COMPUTATION E INFORMATICA

Recibido 03 OCT. 2023 *ReCIBE, Año 12 No.2, NOV. 2023*

Aceptado 24 OCT. 2023

Implementaciones actuales del modelo confianza cero para entornos en la nube: una revisión sistemática

Current implementations of the zero trust model for cloud environments: a systematic review

Johann Castillo Oliva[1]

Bruno Hiroshi Espinosa Luna[1]

Alberto Carlos Mendoza de los Santos[1]

[1]Universidad Nacional de Trujillo

Resumen

La expansión de la computación en la nube en las organizaciones modernas enfrenta nuevos desafíos de seguridad de la información, en consecuencia, surge el paradigma de Confianza Cero como un método de reforzamiento para entornos en la nube. En relación a ello, esta revisión sistemática busca abordar dos preguntas de investigación: ¿Cuáles son las herramientas y procedimientos empleados en los últimos 5 años en las implementaciones de Confianza Cero para entornos de la nube? y ¿Cuáles son los métodos de evaluación utilizados en el modelo de Confianza Cero para entornos de la nube? Bajo la metodología PRISMA 2020, se analizaron 13 estudios de las bases de datos bibliográficas Scopus y Dimensions donde se destacan herramientas como blockchain, algoritmos criptográficos y modelos integrales de confianza, además de métodos de validación como pruebas de funcionalidad y análisis de seguridad. Por último, se da a conocer la falta de un método de evaluación uniforme para las aplicaciones del modelo Confianza Cero en la computación en la nube.

Palabras clave: control de accesos, seguridad de la información, seguridad de la nube, políticas de control, innovaciones

Abstract

The expansion of cloud computing in modern organizations faces new information security challenges; consequently, the Zero Trust paradigm emerges as a reinforcement method for cloud environments. In this regard, this systematic review aims to address two research questions: What are the tools and procedures employed in the last 5 years in Zero Trust implementations for cloud environments? And what evaluation methods are used in the Zero Trust model for cloud environments? Under the PRISMA 2020 methodology, 13 studies from the Scopus and Dimensions bibliographic databases were analyzed, highlighting tools such as blockchain, cryptographic algorithms, and comprehensive trust models, as well as validation methods such as functionality tests and security analysis. Finally, it is highlighted that there is a lack of a uniform evaluation method for Zero Trust model applications in cloud computing.

Keywords: Access control, information security, cloud security, control policies, innovations

1. Introducción

La computación en la nube (CN en adelante) ha sido ampliamente adoptada por organizaciones modernas en los últimos años, abarcando desde pequeñas empresas emergentes hasta las más grandes (Guo et al., 2023; Lawan et al., 2021). Esta tendencia radica en los beneficios tangibles e intangibles que ofrece, como la reducción de costos operativos y de mantenimiento, ahorro de espacio, optimización de recursos, mayor escalabilidad y flexibilidad, aumento de satisfacción de empleados, entre otros. Además, factores recientes, como el incremento del trabajo remoto impulsan la adopción de un entorno en la nube (Bajdor, 2022; Mandal et al., 2021; Shetty & Rajesh, 2021; Zheng et al., 2023).

Sin embargo, a medida que la CN se populariza en las organizaciones modernas, surgen nuevas vulnerabilidades y amenazas para la seguridad de la información. Por lo tanto, resulta necesario fortalecer ciertos aspectos, incluyendo controles de acceso y la autenticación de usuarios (Akbar et al., 2023; Cheng et al., 2022; Gill et al., 2022). Adicionalmente, un factor importante para asegurar la integridad de los datos en la nube es el seguimiento de buenas prácticas por parte de los clientes (George & Sagayarajan, 2023).

En este contexto, surge el modelo de Confianza Cero (CC) como una propuesta para mejorar la seguridad de los servicios en la nube, dejando como complemento a los mecanismos pasivos de seguridad (Chen et al., 2021; S. Liu et al., 2022). El paradigma CC se basa en una postura de desconfianza, incluso de aquellos usuarios o dispositivos que pertenecen a la red de una organización estableciendo un nivel de seguridad a nivel de aplicación (Ali et al., 2022; Z. Liu et al., 2022; Rose et al., 2020), lo que conlleva a que sea considerado uno de los marcos más rigurosos para el control de acceso, especialmente cuando se complementa con tecnologías como *blockchain* y *machine learning* (Feng et al., 2023; Li et al., 2023; Rajasoundaran et al., 2021).

Expuestas estas ideas, con el objetivo de dar a conocer nuevas estrategias para fortalecer la seguridad de la información en un contexto de crecimiento en la adopción de la CN, se plantea la siguiente pregunta de investigación: ¿Cuáles son las herramientas y procedimientos que se usaron en los últimos 5 años en las implementaciones del modelo confianza cero para entornos de la nube?

Además, se destaca la importancia de validar estas herramientas y procedimientos a través de un proceso riguroso para garantizar la validez de sus resultados. Lo que conduce a la segunda pregunta de investigación: ¿Cuáles son los métodos de evaluación de las herramientas y procedimientos utilizados en el modelo confianza cero para entornos de la nube? Con esta pregunta, se busca determinar cómo se puede garantizar la efectividad y utilidad de estas herramientas y métodos analizados.

2. Metodología

2.1. Fundamentación de la metodología

La realización de esta revisión sistemática se basó en la declaración de la metodología PRISMA 2020 (Page et al., 2021), que establece un conjunto de pautas para la elaboración de estudios rigurosos con el fin de recopilar evidencia empírica y desarrollarla de forma estructurada para mejorar la calidad, transparencia y el valor de la literatura científica (Sohrabi et al., 2021).

La estructura de PRISMA consta de 27 ítems, los cuales orientaron la organización del estudio en las secciones: título, resumen, introducción, métodos, resultados, discusión y conclusiones. Siguiendo esta estructura, la redacción de la revisión empezó con el título, donde se identificó claramente el estudio como una revisión sistemática. Luego, en la introducción se dio a conocer la justificación del estudio y se presentaron las preguntas de investigación a ser abordadas.

En la sección de métodos, se describieron los criterios de inclusión y exclusión donde se realizó la eliminación de estudios duplicados y de poca relevancia, así como la selección de estudios que cumplieron el rango de antigüedad de 5 años para la revisión. También se detallaron las fuentes de información utilizadas, la estrategia de búsqueda aplicada en cada una de ellas, así como el procedimiento de selección y síntesis.

Todo esto con el objetivo de recolectar la información más relevante para dar respuesta a las preguntas de investigación planteadas. Además, esta información constituyó una base para la redacción de los resultados, discusión y conclusiones, secciones donde se llevó a cabo el resumen e interpretación general de los hallazgos. Finalmente, se presentaron las recomendaciones para futuras investigaciones.

2.2. Criterios de elegibilidad

La selección de estudios se realizó siguiendo criterios específicos con el propósito de identificar artículos relevantes para la temática de investigación y que fueran útiles para abordar las preguntas de investigación. Los criterios de inclusión se basaron en: (i) estudios que son de tipo artículo o artículos de conferencia, (ii) escritos en idioma inglés o español y (iii) publicados en el rango de tiempo entre 2019 y 2023. A su vez, se definieron como motivos de exclusión: (i) publicaciones no sometidas a revisión por pares de doble ciego, (ii) que no se centran en herramientas o implementaciones destinadas a entornos en la nube y (iii) estudios cuya temática se enfoca únicamente en modelos de evaluación para la arquitectura de CC en la nube.

2.3. Fuentes de información y estrategia de búsqueda

Las bases de datos seleccionadas como fuentes de información fueron *Scopus* y *Dimensions* consultadas por última vez el 7 de septiembre de 2023. La búsqueda se realizó en grupos de términos aplicados en los títulos, resúmenes y palabras clave relacionados con el tema central de la investigación, que fueron "Zero Trust" y "Cloud Computing". Además, con el fin de obtener resultados con mayor enfoque en la temática de investigación, se utilizaron los operadores booleanos "*OR*" y "*AND*", lo que resultó en las búsquedas específicas para cada base de datos que se detallan en la Tabla 1.

Base de datos	**Términos de búsqueda**
Scopus	TITLE-ABS-KEY ("Zero Trust" OR "Zero Trust security") AND (cloud AND (computing OR security OR environment OR infrastructure))
Dimensions	TITLE-ABS ("Zero Trust" OR "Zero Trust security" OR "Confianza Cero") AND ("cloud computing" OR "cloud security" OR "cloud environment" OR "cloud infrastructure" OR "computación en la nube" OR "entorno en la nube")

Tabla 1. Términos de búsqueda empleados

2.4. Proceso de selección

La selección de estudios se llevó a cabo de forma independiente por los autores, utilizando hojas de cálculo en el software Excel como herramienta de automatización. Esto permitió la eliminación de registros duplicados y el seguimiento de la exclusión progresiva de los artículos de acuerdo con los criterios de elegibilidad. Para ello, se crearon diferentes hojas de cálculo para registrar la exclusión de los artículos en cada una de las tres fases del diagrama de flujo de PRISMA: identificación, cribado e inclusión.

2.5. Extracción de datos y síntesis

La información se extrajo siguiendo un proceso sistemático, utilizando como herramienta de automatización el software Excel donde se emplearon tablas dinámicas para tabular los resultados de los estudios y su síntesis. En esta tabla se incluyeron los siguientes campos: título, año, enlace, tipo de documento, base de datos fuente, país, herramientas y procedimientos, y métodos de evaluación.

Adicionalmente, se utilizó la herramienta Zotero como gestor bibliográfico y biblioteca compartida donde fueron almacenados los artículos revisados. El software fue seleccionado con el fin aprovechar las funcionalidades para almacenar síntesis y otras anotaciones para cada artículo en la biblioteca de grupo, de tal forma que estas puedan ser revisadas de forma conjunta entre los autores.

3. Resultados

Se identificaron un total de 227 registros en las bases de datos bibliográficas consultadas, de los cuales se recuperaron 33 registros para realizar una revisión más detallada del contenido. Inicialmente, se consideraron estudios de potencial interés para la revisión; sin embargo, se descartaron aquellos que eran estudios enfocados en analizar otras propuestas de implementación del modelo CC como artículos de revisión (Divya & Sherin, 2022; Justice & Sample, 2022; Teodoro, 2022), ya que se buscaron estudios originales con un enfoque específico en herramientas y métodos de implementación. Además, se descartó un estudio cuya propuesta de implementación no estaba realmente dirigida a un entorno en la nube (Paul & Rao, 2023). Finalmente, se obtuvo una muestra de 13 artículos para la revisión como se muestra en la Figura 1.

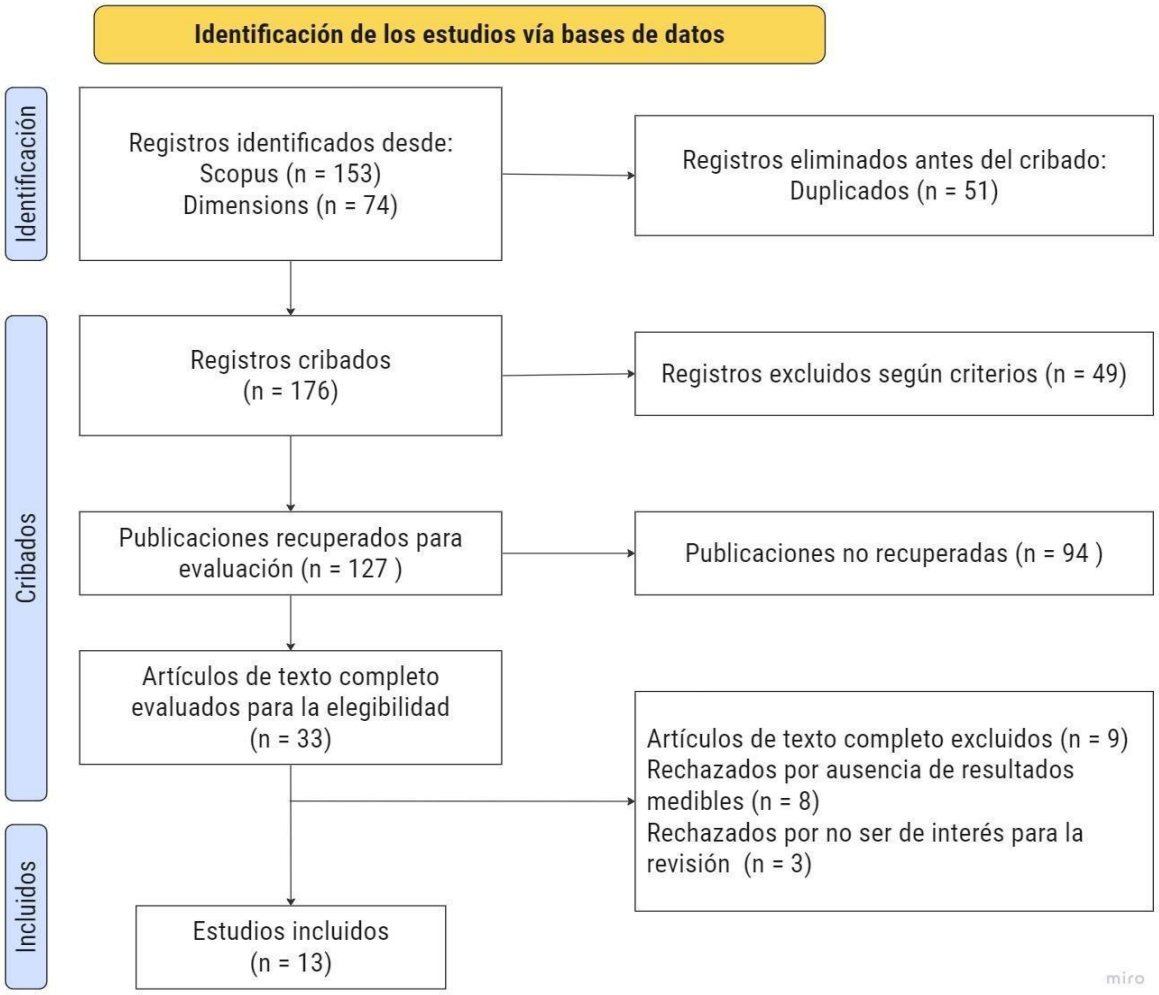

Figura 1. Diagrama de flujo de selección de estudios

Del total de artículos incluidos, 12 provienen de la base de datos Scopus y 1 de Dimensions. Los artículos se caracterizan por ser publicados desde el año 2021, siendo ese mismo el que presenta más publicaciones sobre el tema (38.46%). Mientras que en los años 2022 y 2023 se encontraron 4 artículos por año, representando cada uno el 30.77% del total, como se muestra en la Figura 2.

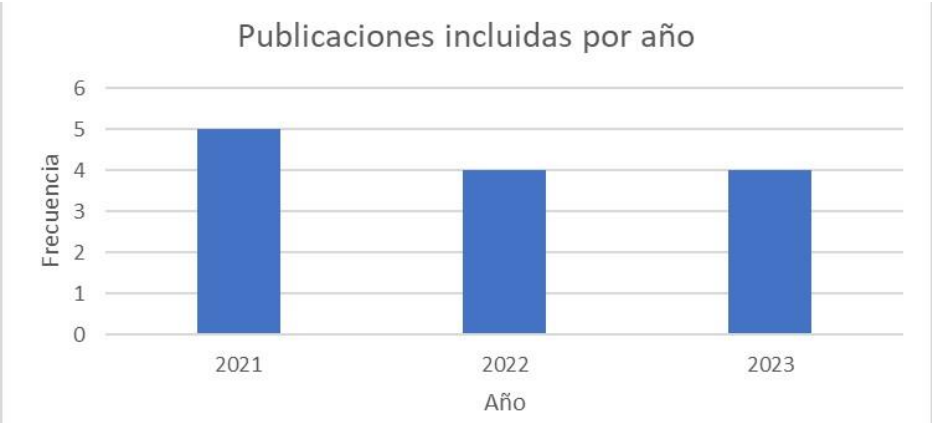

Figura 2. Publicaciones incluidas por año

Respecto al origen de las publicaciones como se detalla en la Figura 3, China es el país con mayor número de investigaciones, seguido por India. Además, se identificaron dos artículos de colaboración internacional: en el artículo de Rajasoundaran et al. (2021) participaron investigadores de India, China y Estados Unidos, mientras que en el artículo de N'goran et al. (2022) colaboraron investigadores de Costa de Marfil y Francia.

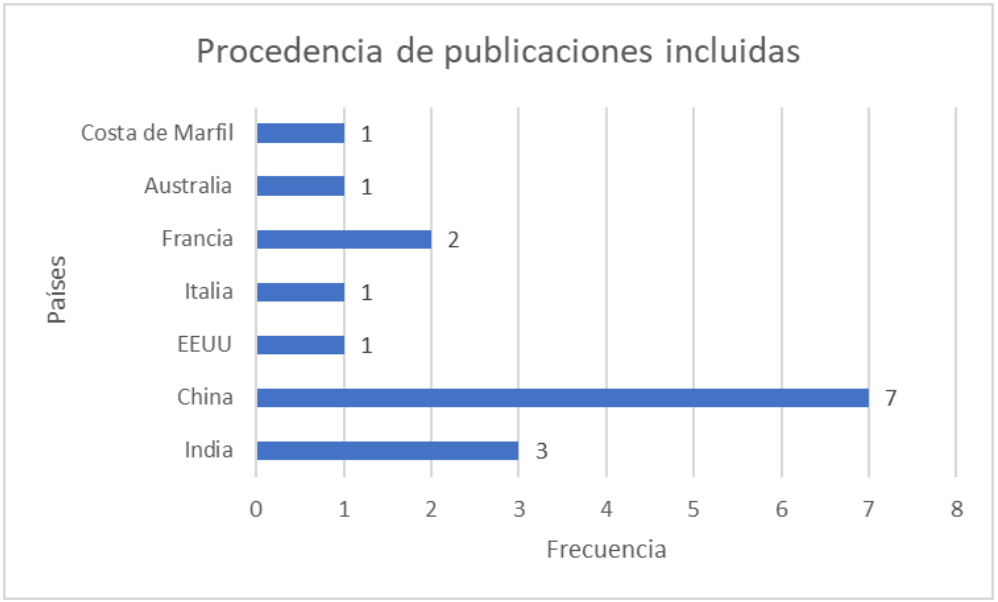

Figura 3. Procedencia de publicaciones incluidas

Sobre los artículos identificados, se elaboró el mapa de co-ocurrencia utilizando el software VOSViewer (Figura 4), el cual permite visualizar los términos más relevantes y sus relaciones entre publicaciones. En este mapa, se destacan tres grupos resaltados en rojo, verde y azul, en los que los términos con mayor ocurrencia son "cloud computing" (72), "approach" (52) e "internet" (54), respectivamente.

Sin embargo, el enfoque principal del estudio es la "zero trust architecture", la cual está vinculada a 33 términos de un total de 40 ítems mostrados en el mapa. En relación a este, los términos con mayor fuerza de enlace son "risk" y "perimeter", ambos con una fuerza de enlace de 8 puntos, seguidos de "challenge" (7) y "cloud computing" (5).

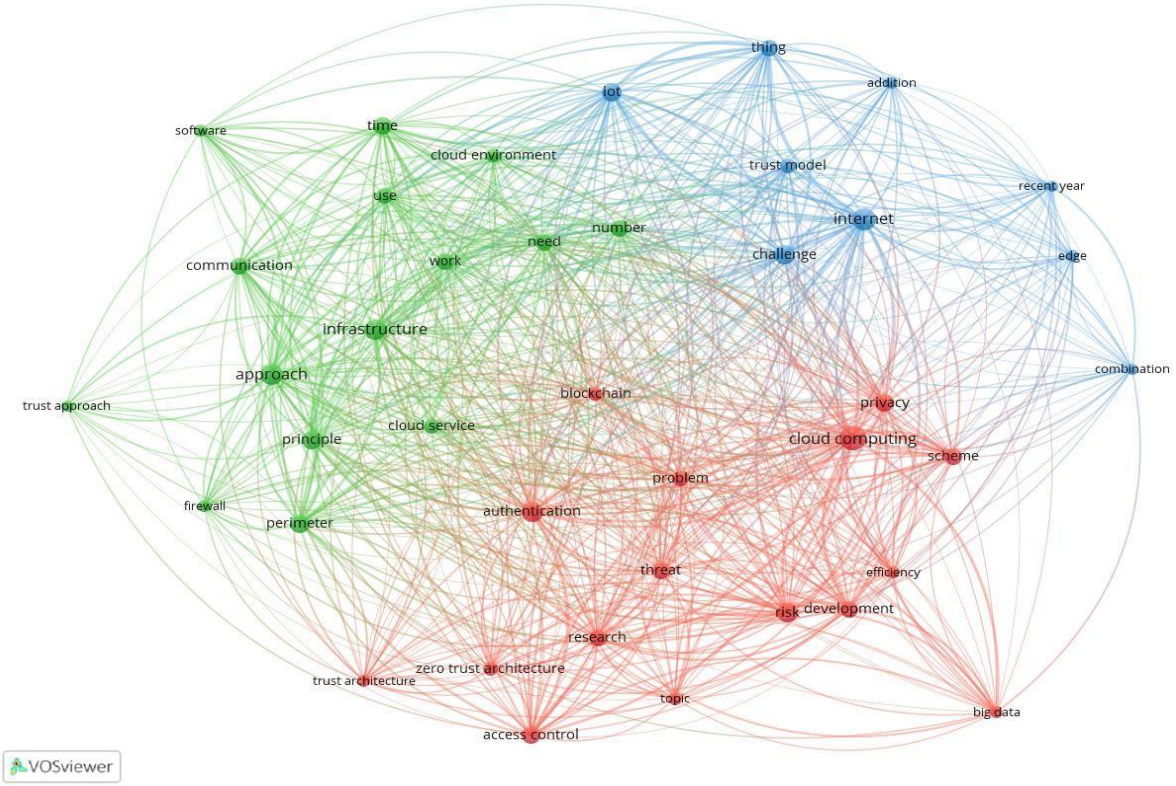

Figura 4. Mapa de co-ocurrencia de términos

Adicionalmente, en la Figura 5 se presenta una nube de palabras clave utilizadas en las publicaciones incluidas, donde prevalece el término "zero trust" con 9 apariciones, seguido por "network" con 4 apariciones y "network security" con 3 apariciones

Figura 5. Palabras claves de publicaciones incluidas

De las 13 publicaciones incluidas, la Tabla 2 expone los siguientes hallazgos sobre las herramientas, procedimientos y métodos de evaluación.

Autores	Título	Herramientas o procedimientos	Métodos de evaluación
Ali et al. (2022)	A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing	Una aplicación de autenticación continúa basada en el algoritmo criptográfico PRESENT para equipos registrados colocados en servidores multiacceso del borde entre la red CC y la nube. Mediante ello, se mejora la tasa de éxito de autenticación, así como reducción del tiempo de autenticación a comparación del CC tradicional.	Formulación de marco de trabajo para analizar la madurez de la red actual de CC, en la que se presentan medidas de protección para una seguridad mínima viable basado en los pilares: dispositivos, usuarios, sesiones, aplicaciones, datos e infraestructura.
Chen et al. (2021)	A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture	El modelo se enfoca en los sujetos, objetos, entornos y comportamientos implicados en un sistema de salud 5G inteligente, para proteger nube, borde y nodos. Se utilizan módulos de análisis del comportamiento de acceso de usuario, de evaluación de riesgo de equipos y de evaluación de la confianza, se reforzó la seguridad de las regiones de datos, computadoras, datos en la nube y dispositivos de Internet de las cosas en una red CC.	Uso de casos de prueba que verifica si el sistema responde con código de estado o de error para los módulos de evaluación de riesgo de equipos, evaluación de confianza y decisión de riesgo
Feng et al. (2023)	Blockchain enabled zero trust based authentication scheme for railway communication networks	La aplicación de *blockchain* permite dentro de una red CC un sistema descentralizado de acceso para almacenar credenciales mediante el árbol *Marke* y una autenticación bilateral en la que se registran usuarios, dispositivos y servicios en la nube implicados en una red de ferrocarril que converge redes públicas, privadas y de la nube. Asimismo, se usa un mecanismo de evaluaciones en tiempo real e histórico para mayor estabilidad del sistema.	Medición de eficiencia de la autenticación, de la actualización de información en el árbol y de la certificación en servicios. Así mismo, se evaluó la estabilidad cuando existe una caída repentina de rendimiento en la arquitectura actual.
Ferretti et al. (2021)	Survivable zero trust for cloud computing environments	El planteamiento de un modelo CC en la nube más agresivo que incluye para su protección a las bases de datos de políticas y accesos por separado y replicados, inicio de sesión único, certificados, control de accesos y proxy de accesos. Se realiza para proteger de cambios anómalos en las políticas de seguridad o toma de control de algún componente de seguridad por un atacante.	Análisis de seguridad a toda la arquitectura, donde se mide su supervivencia a ser comprometido mediante una tabla de costos de ataques, que presenta secuencias de ataque, componentes atacados y el costo de ataque.
Li et al. (2023)	A zero trust and blockchain-based defense model for smart electric	El esquema de seguridad para plataformas en la nube de las estaciones de carga para vehículos eléctricos hace uso de blockchain, CC y algoritmos criptográficos para una protección integral de los sistemas.	Uso del código Guobiao (estándares nacionales de China equivalentes a ISO) para el análisis de la seguridad de la información del proyecto

	vehicle chargers	Esta protección engloba la gestión de acceso, evaluaciones dinámicas de confianza y encriptación de las comunicaciones para asegurar la confidencialidad, integridad y disponibilidad del sistema en una estación de carga en China.	en relación a Blockchain y los algoritmos criptográficos (para servidores financieros y módulos de seguridad).
S. Liu et al. (2022)	Exploiting LSB Self-quantization for Plaintext-related Image Encryption in the Zero-trust Cloud	El algoritmo de autoaprendizaje basado en la incrustación de los dos bits menos significativos es una protección enfocada al ciclo de vida de datos en formato de imagen para almacenamiento de datos *cloud*. Se resuelven problemas relacionados a errores de desencriptación por ataques de ruido y sobrecargas de claves y llaves secretas que no se adaptan a las redes CC por ser ineficientes.	Análisis de ataque criptográficos, ruido y recorte de imágenes para conocer la efectividad del algoritmo empleado.
Z. Liu et al. (2022)	Data-Driven Zero Trust Key Algorithm	El esquema de seguridad CC basado en el análisis de datos de los comportamientos de los usuarios de la nube realiza una mejor detección de comportamientos anómalos y fue más preciso en determinar la confianza de los usuarios cuando acceden a información ubicada en la nube. Esta precisión reduce falsos positivos y sirve como un recurso adicional a las medidas de CC.	Análisis de valores de confianza en la nube y de agregación de eventos de seguridad permite conocer la precisión en la detección de comportamientos maliciosos dentro de una red CC en la nube.
Mandal et al. (2021)	Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic	Una política de control de acceso basado en la predicción y detección de tráfico falsificado mediante MAC para proteger los recursos en la nube de una empresa, accedidos desde inicialmente desde la red propia de un usuario en su hogar. Se aplica una red CC para los recursos en la nube, un algoritmo basado en puntuaciones y umbrales para detectar comportamientos de los usuarios, analizando su IP, MAC y puerto. Este algoritmo es preciso y presenta una menor tasa de falsos positivos de accesos anómalos.	Uso de la curva característica de operación del receptor para comparar la tasa de identificación de verdaderos positivos (suplantación) y la tasa de falsos positivos. Este método de evaluación es usado en otros algoritmos con la misma finalidad de detectar tráfico malicioso.
Miller et al. (2021)	Securing Workflows Using Microservices and Metagraphs	El despliegue de flujos de trabajo que comparten información se puede asegurar mediante la verificación de políticas de seguridad de datos y una arquitectura de microservicios bajo principios de CC en la nube. Esto permite encontrar y evitar fugas de información en entornos en la nube. Finalmente, el uso de metagrafos es importante para manejar una gran cantidad de políticas de seguridad, y, por lo tanto, flujos de trabajo eficientes.	Evaluación de tiempo de ejecución y carga de CPU cuando se crean flujos de trabajo asegurados por las políticas de seguridad.

N'goran et al. (2022)	Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment	El modelo de gestión de confianza de nubes comunitarias está compuesto de un gestor de recursos, de transacciones y de actualizaciones de confianza y de reputación tanto para los repositorios y los usuarios que conforman cada organización de la nube. Mediante el uso de valores de confianza recomendados por otros usuarios u organizaciones y el algoritmo *SeComTrust* planteado, se reconoce proveedores maliciosos según su comportamiento.	Análisis de funcionalidad y escalabilidad de detección de proveedores maliciosos del modelo de gestión planteado a comparación de otros modelos. El modelo detecta correctamente los proveedores maliciosos incluso cuando el número de participantes incrementa.
Rajasoundaran et al. (2021)	Machine learning based deep job exploration and secure transactions in virtual private cloud systems	Los servicios de trabajo en la nube seguros basados en aprendizaje automático son una herramienta para asegurar la confidencialidad y encriptación de los trabajos de usuario y sistema para nubes virtuales privadas basados en CC haciendo uso de modelo de cola para múltiples servidores y el modelo de análisis *VGAN*.	Evaluación mediante análisis de seguridad multinivel, donde se observa la tasa de detección de ataques DDoS, fuerza bruta, falsificación de IP, hombre en el medio y phishing.
Saleem et al. (2023)	Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment	Utilización del algoritmo *Spatial Rich Model* en sus diversas presentaciones bajo criterios de CC, junto al análisis de comportamiento del usuario y servicio, fueron útiles para garantizar la confianza de respuestas brindadas por servicios en la nube de almacenamiento o procesamiento de imágenes. Estas herramientas sirven como recurso forense en caso de que el servicio en la nube haya sido comprometido o se hayan subido imágenes infectadas.	Análisis de dimensionalidad de características y tiempo de extracción de características para cada presentación del modelo Spatial Rich Model en la red CC.
Wang et al. (2023)	Research on Medical Security System Based on Zero Trust	Planteamiento del modelo ABEAC que analiza los comportamientos del usuario para acceso de controles dinámicos en los entornos en la nube aplicados en un modelo CC para entornos médicos, garantiza mayor protección de la información de los pacientes y los equipos médicos al considerar valores de riesgo por usuario y de forma global al tener en cuenta el número de comportamientos anómalos en total de la red.	Comparación con el modelo TMBRE, que es usado actualmente en sistemas médicos, en el cálculo del valor de riesgo y confianza del comportamiento de un usuario y múltiples usuarios en la red.

Tabla 2. Resultados de publicaciones incluidas

En la Tabla 3, se presentan las herramientas y procedimientos utilizados por los autores, los cuales están diseñados para fortalecer el control de accesos o mejorar el motor de políticas de las redes CC. Además, se detallan los métodos de evaluación aplicados a estas herramientas y procedimientos que, en términos generales, se pueden resumir de acuerdo a lo indicado en la tabla.

En general, se observa que el blockchain y los algoritmos estegoanalíticos son las herramientas más recurrentes, mientras que los modelos integrales de confianza predominan en los procedimientos. Por último, el método de evaluación más mencionado es el de pruebas funcionales seguido de los análisis de seguridad.

Materia de estudio	**Temas predominantes**	**Autores**	**Frecuencia**
Herramientas	Blockchain	(Feng et al., 2023; Li et al., 2023)	2
	Algoritmos estegoanalíticos	(S. Liu et al., 2022; Saleem et al., 2023)	2
	Algoritmos criptográficos	(Ali et al., 2022)	1
	Microservicios	(Miller et al., 2021)	1
	Machine Learning	(Rajasoundaran et al., 2021)	1
Procedimientos	Modelos integrales de confianza	(Chen et al., 2021; Ferretti et al., 2021; N'goran et al., 2022)	3
	Análisis de comportamientos	(Z. Liu et al., 2022; Wang et al., 2023)	2
	Políticas de control predictivas	(Mandal et al., 2021)	1
Métodos de evaluación	Pruebas funcionales	(Chen et al., 2021; Z. Liu et al., 2022; Mandal et al., 2021; Saleem et al., 2023)	4
	Análisis de seguridad|	(Ferretti et al., 2021; S. Liu et al., 2022; Rajasoundaran et al., 2021)	3
	Comparación directa de funcionalidad con modelos existentes	(N'goran et al., 2022; Wang et al., 2023)	2
	Pruebas de rendimiento	(Feng et al., 2023; Miller et al., 2021)	2
	Análisis de madurez	(Ali et al., 2022)	1
	Estándares nacionales	(Li et al., 2023)	1

Tabla 3. Herramientas, procedimientos y métodos de evaluación encontrados

A modo de resumen, en el siguiente gráfico de proyección solar de dos niveles (Figura 6), se presentan las herramientas, procedimientos y métodos de evaluación utilizados para la implementación del modelo CC. Se destaca la frecuencia de aparición en los artículos mediante diferentes intensidades de color, de manera que los tonos más oscuros representan una mayor frecuencia.

Figura 6. Gráfico resumen de hallazgos

4. Discusión

Las herramientas y procedimientos propuestas ofrecen ventajas en fortalecer los componentes del modelo CC. El uso de blockchain radica en crear centros descentralizados de identidades con menor carga para la red, de tal forma que el acceso es tolerante a fallos, y, mediante los hashes de los blockchain, evitar ataques relacionados al robo de credenciales y la suplantación de identidad (Feng et al., 2023; Li et al., 2023); mientras tanto los algoritmos estegoanalítcos cubren la necesidad de evitar filtración de datos por medio de archivos multimedia (S. Liu et al., 2022) y gestionar la confianza de en las interacciones entre usuarios y proveedores de almacenamiento de multimedia en la nube dentro de la red CC. (Saleem et al., 2023).

Entre los procedimientos, destacan los modelos integrales de confianza representan la implementación clásica del modelo CC, que abarca las políticas de acceso, manejo de identidades y análisis tanto de comportamientos como de valores de confianza y riesgo dentro de la red CC (Chen et al., 2021; Ferretti et al., 2021; N'goran et al., 2022).

Respecto a los métodos de evaluación de las herramientas y procedimientos, estos varían según el alcance de la propuesta, así como la finalidad del artículo. Li et al. (2023) hace uso de los estándares nacionales de China debido a que su proyecto está operativo para su uso cotidiano por la población, por ello tuvo que pasar por una serie de normativas que aseguran la seguridad de la información. Adicionalmente, se ha realizado comparaciones con modelos ya existentes en el mercado o sector, como en el caso del modelo *SeComTrust*, en el cuál es más efectivo en la detección de proveedores maliciosos a comparación de otros modelos como *Intertrust* o TNASL (N'goran et al., 2022), o un cálculo más efectivo de los valores de confianza y riesgo de usuarios del modelo ABEAC planteado por Wang et al. (2023) comparado con el modelo TMBRE usado actualmente en el sector salud.

Las pruebas de funcionalidad varía en cada publicación pero destacan el uso de casos de prueba para cada módulo planteado (Chen et al., 2021), dimensionalidad de características extraídas de recursos multimedia (Saleem et al., 2023), medición de tasa de verdaderos positivos y falsos positivos de detección de suplantación (Mandal et al., 2021) y el análisis de valores de confianza en la nube en tiempo real (Z. Liu et al., 2022). Asimismo, se hace uso de análisis de seguridad, en donde se simula distintos tipos de ataques según lo que debería proteger las herramientas o procedimientos; entre ellos, el algoritmo de S. Liu et al. (2022) que fue expuesto a ataques criptográficos y ruido, el modelo de Rajasoundaran et al. (2021) que fue valorada ante ataques de fuerza bruta o falsificación de IP y la arquitectura de Ferretti et al. (2021), en la cual se prueba la supervivencia del sistema ante distintos vectores de ataques para cada componente.

Finalmente, Ali et al. (2022) propone un marco de trabajo de madurez de la seguridad de una red CC implementada en la nube, en donde se determina cuáles son los requerimientos para una seguridad mínima viable. Este marco de trabajo puede ser usado por otros autores para analizar la condición actual de la red.

5. Conclusiones

Las implementaciones del modelo de seguridad CC para entornos en la nube se ha visto fortalecida por la adopción de nuevas herramientas y procedimientos, las cuales destacan el uso de blockchain, algoritmos criptográficos o creación de nuevos modelos integrales de confianza, debido a que ofrece mejoras de rendimiento y nuevas capacidades como predicciones, análisis en tiempo real de confianza o tolerancia a fallos. Asimismo, estas tecnologías se adaptan a necesidades específicas según la forma de uso de la red en la nube en donde es utilizado, por lo que puede ser replicado por otros usuarios u organizaciones. Respecto a los métodos de evaluación de las herramientas y procedimientos, se realizan, por lo general, pruebas de funcionalidad, análisis de seguridad y comparaciones directas con modelos existentes. Sin embargo, los métodos de evaluación para cada implementación varían y no se conoce realmente qué mejora en la seguridad de información de toda la red CC se produce.

Por ello, se plantea como línea de investigación futura, que se debe crear un marco de evaluación estandarizado del modelo de seguridad CC para entornos en la nube, que permita conocer qué medidas mínimas o exigentes se deben adoptar según el nivel de criticidad de la red, de tal forma que sea posible conocer el estado actual de seguridad y el impacto de las nuevas adopciones tecnológicas en la seguridad de la red CC en la nube.

6. Referencias bibliográficas

Akbar, undefined H., Zubair, undefined M., & Malik, undefined M. S. (2023). The Security Issues and challenges in Cloud Computing. *International Journal for Electronic Crime Investigation*, *7*(1), Article 1. https://doi.org/10.54692/ijeci.2023.0701125

Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing. *Security and Communication Networks*, *2022*, 1-14. https://doi.org/10.1155/2022/3178760

Bajdor, P. (2022). Perception and evaluation of selected cloud computing factors in the light of conducted research among small and medium-sized enterprises. *Procedia Computer Science*, *207*, 3788-3797. https://doi.org/10.1016/j.procs.2022.09.440

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2021). A Security Awareness and Protection System for 5G Smart Healthcare Based on ZeroTrust Architecture. *IEEE Internet of Things Journal*, *8*(13), 10248-10263. https://doi.org/10.1109/JIOT.2020.3041042

Cheng, M., Qu, Y., Jiang, C., & Zhao, C. (2022). Is cloud computing the digital solution to the future of banking? *Journal of Financial Stability*, *63*, 101073. https://doi.org/10.1016/j.jfs.2022.101073

Divya, P., & Sherin, A. (2022). A Zero Trust Framework Security to Prevent Data Breaches and Mitigate the Cloud Network Attacks. *International Journal for Research in Applied Science and Engineering Technology*, *10*, 3530-3538. https://doi.org/10.22214/ijraset.2022.42976

Feng, Y., Zhong, Z., Sun, X., Wang, L., Lu, Y., & Zhu, Y. (2023). Blockchain enabled zero trust based authentication scheme for railway communication networks. *Journal of Cloud Computing*, *12*(1), 62. https://doi.org/10.1186/s13677-023-00411-z

Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security*, *110*, 102419. https://doi.org/10.1016/j.cose.2021.102419

George, A. S., & Sagayarajan, S. (2023). Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments. *Partners Universal International Research Journal*, *2*(1), Article 1. https://doi.org/10.5281/zenodo.7723187

Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N., Alam, M. Z., & Masud, M. (2022). Security and privacy aspects of cloud computing: A smart campus case study. *Intelligent Automation and Soft Computing*, *31*(1), Article 1. https://doi.org/10.32604/IASC.2022.016597

Guo, R., Tafti, A., & Subramanyam, R. (2023). Internal IT modularity, firm size, and adoption of cloud computing. *Electronic Commerce Research*. https://doi.org/10.1007/s10660023-09691-8

Justice, C., & Sample, C. (2022). Future Needs of the Cybersecurity Workforce. *International Conference on Cyber Warfare and Security*, *17*(1), Article 1.

https://doi.org/10.34190/iccws.17.1.33

Lawan, M. M., Oduoza, C., & Buckley, K. (2021). A Systematic Review of Cloud Computing Adoption by Organisations. *International Journal of Industrial and Manufacturing Systems Engineering*, *6*(3), Article 3. https://doi.org/10.11648/j.ijimse.20210603.11

Li, P., Ou, W., Liang, H., Han, W., Zhang, Q., & Zeng, G. (2023). A zero trust and blockchainbased defense model for smart electric vehicle chargers. *Journal of Network and Computer Applications*, *213*, 103599. https://doi.org/10.1016/j.jnca.2023.103599

Liu, S., Zhuang, Y., Huang, L., & Zhou, X. (2022). Exploiting LSB Self-quantization for Plaintext-related Image Encryption in the Zero-trust Cloud. *Journal of Information Security and Applications*, *66*, 103138. https://doi.org/10.1016/j.jisa.2022.103138

Liu, Z., Li, X., & Mu, D. (2022). Data-Driven Zero Trust Key Algorithm. *Wireless Communications and Mobile Computing*, *2022*, 1-9. https://doi.org/10.1155/2022/8659428

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. *New Generation Computing*, *39*(3-4), 599-622. https://doi.org/10.1007/s00354-021-001306

Miller, L., Mérindol, P., Gallais, A., & Pelsser, C. (2021). Securing Workflows Using Microservices and Metagraphs. *Electronics*, *10*(24), 3087. https://doi.org/10.3390/electronics10243087

N'goran, R., Tetchueng, J.-L., Pandry, G., Kermarrec, Y., & Asseu, O. (2022). Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment. *Engineering*, *14*(11), 479-496. https://doi.org/10.4236/eng.2022.1411036

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *The BMJ*, *372*, undefined-undefined. https://doi.org/10.1136/bmj.n71

Paul, B., & Rao, M. (2023). Zero-Trust Model for Smart Manufacturing Industry. *Applied Sciences (Switzerland)*, *13*(1). Scopus. https://doi.org/10.3390/app13010221

Rajasoundaran, S., Prabu, A. V., Routray, S., Kumar, S. V. N. S., Malla, P. P., Maloji, S., Mukherjee, A., & Ghosh, U. (2021). Machine learning based deep job exploration and secure transactions in virtual private cloud systems. *Computers & Security*, *109*, 102379. https://doi.org/10.1016/j.cose.2021.102379

Rose, S. W., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST*. https://www.nist.gov/publications/zero-trust-architecture

Saleem, M., Warsi, M. R., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of Information Security and Applications*, *72*, 103389. https://doi.org/10.1016/j.jisa.2022.103389

Shetty, J. P., & Rajesh, P. (2021). An overview of cloud computing in SMEs. *Journal of Global Entrepreneurship Research*, *11*. https://doi.org/10.1007/s40497-021-00273-2

Sohrabi, C., Franchi, T., Mathew, G., Kerwan, A., Nicola, M., Griffin, M., Agha, M., & Agha, R. (2021). PRISMA 2020 statement: What's new and the importance of reporting guidelines. *International Journal of Surgery*, *88*, 105918. https://doi.org/10.1016/j.ijsu.2021.105918

Teodoro, D. D. R. (2022). Cloud infrastructure architecture and the zero trust model as a cybersecurity strategy. *Revista Científica Multidisciplinar Núcleo Do Conhecimento*, *13*(11), 204-232. https://doi.org/10.32749/nucleodoconhecimento.com.br/technologyen/zero-trust-model

Wang, Z., Yu, X., Xue, P., Qu, Y., & Ju, L. (2023). Research on Medical Security System Based on Zero Trust. *Sensors*, *23*(7), 3774. https://doi.org/10.3390/s23073774

Zheng, M., Huang, R., Wang, X., & Li, X. (2023). Do firms adopting cloud computing technology exhibit higher future performance? A textual analysis approach. *International Review of Financial Analysis*, *90*, 102866. https://doi.org/10.1016/j.irfa.2023.102866