Revista Amazonía Digital

Vol. 4 Núm. 1: e364 (2025)
https://doi.org/10.55873/rad.v4i1.364
e-ISSN: 2810-8701
Universidad Nacional Amazónica de Madre de Dios

Artículo de Revisión / Review Article

Análisis de la automatización en la ciberseguridad de entornos en la nube: Una revisión de la literatura

Analysis of automation in cybersecurity of cloud environments: A literature review

Richie Bryan Valdivia-Vilchez [1*]; Juan Albarrán-Romero [1]; Brenda Lucia León-Tiravanti [1]; Yngue Elizabeth Ramirez-Pezo [1]

[1] Universidad Peruana Unión, Tarapoto, Perú

Recibido: 15/10/2024
Aceptado: 23/11/2024
Publicado: 30/01/2025

*Autor de correspondencia: richie.valdivia@upeu.edu.pe

Resumen: La creciente adopción de tecnologías en la nube ha planteado nuevos desafíos en materia de ciberseguridad, especialmente ante el aumento de amenazas automatizadas. Este artículo presenta una revisión sistemática de la literatura sobre la automatización en la ciberseguridad de entornos en la nube, enfocándose en las técnicas, herramientas y enfoques recientes implementados para mejorar la detección, respuesta y mitigación de incidentes. Se analizaron 17 estudios relevantes publicados entre 2018 y 2023, considerando criterios como calidad, relevancia y aporte científico. Los resultados muestran que la inteligencia artificial, el aprendizaje automático y los sistemas automatizados de respuesta a incidentes son fundamentales para enfrentar amenazas complejas en la nube. Finalmente, se identifican tendencias, brechas de investigación y recomendaciones para futuros trabajos en el área.

Palabras clave: automatización; chatbots; ciberseguridad; computación en la nube; inteligencia artificial

Abstract: The growing adoption of cloud technologies has introduced new cybersecurity challenges, particularly with the rise of automated threats. This article presents a systematic literature review on automation in cloud cybersecurity, focusing on recent techniques, tools, and approaches implemented to enhance incident detection, response, and mitigation. A total of 17 relevant studies published between 2018 and 2023 were analyzed, considering quality, relevance, and scientific contribution. The results show that artificial intelligence, machine learning, and automated incident response systems play a crucial role in addressing complex threats in cloud environments. Finally, research trends, knowledge gaps, and recommendations for future work in the field are identify.

Keywords: automation; chatbots; cybersecurity; cloud computing; artificial intelligence

Cómo citar / Citation: Valdivia-Vilchez, R. B., Albarrán-Romero, J., León-Tiravanti, B. L. & Ramirez-Pezo, Y. L. (2025). Análisis de la automatización en la ciberseguridad de entornos en la nube: Una revisión de la literatura. *Revista Amazonía Digital*, 4(1), e364. 1https://doi.org/10.55873/rad.v4i1.364

1. Introducción

Actualmente, la seguridad en la nube es un tema crucial para las organizaciones que manejan grandes volúmenes de datos, debido al aumento exponencial de datos y servicios migrados a entornos de computación en la nube (Nawshin et al., 2024). Las amenazas en la nube, como los ciberataques y las brechas de seguridad, han incrementado la preocupación sobre la efectividad de los sistemas de protección. Sin embargo, la complejidad inherente a los entornos en la nube y la naturaleza diversa de las amenazas han demostrado que los sistemas tradicionales de detección y respuesta ante incidentes resultan insuficientes para hacer frente a estos desafíos.

Una de las soluciones emergentes más prometedoras es la incorporación de chatbots de seguridad, los cuales permiten una interacción en tiempo real con los sistemas de seguridad. Esta tecnología no solo facilita la comunicación, sino que también automatiza tareas críticas, mejorando así la capacidad de respuesta ante incidentes en la nube (Golec et al., 2024). Aunque estudios recientes sugieren que los chatbots pueden reducir significativamente los tiempos de respuesta y mejorar la experiencia del usuario, existen barreras tecnológicas y de implementación que deben ser superadas para lograr su adopción generalizada (Bello et al., 2021).

El objetivo de esta revisión sistemática es evaluar cómo la integración de chatbots en sistemas de detección y respuesta ante incidentes en la nube puede optimizar la seguridad, identificando los métodos más efectivos, los desafíos tecnológicos y las posibles ventajas de su implementación. Asimismo, se investigarán las tecnologías emergentes que podrían fortalecer la capacidad de los sistemas de seguridad en la nube para responder de manera más eficiente a las amenazas actuales (Anaya et al., 2024). Asimismo, se investigarán las tecnologías emergentes que podrían potenciar la capacidad de los sistemas de seguridad en la nube para responder de manera más eficiente a las amenazas actuales.

Para guiar esta investigación, se han formulado las siguientes preguntas de investigación:

- ¿Cuáles son los métodos más efectivos para integrar chatbots en sistemas de detección y respuesta en la nube?
- ¿Qué beneficios y desafíos se han documentado en la implementación de estos sistemas de seguridad?
- ¿Cuáles son las principales vulnerabilidades y amenazas de seguridad que afectan a los chatbots en la nube?

A través de esta revisión sistemática, se espera proporcionar una visión clara de cómo los chatbots pueden revolucionar la seguridad en la nube, destacando los avances actuales y los desafíos pendientes para su implementación exitosa.

2. Materiales y métodos

Esta investigación se enmarca en una Revisión Sistemática de la Literatura (RSL), enfocada en el análisis de la Automatización en la Ciberseguridad de entornos en la nube, mediante la Implementación de sistemas de detección y respuesta ante incidentes (IDR) integrados en chatbots de seguridad. Se empleó un diseño observacional no experimental, basado en el análisis de estudios previos publicados en bases de datos científicas. La selección de estudios se realizó aplicando criterios de rigurosidad metodológica para asegurar la Validez, relevancia y calidad de la Información.

Para estructurar la búsqueda de información y formular preguntas clave de investigación, se aplicó la Metodología PICOC:

P (Población/Problema): Sistemas de ciberseguridad en entornos de computación en los ángeles nube.

I (Intervención): Implementación de sistemas de detección y respuesta ante incidentes (IDR) automatizados mediante chatbots de seguridad.

C (Comparación): No se consideró un grupo de control, ya que se evalúan los beneficios frente a la ausencia de automatización o métodos tradicionales.

O (Outcome/Resultados): Mejora en la Capacidad de respuesta, reducción del tiempo de detección de amenazas y mayor eficiencia operativa en la Seguridad en la nube.

C (Contexto): Entornos de computación en la Nube en los sectores público y privado, sin restricción geográfica.

Para la evaluación de la calidad metodológica de los estudios incluidos, se utilizó la herramienta Parsifal, que permite valorar aspectos como la validez interna, el riesgo de sesgo y la relevancia clínica de los resultados. Cada artículo fue analizado de forma independiente por los 3 integrantes del equipo, y cualquier discrepancia fue resuelta mediante consenso. Esta evaluación garantizó la inclusión de estudios con un nivel de evidencia adecuado para los fines de esta revisión. Cada estudio fue evaluado de una escala de 0 a 1, donde:

Tabla 1. Escala de evaluación

Respuesta	Descripción	Puntaje
SI	Cumple completamente con el criterio evaluado	1.0
Parcialmente	Cumple parcialmente con el criterio evaluado	0.5
NO	No cumple con el criterio evaluado	0.0

2.1. Criterios de inclusión y exclusión

En este artículo de revisión, la selección de estudios se llevó a cabo mediante una estrategia sistemática basada en la metodología PRISMA. Se establecieron criterios de inclusión y exclusión con el fin de garantizar relevancia, calidad y validez de los estudios realizados.

Los criterios de inclusión consideraron únicamente artículos publicados en revistas científicas indexadas, priorizando aquellos estudios empíricos o experimentales sobre la implementación de chatbots en sistemas de detección y respuesta ante incidentes en la nube. Además, se incluyeron investigaciones que describieran de manera clara su metodología, métricas de evaluación y resultados, con aplicaciones en sectores públicos y privados.

Por otro lado, se excluyeron estudios duplicados, revisiones teóricas, metaanálisis y capítulos de libros, debido a que no aportan evidencia empírica directa. También se descartaron artículos sin una descripción clara de su metodología o evaluación, así como aquello cuyo contenido no guardara relación con los objetivos de esta revisión. En casos de estudios con contenido similar, se priorizó el más completo y relevante.

Tabla 2. Principales criterios de exclusión y exclusión aplicados

Inclusión	Exclusión
a. Se consideran todos aquellos artículos provenientes de base de datos indexadas.	a. Serán excluidos artículos duplicados.
b. Se incluirán estudios publicados dentro del rango de temporalidad.	b. Se rechazarán artículos con contenido similar, quedándose aquellos con mayor profundidad y relevancia.
c. Se aceptarán artículos provenientes de revistas científicas que incluyan estudios empíricos o análisis experimentales sobre la implementación de chatbots en sistemas de detección y respuesta ante incidentes en la nube.	c. Serán excluidos los estudios secundarios, revisiones teóricas, metaanálisis y capítulos de libros.

d. Se seleccionarán estudios que describan con claridad su metodología, métricas de evaluación y resultados.	d. Se excluirán artículos que no detallen su metodología de implementación o evaluación.

2.2. Fuentes de Información

La presente revisión sistemática se realizó utilizando dos bases de datos académicas: IEEE, Scopus, Web of Science y ScienceDirect. Estas plataformas proporcionan acceso a estudios revisados por pares y publicaciones de alta calidad, especialmente en áreas de ciberseguridad, inteligencia artificial y computación en la nube. Estas bases de datos fueron seleccionadas debido a su relevancia en la investigación tecnológica y su capacidad para ofrecer artículos actualizados sobre la automatización de la seguridad en la nube mediante el uso de chatbots.

Cada una de estas fuentes proporciona herramientas avanzadas de búsqueda, lo que permite identificar de manera eficiente estudios que estén alineados con el objetivo de esta revisión. Estas plataformas facilitan el acceso a estudios que ofrecen evidencia empírica y resultados relevantes sobre la eficacia de estas tecnologías emergentes en entornos de computación en la nube.

2.3. Estrategia de Búsqueda

La búsqueda se limitó a artículos publicados en los últimos cinco años (entre 2019 y 2024), con el objetivo de incluir los estudios más recientes y relevantes sobre la implementación de chatbots en la seguridad en la nube. Durante este proceso, participaron tres investigadores, quienes colaboraron en la identificación y selección de los estudios más relevantes.

En nuestra estrategia de búsqueda, se incluyeron términos relacionados con la ciberseguridad en la nube, incidentes de seguridad, y tecnologías emergentes como chatbots de seguridad. Las palabras clave utilizadas fueron seleccionadas cuidadosamente para abarcar aspectos clave de la seguridad en la nube, con el fin de encontrar estudios que proporcionaran evidencia sobre la eficacia y los desafíos de la implementación de chatbots en sistemas de detección y respuesta.

Tabla 3. Principales cadenas de búsqueda con las principales palabras clave

Cadenas de búsquedas con palabras clave principales
(" cybersecurity automation" OR "security automation ") AND
("cloud environments" OR "cloud infrastructure" OR "cloud platforms") AND
("incident detection" OR "incident response" OR "threat detection" OR "threat response") AND
("artificial intelligence" OR "AI-based automation" OR "machine learning") AND
("implementation" OR "integration" OR "deployment") AND
("effectiveness" OR "efficiency" OR "challenges" OR "limitations") AND
("cloud security frameworks" OR "security orchestration" OR "SIEM" OR "SOAR")

2.4. Proceso de Extracción de los Datos

Para la extracción de datos, se utilizó un formulario estandarizado que incluyó campos clave como año de publicación, tipo de estudio (cualitativo o cuantitativo), diseño de investigación (descriptivo o experimental), beneficios y desafíos en la integración de chatbots de seguridad, tecnologías de inteligencia artificial empleadas y el impacto en los tiempos de respuesta ante incidentes.

El proceso de selección inicio con la identificación de 105 artículos provenientes de base de datos indexadas, distribuidos de la siguiente manera: Scopus (35), IEEE Digital Library (28), Web of Science (17) y ScienceDirect (25). Tras eliminar 37 registros duplicados, se obtuvieron 68 estudios adecuados para el cibrado. En esta fase, se aplicaron los criterios de inclusión y exclusión previamente definidos, lo que llevó a la eliminación de 51 artículos. Estos fueron descartados principalmente porque no implementaban chatbots en entornos de ciberseguridad en la nube, eran revisiones teóricas o capítulos de libros sin resultados empíricos o no evaluaban métricas como tiempos de respuesta y eficacia. Finalmente, 17 artículos fueron seleccionados para la extracción de datos y análisis.

El proceso de extracción fue realizado por los 3 autores de este estudio, quienes trabajamos de manera independiente en la recopilación de datos. Cada autor revisó los artículos seleccionados y completo el formulario de extracción. Posteriormente, se compararon los resultados y en caso de discrepancia se llevó a cabo una discusión en grupo para analizar los datos en conflicto. Si no se llegaba a un acuerdo inmediato, se revisaba nuevamente el artículo en cuestión y se tomaba una decisión consensuada basada en la evidencia presentada en el estudio.

Para gestionar las referencias y evitar duplicaciones, se utilizó la herramienta Parsifal, la cual permitió identificar estudios repetidos y eliminarlos de la base de datos final. Esto aseguró un proceso de extracción de datos preciso y eficiente.

2.5. Lista de datos

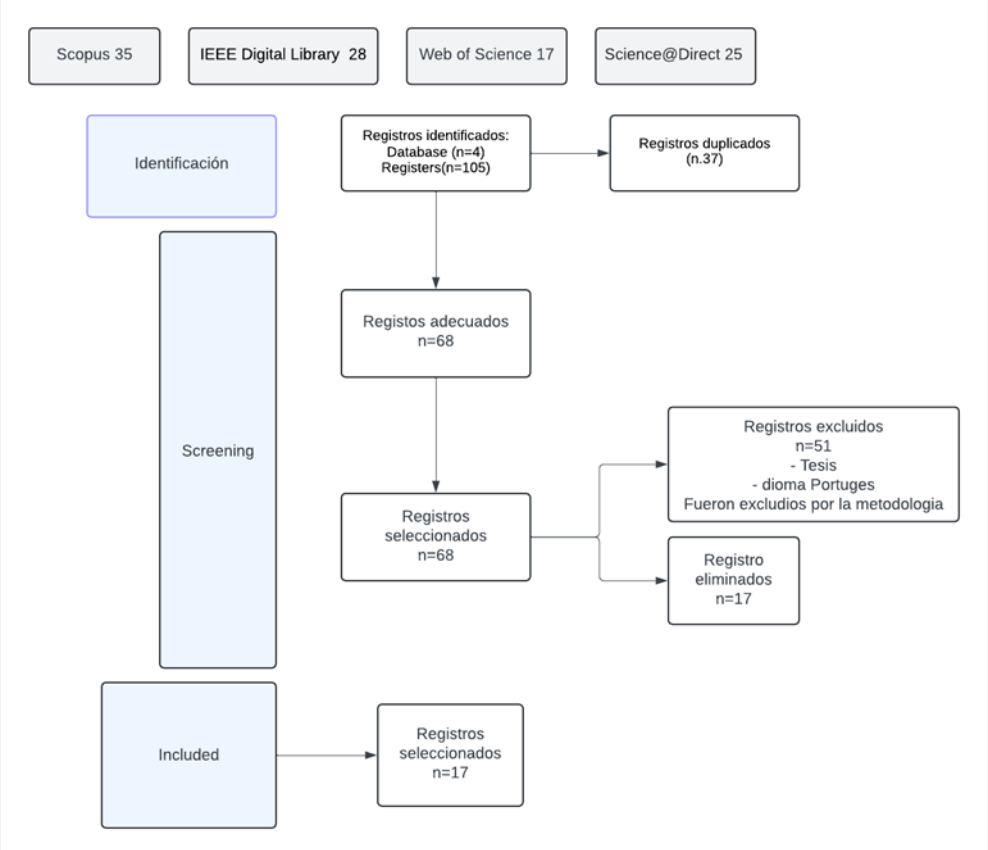

Figura 1. Diagrama de flujo de prisma

3. Resultados y discusión

3.1. Métodos efectivos para integrar chatbots en sistemas de detección y respuesta en la nube

Estos chatbots pueden aprender de incidentes previos y adaptarse a nuevas amenazas sin necesidad de intervención humana constante, lo que los convierte en una herramienta fundamental para la seguridad en la nube (Montes Gil, 2024). Además, los modelos de IA basados en aprendizaje profundo han demostrado ser especialmente útiles para procesar grandes cantidades de datos en tiempo real, lo que permite identificar patrones de comportamiento anómalos en el tráfico de red (Wang et al., 2022).

Otro método que ha demostrado es el uso de algoritmos de machine learning supervisado y no supervisado para mejorar la precisión en la detección de amenazas. Los chatbots que integran estos algoritmos pueden clasificar incidentes de seguridad en función de su gravedad y activar respuestas automáticas o escalarlas según sea necesarios (Vásquez Valarezo, 2020). Según estudios, la capacidad de estos sistemas para identificar amenazas en tiempo real y reducir el tiempo de respuesta ha mejorado significativamente la seguridad en entornos de nube (Mata Suñé, 2023).

Además, se ha explorado la combinación de blockchain con chatbots permite garantizar que las interacciones realizadas por estos sean inmutables y seguras, protegiendo contra la manipulación de datos y asegurando la trazabilidad de todas las acciones realizadas por el chatbot (Adel et al., 2022).

Tabla 4. Métodos de implementación de chatbots en ciberseguridad

Método	Descripción	Ejemplo de implementación
Chatbots cognitivos con IA	Utilizan inteligencia artificial avanzada para identificar y responder a incidentes de manera autónoma.	IBM Watson Security Chatbot
Machine learning supervisado y no supervisado	Permite mejorar la detección de amenazas y automatizar la toma de decisiones.	Algoritmos de detección de anomalías en AWS GuardDuty
Integración con blockchain	Garantiza la seguridad e integridad de los datos manejados por los chatbots.	Aplicaciones de blockchain para la gestión de credenciales de seguridad.

3.2. Beneficios y desafíos en la implementación de sistemas de seguridad con chatbots

Los chatbots conversacionales han revolucionado la atención al cliente. Un estudio de Gartner prevé que el 38% de las organizaciones implementará chatbots en los próximos dos años, lo que representa un aumento del 40% en la adopción (Golec et al., 2024). Pero no se trata solo de integrar IA; el verdadero reto es ofrecer experiencias satisfactorias. Ahí es donde los chatbots con Inteligencia Artificial Conversacional son clave, mejorando la interacción con los usuarios (Anaya et al., 2024).

Tabla 5. Beneficios de implementación de chatbots en ciberseguridad

Beneficios	
Automatización de la respuesta	Permite reducir tiempos de redacción ante incidentes sin intervención humana.
Monitoreo continuo	Ofrece supervisión y detección de amenazas
Reducción de costos	Minimiza la necesidad de personal humano en tareas repetitivas.
Mejora en la precisión	Uso de IA y machine learning para mejorar la detección de amenazas.

Escalabilidad	Capacidad de adaptarse a necesidades cambiantes sin comprometer el rendimiento.
Integración con otras tecnologías	Compatible con blockchain y sistemas de autenticación avanzada.

Con el uso generalizado de computadoras cuánticas con alto poder de procesamiento, los algoritmos criptográficos se volverán vulnerables. Por esta razón, los datos almacenados en QCC pueden causar problemas de privacidad ya que serán obtenidos por terceros (Mukherjee et al., 2017). Los chatbots con IA pueden mejorar la eficiencia del sistema de seguridad mediante la automatización de tareas, como la respuesta a incidentes o la resolución de consultas de seguridad sin la intervención humana (Shruti et al., 2024).

Tabla 6. Desafíos de implementación de chatbots en ciberseguridad

Desafíos	
Altos costos iniciales	La implementación requiere una inversión en infraestructura y desarrollo
Dependencia de infraestructura en la nube	Requiere acceso constante a servicios de computación en la nube.
Limitaciones en la comprensión del lenguaje natural	Los chatbots pueden tener dificultades para interpretar consultas complejas.
Riesgos de ataques dirigidos	Vulnerabilidad a ataques como la manipulación de IA o ingeniería social.
Problemas de privacidad y seguridad	Puede existir riesgo de exposición de datos si no se aplican medidas adecuadas.
Mantenimiento y actualización constante	Es necesario monitorear y actualizar regularmente los modelos de IA.

3.3. Vulnerabilidades y amenazas de seguridad que afectan a los chatbots en la nube

Los chatbots también son susceptibles a descargas automáticas de software malicioso, que pueden instalar troyanos o ransomware sin el consentimiento del usuario. Estas descargas son facilitadas por vulnerabilidades en sistemas operativos o navegadores, permitiendo a los atacantes obtener control sobre el sistema y extraer información confidencial. Además, los chatbots son objeto de amenazas externas, como el phishing y el spearphishing, donde los ciberdelincuentes envían correos electrónicos o mensajes personalizados para engañar a los usuarios y obtener credenciales de acceso, aumentando la probabilidad de éxito de estos ataques (Charfeddine et al., 2024) y (Bokolo & Daramola, 2024).

Las vulnerabilidades y amenazas de seguridad que afectan a los chatbots en la nube se pueden clasificar en varias categorías, destacando la inyección de prompts maliciosos y la explotación de vulnerabilidades en APIs y sistemas de backend. Las APIs utilizadas por los chatbots representan un riesgo significativo si no están bien protegidas. Los atacantes pueden aprovechar estas vulnerabilidades para acceder a bases de datos y obtener información confidencial. Además, los sistemas de backend, que a menudo tienen menos protección, son objetivos fáciles para los atacantes, comprometiendo los servicios en la nube y la integridad de los datos (Mata Suñé, 2023).

Tabla 7. Principales vulnerabilidades en ciberseguridad y sus ejemplos

Vulnerabilidad	Descripción	Ejemplo
Ejecución remota de código RCE	Permite a los atacantes ejecutar comandos maliciosos en el sistema.	Ataques dirigidos a APIs vulnerables
Inyección de SQL	Introducción de código malicioso en consultas de bases de datos.	Acceso no autorizado a credenciales

Ataques de fuerza bruta	Intentos repetidos de acceso mediante combinaciones de contraseñas.	Robo de credenciales en plataformas de autenticación
Phishing y spear phishing	Engaños para obtener credenciales o acceso no autorizado.	Suplantación de identidad en interfaces de chatbots
Fallas en APIs y backend	Errores en la implementación de seguridad en sistemas conectados.	APIs expuestas sin autenticación adecuada

3.4. Malware y descargas automáticas

Los chatbots de seguridad en la nube pueden ser vulnerables a ataques de malware, que afectan la integridad y confiabilidad de los sistemas de detección y respuesta ante incidentes. Los atacantes pueden explotar vulnerabilidades en los chatbos para distribuir software malicioso a través de interacciones automatizadas o respuestas manipuladas.

Además, algunas técnicas de ingeniería social pueden inducir a los usuarios a descargar archivos infectados a través de chatbots mal protegidos. Para mitigar estas amenazas, es crucial implementar filtros avanzados de detección de malware en los chatbots, combinados con tecnologías de sandboxing y monitoreo en tiempo real (Sai et al., 2024).

3.5. Riesgos asociados a la inteligencia artificial avanzada

Se mencionan bien la inteligencia artificial ha mejorado significativamente la detección y respuesta a incidentes en la nube, también presenta nuevos riesgos. Los chatbots basados en IA pueden ser manipulados mediante ataques adversariales, donde se introducen datos diseñados para engañar a los algoritmos de seguridad y evitar la detección de amenazas reales. Otro riesgo es el uso de IA generativa para automatizar ataques, lo que podría facilitar la propagación de malware, pishing o fraudes en línea. Para mitigar estos riesgos, se recomienda la implementación de auditorías continuas en los modelos de IA, así como mecanismos de aprendizaje seguro y controlado para evitar la manipulación de los chatbots de seguridad (Sai et al., 2024) y (Torres Arrabal, 2024).

4. Discusión

Al analizar estudios que abordan las vulnerabilidades y amenazas que enfrentan los chatbots en entornos de nube, se observa una amplia variedad de enfoques para identificar riesgos y proponer soluciones. Una tendencia clara es la preferencia por el uso de tecnologías emergentes, como la inteligencia artificial generativa, con el objetivo de mejorar la capacidad de detección y respuesta ante incidentes. Por ejemplo, Nawshin et al. (2024) destaca el uso de IA junto con técnicas de privacidad diferencial como herramientas prometedoras para fortalecer la seguridad en redes IoT, mejorando la respuesta ante ataques. Sin embargo, no todos los estudios son optimistas: autores como Charfeddine et al. (2024) advierten sobre las limitaciones de estas tecnologías, especialmente en cuanto a la escalabilidad y la protección de la privacidad, lo que sugiere que su implementación aún enfrenta barreras importantes.

Una de las principales críticas a los estudios analizados es su tendencia a centrarse en soluciones técnicas, dejando de lado aspectos humanos y organizacionales que también impactan en la efectividad de los chatbots. Por ejemplo, Anaya et al. (2024) se enfoca en los beneficios técnicos de estas herramientas sin considerar factores como la cultura organizacional, las políticas internas de seguridad o el nivel de formación de los usuarios. Esta omisión es relevante, ya que una implementación eficaz no solo requiere tecnología avanzada, sino también una preparación adecuada del personal y una estrategia organizacional alineada. Además, existen diferencias notables entre sectores: el sector privado tiende a adoptar estas tecnologías con mayor agilidad debido a su capacidad de inversión, mientras que el sector público enfrenta mayores restricciones

presupuestarias y regulatorias, lo que retrasa la adopción y adaptación de soluciones innovadoras.

Respecto a las vulnerabilidades más críticas, estudios como Nawshin et al. (2024) y Mata Suñé (2023) coinciden en señalar la ejecución remota de código (RCE) y la inyección SQL como amenazas predominantes. Si bien algunos autores apuestan por soluciones basadas en IA, otros, como Bokolo & Daramola (2024), sostienen que estas tecnologías deben integrarse dentro de un marco más amplio que incluya prácticas tradicionales de seguridad, como el cifrado y la autenticación robusta. Esta visión conservadora toma especial relevancia en contextos donde existen sistemas heredados, especialmente en el sector público, lo que eleva la exposición a riesgos cibernéticos.

Un aporte original es el de Mata Suñé (2023), quien plantea el uso ofensivo de la IA generativa por parte de actores maliciosos. Esta perspectiva genera un debate importante sobre el doble filo de estas tecnologías: así como permiten defender infraestructuras críticas, también pueden ser empleadas para lanzar ataques sofisticados. Esto plantea la necesidad urgente de una reflexión ética en torno al desarrollo y uso de la inteligencia artificial, tanto desde la perspectiva empresarial como desde la función reguladora del sector público.

Finalmente, los estudios coinciden en recomendar un enfoque híbrido que combine tecnologías emergentes con estrategias de seguridad más tradicionales. Autores como Torres Arrabal (2024), sostienen que depender exclusivamente de soluciones basadas en IA o blockchain puede ser insuficiente. Por el contrario, integrar estas tecnologías con prácticas consolidadas como la segmentación de redes, autenticación multifactor o control de acceso granular ofrece mayores garantías de seguridad. Sin embargo, es necesario tener en cuenta que la efectividad de estas estrategias varía según el contexto: mientras en el sector privado la rápida adopción tecnológica puede ser vista como una ventaja competitiva, en el sector público se requiere un equilibrio entre innovación, normativas y tiempos de implementación más prolongados.

5. Conclusiones

La revisión sistemática permitió evidenciar que la integración de chatbots en la ciberseguridad de entornos en la nube representa una innovación tecnológica con alto potencial para optimizar los procesos de detección y respuesta ante incidentes. La aplicación de modelos de inteligencia artificial avanzada, como el aprendizaje automático y el procesamiento de lenguaje natural, potencia la capacidad de estos sistemas para analizar grandes volúmenes de datos en tiempo real, responder de manera autónoma y adaptarse a nuevas amenazas. Además, enfoques híbridos como la combinación de blockchain con chatbots ofrecen un valor añadido al reforzar la integridad y seguridad de las interacciones, haciendo que la respuesta a incidentes sea más rápida, precisa y confiable.

No obstante, la implementación de estos sistemas no está exenta de retos. Las principales barreras incluyen la escalabilidad de los recursos, la gestión de datos sensibles y las vulnerabilidades frente a ataques cibernéticos complejos. Aunque los beneficios como la automatización, la reducción de costos operativos y la vigilancia continua son significativos, es crucial que las organizaciones desarrollen estrategias de protección robustas, incluyendo cifrado de extremo a extremo y controles de acceso avanzados. Solo mediante una implementación responsable y consciente de sus riesgos, los chatbots podrán consolidarse como herramientas clave en la ciberseguridad en la nube.

En conclusión, la integración de chatbots en la ciberseguridad de entornos en la nube es una estrategia prometedora que puede revolucionar la forma en que las organizaciones gestionan la detección y respuesta ante incidentes. Sin embargo, para su adopción exitosa, es esencial que las empresas aborden los desafíos de privacidad y escalabilidad, al tiempo que refuerzan las medidas de seguridad para mitigar las vulnerabilidades inherentes a estos sistemas.

Financiamiento

Ninguno.

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

Contribución de autores

R. B. Valdivia Vilchez: Definió y conceptualizó el tema de investigación, participó en el diseño metodológico, colaboró en la elaboración y aplicación de los instrumentos, y realizó la investigación. Además, elaboró el primer borrador del artículo científico, y contribuyó a la revisión y edición final del documento.

J. Albarrán Romero: Participó en el diseño metodológico del estudio, estableció los indicadores para la elaboración de los instrumentos, y colaboró en la aplicación de los mismos. Realizó el análisis estadístico de los datos obtenidos y participó activamente en la redacción del primer borrador. También revisó y editó el artículo.

B. L. León Tiravanti: Supervisó el desarrollo completo de la investigación, apoyó en la definición del marco teórico y conceptual, y revisó el análisis de los resultados. Contribuyó en la revisión general del artículo y coordinó las mejoras en la versión final.

Y. L Ramírez-Pezo: Colaboró en el análisis estadístico de los datos y brindó apoyo técnico en la interpretación de los resultados. También participó en la revisión del manuscrito y la edición final del artículo.

Referencias bibliográficas

Adel, K., Elhakeem, A., & Marzouk, M. (2022). Chatbot for construction firms using scalable blockchain network. *Automation in Construction*, *141*, 104390. https://doi.org/10.1016/j.autcon.2022.104390

Anaya, L., Braizat, A., & Al-Ani, R. (2024). Implementing AI-based Chatbot: Benefits and Challenges. *Procedia Computer Science*, *239*, 1173-1179. https://doi.org/10.1016/j.procs.2024.06.284

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Davila Delgado, J. M., Akanbi, L. A., Ajayi, A. O., & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441. https://doi.org/10.1016/j.autcon.2020.103441

Bokolo, Z., & Daramola, O. (2024). Detección de amenazas y vulnerabilidades de seguridad en chatbots de seguros mediante STRIDE. *Scientific Reports*, *14*(1), 17920. https://doi.org/10.1038/s41598-024-68791-z

Charfeddine, M., Kammoun, H. M., Hamdaoui, B., & Guizani, M. (2024). ChatGPT's Security Risks and Benefits: Offensive and Defensive Use-Cases, Mitigation Measures, and Future Implications. *IEEE Access*, *12*, 30263-30310. https://doi.org/10.1109/ACCESS.2024.3367792

Golec, M., Hatay, E. S., Golec, M., Uyar, M., Golec, M., & Gill, S. S. (2024). Quantum cloud computing: Trends and challenges. *Journal of Economy and Technology*, *2*, 190-199. https://doi.org/10.1016/j.ject.2024.05.001

Mata Suñé, E. (2023). *Chatbot cognitivo capaz de dar respuesta y gestionar incidentes de ciberseguridad*

[Universidad Politécnica de Catalunya]. https://upcommons.upc.edu/server/api/core/bitstreams/652a59b8-eb80-45f2-9f11-b395df31a629/content

Montes Gil, J. A. (2024). *Servicios en la Nube para la deteccion de ataques de denegacion de servicios*.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and Privacy in Fog Computing: Challenges. *IEEE Access*, *5*, 19293-19304. https://doi.org/10.1109/ACCESS.2017.2749422

Nawshin, F., Unal, D., Hammoudeh, M., & Suganthan, P. N. (2024). AI-powered malware detection with Differential Privacy for zero trust security in Internet of Things networks. *Ad Hoc Networks*, *161*, 103523. https://doi.org/10.1016/j.adhoc.2024.103523

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. *IEEE Access*, *12*, 53497-53516. https://doi.org/10.1109/ACCESS.2024.3385107

Shruti, Rani, S., Shabaz, M., Dutta, A. K., & Ahmed, E. A. (2024). Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing. *Alexandria Engineering Journal*, *102*, 66-74. https://doi.org/10.1016/j.aej.2024.05.085

Torres Arrabal, M. (2024). *Sistema de Detección de Amenazas en la Nube para Entornos Híbridos* [Escuela Politécnica Superior de Ingeniería de Villanueva y Geltrú]. https://upcommons.upc.edu/server/api/core/bitstreams/15a2cce3-ede5-4bb7-9664-8acf531c9dbe/content

Vásquez Valarezo, E. W. (2020). *Implementación de un Chatbot en lenguaje natural, utilizando técnicas de inteligencia artificial y aprendizaje profundo para el aprendizaje de las tecnologías de la información* [Universidad de las Américas]. http://dspace.udla.edu.ec/handle/33000/13094

Wang, B.-X., Chen, J.-L., & Yu, C.-L. (2022). An AI-Powered Network Threat Detection System. *IEEE Access*, *10*, 54029-54037. https://doi.org/10.1109/ACCESS.2022.3175886