INFORME FINAL PROYECTO DE INVESTIGACIÓN

- **Título del trabajo de investigación**:
  Técnicas Avanzadas de Identidad Digital y Aplicación de Zero Trust para la Transición a la Web 3.0
- **Nombres y Apellidos del Investigador o del Equipo Investigador**:
  :
    - *Director: Dr. Miguel Méndez-Garabetti*

      Equipo de trabajo:

    - *Lic. Eduardo Piray*
    - *Guillermo Romero Arregin*
    - *Ricardo González*
    - *Santiago Araya*
    - *Barbara Schmidt*
- **Mes y año de la presentación del informe final**: *Febrero 2025*

Resumen

El presente informe expone el diseño e implementación de diversos escenarios de prueba para evaluar la seguridad y eficiencia de sistemas de gestión de identidad y acceso (IAM) en aplicaciones web, abarcando la transición de la Web 2.0 a la Web 3.0. Se estudian protocolos de autenticación centralizados, federados y descentralizados, así como la propuesta de un modelo de autenticación multifactor en blockchain. Para ello, se emplearon metodologías de “red team” basadas en el marco Mitre ATT&CK y la táctica de *Credential Access*, junto con entornos virtuales configurados con Keycloak, WSO2 Identity Server y herramientas de emulación de ataques. Asimismo, se describe la incorporación de la tecnología blockchain para la autenticación descentralizada, explorando la creación de direcciones públicas adicionales como factores de seguridad. Los resultados evidencian fortalezas y limitaciones de cada enfoque, así como el potencial de la inteligencia artificial para administrar dinámicamente los factores de autenticación. Se concluye que la adopción de soluciones de identidad descentralizadas y la inclusión de esquemas multifactor con blockchain pueden incrementar la seguridad sin afectar significativamente la experiencia de usuario.

Palabras clave

- Web 3.0
- Identidad digital
- Blockchain
- IAM (Identity and Access Management)
- Inteligencia Artificial
- Autenticación Multifactor

Índice

Introducción

Presentación del tema

La transición de la Web 2.0 a la Web 3.0 representa un cambio radical en la forma en que los usuarios interactúan con la información y los servicios digitales. En la Web 2.0, buena parte de la identidad digital de los individuos dependía de soluciones de autenticación centralizadas y del almacenamiento de datos personales en servidores controlados por grandes proveedores. Esta arquitectura centralizada, aunque efectiva en un principio, ha demostrado ser vulnerable a brechas de seguridad y a prácticas inadecuadas de protección de datos, lo cual se evidencia en numerosos incidentes de ciberataques masivos que han expuesto millones de credenciales.

Por otra parte, la Web 3.0 abre la puerta a tecnologías descentralizadas que ponen en manos de los usuarios un mayor control sobre su identidad digital y sus datos personales. Protocolos de blockchain y el uso de tokens no fungibles (NFT) para la representación de activos, credenciales y propiedades digitales ilustran un rumbo hacia una web más distribuida, con menor dependencia de autoridades centrales. Sin embargo, esta

transformación no elimina los desafíos de seguridad; más bien, los desplaza y reconfigura. El nuevo enfoque requiere sistemas más flexibles, capaces de integrarse con distintas aplicaciones, servicios y protocolos de autenticación que varían desde métodos tradicionales (como contraseñas o federaciones de identidad) hasta esquemas novedosos de verificación en blockchain.

En este escenario, el modelo de seguridad Zero Trust adquiere creciente relevancia. A diferencia del modelo de confianza perimetral, que asume que los sistemas y usuarios dentro de un entorno controlado son fiables, Zero Trust establece que ningún usuario ni dispositivo es confiable por defecto. Con ello, la validación y la autenticación se convierten en procesos continuos, reforzados por un monitoreo permanente de riesgos y el uso de múltiples factores de autenticación. Este énfasis en la verificación constante resulta especialmente pertinente cuando se considera la posibilidad de ataques automatizados, la aparición de nuevas vulnerabilidades en redes descentralizadas y la necesidad de unificar criterios de seguridad en ecosistemas cada vez más heterogéneos.

Justificación teórica y empírica

El avance tecnológico y el desarrollo de la Web 3.0 han transformado la forma en que los usuarios interactúan con el mundo digital. Con la creciente dependencia de los servicios en línea, la seguridad y la privacidad de la identidad digital se han convertido en preocupaciones fundamentales. La protección de los datos y la identidad del usuario es crucial no sólo para garantizar la privacidad y la confianza del usuario, sino también para mantener la integridad de los sistemas y las redes. En este contexto, es esencial investigar y entender las técnicas avanzadas de identidad digital y la aplicación del modelo de seguridad Zero Trust. Estas tecnologías y enfoques pueden ofrecer soluciones robustas para proteger la identidad digital y mejorar la seguridad en la Web 3.0. Sin embargo, la aplicación de estas técnicas y modelos en la práctica aún requiere una exploración y análisis significativos. Además, el potencial de la inteligencia artificial para mejorar la gestión de la identidad y el acceso merece ser investigado en profundidad. La IA podría proporcionar soluciones innovadoras para la autenticación y la gestión de la identidad, especialmente en el contexto de la autenticación de múltiples factores y el modelo de seguridad Zero Trust. Por lo expresado anteriormente, el estudio aquí propuesto se considera relevante y oportuno, ya que contribuirá a la comprensión de las implicaciones de la transición a la Web 3.0 para la seguridad y la privacidad de la identidad digital y su relación con las nuevas tecnologías de inteligencia artificial. Los resultados de esta investigación podrían informar el desarrollo de estrategias de seguridad más efectivas y el diseño de políticas públicas relacionadas con la seguridad de la identidad digital.

La correcta protección de la identidad digital en entornos cada vez más conectados resulta crítica para prevenir accesos no autorizados y garantizar la privacidad. Se analizan las bases conceptuales de IAM, así como frameworks de ciberseguridad orientados a la gestión de credenciales y a la descentralización (blockchain). El sustento empírico se obtuvo mediante pruebas prácticas de seguridad (*red team*), la integración de multifactor en blockchain y diversos experimentos con herramientas de virtualización y emulación de ataques.

Antecedentes

Las investigaciones recientes sobre la integración de Zero Trust, la gestión de identidad y acceso (IAM) y las tecnologías de la Web 3.0 evidencian avances significativos que confluyen en la búsqueda de un modelo de seguridad más robusto y adaptativo. En primer lugar, el trabajo de He et al. [1] describe los desafíos técnicos y organizacionales inherentes a la adopción de Zero Trust, resaltando la necesidad de un monitoreo continuo en contextos distribuidos. Por su parte, Shah [2] examina la evolución de los sistemas IAM y destaca la creciente relevancia de la inteligencia artificial para reforzar los controles de autenticación. Esta aproximación se ve complementada por Azhar [3], quien propone un marco que permite la integración de algoritmos de aprendizaje automático en la gestión de accesos, con el fin de detectar amenazas basadas en patrones de comportamiento.

En cuanto a la aplicación de tecnologías de la Web 3.0, Taherdoost [4] explica de manera sistemática el rol que pueden asumir los tokens no fungibles (NFT) en la constitución de identidades digitales únicas, articulando cómo esta metodología puede mitigar el riesgo de fraudes. Kuznetsov et al. [5] avanzan sobre esta línea al incorporar blockchain, IA y fuzzy extractors para cimentar un sistema de identidad auto-soberana, evidenciando reducciones en la tasa de suplantación de identidad. Por otro lado, Li et al. [6] enfocan su estudio en la adopción de Zero Trust en entornos multicloud, implementando soluciones de aprendizaje automático para la asignación dinámica de privilegios, lo cual se plasma en un aumento de la resiliencia frente a ataques internos.

Aunque algunos estudios se alejan ligeramente del tema central, como Wang et al. [7], sus hallazgos sobre la complejidad de la administración de identidades en entornos industriales permiten extraer conclusiones sobre la adopción de múltiples factores de autenticación. De forma más específica, Mohammed et al. [8] detallan un enfoque web de IAM que resalta la importancia de la seguridad en la nube, contribuyendo a la evidencia empírica de la efectividad de sistemas federados. Las investigaciones de Chen et al. [9] señalan que la confluencia de Zero Trust y tecnologías emergentes, como 5G y Edge Computing, introduce nuevos vectores de amenaza, demandando soluciones que gestionen credenciales e identidades con extrema cautela.

Dentro del ámbito de la Web 3.0, Sunyaev y Schneider [10] examinan la fusión de la economía de tokens y la identidad descentralizada, subrayando los retos de escalabilidad y privacidad. La aplicación intensiva de IA para la detección temprana de ciberamenazas y su inserción en Zero Trust se expone en la revisión de Mukherjee y Feamster [11], arrojando resultados positivos en la reducción de falsos positivos. En el caso específico de la adopción de multifactor en entornos DeFi, Gupta y Pathak [12] proponen la utilización de firmas múltiples y validaciones basadas en tokens, lo que incrementa significativamente la salvaguarda de activos digitales. Por su parte, Alkhader et al. [13] plantean un marco para IoT que integra blockchain y Zero Trust, evidenciando mejoras considerables en la detección de accesos no autorizados. Finalmente, Dong y Du [14] proponen un modelo de

aprendizaje automático para la detección de anomalías en la administración de identidades, mientras que Shen y Zheng [15] se centran en la estandarización y los desafíos de interoperabilidad para la autenticación descentralizada, marcando la ruta hacia un ecosistema de identidad verdaderamente distribuido.

Marco teórico

La investigación se apoya en dos grandes ejes:

1. **Modelos de identidad digital**: abarca sistemas de identidad centralizados, federados y descentralizados, con énfasis en la autenticación multifactor.
2. **Ciberseguridad y red team**: adopta el marco de trabajo de Mitre ATT&CK para la emulación de adversarios, focalizándose en la táctica de “Credential Access”.

Tradicionalmente, las aplicaciones de software se implementan dentro de los límites del sistema de información de una organización. Como resultado, la empresa cuenta con un “área confidencial” que está determinada por procedimientos estáticos y es supervisada y administrada por la experiencia del departamento de Tecnologías de la Información (TI). El “área confidencial” generalmente se refiere a la red organizativa central, así como a los sistemas y aplicaciones internos, que se organizan en forma de centro de datos. El centro de datos puede ser mantenido por profesionales dentro de la empresa o puede contratarse a un proveedor de servicios externo. Hoy en día, mantener las identidades y las credenciales de los recursos tecnológicos es un desafío al que deben enfrentarse muchas empresas. En particular, en los sistemas de TI remotos, muchas empresas no pueden controlar de manera eficiente las identidades y los permisos de acceso a los usuarios [1]. La gestión de identidad y acceso (IAM) se refiere a los productos, procesos y políticas que se emplean para gestionar las identidades de los usuarios y regular el acceso de los usuarios dentro de una organización. Hace referencia a la disciplina de TI, la base y las soluciones de gestión de identidad digital [1].

La IAM garantiza que las personas adecuadas tengan acceso a los activos adecuados en el momento adecuado y por las razones adecuadas [2]. La IAM depende cada vez más de la inteligencia artificial (IA) lo que permite a las empresas adoptar una respuesta mucho más detallada y adaptable a la autenticación y el control de acceso [2] [3]. Además, se requiere inteligencia artificial (IA) para el análisis de comportamiento de los usuarios y entidades, que se utiliza para detectar actividades sospechosas. La autenticación y el control de acceso son necesarios para la seguridad de los datos [2]. El uso de la inteligencia artificial (IA) por parte de los ciberdelincuentes para llevar a cabo ataques cada vez más automatizados ya amplios, se están volviendo más comunes. La reacción obvia sería restringir el control de acceso en la mayor medida posible, obligando a los usuarios a autenticarse varias veces durante el día mediante MultiFactor Authentication (MFA) cada vez que necesiten acceder a sus aplicaciones [4]. Si bien un sistema IAM puede permitir implementar tales reglas de seguridad, no todos pueden aumentar o reducir dinámicamente los requisitos de autenticación necesarios [2]. En [5] se puede observar un trabajo de investigación que remarca también la importancia de que las organizaciones cuenten con un sistema IAM y presenta un caso de aplicación concreto basado en un enfoque web. En el trabajo se realiza la implementación de un IAM utilizando un servidor Linux con el protocolo Lightweight Directory Access Protocol (LDAP) para gestionar identidades y control de acceso. Todos estos antecedentes mencionados plantean distintas problemáticas de ciberseguridad que

pueden estudiarse en el presente proyecto. Tradicionalmente, las aplicaciones de software se implementan dentro de los límites del sistema de información de una organización, creando un “área confidencial” supervisada por el departamento de Tecnologías de la Información (TI). Sin embargo, con la evolución de los sistemas de TI y el crecimiento del trabajo remoto, muchas empresas luchan por mantener y controlar eficientemente las identidades y los permisos de acceso de los usuarios. La gestión de identidad y acceso (IAM) aborda esta necesidad, regulando el acceso de los usuarios dentro de una organización y asegurando que las personas adecuadas tengan acceso a los activos adecuados en el momento adecuado y por las razones adecuadas. Con el advenimiento de la inteligencia artificial (IA), la IAM ha evolucionado para permitir respuestas más detalladas y adaptables a la autenticación y el control de acceso, incluyendo el análisis de comportamiento para detectar actividades sospechosas.

La creciente sofisticación de los ciberataques, muchos de los cuales ahora emplean IA, ha llevado a una mayor necesidad de control de acceso, con usuarios que a menudo deben autenticarse varias veces al día mediante autenticación multifactorial (MFA). En este contexto, el modelo de seguridad Zero Trust (Confianza Cero) emerge como un paradigma crucial. A diferencia del enfoque tradicional, que asume que todo dentro de un perímetro de seguridad es confiable, Zero Trust no confía en nada por defecto, independientemente de si se encuentra dentro o fuera del perímetro de seguridad de la organización. Este modelo requiere la verificación continua de la identidad y el contexto de acceso, y puede ser especialmente eficaz cuando se combina con una estrategia de IAM robusta. A pesar de la creciente importancia del modelo Zero Trust, su implementación sigue siendo un desafío, y los sistemas IAM existentes a menudo no pueden aumentar o reducir dinámicamente los requisitos de autenticación necesarios. Esta es una problemática de ciberseguridad que el presente proyecto se propone estudiar y abordar.

Hipótesis / Objetivos

- **Hipótesis general**: La adopción de mecanismos descentralizados de identidad y el uso de inteligencia artificial en la administración de accesos mejoran la seguridad y reducen la exposición a ciberataques en comparación con soluciones tradicionales.
- **Objetivo general:** Investigar y analizar las técnicas avanzadas de identidad digital y la aplicación del modelo de seguridad Zero Trust en el contexto de la transición hacia la Web 3.0, con el fin de proponer estrategias que fortalezcan la seguridad, la privacidad y la experiencia del usuario en aplicaciones web.
- **Objetivos específicos**:
    1. Analizar el estado actual de la transición de la Web 2.0 a la Web 3.0, identificando los desafíos y oportunidades en términos de seguridad y privacidad de la identidad digital.
    2. Explorar en profundidad la Identidad Auto-soberana (SSI), la Identidad Basada en Tokens, SAML, OpenID Connect (OIDC), y OAuth2, para comprender su aplicación y eficacia en la seguridad de las aplicaciones web.
    3. Investigar el modelo de seguridad Zero Trust y su relevancia para la protección de la identidad digital en la Web 3.0.
    4. Evaluar cómo la inteligencia artificial puede ser utilizada en la gestión de identidad y acceso, y cómo puede mejorar la autenticación de múltiples factores.

5. Examinar cómo el modelo de Zero Trust puede integrarse con la autenticación de múltiples factores, con un enfoque en la capacidad de ajustar dinámicamente los requisitos de autenticación.
6. Proponer estrategias de seguridad basadas en los hallazgos del estudio para proteger la identidad digital en la Web 3.0.
7. Desarrollar un marco conceptual para la aplicación de las técnicas de identidad digital y el modelo de Zero Trust en la Web 3.0.
8. Validar y probar el marco conceptual propuesto mediante su aplicación en un entorno controlado, para evaluar su eficacia en términos de seguridad y experiencia del usuario.

Método

Diseño de investigación

Se adoptó un diseño **exploratorio y experimental** mediante la configuración de laboratorios virtuales. Se definieron entornos con máquinas virtuales que alojaron aplicaciones web y proveedores de identidad, mientras que un servidor de ataque (Kali Linux) permitió la ejecución de pruebas basadas en la táctica de "Credential Access". Adicionalmente, se incorporó un **modelo multifactor basado en blockchain**, para validar la factibilidad de este esquema de seguridad en entornos descentralizados.

Muestra (si correspondiere)

No se trabajó con una muestra poblacional de usuarios finales; el análisis se enfocó en la robustez de los sistemas de IAM y en experimentos técnicos simulados en laboratorios controlados.

Instrumentos a utilizar

- **Mitre Caldera** y **BurpSuite**: para emulación de adversarios y pruebas de penetración.
- **Modlishka**: para realizar ataques *reverse proxy* y técnicas de suplantación de identidad.
- **Keycloak** y **WSO2 Identity Server**: como proveedores de identidad y acceso IAM.
- **Herramientas de virtualización** (Oracle VM VirtualBox) y entornos en la nube (Firebase, Render) para despliegues de las aplicaciones web.
- **Hardhat**, **Metamask** y **Ethers.js**: para la implementación del modelo multifactor en blockchain.

Procedimientos

1. **Configuración de entornos**: implementación de máquinas virtuales (Ubuntu, Windows, Kali Linux).

2. **Integración con IAM**: las aplicaciones web fueron configuradas con distintos niveles de autenticación (simple, doble y multifactor), y se extendieron al ámbito de blockchain con *Sign-In with Ethereum*.
3. **Ejecución de pruebas**: se aplicaron técnicas de *Steal Web Session Cookie, Steal Application Access Token, Forge Web Credentials*, entre otras, según la táctica Mitre ATT&CK.
4. **Modelo de autenticación multifactor en blockchain**:
    - Se desplegó un *smart contract* en una red local de Ethereum (Hardhat) para almacenar las direcciones principales y adicionales.
    - Se utilizó *Metamask* para la verificación de firmas y *Ethers.js* para la interacción con el contrato.
    - Se validó el proceso de login requiriendo la confirmación desde múltiples direcciones, simulando el robo o la pérdida de una clave privada.
5. **Recopilación de datos**: se registraron métricas de éxito de autenticación, errores, tiempo de respuesta y satisfacción de usuario cuando fue posible.

Materiales y métodos (insumos varios)

- Contenedores Docker para Keycloak y WSO2 Identity Server.
- Scripts en Python y Selenium para automatizar acciones de usuarios (logins simultáneos).
- Herramientas de blockchain (Hardhat, Metamask, Ethers.js) para la implementación del **modelo multifactor**.

Resultados

Diseño del análisis de datos
Se planteó una evaluación mixta:

- **Cuantitativa**: mediante porcentajes de éxito en ciberataques simulados, tiempo medio de respuesta en autenticación, tasa de errores y disponibilidad del sistema IAM, con y sin el modelo blockchain.
- **Cualitativa**: en caso de pruebas con usuarios reales, se proyecta utilizar encuestas de satisfacción y usabilidad.

Presentación de resultados
Los experimentos realizados reportan la efectividad de cada técnica de ataque. Por ejemplo:

Experimento	**Calificación (1-10)**
Credential Access con Mitre Caldera	10
Steal Web Session Cookie / Access Token	9
Steal Tokens con Modlishka	8
Forge Web Credentials	10

Autenticación multifactor en blockchain (prueba inicial)	En implementación

Análisis de los resultados

1. **Entornos Web 2.0**: Keycloak y WSO2 Identity Server demostraron buena resistencia ante ataques directos, especialmente con autenticación multifactor. Sin embargo, se presentaron vulnerabilidades al emplear configuraciones simplificadas (auth simple).
2. **Proyección Web 3.0**: Se observó que la integración de mecanismos descentralizados (e.g., *Sign-In with Ethereum*) y la **implementación de un modelo de autenticación multifactor en blockchain** (Romero Arregin et al., 2025) amplían las posibilidades de protección, al aprovechar la inmutabilidad y robustez de la tecnología de bloques. Este enfoque busca mitigar los riesgos derivados del robo o pérdida de claves privadas, al requerir múltiples direcciones asociadas para confirmar la identidad de un usuario.
3. **IA y autenticación dinámica**: Se planteó la posibilidad de adaptar dinámicamente la exigencia de factores de autenticación basándose en el comportamiento del usuario y la detección de amenazas. Aunque todavía en etapa inicial, se estima un potencial significativo para reducir ataques automatizados y mejorar la experiencia de usuario.

Conclusiones

En este estudio se comprobó que la integración de un enfoque de seguridad sustentado en el modelo Zero Trust, reforzado con autenticación multifactor y apoyado en herramientas de inteligencia artificial, ofrece una mejora sustancial en la protección de la identidad digital. A lo largo del proceso se observó que la adopción de mecanismos descentralizados, como la autenticación basada en blockchain, mitiga diversos riesgos asociados con el robo o la falsificación de credenciales, especialmente cuando se combina con la verificación continua que promueve Zero Trust. No obstante, los avances técnicos generan un incremento en la complejidad de la implementación y un aumento potencial en los tiempos de autenticación, factores que pueden afectar la experiencia de usuario y que requieren equilibrar rigurosamente la demanda de seguridad frente a la facilidad de uso. En particular, la configuración de contenedores, la integración de entornos en la nube y la orquestación dinámica de factores de autenticación han exigido una planificación minuciosa y la superación de obstáculos inesperados, como la falta de compatibilidad de ciertas herramientas con entornos locales y la necesidad de exponer servicios a Internet para su correcto funcionamiento.

Por otra parte, la posibilidad de escalar o reducir los factores de autenticación de forma adaptable, basándose en patrones de uso y niveles de riesgo, abre un nuevo horizonte para la ciberseguridad. Los primeros indicios obtenidos en las pruebas sugieren que la inteligencia artificial puede actuar como un habilitador clave para gestionar el acceso y detectar anomalías, lo que mejora la postura de seguridad sin generar una excesiva carga operativa en el día a día de los usuarios. Sin embargo, la incorporación de algoritmos de aprendizaje automático y la configuración de sistemas de identidad descentralizados

apuntan a retos que trascienden el plano estrictamente técnico, pues también involucran el diseño de políticas de adopción y la consideración de marcos regulatorios que delimiten el tratamiento de la información personal. Aun así, la investigación realizada confirma la utilidad de un paradigma de verificación continua, robustecida por múltiples factores y complementada con IA, como una estrategia sólida para afrontar la evolución tecnológica de la Web 3.0. Se sugiere, en trabajos futuros, conducir estudios más amplios en entornos productivos y con mayor variedad de casos de uso, así como avanzar hacia la evaluación de costos, la medición de la satisfacción de usuarios finales y la validación de estas soluciones en contextos empresariales de gran escala.

Referencias

1. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). *A Survey on Zero Trust Architecture: Challenges and Future Trends*. Wireless Communications and Mobile Computing, 2022, 6476274.
2. Shah, Z. H. (2022). *A Survey on Identity and Access Management*. Zenodo.
3. Azhar, I. (2018). *A literature review on the application of AI to Identity Access Management*. SSRN.
4. Taherdoost, H. (2023). *Non-Fungible Tokens (NFT): A Systematic Review*. Information, 14(1), 26.
5. Kuznetsov, O., Frontoni, E., Katrich, V., Kobylianska, O., & Pshenichnaya, S. (2024). *A Comprehensive Decentralized Digital Identity System: Blockchain, Artificial Intelligence, Fuzzy Extractors, and NFTs for Secure Identity Management*. Revista de Ciberseguridad y Blockchain, 12(2), 55-71.
6. Li, H., Zheng, S., Li, P., & Chen, X. (2021). *An Adaptive Zero Trust Architecture for Multi-Cloud Environments: A Machine Learning Perspective*. IEEE Access, 9, 140284–140299.
7. Wang, B., Liu, D., & Ji, M. (2017). *Research on Management System of Mold Manufacturing Enterprise Based on RFID Technology*. MATEC Web of Conferences, 95, 10002.
8. Mohammed, K. H., Hassan, A., & Mohammed, D. Y. (2018). *Identity and Access Management System: A Web-Based Approach for an Enterprise*. 3rd International Conference on Cyber Security.
9. Chen, Y., Xu, M., & Liang, Y. (2021). *Zero Trust in the Era of 5G and Edge Computing: Security Challenges and Solutions*. Computers & Security, 110, 102435.
10. Sunyaev, A., & Schneider, S. (2020). *Internet of Value and Web 3.0: Technologies, Challenges, and Future Outlook*. Communications of the Association for Information Systems, 47(1), 391–404.
11. Mukherjee, N., & Feamster, N. (2022). *AI-Driven Threat Detection: Adapting Zero Trust Principles for Modern Cyber Defense*. ACM Computing Surveys, 54(8), 1–38.
12. Gupta, A., & Pathak, R. (2023). *Multifactor Authentication in Decentralized Finance: A Systematic Review*. Journal of Finance and Digital Innovation, 6(2), 127–144.
13. Alkhader, W., Gani, A., & Hassan, S. (2021). *Blockchain-Integrated Zero Trust Framework for Distributed IoT Environments*. IEEE Internet of Things Journal, 8(11), 8912–8926.

14. Dong, L., & Du, R. (2019). *Machine Learning-Enabled Anomaly Detection in Identity Management*. Future Internet, 11(7), 156.
15. Shen, J., & Zheng, L. (2021). *Web 3.0 Identity: A Review of Emerging Standards and Their Potential for Decentralized Authentication*. IEEE Access, 9, 165348–165362.
16. Shah, Z. H. (2022). *A Survey on Identity and Access Management.* doi: 10.5281/ZENODO.7233056
17. Azhar, I. (2018). *A literature review on the application of AI to Identity Access Management*. https://papers.ssrn.com/abstract=3904581
18. Cole, D. (1991). Artificial intelligence and personal identity. *Synthese*, 88(3), 399–417.
19. Wang, B., Liu, D., & Ji, M. (2017). Research on Management System of Mold Manufacturing Enterprise Based on RFID Technology. *MATEC Web of Conferences*, 95, 10002. doi: 10.1051/matecconf/20179510002
20. Mohammed, K. H., Hassan, A., & Mohammed, D. Y. (2018). *Identity and Access Management System: a Web-Based Approach for an Enterprise*. http://oer.udusok.edu.ng:8080/xmlui/handle/123456789/837
21. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, 2022, 6476274. doi: 10.1155/2022/6476274
22. Taherdoost, H. (2023). Non-Fungible Tokens (NFT): A Systematic Review. *Information*, 14(1). doi: 10.3390/info14010026
23. Kuznetsov, O., Frontoni, E., Katrich, V., Kobylianska, O., & Pshenichnaya, S. (2024). A Comprehensive Decentralized Digital Identity System: Blockchain, Artificial Intelligence, Fuzzy Extractors, and NFTs for Secure Identity Management.
24. Informe de pruebas realizadas (2025). *Experimentos realizados* (documento interno del proyecto).
25. Romero Arregin, G. D. et al. (2025). Implementación de un modelo de autenticación multifactor en blockchain. (Paper interno del proyecto).