciones de seguridad en la nube ofrece una capacidad integral para gestionar y salvaguardar todo el ecosistema de una organización, independientemente de si sus datos y aplicaciones residen en la nube, en infraestructuras locales o en una combinación de ambas. Esto implica que los servidores y sistemas de almacenamiento en el centro de datos, los dispositivos de Internet de las Cosas en almacenes, las computadoras portátiles remotas, los teléfonos móviles y todos los empleados en las sucursales pueden contar con una cobertura de seguridad proporcionada por soluciones en la nube.

La computación en la nube en términos simples significa almacenar y acceder a datos y programas a través de Internet en lugar del disco duro de nuestra computadora" (Rashid & Chaturvedi, 2019; NIST, 2011). De acuerdo a Ahmed et al. (2020) detalla los siguientes tipos de servicios que ofrece la nube: Infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).

Los riesgos que conllevan el uso de servicios en la nube son múltiples y van en incremento. Según Abbas et al. (2021), los riesgos más conocidos son: la restricción de servicios y acceso, las amenazas internas, la falta de actualización en seguridad de datos, la vulnerabilidad en computación en la nube compartida, la falta de experiencia del personal de TI, no tener un plan de recuperación ante desastres y pérdida de datos y poseer copias de seguridad inadecuadas.

En la tabla 1 se presentan los investigadores que se enfocaron en un método de seguridad y encontraron que dicho método cumplía con ciertos objetivos de seguridad de la información en la nube.

Tabla 1

Medidas de seguridad propuesta por autores según los objetivos que cumple

	Esquemas	Objetivos de seguridad en la nube												
		SG1	SG2	SG3	SG4	SG5	SG6	SG7	SG8	SG9	SG10	SG11	SG12	SG13
1	Walsh and Manferdelli	Sí	Sí	Sí	No	Sí	Sí	No	No	No	Sí	Sí	No	Sí
2	Khodabacchus et al.	Sí	Sí	Sí	Sí	Sí	No	No	No	No	Sí	Sí	No	Sí
3	Huszti and Olah	Sí	Sí	Sí	No	Sí	No	Sí	No	No	Sí	No	No	Sí
4	Moghaddam et al.	Sí	Sí	Sí	No	No	Sí	No	No	No	No	No	No	No
5	Maitiri and Verma	Sí	Sí	Sí	No	No	Sí	No	No	No	No	No	No	No
6	Hitaswi and Chandrasekaran	Sí	Sí	Sí	No	No	Sí	No	No	No	No	No	No	No
7	Karame et al.	Sí	Sí	Sí	No	No	Sí	No	No	No	No	No	No	Sí
8	Kotlarz and Kutulsk	Sí	Sí	Sí	No	No	Sí	No	No	No	No	Sí	No	No
9	Zhang et al.	Sí	Sí	Sí	No	No	Sí	Sí	No	No	Sí	No	Sí	Sí
10	Mislovaty et al.	Sí	Sí	Sí	No	No	Sí	No	No	No	No	No	No	Sí
11	Abadi and Andersen	No	Sí	Sí	No	No	Sí	No	No	No	No	No	Sí	No
12	Volna et al.	No	Sí	Sí	No	No	Sí	Sí	No	No	Sí	No	Sí	Sí
13	Wang and Wang	Sí	Sí	Sí	Sí	No	Sí	No	No	No	Sí	No	No	Sí

Nota. Obtenido de Sheik y Muniyandi (2023) donde SG1=Autenticación; SG2=Confidencialidad de datos; SG3= Integridad de datos; SG4=Responsabilidad; SG5=Certificados de seguridad; SG6= Gestión de claves; SG7=Ataque de denegación de servicio; SG8=Transparencia de datos; SG9= Recuperación de datos; SG10=Ataque de intermediario; SG11=Suplantación; SG12=Interrupción; SG13=Ataque malicioso.

El objetivo de la investigación es realizar una revisión sistemática para proporcionar información actualizada, evaluación crítica y orientación en el campo de la seguridad de la información en la nube, con el propósito de responder a la siguiente pregunta: ¿Cuáles son las principales medidas de seguridad para proteger la información y los datos en la nube?

2. Metodología

2.1. Tipo de estudio

Para esta revisión sistemática se usó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) como marco de referencia, en el cual permite organizar y analizar todos los artículos relacionados al tema para poder sintetizar y dar una respuesta más clara. El propósito de la revisión sistemática fue indagar acerca de la siguiente interrogante: ¿Cuáles son las principales medidas de seguridad para proteger la información y datos en la nube?

2.2. Fundamentos de la metodología

Al utilizar la metodología PRISMA en esta revisión sistemática sobre las medidas de seguridad fundamentales para proteger la información en la nube, se establecen criterios específicos y

rigurosos para la selección de artículos pertinentes. Esto contribuye a mejorar la validez, integridad y credibilidad de los resultados obtenidos en el estudio.

La revisión sistemática implica llevar a cabo la evaluación e interpretación exhaustiva de toda la investigación disponible, lo cual resulta crucial para abordar de manera integral en una pregunta de investigación específica o del área de interés (Manterola, 2013). Además, el uso de PRISMA facilita la comparación de los resultados obtenidos con otras revisiones sistemáticas y meta-análisis en el mismo campo, lo que permite la integración de los resultados de distintas investigaciones.

2.3. Criterios de inclusión y exclusión

En el desarrollo de este estudio se consideraron únicamente publicaciones a partir del año 2018, dado que la tecnología está en constante evolución y es importante tener en cuenta las investigaciones más actualizadas. Además, se incluyeron publicaciones en inglés o español, ya que ambos idiomas son ampliamente reconocidos en el ámbito de la tecnología y la ciencia. Por último, los temas abordados en los artículos estaban relacionados con las medidas de seguridad en la nube.

Para asegurar la selección de los estudios más relevantes y confiables, se estableció excluir investigaciones presentadas en formato de diapositivas y ejemplares. Estos formatos no proporcionan la certeza necesaria en cuanto a la información empleada. Adicionalmente, se consideró descartar publicaciones que se clasifican como "lecturas grises", es decir, escritos no divulgados de manera adecuada. La implementación de estos criterios garantizó la calidad y fiabilidad de los artículos seleccionados para esta revisión sistemática.

2.4. Proceso de recolección de información

El proceso de búsqueda combinó términos relevantes para la pregunta de investigación, fueron: "cloud computing", “security measures” “information security”, “cybersecurity" entre otros como se detalla en la tabla 2. La búsqueda se realizó en bases de datos reconocidas con grandes cantidades de artículos, tales como: Google académico, IOPScience y ScienceDirect. Luego se aplicaron los criterios de inclusión y exclusión que fueron definidos en el punto 2.3 y 2.4 de los cuales se seleccionaron los artículos que se alineaban a la investigación.

Tabla 2

Términos de búsquedas en base de datos

Base de datos	Términos de búsqueda	Seleccionados
Google Académico	"cloud" AND "security" AND "measures" AND "cybersecurity" AND "information" AND "Data privacy" AND "Cloud computing" AND "information in the cloud"	6
ScienceDirect	"cloud computing") AND ("security measures"	8
IOPScience	"cloud computing") AND ("security measures"	3

Tal como se aprecia en la tabla 2, las bases de datos académicas que aportan más información para la investigación fueron google académico y ScienceDirect.

3. Resultados

Tras un exhaustivo análisis de los artículos seleccionados, en la tabla 3 se muestra las principales medidas de seguridad recopilado.

Tabla 3

Resultados de los artículos analizados

ID	Autores	Descripción	Medidas de protección
A1	Omaza, K. (2020)	Describe una evaluación de seguridad llevada a cabo en una empresa mediana que ofrece servicios de financiación en línea. El enfoque principal de la evaluación fue a la plataforma en la nube de Amazon Web Services (AWS). El informe resalta los riesgos identificados, se hace hincapié en la importancia de mitigar los riesgos y fortalecer la seguridad de la infraestructura en la nube de la organización.	- Autenticación multifactorial. - Aplicación a los segmentos. - Utilizar subredes públicas y privadas. - Uso de cortafuegos o listas de control de acceso (ACL). - Denegar el acceso según la dirección IP de origen. - Segregación de cuentas. - Despliegue de la gestión de claves SSH en AWS. - Implementación de la solución CASB.
A2	Sivan, R. & Zukarnain, Z. (2021).	La computación en la nube ha transformado la atención médica, pero también plantea desafíos de seguridad y privacidad. Este estudio revisó la literatura existente sobre el uso de técnicas avanzadas en la salud, identificando modelos y evaluando fortalezas y debilidades. Se destacó la importancia de abordar la gestión, seguridad y problemas legales asociados con la computación en la nube en el ámbito de la salud.	- PKE (cifrado de clave pública) - SKE (cifrado de clave simétrica). - Programas de encriptación de transmisiones. - Cifrado calificado. - Cifrado basado en blockchain. - Cifrado simétrico con capacidad de búsqueda. - Administrador de control de acceso (AAM). - Blockchain privado completo (FPB) - Blockchain de consorcio (CB). - Métodos de control de acceso (RBAC, ABAC,MAC, IBAC).
A3	Ahmed, U., Mehmood, M., Hussain, S., Amin, R., Waqas, M., Mohsan, S., Young, D., Piran, J. (2020).	El artículo afirma que tanto Computación en la nube (CC) como la computación en el borde presentan desafíos de seguridad que dificultan su adopción. El aprendizaje automático (ML) es el estudio de algoritmos informáticos que mejoran con la experiencia. En este artículo, se analizan las amenazas, problemas y soluciones de seguridad de CC utilizando algoritmos de ML.	Algoritmos de Machine Learning (ML) para la seguridad en la nube: - RNA supervisadas - Algoritmo K-NN - Bayesiana ingenua - Algoritmo SVM - ANN no supervisadas - K-medias - Descomposición de valores singulares (SVD)

Tabla 3 (continuación/1)

ID	Autores	Descripción	Medidas de protección
A4	Chenthara, S., Ahmed, K., Wang, H., Whittaker, F. (2019).	La investigación se ha centrado en ciberseguridad en la nube, requisitos de seguridad y privacidad de los datos de salud electrónica (EHR) en la nube. se identifica soluciones de salud electrónica para preservar la seguridad y privacidad de los registros.	- Mecanismos criptográficos: SKE, PKE, ABE, SSE - encriptación de proxy - cifrado homomórfico, etc. - Mecanismos no criptográficos.
A5	Orantes, S., Aguirre, E. (2021)	Este artículo aborda los riesgos de seguridad asociados con el almacenamiento y procesamiento de datos en la nube. También menciona varias técnicas de cifrado que se utilizan para fortalecer la seguridad en este entorno. Se enfatiza la importancia de que los usuarios comprendan los riesgos y tomen medidas para proteger sus datos en la nube	- Cifrado Vigenère. - Cifrado de juegos limpios. - Cifrado de la colina. - Cifrado Vernam. - Esquemas de cifrado de proxy. - Cifrado RailFence.
A6	Telo, J. (2023)	El estudio se afirma que las ciudades inteligentes están utilizando tecnologías emergentes como el IoT, la computación en la nube, el análisis de big data y la inteligencia artificial. Además, destaca la importancia de abordar los desafíos de seguridad en las ciudades inteligentes y ofrece recomendaciones para desarrollar estrategias de seguridad efectivas.	- Autenticación multifactor (MFA) - Controles de acceso - Sistemas de cifrado solidos - Auditorias regulares - Capacitación de empleados - Sistemas de detección de intrusos
A7	Eddermoug, N., Mansour, A., Azmi, M. et al (2023)	El estudio afirma que la computación en la nube está sujeta a ataques de seguridad. Su objetivo es proporcionar soluciones ampliamente existentes para prevenir y perfilar ataques de seguridad en la computación en la nube, así como sus limitaciones para detectar ataques (des)conocidos.	- Sistemas de detección (IDS) - Sistemas de prevención de intrusos (IPS) - Sistemas OTP - Técnicas de autenticación fuerte - Técnica de K-medias
A8	Mohamad M., Divya M (2022).	El artículo se realiza una revisión de la literatura sobre el uso de algoritmos de aprendizaje automático y aprendizaje profundo como técnicas de seguridad en la nube. Es más, presenta una taxonomía de los distintos tipos de ataques y amenazas en las capas de seguridad de la nube, así como las defensas generales contra estos ataques. Se discuten las limitaciones de las técnicas de seguridad tradicionales para analizar cómo proteger los entornos de la nube de ataques y desafíos.	- Máquinas de vectores de apoyo (SVM) - Técnica de K-Nearest Neighbor(KNN), usada para problemas de clasificación y regresión. - Técnica de Random Forest (RF), Se basa en conceptos de aprendizaje conjunto - Técnica de decisión Tree (DT) basado en aprendizaje automático (Machine learning) - Algoritmo de Recurrent Neural Network (RNN)

Tabla 3 (continuación/2)

ID	Autores	Descripción	Medidas de protección
A9	Abdulkader, Z. (2022)	Se describe que la computación en la nube tiene problemas fundamentales en términos de confidencialidad, integridad, disponibilidad, autorización, entre otros. Además, se investiga sobre las opciones disponibles para asegurar la información.	Mecanismo de "Criptografía ligera" - Algoritmo AES - Algoritmo DES Algoritmo triple DES
A10	Sheik y Muniyandi (2023).	La seguridad en la nube juega un rol esencial para establecer la confianza entre los proveedores de servicios en la nube, los consumidores y los usuarios, asegurando niveles adecuados de protección de datos. Este artículo se enfoca en examinar los desafíos de seguridad en la nube a través de una encuesta, explorar los esquemas de autenticación existentes y las tecnologías de almacenamiento de datos, y proporcionar una visión general sobre la aplicación de Redes Neuronales Artificiales (ANNs) en el contexto de la seguridad en la nube.	- El inicio de sesión único (SSO). - Seguridad de autenticación de 2 capas - Esquema de autenticación - Autenticación de usuario con dos agentes. - Algoritmo híbrido de cifrado, descifrado y esteganografía. - Esquema Bastión - Esquema todo o nada (AON) - Algoritmo Estándar de cifrado avanzado (AES) - Esquema de aplicación de la S-Box - Esquema cifrado basado en redes neuronales
A11	Kumar, R., Raj, H., Jelciana P. (2018)	La computación en la nube se posiciona como una de las tecnologías en rápido crecimiento en el campo de la informática. Aunque presenta diversas ventajas, también plantea desafíos en términos de seguridad. El presente estudio examina los distintos problemas de seguridad de datos asociados a la computación en la nube en un entorno de múltiples inquilinos, y propone enfoques para mitigar dichos problemas y fortalecer la seguridad en este ámbito.	- Control de acceso - Autenticación - Cifrado de datos - Métodos de encriptación - Auditoría de terceros (TPA) - Posesión de datos comprobables (PDP) - Gestión de identidad y acceso (IAM) - Copias de seguridad o duplicación de datos.
A12	Mishara, A., Alzoubi, Y., Anwar, M. & Gil, A. (2022)	Indican que el incremento en el uso de Internet ha resultado en un aumento de las amenazas cibernéticas. Por esta razón, las organizaciones deben implementar políticas de ciberseguridad eficaces, así como también los gobiernos deben tener regulaciones eficientes de ciberseguridad para las empresas que salvaguarden información.	- EE. UU, India y Malasia regulan a las empresas con medidas de seguridad de TI, como antivirus y cortafuegos para proteger sus datos. - En Australia, cuenta con una ley de privacidad y protección de datos.
A13	Yonghong, L., Ruifeng, L., Xiaoyu, L., Hong, L. & Qingwen, S.(2021)	Se presenta un enfoque sofisticado para evaluar los riesgos de seguridad de la información utilizando árboles de decisión y también presenta las medidas de seguridad en la comunicación de datos basados en algoritmos de computación en la nube	- Cifrado en la capa de red - Cifrado en la capa de aplicación - Tecnologías de autenticación - Tecnologías para Detección de intrusos - Protección activamente contra virus informático

Tabla 3 (continuación/3)

A14	Kun, H.(2021)	El artículo se centra principalmente en analizar y explorar cómo asegurar la protección de los datos empresariales y personales en la nube. Se abordan temas como la seguridad de la información, desde enfoques defensivos hasta la vigilancia y la respuesta activa.	- Verificación múltiple para evitar vulnerabilidades y prevenir intrusión ilegal de hackers - Autenticación múltiple para evitar que visitantes ilegales roben y destruyan datos de información - Inteligencia artificial para análisis de seguridad y procesamiento
A15	Abbas, H., Jaaz, Z., Al_Barazanchi, I. & Abdulshaheed, H. (2021).	El documento se centra en los diversos aspectos de la nube y sus características de seguridad, así como en cómo se pueden mejorar estas características. Algunas medidas de seguridad implican actualizar y regular los términos y condiciones de la nube, mientras que otras incluyen múltiples métodos de autorización y acceso controlado a los servicios en la nube.	- Autenticación biométrica - Clave de acceso aleatorio - Sistemas de copia de seguridad y cifrado de datos - Auditorías y actualizaciones de seguridad
A16	Abiodun, O., Alawida, M., Omolara, A & Alabdulatif, A. (2022).	El estudio proporciona una revisión de los problemas actuales en cuanto a la trazabilidad de los datos en el ámbito de la computación en la nube, una taxonomía de la procedencia y cuestiones de seguridad asociadas.	- Redes de sensores inalámbricos - Blockchain - Apoyo en Internet de las cosas (IoT) - Políticas de control de acceso.
A17	Amamou, S., Trifa, Z., Khmakhem, M. (2019)	El documento aborda los riesgos potenciales que los datos pueden enfrentar durante su transferencia y recuperación en la nube. Se examinan varios ataques conocidos y se analizan las ventajas y desventajas de diferentes técnicas propuestas en la literatura para mitigar los impactos de estos ataques.	- Anonimización de K-anonimato - Anonimización L-diversidad - Anonimización T-proximidad - Tokenización basada en bóveda - Tokenización sin bóveda - Cifrado de clave simétrica - Cifrado de clave asimétrica

De la tabla 3 se puede observar que hay medidas de seguridad que coinciden entre los autores en estudio. En base a ello, el número de artículos que abordan las principales medidas de seguridad se divide en las siguientes categorías: cifrado de datos (13), control de acceso (13), autenticación biométrica y multifactorial (8), machine learning (7) y criptografía basada en blockchain (5).

4. Discusión

En cuanto a las medidas de protección propuestas, se observa que existe una diversidad de enfoques abordados por los investigadores. Entre las medidas más destacadas se encuentran: la implementación de políticas de contraseñas y autenticación multifactorial, el uso de cortafuegos o listas de control de acceso, el cifrado de clave pública y clave simétrica, así como el uso de algoritmos de Machine Learning (ML) para aumentar la seguridad en la nube.

En relación al cifrado, se evidencia su importancia como medida fundamental para proteger la confidencialidad de los datos. Sivan y Zukarnain (2021) mencionan diferentes técnicas criptográficas, como el cifrado de clave pública y clave simétrica, así como programas de encriptación de transmisiones. Por otro lado, Orantes y Aguirre (2021) proponen esquemas de cifrados específicos, como el cifrado Vigenère y el cifrado de la colina.

Otro aspecto relevante identificado en esta comparativa es la necesidad de implementar mecanismos de control de acceso y autenticación robustos. Telo (2023) resalta la importancia de la autenticación multifactorial y los controles de acceso, mientras que Sheik y Muniyandi (2023) proponen medidas como la autenticación dentro y fuera de la nube, algoritmos híbridos de cifrado y el inicio de sesión único.

Además, se destaca la importancia de contar con sistemas de detección y prevención de intrusos, así como técnicas de autenticación fuerte, como mencionado por Eddermoug et al. (2023). Estas medidas contribuyen a fortalecer la seguridad en la nube y proteger los datos contra posibles amenazas.

En términos de tendencias emergentes, se identifica el uso de tecnologías como el Machine Learning (ML) y la inteligencia artificial (IA) para mejorar la seguridad en la nube. Ahmed et al. (2020) proponen el uso de algoritmos de ML, como SVM y K-Nearest Neighbor. Mientras que, Kun (2021) destaca el uso de inteligencia artificial para el análisis de seguridad y procesamiento.

Para fomentar el avance del conocimiento en el campo de la seguridad en la nube, es plausible investigar sobre el uso de tecnologías emergentes como el blockchain, internet de las cosas, Machine Learning y entre otros; debido a que son tecnologías nuevas y se estima que son medidas de seguridad altamente eficaces para la nube.

5. Conclusiones

Mediante la evaluación comparativa de las diferentes medidas de seguridad propuestas por los autores analizados, se han identificado medidas y estrategias eficientes para la protección de datos en la nube por lo cual se concluye que las principales medidas de protección son las políticas de contraseñas y autenticación multifactorial, el uso de cifrado de clave pública y clave simétrica, así como el empleo de técnicas de Machine Learning para fortalecer la seguridad.

Además, se ha resaltado la importancia de contar con mecanismos de control de acceso y sistemas de detección de intrusos, así como el uso de tecnologías emergentes como el blockchain para proteger los datos en la nube.

Asimismo, para mejorar la seguridad tanto para usuarios finales como para organizaciones y empresas es altamente recomendable seguir las siguientes medidas: hacer uso de contraseñas seguras que combinen letras mayúsculas y minúsculas, números y caracteres especiales. Las organizaciones deben educar a sus clientes sobre la importancia de cambiar regularmente sus contraseñas y no utilizar contraseñas comunes o fáciles de adivinar. Emplear la autenticación en dos o más pasos, como el envío de un código de verificación a través de un dispositivo móvil, junto con la contraseña, para acceder a los recursos en la nube. Utilizar técnicas de cifrado tanto para el almacenamiento como para la transmisión de datos en

la nube. Esto garantiza que, si los datos son interceptados, no puedan ser accedidos sin la clave de cifrado correspondiente.

Por último, en el estudio se enfatiza la importancia de implementar medidas de seguridad sólidas y adaptadas a las necesidades específicas de cada entorno en la computación en la nube. Al aplicar las medidas recomendadas y mantenerse al tanto de las tendencias y avances en seguridad, las organizaciones podrán proteger eficazmente sus datos en la nube y mitigar los riesgos asociados.

6. Referencias Bibliográficas

Abbas, H., Jaaz, Z., Al Barazanchi, I., & Abdulshaheed, H. (2021). Survey on Enhanced Security Control measures in Cloud Computing systems. Journal of Physics: Conference Series, 1878, 012004. https://doi.org/10.1088/1742-6596/1878/1/012004

Abiodun, O., Alawida, M., Omolara, A & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey, Journal of King Saud University - Computer and Information Sciences, (Vol 34, Pag 10217-10245). https://doi.org/10.1016/j.jksuci.2022.10.018

Abdulkader, Z. (2022). Cloud data security mechanism using the lightweight cryptography. Optik, 271, 170084. https://doi.org/10.1016/j.ijleo.2022.170084

Ahmed, U., Mehmood, M., Hussain, S., Amin, R., Waqas, M., Mohsan, S., Young, D., & Piran, J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. Electronics, 9, 1379. https://doi.org/10.3390/electronics9091379

Amamou, S., Trifa, Z., Khmakhem, M. (2019). Data protection in cloud computing: A Survey of the State-of-Art. Procedia Computer Science, (Vol. 159, p. 155-161). https://doi.org/10.1016/j.procs.2019.09.170

Amazon Web Services. Security Learning. Consultado el 20/06/2023. https://n9.cl/nwhs9

Belal, M. M., & Sundaram, D. M. (2022). Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. Journal of King Saud University - Computer and Information Sciences, 34. https://doi.org/10.1016/j.jksuci.2022.08.035

Cisco. ¿Qué es seguridad en la nube? Consultado el 18/06/2023. https://n9.cl/ztlay

Castillo H. (2015). Seguridad en cloud computing. http://repository.unipiloto.edu.co/handle/20.500.12277/2929

Eddermoug, N., Mansour, A., Azmi, M., Sadik, M., Sabir, E., & Bahassi, H. (2023). A Literature Review on Attacks Prevention and Profiling in Cloud Computing. Procedia Computer Science, 220, 970-977. https://doi.org/10.1016/j.procs.2023.03.134

Joyanes L. (2022). Computación en la nube. https://n9.cl/79xx0

Kumar, R., Raj, H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. https://doi.org/10.1016/j.procs.2017.12.089

Kun, H.(2021).Information Security Problems and Solutions in Cloud Era.Journal of Physics: Conference Series,2066,012005. https://doi.org/10.1088/1742-6596/2066/1/012005

Manterola C. (2013). Revisiones sistemáticas de la literatura. Qué se debe saber acerca de ellas. https://doi.org/10.1016/j.ciresp.2011.07.009

Mishra, A., Alzoubi, Y., Anwar, A., Gill, A. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security,120, 102820, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2022.102820

National Institute of Standards and Technology. (2011). Cloud Computing [Special Publication 800-145]. https://doi.org/10.6028/NIST.SP.800-145

Omaza, K. (2020). Arquitectura de Seguridad en la nube: Revisión de la Implementación en AWS(Trabajo de fin de grado,Universidad politécnica de madrid). https://oa.upm.es/58279/1/TFG_KIYOSHI_JOSE_OMAZA_SALDANA.pdf

Orantes Jiménez, Sandra Dinora, & Aguirre Anaya, Eleazar. (2020). A Survey on Information Security in Cloud Computing. Computación y Sistemas, 24(2), 819-833. Epub 04 de octubre de 2021.https://doi.org/10.13053/cys-24-2-3119

Rashid Aaqib, Chaturvedi Amit, (2019). Cloud Computing Characteristics and Services: A Brief Review. International Journal of Computer Sciences and Engineering, 7(2), 421-426. https://doi.org/10.26438/ijcse/v7i2.421426

S. Chenthara, K. Ahmed, H. Wang and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," in IEEE Access, vol. 7, pp. 74361 74382, 2019, https://doi.org/10.1109/ACCESS.2019.2919982.

Sheik, S. A. & Muniyandi, A. P. (2023). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. Cyber Security and Applications, 1, 100002. https://doi.org/10.1016/j.csa.2022.100002

Sivan, R. & Zukarnain, Z. (2021). Security and Privacy in Cloud-Based E-Health System.Symmetry,13,5. https://doi.org/10.3390/sym13050742

Telo, J. (2023). Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing, 6(1), 31–45. https://research.tensorgate.org/index.php/IJIAC/article/view/18

Yonghong Li, Ruifeng Liu, Xiaoyu Liu, Hong Li and Qingwen Sun.(2021).Research on Information Security Risk Analysis and Prevention Technology of Network Communication Based on Cloud Computing Algorithms. Journal of Physics: Conference Series, (Vol. 1982, p.12129). https://doi.org/10.1088/1742-6596/1982/1/012129