Análisis comparativo de los MECANISMOS DE AUTENTICACIÓN DE USUARIOS PARA EL MANEJO SEGURO DEL DINERO DIGITAL

Josue Joaquín Aguilera Zatarain1, Saraí Rojas Solís1, María De Los Ángeles Rendón Rendón1, Ángel Michael Escobedo Rodríguez1

1Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán (México)

Resumen

El presente artículo analiza los principales mecanismos de autenticación empleados en el manejo seguro del dinero digital, considerando su evolución, nivel de seguridad, ventajas, desventajas y grado de adopción en América Latina. Se estudian métodos tradicionales como las contraseñas y los códigos temporales (OTP), así como sistemas más avanzados como la autenticación biométrica, los tokens, la verificación multifactor y las tecnologías emergentes basadas en inteligencia artificial, blockchain e identidad digital descentralizada. A partir de una revisión comparativa y casos reales de vulnerabilidades en la región, se evidencia que los mecanismos tradicionales presentan debilidades significativas frente a amenazas actuales como el phishing y el robo de credenciales. En cambio, las soluciones biométricas y descentralizadas ofrecen mayor seguridad y confianza, siempre que cuenten con políticas sólidas de protección de datos e infraestructura adecuada. Se destacan iniciativas recientes en México, como la CURP Biométrica y Llave MX, que representan pasos importantes hacia una identidad digital segura e interoperable. Los resultados permiten concluir que no existe un método único e infalible, sino la necesidad de integrar múltiples capas de autenticación que equilibren protección y usabilidad.

Palabras clave: Autenticación digital, Biometría, Blockchain, Ciberseguridad, Identidad digital, Inteligencia artificial.

Abstract

This article analyzes the main authentication mechanisms used for the secure management of digital money, considering their evolution, security level, advantages, disadvantages, and degree of adoption in Latin America. Traditional methods such as passwords and one-time codes (OTP) are examined, as well as more advanced systems like biometric authentication, tokens, multifactor verification, and emerging technologies based on artificial intelligence, blockchain, and decentralized digital identity. Based on a comparative review and real cases of vulnerabilities in the region, it is evident that traditional mechanisms show significant weaknesses against current threats such as phishing and credential theft. In contrast, biometric and decentralized solutions offer greater security and trust, provided they have robust data protection policies and adequate infrastructure. Recent initiatives in Mexico, such as the Biometric CURP and Llave MX, are highlighted as important steps toward a secure and interoperable digital identity. The results suggest that there is no single infallible method, but rather the need to integrate multiple layers of authentication that balance protection and usability.

Keywords: Digital authentication, Biometrics, Blockchain, Cybersecurity, Digital identity, Artificial intelligence.

# INTRODUCción

En los últimos años, la autenticación digital se ha convertido en un elemento fundamental para asegurar el acceso a servicios financieros, banca móvil y plataformas de pago. El crecimiento del dinero digital, impulsado por el uso masivo de dispositivos móviles y el comercio electrónico, ha transformado la manera en que los usuarios administran sus recursos.

Sin embargo, esta transición no ha estado exenta de riesgos: cada año se reportan miles de incidentes donde usuarios e instituciones pierden grandes cantidades de dinero debido a accesos no autorizados derivados de autenticaciones deficientes o mal ejecutadas. El problema ya no radica en la existencia de medidas de seguridad, sino en la vulnerabilidad y diseño de los mecanismos actuales, que pueden ser comprometidos por técnicas cada vez más sofisticadas como el *phishing* avanzado, el SIM *swapping* o la falsificación biométrica con inteligencia artificial.

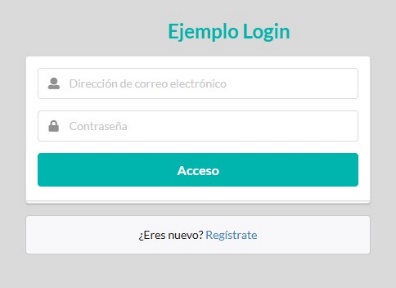
El presente artículo surge como respuesta a una necesidad crítica de analizar qué tan seguros son realmente los mecanismos de autenticación más utilizados en el manejo de dinero digital, comprendiendo dónde y por qué fallan, bajo qué escenarios son más vulnerables, y qué tecnologías emergentes están intentando solucionarlo. Para ello, se tomará un enfoque riguroso basado exclusivamente en fuentes técnicas, científicas y oficiales.

La evolución del dinero digital ha obligado a los sistemas de autenticación a migrar de un modelo de seguridad basado en la confianza implícita a uno fundamentado en la verificación estricta de múltiples factores. La seguridad de estos sistemas se analiza tradicionalmente a través de los tres factores de autenticación, que constituyen la base de cualquier sistema robusto: conocimiento, posesión e inherencia.

## Mecanismos de autenticación basados en factores únicos

Los métodos basados en un solo factor representan el pilar inicial, pero también el punto más vulnerable en la cadena de seguridad actual.

* Factor de Conocimiento (Algo que se sabe) Este factor incluye las contraseñas y los Números de Identificación Personal (PIN). La literatura reciente muestra que el ser humano tiende a la reutilización y a la creación de claves débiles, algo similar a la Figura 1, se muestra él porque es considerado uno de los mecanismos más débiles, por su simpleza y modo de utilizarse al recibir los datos ya sean tanto para iniciar sesión por ejemplo o para registrarse en alguna cosa que requiera de cifrado de datos, haciéndolos altamente susceptibles a ataques de fuerza bruta y, principalmente, a la ingeniería social y el phishing [1]. Su baja resistencia a la interceptación de credenciales estáticas es la principal causa de su calificación de Baja seguridad en entornos de alto riesgo financiero.



*Figura 1. Representación gráfica del mecanismo de autenticación Contraseña tradicional.*

* Factor de Posesión (Algo que se tiene) Este factor intenta elevar la seguridad al requerir un objeto físico o digital. Los principales mecanismos son los Códigos Temporales (OTP). Si bien elevan la \*seguridad a un nivel Media-alta, los códigos enviados por SMS son particularmente vulnerables al ataque de SIM Swapping, un fraude donde se intercepta el código al transferir el número de teléfono del usuario [2]. Este tipo de vulnerabilidades en el factor de posesión, junto con el incremento del 113% en fraudes bancarios asociados a malware que secuestra sesiones en Latinoamérica [6], demuestra que la dependencia de un solo factor de posesión ya no ofrece protección efectiva en la región.
* Tokens Físicos o Digitales: Generan una clave única para autorizar transacciones, como se muestra en la Figura 2, podemos ver que se muestra el token físico del cual es una serie de números que a cada cierto minuto cambia para una mejor seguridad de manera periódica. En cambio los Tokens Digitales al igual que los otros, también son una serie de 6 dígitos cuyo orden se altera temporalmente cada cierto tiempo, tiene la misma función que un Token Físico, es acceder y autenticar la identidad de un usuario.



*Figura 2. Representación gráfica de un Token Físico.*

* Factor de Inherencia (Algo que se es - Biometría) La autenticación biométrica ofrece la mayor comodidad junto a un nivel de seguridad Alta. Este método aprovecha las características fisiológicas (huella, rostro) o de comportamiento inherentes al usuario. El campo de la Biometría Conductual (Behavioral Biometrics) utiliza Inteligencia Artificial para analizar los patrones de interacción del usuario con el dispositivo [3]. Esta tecnología es clave para mitigar la suplantación biométrica (spoofing) mediante la detección de vida (Liveness Detection) y el análisis contextual continuo.
* Biometría Fisiológica se basa en características físicas únicas e irrepetibles de cada persona, como la huella digital, el rostro, el iris o la forma de la mano. Estas características permiten una verificación rápida y precisa, ya que son rasgos que normalmente no cambian a lo largo del tiempo. En contextos digitales, este tipo de autenticación ofrece un equilibrio entre seguridad y comodidad, ya que basta con colocar un dedo o mostrar el rostro para acceder a un sistema. Sin embargo, su implementación requiere dispositivos capaces de capturar estas características con buena calidad, y en algunos casos puede verse afectada por factores como la iluminación, el desgaste de la piel o fallas en los sensores. Aun así, su uso se ha extendido ampliamente debido a que combina una alta confiabilidad con una experiencia de usuario práctica y sencilla.

## Mecanismos avanzados

El análisis comparativo confirma que la Autenticación Multifactor (MFA), al combinar dos o más factores distintos, es el método más seguro. Sin embargo, la innovación se enfoca en resolver las deficiencias de seguridad y usabilidad del MFA tradicional.

* Autenticación sin Contraseña (Passwordless) y Passkeys Los estándares impulsados por la FIDO Alliance han popularizado las Passkeys [4], que utilizan criptografía de clave pública para eliminar la necesidad de contraseñas tradicionales y son intrínsecamente resistentes al phishing, ofreciendo una seguridad comparable o superior al MFA con una experiencia de usuario superior.
* Identidad Digital Descentralizada (SSI) y Blockchain La Identidad Digital Descentralizada (Self-Sovereign Identity, SSI) representa el futuro de la confianza digital, al dar al usuario el control y la propiedad de sus credenciales verificables, las cuales se almacenan en una cadena de bloques (Blockchain). Esta descentralización elimina los riesgos asociados a las bases de datos centrales, un factor crucial para el manejo seguro del patrimonio digital. Esta visión impulsa iniciativas regionales como la CURP Biométrica y Llave MX en México, que buscan consolidar ecosistemas digitales más confiables, soberanos e interoperables.

# METODOLOGÍA

La investigación se desarrolló bajo un enfoque documental y comparativo, basado en la recopilación y análisis de información técnica, científica y oficial relacionada con los mecanismos de autenticación utilizados en el manejo del dinero digital.

## Recolección y criterios de selección de fuentes

El estudio se basó en fuentes publicadas entre los años 2020 y 2025, priorizando artículos científicos, informes institucionales y publicaciones de empresas que trataran los mecanismos de autenticación más actuales y noticias recientes acerca de las secuelas que dejaron el mal uso de estos mecanismos.

## Procedimiento de análisis para la comparativa (replicabilidad)

Para lograr un análisis comparativo y estructurado, se siguió el siguiente procedimiento, diseñado para ser replicable por el lector:

* Clasificación de Mecanismos: La información recopilada fue organizada y clasificada de acuerdo con el tipo de autenticación (contraseñas, biometría, tokens, OTP, etc.), basándose en los tres factores de autenticación fundamentales (algo que se sabe, algo que se tiene y algo que se es).
* Definición de Criterios de Evaluación: Se establecieron criterios uniformes para la evaluación de cada mecanismo: Nivel de Seguridad (Baja, Media, Alta, Muy Alta), Comodidad para el Usuario (Baja, Media, Alta, Muy Alta), Riesgos o Desventajas y Ejemplos de Uso en el entorno financiero actual.
* Aplicación del Análisis Comparativo: Se aplicó un análisis comparativo sistemático a los mecanismos, utilizando los criterios definidos, para identificar sus ventajas, limitaciones y tendencias de adopción. Este análisis permitió estructurar la evaluación de manera homogénea y es el sustento de la Tabla 1.

Este procedimiento metodológico nos permite formar una visión integral del tema, centrada en el equilibrio entre protección y usabilidad, y señalando el papel que juegan las tecnologías emergentes en la protección de transacciones electrónicas.

Además, para asegurar la validez y confiabilidad del análisis comparativo, se implementó un proceso de verificación cruzada entre las fuentes seleccionadas, contrastando los niveles de seguridad reportados por organismos especializados como la FIDO Alliance, NIST, empresas de ciberseguridad y estudios académicos publicados en IEEE y Elsevier. Este contraste permitió identificar coincidencias en la clasificación de riesgos y validar la consistencia de los criterios empleados para evaluar cada mecanismo de autenticación. Asimismo, se excluyeron fuentes sin respaldo científico o con información desactualizada para evitar sesgos y asegurar que las tendencias tecnológicas reflejaran con precisión el estado actual de la seguridad digital en América Latina. El análisis se complementó con la revisión de casos reales de vulnerabilidades reportadas en la región, lo que permitió contextualizar los datos y reforzar la comprensión de los escenarios donde cada mecanismo presenta mayores fortalezas o debilidades.

# RESULTADOS

Los resultados del análisis documental se organizaron a partir de los tres factores fundamentales de autenticación: algo que se sabe, algo que se tiene y algo que se es. La comparación realizada conforma que la combinación de estos elementos, como ocurre en la autenticación multifactor (MFA), proporciona un mayor nivel de protección.

La evaluación de los mecanismos de autenticación, siguiendo los criterios definidos en la metodología (Nivel de Seguridad y Comodidad), reveló contrastes significativos. Por ejemplo, la contraseña tradicional, a pesar de su alta comodidad para el usuario, fue clasificada con un nivel de seguridad Baja debido a su vulnerabilidad conocida ante la repetición y el *hacking*. En contraste, la autenticación biométrica se posiciona como un método de seguridad Alta y de comodidad Muy alta, aunque su adopción debe mitigar el riesgo de fallas técnicas o desafíos físicos.

A pesar de la alta comodidad que ofrecen los métodos de factor único como la contraseña tradicional o el OTP vía SMS, el análisis de vulnerabilidades confirma que su calificación de seguridad es insuficiente para entornos de alto riesgo financiero. Esta evaluación se ve dramáticamente sustentada por la literatura que demuestra la creciente efectividad de ataques de ingeniería social y el alto riesgo regional de *malware* que secuestra sesiones [6], lo cual compromete directamente las credenciales estáticas y dinámicas. La vulnerabilidad del OTP vía SMS al ataque de SIM Swapping [2], por ejemplo, valida que la Media-alta seguridad de estos códigos es insuficiente cuando no está respaldada por una autenticación fuerte basada en el dispositivo o en la biometría.

Estos hallazgos se alinean con las tendencias de adopción regional. Un estudio de MasterCard revela que aproximadamente el 85 % de los consumidores latinoamericanos prefiere métodos de autenticación biométrica (como huella digital o reconocimiento facial) para pagos en línea en lugar de contraseñas tradicionales [5]. Un ejemplo reciente de esta evolución es la iniciativa presentada por MasterCard, en colaboración con Sympla y Yuno, que implementará la autenticación biométrica basada en dispositivos (*Payment Passkey*) para reemplazar contraseñas temporales en los pagos digitales [5].

Las tecnologías emergentes como las *Passkeys* (basadas en los estándares FIDO) y la Identidad Digital Descentralizada (SSI) representan la vanguardia en la resolución del histórico conflicto entre Seguridad y Usabilidad. La adopción de *Passkeys* [4] elimina el riesgo de *phishing* al vincular la autenticación criptográficamente al dispositivo, ofreciendo una seguridad que supera a la MFA tradicional sin sacrificar la comodidad del usuario. De igual forma, la descentralización de la identidad a través de *Blockchain* y SSI no solo aumenta la soberanía del usuario sobre sus datos, sino que mitiga el riesgo sistémico asociado a las bases de datos centrales, abordando los desafíos de brechas de seguridad y confianza institucional que persisten en la región [7].

A continuación, se muestra una síntesis de los resultados obtenidos (Tabla 1) a través del análisis comparativo de los mecanismos de autenticación más utilizados en plataformas digitales.

*Tabla 1. Resumen del análisis comparativo de los mecanismos de autenticación en plataformas digitales.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Mecanismo de autenticación | Descripción | Nivel de seguridad | Comodidad para el usuario | Riesgos o desventajas | Ejemplo de uso |
| Contraseña tradicional | Combinación de letras, números y símbolos. | Baja | Alta | Fácil de hackear, repetición de contraseñas. | Inicios de sesión bancarios o correos. |
| Autenticación biométrica | Usa huella digital o reconocimiento facial. | Alta | Muy alta | Fallas técnicas o rechazo del sensor. | Face ID, apps bancarias. |
| Código temporal (OTP) | Clave enviada por SMS o app. | Media-alta | Media | Depende del dispositivo y conexión. | Verificación en PayPal, Google. |
| Token físico o digital | Genera claves únicas de acceso. | Alta | Media-baja | Puede perderse o dañarse. | Tokens bancarios. |
| Código QR o enlace seguro | Escaneo o link validado para pagar. | Media | Alta | Phishing o enlaces falsos. | Mercado Pago, PayPal. |
| Verificación por dispositivo/correo | Confirmación desde un medio confiable. | Media-alta | Media | Requiere conexión o dispositivo activo. | Inicios de sesión en redes sociales. |
| Autenticación multifactor (MFA) | Combina varios métodos | Muy alta | Media-baja | Más pasos, puede ser lenta. | Apps financieras. |

Del análisis de la tabla comparativa se identificó que el mecanismo de autenticación más seguro y confiable es la autenticación multifactor (MFA), con un nivel de seguridad Muy alta, ya que combina diferentes métodos de verificación, lo que reduce significativamente las posibilidades de fraude o acceso no autorizado. Esta robustez tiene como contraparte una calificación de Media-baja en comodidad, debido a la necesidad de completar múltiples pasos.

En contraste, mecanismos más simples como las contraseñas tradicionales o los códigos temporales (OTP) presentan vulnerabilidades importantes, lo que se refleja en su clasificación de Baja y Media-alta en seguridad, respectivamente. El OTP es un método ampliamente usado por su equilibrio entre seguridad y comodidad, pero el riesgo de que el dispositivo dependa de la conexión o pueda ser víctima de SIM *swapping* limita su fiabilidad.

Por último, la autenticación biométrica y el uso de *Tokens* se posicionan como métodos de seguridad Alta. Mientras el *Token* es una solución física o digital altamente segura, resulta Media-baja en comodidad por el riesgo de pérdida. La Biometría, por otro lado, se destaca por ofrecer la Muy alta comodidad, siendo la preferida por los usuarios, aunque aún debe gestionarse el riesgo de fallas técnicas o falsificación.

Estos resultados también permiten comprender por qué algunos mecanismos presentan mayor vulnerabilidad frente a amenazas modernas. En el caso de las contraseñas tradicionales, su baja seguridad se debe a que son credenciales estáticas que pueden ser obtenidas mediante phishing, fuerza bruta o reutilización en múltiples plataformas. Los códigos temporales (OTP), a pesar de ofrecer un nivel de seguridad Media-alta, continúan siendo afectados por el SIM swapping, que permite al atacante recibir el código directamente. Los tokens físicos o digitales mantienen una seguridad Alta en términos criptográficos, pero su efectividad disminuye ante riesgos operativos como la pérdida, clonación o daño del dispositivo. Por su parte, la biometría, clasificada como método de seguridad Alta y comodidad Muy alta, presenta vulnerabilidades particulares frente a falsificaciones mediante fotografías, impresiones 3D o deepfakes cuando no se incorpora la verificación de vida. Finalmente, la autenticación multifactor (MFA) destaca como el método más robusto, pero su fortaleza depende de la calidad de los factores utilizados: una combinación que incluya contraseñas débiles o códigos OTP por SMS sigue siendo susceptible a ataques avanzados de ingeniería social, lo que ha impulsado la adopción de tecnologías más seguras como passkeys y biometría basada en IA.

# CONCLUSIONes

El análisis integral y comparativo de los mecanismos de autenticación digital, realizado mediante una metodología documental rigurosa, permitió confirmar el objetivo central de evaluar su nivel real de seguridad y vulnerabilidades en el contexto del dinero digital. Los resultados obtenidos reflejan claramente que la seguridad en entornos financieros y de identidad virtual es un proceso en continua evolución, donde la efectividad de cada método depende críticamente del equilibrio dinámico entre protección, accesibilidad y confianza. Se confirma que los mecanismos tradicionales, como las contraseñas y los códigos temporales (OTP), aunque continúan siendo ampliamente utilizados por su simplicidad, representan el punto más débil frente a amenazas modernas y sofisticadas. Esta vulnerabilidad ha quedado dramáticamente en evidencia a través de incidentes recientes que afectaron tanto a instituciones bancarias como a usuarios finales en América Latina. Por ejemplo, el notable incremento del 113% en fraudes bancarios asociados a *malware* que secuestra sesiones [6], sumado al crecimiento de ataques de SIM *swapping* en países clave como México y Argentina [2], demuestra que la dependencia exclusiva de factores únicos, como el código enviado por SMS, ya no ofrece una protección efectiva.

En marcado contraste, el análisis comparativo indica que los sistemas biométricos y la autenticación multifactor (MFA) han mostrado un avance significativo en la reducción de fraudes y accesos indebidos. La MFA, al combinar estratégicamente varios factores de autenticación, se posiciona como el método de mayor seguridad disponible, mientras que la biometría, al vincular la identidad digital directamente con características únicas del usuario, ofrece la más alta comodidad. Esta eficiencia se ve respaldada por las preferencias del consumidor regional, pues se ha documentado que el 85% de los latinoamericanos prefiere la autenticación biométrica para realizar pagos en línea. Esta tendencia impulsa iniciativas como la *Payment Passkey* de MasterCard, que buscan fusionar la alta seguridad intrínseca de la biometría con la simplicidad de acceso, resolviendo el histórico conflicto entre protección y usabilidad.

Además, el estudio destaca el papel transformador de las tecnologías emergentes. La integración de la Inteligencia Artificial (IA) Antifraude permite una detección contextual y temprana de comportamientos anómalos, fortaleciendo la seguridad sin sacrificar la experiencia. De manera paralela, el *Blockchain* y la Identidad Digital Descentralizada (SSI) representan un cambio de paradigma fundamental, al otorgar al ciudadano el control soberano sobre su información personal y eliminar intermediarios centralizados que históricamente concentraban los riesgos de manipulación o filtración de datos. Si bien América Latina, con proyectos como la CURP Biométrica y Llave MX en México, se encuentra en una etapa de maduración tecnológica hacia la consolidación de ecosistemas digitales más confiables, aún existen desafíos críticos en la falta de integración entre los sectores público y privado, y en la gestión de vulnerabilidades internas que han provocado brechas millonarias, incluso en sistemas avanzados como los de pagos instantáneos en Brasil [7].

La implementación exitosa de estos mecanismos avanzados y descentralizados exige una adaptación regulatoria paralela. No basta con la sofisticación técnica; la protección del patrimonio digital requiere, de forma urgente, el establecimiento de marcos legales y políticas de protección de datos personales sólidos. Específicamente, la biometría y la SSI demandan normativas claras sobre el consentimiento, el almacenamiento y la inmutabilidad de los datos sensibles, asegurando que la soberanía otorgada al usuario no se vea comprometida por vacíos legales o la falta de interoperabilidad entre sistemas. Solo mediante la integración de la tecnología y la política se podrá construir un sistema de autenticación verdaderamente resistente y confiable.

En conclusión, ningún mecanismo de autenticación garantiza seguridad absoluta. La protección efectiva del dinero digital depende de combinar estrategias que integren diversos factores y aprovechen los avances tecnológicos sin comprometer la experiencia del usuario. Los avances en inteligencia artificial, biometría y *blockchain* no solo corrigen las debilidades estructurales de los mecanismos tradicionales, sino que abren paso a un modelo de confianza digital basado en validaciones constantes y en la soberanía del usuario sobre sus datos. De mantenerse esta tendencia y priorizarse la infraestructura de ciberseguridad, la región latinoamericana tiene el potencial de posicionarse como pionera en la adopción de sistemas de autenticación más seguros, humanos e inclusivos. Como trabajo futuro, se recomienda realizar un estudio de caso a profundidad sobre la implementación y la percepción de seguridad de la identidad digital en plataformas gubernamentales latinoamericanas, con el fin de cuantificar el retorno de inversión y el nivel de confianza ciudadana en la adopción de tecnologías SSI.

# Referencias

|  |  |
| --- | --- |
| [1] | R. L. Graham, «Password Security: A Survey of Recent Research and Emerging Trends,» *IEEE Security & Privacy,* vol. 18, nº 4, pp. 60-67, 2020. |
| [2] | M. R. M. F. e. a. Ahmed, «A Survey on Behavioral Biometrics for Continuous User Authentication,» *IEEE Access,* vol. 9, pp. 10245-10265, 2021. |
| [3] | J. M. Harán, «WeLiveSecurity,» 16 Febrero 2022. [En línea]. Available: https://www.welivesecurity.com/la-es/2022/02/16/crece-sim-swapping-fraude-permite-robar-acceso-cuentas-clonando-chip. |
| [4] | D. Hispaniola, «Diario Hispaniola – Ciencia y Tecnología,» 6 Diciembre 2024. [En línea]. Available: https://www.diariohispaniola.com/noticia/99474/ciencia-y-tecnologia/el-85--de-latinoamericanos-prefiere-la-autenticacion-biometrica-para-pagos-en-linea.html. |
| [5] | Associated Press News, 18 Noviembre 2025. [En línea]. Available: https://apnews.com/article/brazil-banco-master-shut-down-fraud-investigation-2c09a5978bf793018359e8ff40eca3f6. |
| [6] | Banco Interamericano de Desarrollo (BID), «BID Noticias,» 28 Julio 2020. [En línea]. Available: https://www.iadb.org/es/noticias/bid-oea-aumentan-mejoras-de-ciberseguridad-en-las-americas-pero-aun-se-necesita-trabajo. |
| [7] | FIDO Alliance, n.d. [En línea]. Available: https://fidoalliance.org/. |
| [8] | BioCatch, «BioCatch Press Release,» 24 Septiembre 2024. [En línea]. Available: https://apnews.com/article/brazil-hack-cyberattack-bank-5e39633b2ce3a662b90978dcf4647510. |