RELIGACIÓN
REVISTA

Serverless Computing en el campo de la Ciberseguridad. Una revisión sistemática de literatura

Serverless Computing in the field of Cybersecurity. A systematic literature review

Ximena del Carmen Pacheco Armijos, Andrés Sebastián Quevedo Sacoto

Resumen

En la última década, Serverless Computing ha emergido como una revolución en la forma en que se desarrollan y despliegan aplicaciones, permitiendo a los desarrolladores centrarse exclusivamente en la lógica de sus aplicaciones y delegando la gestión de la infraestructura a proveedores de servicios en la nube. Es por ello, que la adopción de Serverless Computing ha crecido rápidamente debido a sus ventajas en términos de escalabilidad, costo y simplicidad operativa. Sin embargo, como cualquier tecnología emergente, el modelo sin servidor introduce nuevas vulnerabilidades y amenazas de seguridad que deben ser abordadas para garantizar la protección de los datos y la integridad de las aplicaciones. En el presente documento, se lleva a cabo una revisión sistemática acerca de serveless computing en el ámbito de la ciberseguridad, para analizar e identificar los desafíos y amenazas a los que se enfrentan los entornos serverless, así como sus beneficios y las soluciones propuestas para abordar estos desafíos. Los resultados de la revisión ofrecen el estado actual de la ciberseguridad en entornos de computación sin servidor.

Palabras clave: serverless computing; ciberseguridad; desafíos; soluciones.

Ximena del Carmen Pacheco Armijos
Universidad Católica de Cuenca | Cuenca | Ecuador | xpacheco.31@est.ucacue.edu.ec
https://orcid.org/0009-0003-9431-451X
Andrés Sebastián Quevedo Sacoto
Universidad Católica de Cuenca | Cuenca | Ecuador | asquevedos@ucacue.edu.ec
https://orcid.org/0000-0001-5585-0270

http://doi.org/10.46652/rgn.v9i42.1266
ISSN 2477-9083
Vol. 9 No. 42 octubre-diciembre, 2024, e2401266
Quito, Ecuador

Enviado: mayo 01, 2024
Aceptado: julio 03, 2024
Publicado: julio 18, 2024
Publicación Continua

Abstract

In the last decade, Serverless Computing has emerged as a revolution in the way applications are developed and deployed, allowing developers to focus exclusively on the logic of their applications and delegating infrastructure management to cloud service providers. This is why the adoption of Serverless Computing has grown rapidly due to its advantages in terms of scalability, cost and operational simplicity. However, like any emerging technology, the serverless model introduces new vulnerabilities and security threats that must be addressed to ensure data protection and application integrity. In this document, a systematic review of serveless computing in the field of cybersecurity is carried out, to analyze and identify the challenges and threats faced by serverless environments, as well as their benefits and the solutions proposed to address them. these challenges. The results of the review provide the current state of cybersecurity in serverless computing environments.

Keyword: serverless computing; cybersecurity; challenges; solutions.

Introducción

La computación sin servidor (Serverless Computing) está ganando popularidad debido a su ligereza y facilidad de uso. Estos beneficios se logran reduciendo el detalle de la unidad computacional al nivel funcional. En particular, la tecnología sin servidor permite a los usuarios centrarse directamente en la funcionalidad misma, dejando otras cuestiones engorrosas de desarrollo y gestión al proveedor de la plataforma, quien es responsable de lograr el equilibrio entre una programación de alto rendimiento y bajos costos de recursos (Li et al., 2023).

Se estima que el tamaño del mercado sin servidor alcance casi $22 mil millones de dólares en 2025, permitiendo que la informática sin servidor sea empleada en un 50% de las empresas globales para el mismo año (Wen et al., 2023). La computación sin servidor es un paradigma nuevo y potencial de computación en la nube, con la importante ventaja de que libera a los desarrolladores de software de la carga de tareas de administración complejas y propensas a errores.

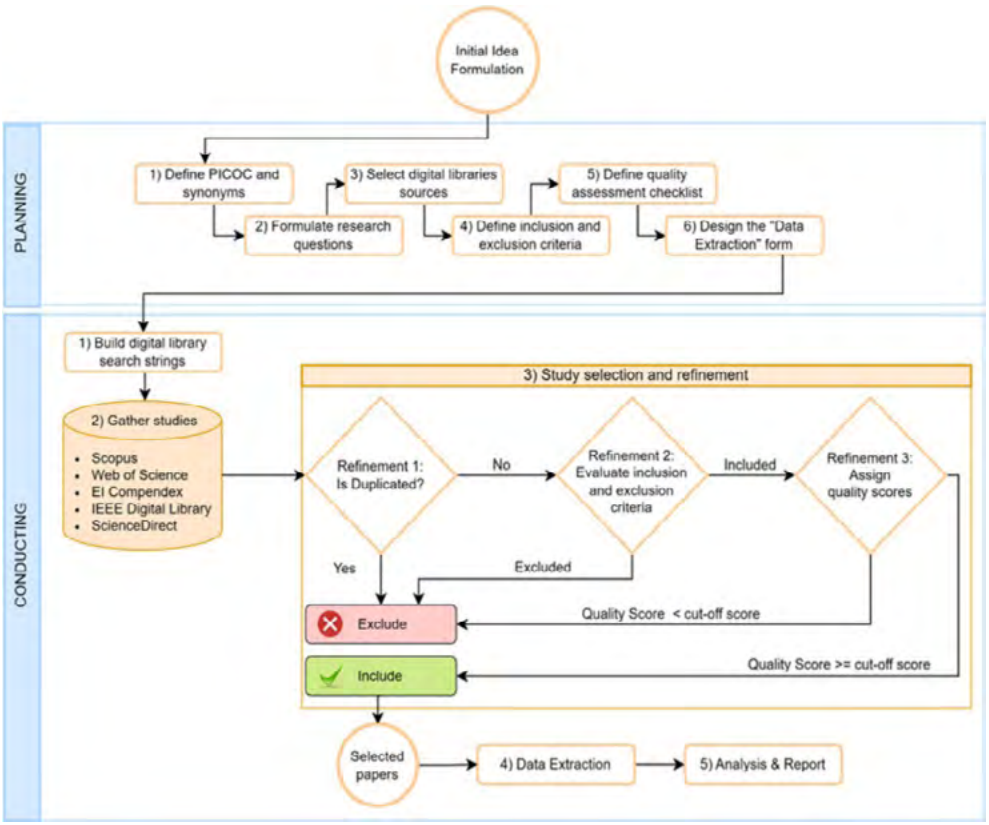
Así también, la computación en la nube sin servidor ofrece backend como servicio (BaaS) y función como servicio (FaaS). El BaaS incluye servicios como almacenamiento, mensajería, gestión de usuarios, etc. Mientras que FaaS permite a los desarrolladores implementar y ejecutar su código en plataformas informáticas. El FaaS se basa en los servicios proporcionados por el BaaS, como una base de datos, mensajería, autenticaciones de usuarios, entre otros (Hassan et al., 2021).

No obstante, cualquier tecnología nueva enfrentará numerosos problemas y obstáculos técnicos y operativos al principio. En este caso esta nueva tecnología carece de herramientas que ayuden a administrar y monitorear aplicaciones sin servidor, siendo la seguridad uno de los principales desafíos, ya que son dependientes del proveedor. Por lo tanto, el objetivo de esta revisión sistemática de literatura es identificar los desafíos de seguridad y las soluciones propuestas para abordar los mismos que plantean diversos autores.

Metodología

En esta revisión sistemática de literatura se empleó la guía rápida para la investigación en informática, planteada por Carrera-Rivera et al. (2022), que consta de las etapas de planificación y conducción, las cuales se detallan en el Gráfico 1.

Gráfico 1. Diagrama de flujo de las etapas de la metodología.



Fuente: Carrera-Rivera et al. (2022).

El primer paso consiste en desarrollar la fase de planificación, teniendo que definir el protocolo de investigación, en donde se definen las palabras claves, preguntas de investigación, bibliotecas digitales, criterios de inclusión y exclusión, evaluación de calidad y el formulario de extracción de datos.

En esta revisión sistemática de literatura se centra en identificar aspectos relacionados con serverless computing, ciberseguridad, desafíos, amenazas, beneficios y soluciones de seguridad. Es por ellos, que definieron cuatro preguntas de investigación, relacionadas con: ¿Cuáles son los beneficios de utilizar la informática sin servidor?, ¿Cuáles son los principales desafíos de ciberseguridad asociados con el uso de Serverless Computing?, ¿Cuáles son las amenazas a las que se enfrenta el Serverless Computing? y ¿Qué soluciones se han propuesto para mitigar los riesgos de seguridad asociados con el uso de Serverless Computing?

Las publicaciones se extrajeron de las bases de datos Scopus y Web Of Sience, en donde se aplicaron las siguientes cadenas de búsqueda:

1. Web of Science: TOPIC (serverless AND computing AND security OR privacy AND challengs)
2. Scopus: (TITLE-ABS-KEY (serverless AND computing) AND TITLE-ABS-KEY (privacy) AND TITLE-ABS-KEY (challenges)

De igual forma, se definieron los criterios de inclusión y exclusión para un filtrado y ayuda a la selección de los artículos de estudio. En el caso de los criterios de inclusión de consideró publicaciones de los últimos cinco años, en idioma inglés y español, los cuales aborden directamente la temática planteada y palabras claves, y de libre acceso. Mientras, que para la exclusión consideramos la calidad de las publicaciones y la duplicidad.

Para la evaluación de la calidad se han definido tres preguntas, cada una tiene una valoración de 1 punto, por lo que cada artículo deberá cumplir un mínimo de 2 puntos para ser incluido, mimas que se presentan en la Tabla 1.

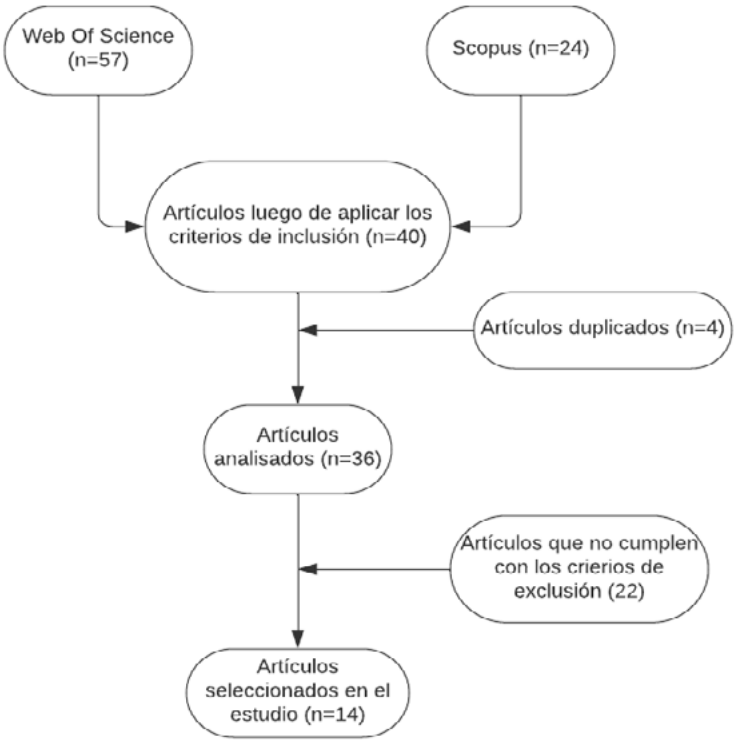
Tabla 1. Lista de verificación para la evaluación de calidad.

Nº	Pregunta de evaluación de calidad	Respuesta
1	¿En el artículo se mencionan claramente los objetivos de investigación?	Sí=1 / No= 0
2	¿El artículo muestra resultados sobre seguridad en entornos de serveless computing?	Sí=1 / No= 0
3	¿El artículo muestra resultados sobre desafíos en entornos de serveless computing?	Sí=1 / No= 0

Fuente: Producción propia.

Una vez definido el protocolo, el siguiente paso consiste en la fase conductual, donde desarrollaremos la revisión sistemática de literatura (RSL). Tras aplicar cadenas de búsqueda en las bases de datos científicas antes mencionadas, encontramos un total de 81 artículos, a los cuales les aplicamos los criterios de inclusión y exclusión, seleccionando 14 artículos para análisis en esta RSL. El proceso de selección se presenta en el Gráfico 2.

Gráfico 2. Proceso de selección de los artículos de estudio.



Fuente: Producción propia.

Finalmente, se extrajeron los datos relevantes que permitan responder las preguntas de investigación, considerándose el artículo y los hallazgos (beneficios, desafíos y soluciones). La Tabla 2 muestra los resultados de la extracción de datos.

Tabla 2. Extracción de datos para responder a las preguntas de investigación.

Autor	Hallazgos
Li et al. (2023).	Beneficios: flexibilidad, agilidad, escalamiento y pago por uso. Desafíos: Aislamiento de recursos, monitoreo de seguridad, gestión de seguridad y protección de datos. Amenazas: Acceso interno ilegal, ataques de rastreo, ataques de inyección, DoS, ataques de escape de contenedores, ataques a aplicaciones desde plataformas maliciosas. Soluciones: Crear un sistema de defensa en profundidad para proteger las aplicaciones sin servidor y plataformas en múltiples etapas y niveles, aislamiento, monitoreo y cifrado.
Marin et al. (2022).	Beneficios: Gestión de la infraestructura y las tareas operativas realizadas por los proveedores de la nube, desarrolladores centrados únicamente en la lógica empresarial de sus aplicaciones, pago por uso de los recursos que consumen, flexibilidad, escalabilidad, optimización del uso de recursos. Desafíos: Gestión de la seguridad de los flujos de trabajo, configuración de los microservicios. Amenazas: Recuperación de datos confidenciales mediante tokens de sesión almacenados en tablas de entorno, alterar la ejecución de cualquier función o servicio en la nube que reciba datos de entrada, no aplicar técnicas adecuadas de saneamiento de datos de entrada., ataques de inyección de código, DoS, DoW, typosquatting.

Autor	Hallazgos
Gill (2024).	Beneficios: Mejora la velocidad computacional del procesamiento de los datos entrantes, aumenta la escalabilidad de los sistemas informáticos para un mejor rendimiento. Desafíos: Aplicar restricciones de confianza y privacidad en la programación de tareas para un número limitado de recursos en serverless. Amenazas: Piratería. Soluciones: Mecanismos de cifrado y hash.
Morabito et al. (2023)	Beneficios: Los desarrolladores se centran en la lógica empresarial y los proveedores se encargan de la implementación. Desafíos: El nivel de seguridad depende estrictamente de las características proporcionadas por el proveedor, si se utiliza código inseguro para funciones sin servidor, la superficie de ataque se amplía. Amenazas: Inyección de código, exposición de datos confidenciales, fallas en la autenticación, control de acceso, configuraciones erróneas de seguridad, monitoreo insuficiente. Soluciones: Introducir una cultura de colaboración, crear arquitecturas de seguridad por diseño, introducir un modelado y limitación de amenazas de autorización, implementar estándares de codificación segura, automatizar sistemas de implementación seguros, aprovechando el monitoreo continuo.
Li et al. (2022).	Beneficios: El servicio se carga y ejecuta bajo demanda en lugar de implementarse en una instancia de ejecución a largo plazo, optimización a nivel de aplicación, reorganizar las aplicaciones de la nube en microservicios. Desafíos: Falta de disponibilidad Amenazas: Ataques de agotamiento de invocaciones, DoW, DDoS. Soluciones: Restringir el acceso, reglas de filtrado en caso de activación de eventos.
Palma et al. (2023)	Beneficios: Rentabilidad, escalabilidad, los desarrolladores se centran en el código y delegan la gestión del servidor y el escalado al proveedor. Desafío: Permitir que el desarrollador coloque explícitamente las funciones de la nube en la misma instancia de la máquina virtual. Soluciones: Especificar políticas de restricción, política de verificación de propiedades.
Park et al. (2024).	Beneficios: Proveedor gestiona el servidor, mientras que los desarrolladores pueden centrarse en sus servicios, escalabilidad, costos por uso. Amenazas: Código malicioso, ataques de canal lateral, ataques de reutilización de código, invocación arbitraria de API. Soluciones: Aislamiento de funciones en nubes remotas, utilización de parches previos.
Ouyang et al. (2023), the transmission and processing of logistics information directly affect the trading experience and efficiency. The use of Internet of Things (IoT	Beneficios: Alta concurrencia, rendimiento y disponibilidad, valor económico sustancial. Desafíos: Seguridad y privacidad de la información, exposición de la interfaz. Amenazas: Fuga de datos durante la transmisión. Soluciones: Cifrado en las comunicaciones.
Barrak et al. (2022).	Beneficios: Velocidad, eficiencia, reducción de costos, escalabilidad. Desafíos: Reducir la latencia de inicio, gestionar y analizar datos confidenciales. Amenazas: Inyección de código. Soluciones: Reducir la asignación de recursos para alcanzar un rendimiento óptimo en los servicios de inferencia, establecer roles para cada función de la nube con políticas de seguridad específicas, control de acceso, cifrar las solicitudes de funciones HTTP.

Autor	Hallazgos
Kelly et al. (2021)	Beneficios: Escalamiento, costo por uso. Desafíos: Problemas financieros. Amenazas: Robo de información, DoW, DoS, inundación HTTP, ReDoS, usuarios falsos. Soluciones: Límite de tiempo para ejecución de funciones, limitación de solicitudes en llamadas API, controles de acceso, construir gráficos de uso común que se utilizarán en el análisis de tráfico para señalar a usuarios sospechosos.
Ortega Candel et al. (2024).	Beneficios: Pago por uso, crear y ejecutar aplicaciones sin la necesidad de administrar la infraestructura de servidor tradicional, flexibilidad, escalamiento. Desafíos: Agotamiento de los recursos financieros de una organización. Amenazas: DoW. Soluciones: Crear modelos de aprendizaje automático, recopilar y analizar datos históricos sobre funciones activas y uso de recursos, definir indicadores importantes que pueden ayudar a predecir y mitigar amenazas financieras.
Zhang et al. (2021).	Beneficios: Pago por uso, el proveedor de la nube aborda todas sus complejidades operativas, escalabilidad. Desafíos: Falta de comprensión de la tecnología en la nube y la falta de confianza en la seguridad de la nube. Soluciones: Cifrado, autenticación, gestión de identidades, rotación de claves, autorización de acceso según las instrucciones proporcionadas.
Bocci et al. (2021).	Beneficios: Aprovisionamiento de recursos, escalamiento, pago por uso. Desafíos: Preservar y hacer cumplir las restricciones de seguridad, proteger la confidencialidad de los datos. Amenazas: Aislamiento entre los usuarios y una contabilidad precisa en efectos de facturación, atacantes externos, aplicaciones mal configuradas. Soluciones: políticas de autorización, responsabilidad compartida (seguridad de la nube y en la nube), cifrado, aislamiento de funciones.
Ebrahimpour et al. (2023)	Beneficios: Pago por uso, mejorar la utilización de recursos, los desarrolladores a centrarse en la lógica central de las aplicaciones, escalamiento. Desafíos: Equilibrar costos, rendimiento, modelos de programación, problemas de arranque en frío de contenedores, datos que se guardan en cachés. Amenazas: Transferencia de las funciones del usuario al destino sean expuestas, código malicioso que afecte el costo final. Soluciones: Algoritmos de aprendizaje profundo para considerar los patrones.

Fuente: Producción propia.

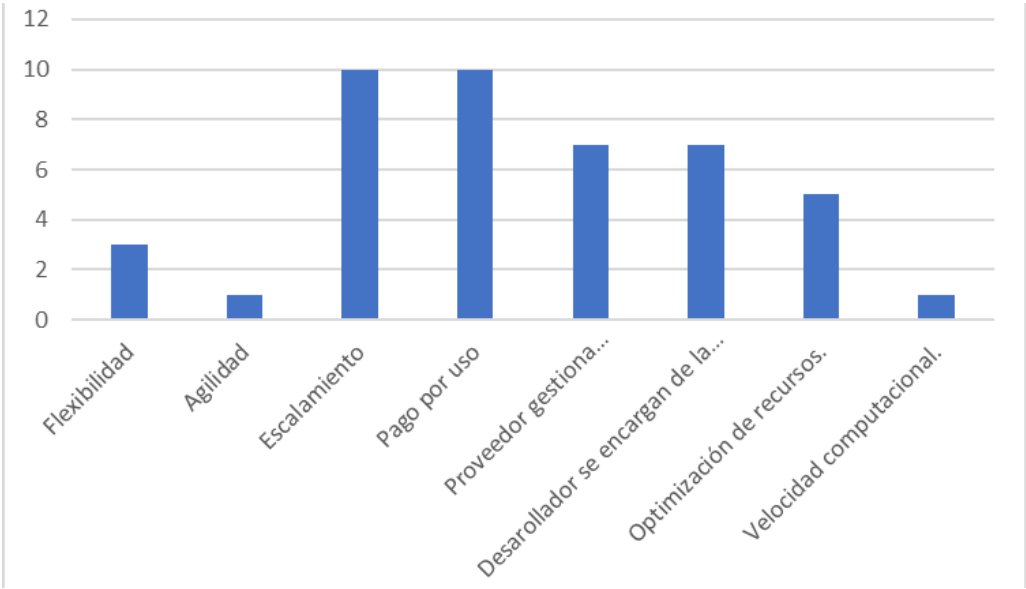
Resultados

Los resultados responden a las preguntas de investigación planteadas mediante el análisis e interpretación de los artículos seleccionados para el estudio.

1. ¿Cuáles son los beneficios de utilizar la informática sin servidor?

Con base en los estudios, un 21% hace mención a la flexibilidad, un 7% la agilidad, un 71% la escalibilidad, un 71% el pago según el uso, un 50% la gestión de infracestructura que realiza el proveedor de la nube, un 50% la lógica empresarial por parte de los desarrolladores, un 36% la opmitimización de recursos y un 7% la velocidad computacional. El Gráfico 3 muestra beneficios del serveless computing mencionados en los artículos analizados.

Gráfico 3. Beneficios del serveless computing.

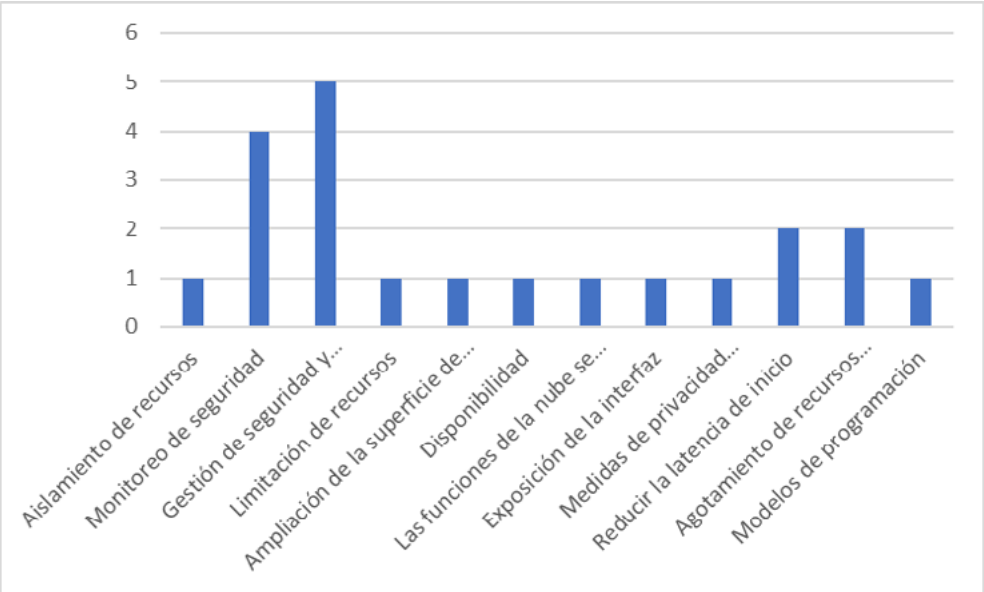


Fuente: Producción propia.

2. ¿Cuáles son los principales desafíos de ciberseguridad asociados con el uso de Serverless Computing?

Basados en el análisis de los artículos de estudio, se obtuvo como resultado que los desafíos a los cuales se enfrenta el Serveless Computing están enfocados en: un correcto aislamiento de recursos, monitoreo de seguridad, gestión de seguridad y protección de datos, limitación de recursos para los usuarios, ampliación de la superficie de ataque, disponibilidad de los servicios, que las funciones de la nube se coloquen en la instancia de la VM, exposición de la interfaz, medidas de privacidad inadecuadas en microservicios y funciones, reducir la latencia de inicio, agotamiento de recursos financieros, y en el manejo de modelos de programación óptimos. El Gráfico 4 indica los principales desafíos de acuerdo con el número de artículos.

Gráfico 4. Desafíos del serveless computing.

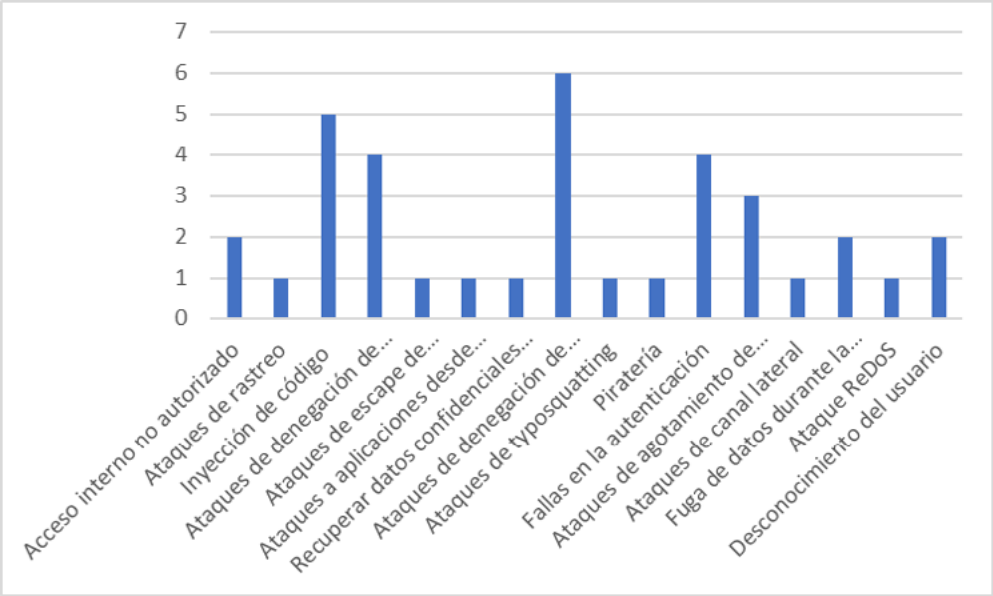


Fuente: Producción propia.

3. ¿Cuáles son las amenazas a las que se enfrenta el Serverless Computing?

Para este caso como resultado del análisis encontramos que, El 14% indica como amenza el acceso interno no autorizado, el 7% a los ataques de rastreo, el 36% la inyección de código, el 29% los ataques de denegación de servicio, el 7% ataques de escape de contenedores, el 7% ataques a aplicaciones desde plataformas maliciosas, el 7% recuperar datos confidenciales mediante tokens de sesión almacenados en tablas de entorno, el 43% ataques de denegación de billetera, el 7% ataques de typosquatting, el 7% piratería, el 29% fallas en la autenticación, el 21% ataques de agotamiento de invocaciones, el 7% ataques de canal lateral, el 14% fuga de datos durante la transmisión, el 7% ataque ReDos y el 14% el desconocimiento del usuario. El Gráfico 5 evidencia las amenazas relacionadas con el serveless computing según los artículos.

Gráfico 5. Amenazas en entornos de serveless computing.

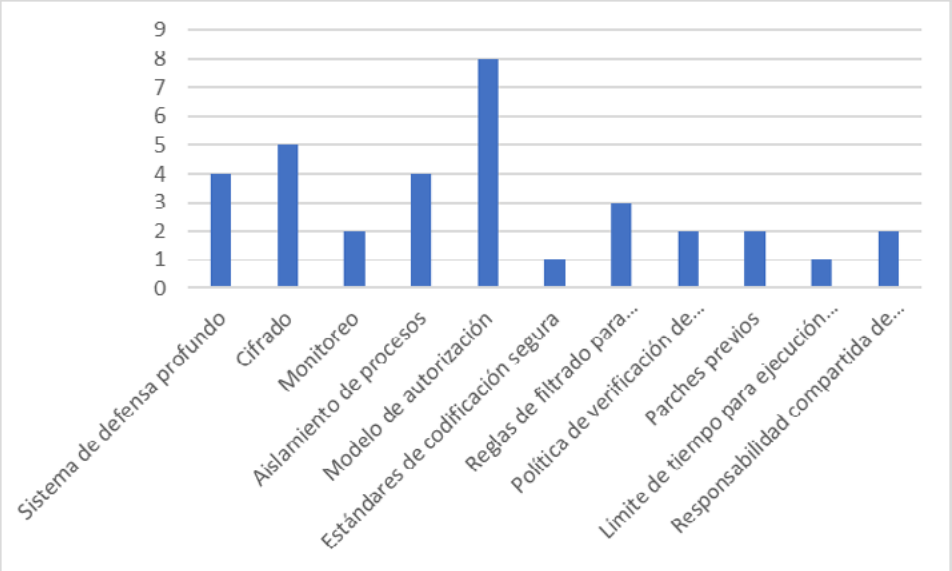


Fuente: Producción propia.

4. ¿Qué soluciones se han propuesto para mitigar los riesgos de seguridad asociados con el uso de Serverless Computing?

El resultado final del análisis, dio como resultado que las soluciones planteadas para mitigar las amenzas que enfrenta el Serveless Computing están direccionadas a: crear e implementar sistemas de defensa profundos, cifrado de los datos y comunicaciones, monitoreo de las funciones, el aislamiento de los procesos, implementar un modelo de autorización para los distintos usuarios, usar estándares de codificación segura, implementar reglas de filtrado para invocaciones de funciones, definir una política de verificación de propiedades, implementar parches previos a modo de prevención, establecer un límite de tiempo para ejecución de funciones, mantener una responsabilidad compartida de la nube y en la nube. El Gráfico 6 muestra las soluciones que plantean los autores de los artículos.

Gráfico 6. Soluciones para mitigar amenazas en entornos de serveless computing.



Fuente: Producción propia.

Discusión

Como podemos observar, serverless computing ha emergido como una innovación significativa en el ámbito de la computación en la nube, permitiendo a los desarrolladores centrarse en la lógica empresarial sin preocuparse por la gestión de infraestructura que estará a cargo directamente del proveedor, además el escalamiento automático y el costo según el servicio utilizado está captando cada vez más la atención de los usuarios.

Sin embargo, al ser una tecnología relativamente nueva, enfrenta varios desafíos relacionados mayormente con la gestión y monitoreo de la seguridad y privacidad, ya que se debe garantizar la confidencialidad, integridad y disponibilidad de los datos, tal como se muestra en el Gráfico 4.

Se destacan varias amenzas a las que se enfrentan los entornos serveless que son los ataques de denegación de billetera, la inyección de código, ataques de denegación de servicio, fallos de autenticación y los ataques de agotamiento de invocaciones, los cuales se mencionan en el Gráfico 5.

Al tener conocimiento de los posibles ciberataques, existe la capacidad de responder a estos de forma preventiva. Es por ello, que en la Figura 6 se indican las soluciones de seguridad recomendadas por los autores, las cuales abarcan el uso de un modelo de autorización para los distintos usuarios, el cifrado de los datos y comunicaciones, la creación e implementación de un sistema de defensa basado en datos de prueba, el aislamiento de procesos entre funciones, establecer reglas de filtrado para invocación de funciones y límites de tiempo para su ejecución.

Conclusión

El objetivo de esta revisión sistemática de literatura fue identificar el estado actual de serverless computing desde el ámbito de la ciberseguridad, determinando los beneficios, desafíos de seguridad y las soluciones propuestas en 14 artículos seleccionados.

En resumen, el estudio puede ayudar a identificar y contrarrestar los ciberdelitos, ya que se conoce los principales desafíos y amenazas que deben ser considerados cuidadosamente. Las amenazas relacionadas la latencia de arranque en frío, la limitada capacidad de control sobre la infraestructura y la complejidad en la gestión de estados son problemas técnicos que pueden impactar negativamente el rendimiento y la funcionalidad de las aplicaciones, convirtiéndose en una preocupación financiera para las empresas.

Las soluciones de seguridad están enfocadas en salvaguardar la confidencialidad, integridad y disponibilidad de los datos y comunicaciones entre invocaciones. Además, la educación y capacitación para los usuarios es indispensable para este sector.

Referencias

Barrak, A., Petrillo, F., & Jaafar, F. (2022). Serverless on Machine Learning: A Systematic Mapping Study. *IEEE Access*, 10, 99337-99352. https://doi.org/10.1109/ACCESS.2022.3206366

Bocci, A., Forti, S., Ferrari, G.L., & Brogi, A. (2021). Secure FaaS orchestration in the fog: ¿How far are we? *Computing*, *103*(5), 1025-1056. https://doi.org/10.1007/s00607-021-00924-y

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, 9. https://doi.org/10.1016/j.mex.2022.101895

Ebrahimpour, H., Ashtiani, M., Bakhshi, F., & Bakhtiariazad, G. (2023). A heuristic-based package-aware function scheduling approach for creating a trade-off between cold start time and cost in FaaS computing environments. *The Journal of Supercomputing*, *79*(11), 12142-12190. https://lc.cx/vUebib

Gill, S. S. (2024). Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions. *Internet Technology Letters*, *7*(1). https://doi.org/10.1002/itl2.275

Hassan, H. B., Barakat, S. A., & Sarhan, Q. I. (2021). Survey on serverless computing. *Journal of Cloud Computing*, *10*(1), 39. https://doi.org/10.1186/s13677-021-00253-7

Kelly, D., Glavin, F. G., & Barrett, E. (2021). Denial of wallet—Defining a looming threat to serverless computing. *Journal of Information Security and Applications*, 60. https://doi.org/10.1016/j.jisa.2021.102843

Li, X., Leng, X., & Chen, Y. (2023). Securing Serverless Computing: Challenges, Solutions, and Opportunities. *IEEE Network*, *37*(2), 166-173. https://doi.org/10.1109/MNET.005.2100335

Li, Y., Lin, Y., Wang, Y., Ye, K., & Xu, C. (2023). Serverless Computing: State-of-the-Art, Challenges and Opportunities. *IEEE Transactions on Services Computing*, *16*(2), 1522-1539. https://doi.org/10.1109/TSC.2022.3166553

Li, Z., Guo, L., Cheng, J., Chen, Q., He, B., & Guo, M. (2022). The Serverless Computing Survey: A Technical Primer for Design Architecture. *ACM Computing Surveys*, *54*(10), 1-34. https://doi.org/10.1145/3508360

Marin, E., Perino, D., & Di Pietro, R. (2022). Serverless computing: A security perspective. *Journal of Cloud Computing*, *11*(1), 69. https://doi.org/10.1186/s13677-022-00347-w

Morabito, G., Sicari, C., Ruggeri, A., Celesti, A., & Carnevale, L. (2023). Secure-by-design serverless workflows on the Edge–Cloud Continuum through the Osmotic Computing paradigm. *Internet of Things*, 22. https://doi.org/10.1016/j.iot.2023.100737

Ortega Candel, J. M., Mora Gimeno, F. J., & Mora Mora, H. (2024). Generation of a dataset for DoW attack detection in serverless architectures. *Data in Brief*, 52. https://doi.org/10.1016/j.dib.2023.109921

Ouyang, R., Wang, J., Xu, H., Chen, S., Xiong, X., Tolba, A., & Zhang, X. (2023). A Microservice and Serverless Architecture for Secure IoT System. *Sensors*, *23*(10), 4868. https://doi.org/10.3390/s23104868

Palma, G. D., Giallorenzo, S., Mauro, J., Trentin, M., & Zavattaro, G. (2023). Formally Verifying Function Scheduling Properties in Serverless Applications. *IT Professional*, *25*(6), 94-99. https://doi.org/10.1109/MITP.2023.3333071

Park, J., Kang, S., Lee, S., Kim, T., Park, J., Kwon, Y., & Huh, J. (2024). Hardware-hardened Sandbox Enclaves for Trusted Serverless Computing. *ACM Transactions on Architecture and Code Optimization*, *21*(1), 1-25. https://doi.org/10.1145/3632954

Wen, J., Chen, Z., Jin, X., & Liu, X. (2023). Rise of the Planet of Serverless Computing: A Systematic Review. *ACM Transactions on Software Engineering and Methodology*, *32*(5), 1-61. https://doi.org/10.1145/3579643

Zhang, S., Luo, X., & Litvinov, E. (2021). Serverless computing for cloud-based power grid emergency generation dispatch. *International Journal of Electrical Power & Energy Systems*, 124. https://doi.org/10.1016/j.ijepes.2020.106366

Autores

Ximena del Carmen Pacheco Armijos. Ingeniero de Sistemas, estudiante del máster de Ciberseguridad de la Universidad Católica de Cuenca.

Andrés Sebastián Quevedo Sacoto. Master in Geometry and Systems Engineer: Teacher and researcher at the at the University Católica of Cuenca.

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes ajenas a este artículo.

Notas

Este artículo es realizado como parte del proceso de titulación de posgrado.