Banca & Economía

2025

Edición 1469

Deepfake: una amenaza latente para el sistema financiero

21 de abril de 2025

Director:

Jonathan Malagón González

ASOBANCARIA:

Jonathan Malagón González
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

- El avance de la inteligencia artificial (IA) ha transformado la interacción digital pero también ha introducido nuevos riesgos como los *deepfakes*. Esta es una tecnología basada en modelos avanzados de IA que permite generar contenido audiovisual falso mediante la replicación precisa de rasgos y patrones de voz, planteando importantes desafíos en ciberseguridad.

- El crecimiento exponencial de los *deepfakes* ha intensificado los riesgos en seguridad digital. Su disponibilidad facilita la implementación por parte de los ciberdelincuentes, quienes emplean estas tecnologías para evadir mecanismos de autenticación y engañar tanto a usuarios como a entidades.

- En el sector bancario, los *deepfakes* representan un riesgo significativo para la seguridad digital y la protección de datos. Es crucial que las entidades financieras y los usuarios estén informados frente a nuevas modalidades de fraude y adopten medidas preventivas para mitigar los riesgos de suplantación de identidad con IA.

Para suscribirse a nuestra publicación semanal Banca & Economía, por favor envíe un correo electrónico a bancayeconomia@asobancaria.com

Banca & Economía

2025

Edición 1469

Deepfake: una amenaza latente para el sistema financiero

Editor

Germán Montoya
Director Económico

Participaron en esta edición:
Jaime Andrés Rincón Arteaga
Carol Alejandra Rodríguez Calderón

En la última década, la inteligencia artificial (IA) ha impulsado el desarrollo de tecnologías innovadoras que revolucionan la forma de interacción con los usuarios y la percepción de la realidad, un progreso que también plantea un panorama de riesgos asociados con su implementación. Uno de esos riesgos tiene que ver con los llamados *deepfakes*, una técnica avanzada de IA que es utilizada para la creación de contenido audiovisual como videos, imágenes o audios, mediante la imitación de características distintivas de una persona asociadas al tono de la voz, movimientos faciales y apariencia física. Hoy en día, la proliferación de este tipo de material multimedia dificulta la distinción entre lo real y fraudulento, pues supone un alto grado de credibilidad para el público, ya que a simple vista son casi imperceptibles las manipulaciones de estas creaciones, aparentando ser contenido real.

El auge de los *deepfakes* en los últimos años ha generado afectaciones a la imagen y protección digital de celebridades, personajes públicos, usuarios y entidades a nivel global. Además, se evidencia un incremento en los actos delictivos digitales de suplantación tras el uso de tecnología *deepfake*, promovidos por la accesibilidad a herramientas de creación de contenido a partir de inteligencia artificial y el desconocimiento de los usuarios sobre técnicas de estafas emergentes.

Esta edición de Banca & Economía explora, en este escenario, las implicaciones del uso de esta técnica avanzada de IA en el sector bancario ante el desafío presentado en términos de seguridad y protección de identidad digital. Finaliza con algunas conclusiones en la materia.

Explorando el término *deepfake*: una mirada histórica

Los *deepfakes* son una de las aplicaciones de la inteligencia artificial, originada de una forma especializada del *machine learning*. La primera parte del término, correspondiente a "*deep*", se origina de la implementación de la técnica *deep learning*, la cual incorpora algoritmos de aprendizaje automático a partir de grandes cantidades de datos para generar predicciones[2]. De otro lado, el término "*fake*" está asociado con la alteración del contenido, ya que la pieza original es manipulada, generando una nueva pieza distorsionada de acontecimientos reales.

El término *deepfake* se difundió en 2017. Este era el nombre de un usuario de *Reddit*, quien utilizaba el sitio web para publicar contenido pornográfico a través del intercambio de rostros empleando inteligencia artificial. La acción del usuario causó que el término adquiriera una connotación negativa, lo cual ha contribuido al uso de otras expresiones como "medios sintéticos generados por IA"[3] para referirse a los videos, imágenes y audios manipulados digitalmente con inteligencia artificial, de acontecimientos que no ocurrieron en la realidad. Sin embargo, la expresión más empleada sigue siendo *deepfake*.

[1] Homeland Security. (s.f.). Increasing threat of Deepfake. Recuperado de: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
[2] IBM. (2024). ¿Qué es Deep learning?. Recuperado de: https://www.ibm.com/es-es/topics/deep-learning
[3] Somers, M. (2020). Deepfakes, explained. MIT. Recuperado de: https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

Una de las primeras contribuciones al desarrollo de la tecnología deepfake podría remontarse al año 1997 con el programa Video Rewrite de Christoph Bregler, Michele Covell y Malcolm Slaney[4]. Este programa fue el primer sistema de animación facial que automatizó los procesos de reanimación de videos.

En el documento "*Video Rewrite: Driving Visual Speech with Audio de 1997*"[5], se presentan una serie de experimentos realizados con el programa *Video Rewrite*. En ese trabajo, se destacó la utilidad del programa en la industria cinematográfica, especialmente para optimizar el proceso de doblaje y la creación de películas. Utilizaba técnicas de visión por computadora para identificar el video original y realizar una segmentación de etiquetas faciales, así como el etiquetado de fonemas. Estas acciones en conjunto conforman los visemas de la base de datos usada para la resincronización del contenido audiovisual. Este sistema permitía la generación de un nuevo video mediante el análisis de los movimientos faciales de pronunciación del video original para sincronizar los gestos de habla con una nueva pista de audio. De esta manera, la persona en el nuevo video podía articular palabras diferentes a las del video original. Los autores también realizaron pruebas aplicando el programa a imágenes de dominio público, como las de John F. Kennedy (presidente de los Estados Unidos en el periodo 1961-1963). A partir de un discurso de 2 minutos en el que Kennedy efectuaba declaraciones sobre la crisis de los misiles en Cuba, crearon nuevas animaciones del presidente mencionando frases distintas a las del video original. Según los autores, el resultado de estas animaciones no alcanzó una calidad óptima. No obstante, los experimentos de *Video Rewrite* demostraron la capacidad y el alto potencial de desarrollo que se empezaba a gestar en esa época, la tecnología *deepfake* que años más tarde estaría en auge tras su evolución y perfeccionamiento.

El impacto en el mercado: cifras y perspectivas

Desde una óptica positiva, el progreso de las técnicas *deepfake* como potencial de creación y personalización de medios audiovisuales, representa un beneficio para las entidades, ya que promueve la innovación y competitividad de industrias como el cine, el entretenimiento, el marketing, el comercio electrónico, entre otras. Esta exploración y adaptación de la inteligencia artificial en las organizaciones se ve reflejado en un crecimiento del mercado. De acuerdo con las proyecciones, el mercado de inteligencia artificial *deepfake* tendrá una tasa de crecimiento anual compuesta (CAGR) de 33,5% durante el periodo 2024-2030 y pasará de un valor de 7.000 millones de dólares en 2024 a 38.500 millones de dólares en 2030[6].

Los pronósticos de crecimiento subrayan el impacto de la introducción de técnicas avanzadas de inteligencia artificial y las novedosas aplicaciones en la sociedad. Y es que las cifras de *deepfakes* han tenido un crecimiento exponencial en los últimos años. Entre el 2019 y el 2020, la cantidad de este contenido en línea aumentó 900%[7] como resultado de la alta accesibilidad a herramientas de creación de contenido a partir de inteligencia artificial. Comparativamente, el avance de *deepfake* conlleva riesgos considerables, teniendo en cuenta que el desarrollo actual ha planteado desafíos relacionados con la seguridad, la integridad personal y desinformación, promovidos en gran medida por la difusión en internet de contenido *deepfake* de ciberdelincuentes o hackers, lo que promueve el incremento en el número de casos de fraude. En 2022 el 66% de los profesionales de la ciberseguridad experimentó ataques *deepfake* dentro de sus organizaciones[8] y de 2022 a 2023 se incrementó en 10 veces el número de intentos de fraude de este tipo[9]. Dentro de los principales casos de fraude generados con técnicas *deepfakes* se encuentran los fraudes relacionados con suplantación de identidad, en donde los delincuentes roban la identidad del usuario para ejecutar acciones de fraude bancario, accediendo a sus cuentas o incluso usando esa identidad para crear perfiles falsos en redes sociales.

En 2023, el fraude mediante inteligencia artificial (principalmente *deepfakes*) fue uno de los principales riesgos de identidad al presentar notables crecimientos en los casos de usurpación de identidad a nivel mundial. Los países con mayores aumentos de incidentes fraudulentos de identidad en el periodo de 2022 a 2023 fueron Filipinas, con un aumento de 4.500% en el número de casos, seguido de Vietnam, con un aumento de 3.050% y Estados Unidos, con uno de 3.000%[10]. En cuanto a Latinoamérica, las cifras de crecimiento en el número de incidentes estuvieron concentradas en

[4] Sarmiento, S. (2023). Deepfakes: origen, riesgo y amenazas. Platzi. Recuperado de: https://platzi.com/blog/como-hacer-un-deepfake/#:~:text=Origen%20de%20la%20t%C3%A9cnica%20deepfake,y%20fue%20generado%20en%201997.
[5] Bregler, C., Covell, M., & Slaney, M. (1997). Video Rewrite: Driving visual speech with Audio. Recuperado de: https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/human/bregler-sig97.pdf
[6] Markets & Markets. (2024). Deepfake AI Market- Global Forecast to 2030. Report Code: UC 6472. Recuperado de: https://www.marketsandmarkets.com/Market-Reports/deepfake-ai-market-256823035.html#:~:text=The%20deepfake%20AI%20market%20is,33.5%25%20over%20the%20forecast%20period.
[7] World Economic Forum. (2023). *Cómo combatir el preocupante aumento del uso de deepfakes en la ciberdelincuencia*. Foro Económico Mundial. Recuperado de: https://es.weforum.org/agenda/2023/05/como-combatir-el-preocupante-aumento-del-uso-de-deepfakes-en-la ciberdelincuencia/#:~:text=En%202022%2C%20el%2066%25%20de,podr%C3%ADan%20generarse%20sint%C3%A9ticamente%20en%202026.
[8] World Economic Forum. (2023). *Cómo combatir el preocupante aumento del uso de deepfakes en la ciberdelincuencia*. Foro Económico Mundial. Recuperado de: https://es.weforum.org/agenda/2023/05/como-combatir-el-preocupante-aumento-del-uso-de-deepfakes-en-la-ciberdelincuencia/#:~:text=En%202022%2C%20el%2066%25%20de,podr%C3%ADan%20generarse%20sint%C3%A9ticamente%20en%202026.
[9] Sumsub. (2023). *Sumsub research: Global deepfake incidents surge tenfold from 2022 to 2023*. Recuperado de: https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
[10] Statista. (2023). *Países con mayores aumentos de casos de fraude de deepfake*. Recuperado de: https://es.statista.com/grafico/31907/paises-con-mayores-aumentos-de-casos-de-fraude-de-deepfake/

Brasil con un incremento de 828%, seguido por Argentina con un aumento de 766% y México con un incremento de 700%. Para el caso de Colombia se incrementaron en un 533% los casos de intentos de fraude mediante *deepfakes* para el mismo periodo[11]. Adicionalmente, se suman los casos de desinformación a causa de la proliferación de contenido *deepfake*, los cuales representan uno de los mayores riesgos a nivel social, de acuerdo con lo expuesto por el World Economic Forum en su informe global de riesgos 2024[12]. Recientemente, personas con fines mal intencionados han empleado técnicas *deepfake* usando la imagen de personajes públicos para difundir contenido falso con el fin de manipular la opinión pública e influir en las decisiones de la sociedad. Un claro ejemplo de desinformación fue el video difundido en redes sociales donde el presidente de Rusia, Vladimir Putin, anunciaba la paz con Ucrania en el año 2023[13].

Los índices de fraude mencionados anteriormente y las preocupantes consecuencias a raíz de los riesgos de desinformación en la sociedad amenazan la ciberseguridad global, por lo que será fundamental el trabajo conjunto entre el gobierno, sociedad civil y entidades a fin de mitigar el *deepfake* por parte de ciberdelincuentes.

Desafíos para el sector bancario

El sector bancario puede verse afectado por la creación de *deepfakes* ya sean de video, audio o imagen. Estos medios sintéticos generados por inteligencia artificial presentan amenazas latentes que permiten llevar a cabo ataques dirigidos a las entidades financieras a través de diferentes técnicas *deepfake* relacionadas con: (i) el intercambio de rostros; (ii) sincronización labial; (iii) recreaciones o *puppet master*, (iv) síntesis facial y manipulación de atributos y (v) audio *deepfake*[14].

(i) Intercambio de rostros: se refiere al uso de deepfake para reemplazar el rostro de una persona en un video o fotografía por el de otra persona. Esta práctica representa un riesgo significativo de suplantación de identidad para los usuarios y directivos de las entidades financieras. Los delincuentes pueden utilizar esta técnica como evasión de verificaciones de identidad, difusión de videos falsos de directivos en los que parecen autorizar transacciones o solicitar información confidencial.

(ii) Sincronización labial: en esta técnica se altera el audio original de un video para sincronizar un nuevo audio que coincida con los movimientos de la boca y las expresiones faciales. Aunque esta práctica se usa comúnmente en el doblaje de películas, también puede ser utilizada por ciberdelincuentes para crear audios falsos a partir de figuras públicas o miembros de las entidades con el fin de suplantar a individuos o difundir declaraciones falsas que afecten la imagen y reputación.

(iii) Recreaciones o *puppet master*: este método es conocido como *puppet master* debido a que una persona detrás de la cámara (titiritero) puede controlar las expresiones y los movimientos faciales de la imagen digital de una persona "marioneta" que se está proyectando en un video o transmisión en tiempo real[15]. Esto facilita a los estafadores realizar interacciones fraudulentas, suplantar identidades y afectaciones graves a los controles de verificación en tiempo real para cometer delitos como el robo de dinero o robo de datos personales.

(iv) Síntesis facial y manipulación de atributos: en primera instancia, la síntesis facial está relacionada con la creación de rostros inexistentes a partir de imágenes de rostros reales para generar una apariencia realista. Por otro lado, la manipulación de atributos permite modificar características faciales específicas de la persona[16], lo cual presenta riesgos como la creación de cuentas falsas para ejecutar transacciones fraudulentas.

(v) Audio *deepfake*: la práctica de audio *deepfake* permite clonar la voz de una persona para generar un nuevo audio falso que simula declaraciones que no se hicieron. La combinación de este tipo de técnica con otras de las mencionadas facilita a los delincuentes ataques de suplantaciones mediante llamadas telefónicas o de elusión a verificaciones biométricas de voz, así como para realizar declaraciones falsas o predicciones engañosas.

Las técnicas de *deepfake* descritas anteriormente generan un amplio espectro de riesgos para las entidades que abarcan la evasión de los sistemas de autenticación, la suplantación de identidad, el robo de datos personales, la elusión de la verificación de identidad conocida como *Electronic Know Your Customer* (EKYC), la falsificación de documentos, el daño reputacional, las interacciones fraudulentas y la desinformación[17]. Estos desafíos preocupan a las entidades financieras, especialmente en un contexto donde los ciberdelincuentes se benefician de la creación de medios sintéticos generados por inteligencia artificial. Los ataques de *deepfake* están siendo utilizados para potenciar ataques

[11] Sumsub (2023). Sumsub identity fraud report 2023. Recuperado de: https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
[12] World Economic Forum. (2024). The Global Risks Report 2024. ISBN: 978-2-940631-64-3. Recuperado de: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
[13] Agencia SINC. (2023). *Los deepfakes como arma de desinformación y propaganda en tiempos de guerra*. Recuperado de: https://www.agenciasinc.es/Noticias/Los-deepfakes-como-arma-de-desinformacion-y-propaganda-en-tiempos-de-guerra.
[14] Masood, M., Nawaz, M., Malik, K. M., Javed, A., & Irtaza, A. (2021). *Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward*. Recuperado de:https://arxiv.org/vc/arxiv/papers/2103/2103.00484v1.pdf
[15] iProov. (2023). *Generative AI attack types explained*. Recuperado de:https://www.iproov.com/blog/generative-ai-attack-types-explained
[16] Masood, M., Nawaz, M., Malik, K. M., Javed, A., & Irtaza, A. (2021). *Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward*. Recuperado de:https://arxiv.org/vc/arxiv/papers/2103/2103.00484v1.pdf
[17] Deloitte. (2023). *Safeguarding against deepfake technology* Recuperado de:https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-safeguarding-against-deepfake-technology-noexp.pdf

de *phishing* y suplantación de identidad, afectando tanto a los clientes como a los funcionarios de las entidades financieras. Un estudio reciente evidenció que el sector bancario está particularmente preocupado por los ataques *deepfake*, con un 92% de ciberprofesionales preocupados por su uso fraudulento[18].

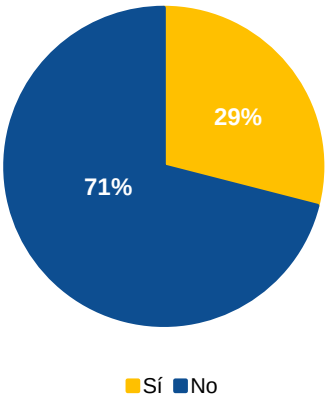
Un caso reciente demuestra los riesgos relacionados con *deepfake*. Se hizo viral el empleo de tecnología *deepfake* en la suplantación de un director financiero de una multinacional para recrear una videoconferencia en la cual le solicitó a uno de sus empleados la consignación de 25 millones de dólares. La estafa fue descubierta luego de la consulta por parte del empleado a la oficina central de la organización. Sin embargo, el dinero ya había sido desembolsado a los estafadores[19].

Otra técnica ya empleada por los ciberdelincuentes es el *deepfake* de voz. Un reportaje del New York times en 2023[20] informó sobre el intento de estafa a un inversionista quien contactó a su entidad bancaria para acordar una transferencia que estimaba realizar. El banco recibió otra llamada en la que afirmaban ser esta persona. Sin embargo, era un programa que estaba imitando la voz del inversionista para intentar transferir este dinero hacia otro destino. Finalmente, la entidad detectó el fraude antes de transferir el dinero e informó al equipo de ciberseguridad bancaria.

Estos casos de fraude financiero resaltan la necesidad de explorar e identificar el impacto que representa para el sistema el desarrollo de la inteligencia artificial, particularmente de los *deepfakes*, dada la facilidad que se tiene en el acceso a herramientas para suplantar identidades, así como los mecanismos de prevención para mitigar las amenazas a la seguridad contra el sistema financiero. Para ello, es importante que todas las partes involucradas identifiquen y conozcan los fraudes emergentes relacionados con nuevas técnicas en la manipulación de contenido audiovisual. Una encuesta global aplicada en 2022 expuso que sólo el 29% de las personas encuestadas conocían acerca de un video *deepfake*, mientras que el otro 71% no estaban familiarizados con este término[21] (Gráfico 1). Por otro lado, sólo el 0.1% de los participantes pudo identificar correctamente contenidos reales y *deepfake*[22].

En el contexto latinoamericano, según una encuesta realizada por una compañía internacional de ciberseguridad a usuarios latinoamericanos, el 70% de los usuarios encuestados desconocía

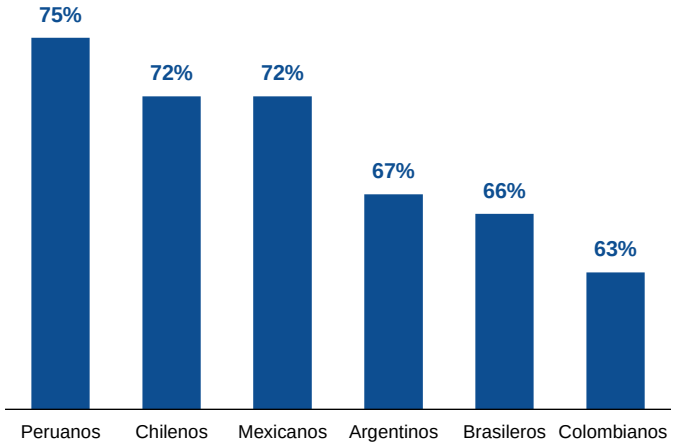
Gráfico 1. Porcentaje de consumidores globales que conocen sobre un *video deepfake*



Fuente: Iproov (2025).

las prácticas *deepfakes*. En este estudio se evidenció que los peruanos concentraban la cifra más alta de desconocimiento, con un 75%, seguidos de los mexicanos con el 72% y, en el caso de Colombia, se evidenció una cifra de 63% de desconocimiento de *deepfakes*[23](Gráfico 2).

Gráfico 2. Porcentaje de usuarios latinoamericanos que desconocen sobre *deepfakes*



Fuente: Kaspersky (2022).

[18] World Economic Forum. (2023). *¿Cómo combatir el preocupante aumento de contenidos deepfake?* Recuperado de: ¿Cómo combatir el preocupante aumento de contenidos deepfake? | Foro Económico Mundial (weforum.org)
[19]Chen,H . & Magramo,K.(2024) Finance worker pays out $ 25 million after video call with deepfake "chief financial officer" CNN Recuperado de: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[20]Cowley,S. & Filtter. E. (2023) Voice deepfakes are coming for your bank balnace.The New York Times Recuperado de: https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
[21] Iproov (2025) Estadísticas y soluciones sobre deepfakes | Cómo protegerse de los deepfakes. Recuperado de: Deepfake Estadísticas y soluciones | Protegerse contra los deepfakes
[22] Iproov (2025) Estadísticas y soluciones sobre deepfakes | Cómo protegerse de los deepfakes. Recuperado de: Deepfake Estadísticas y soluciones | Protegerse contra los deepfakes
[23] Kaspersky (2022). 7 de cada 10 lationamericanos desconoce qué es un "Deepfake". Recuperado de: https://latam.kaspersky.com/blog/lena-para-la-infodemia-7-de-cada-10-latinoamericanos-desconoce-que-es-un-deepfake-contribuyendo-a-la-sobrecarga-mental/23773/

Las cifras de desconocimiento por parte de los usuarios incrementan significativamente el riesgo en la industria financiera al facilitar la materialización de diversas amenazas. Además de los intentos de estafa previamente señalados, se han identificado casos de creación de cuentas fraudulentas e identidades falsas, donde se emplean elementos de identidad reales para asociarlos a individuos inexistentes. Así mismo, se presenta el riesgo asociado a la autorización indebida de pagos a causa de la suplantación de identidad de la persona titular de los servicios financieros, así como la suplantación de directivos dentro de las entidades, lo que podría inducir a los empleados a ejecutar acciones no autorizadas como transferencias de dinero o revelación de información confidencial. Adicionalmente, la manipulación del mercado mediante la difusión de información errónea por parte de ciberdelincuentes representa una amenaza significativa para la estabilidad del sector[24].

Preparándonos para el desafío

Las preocupantes tendencias de fraude asociadas al uso de *deepfake* sugieren la urgencia de analizar e implementar a fondo mecanismos de defensa para combatir y reducir las actividades delictivas de suplantación de identidad. Desde la perspectiva de las entidades financieras será crucial reforzar los mecanismos de autenticación biométrica y detección de *deepfakes*. Para esto, la inversión en nuevas tecnologías de protección desempeñará un papel fundamental en garantizar la seguridad digital en la banca. De acuerdo con el informe de gestión gremial de Asobancaria, en el 2023 se invirtieron $543 mil millones de pesos en ciberseguridad, lo que significa un aumento de 17% respecto a 2022. También se destaca que 27 de las 38 entidades están utilizando *blockchain* como medios tecnológicos para proteger la seguridad digital y 24 entidades implementan inteligencia artificial como medio de protección[25]. El reto a nivel gremial consistirá en fomentar las inversiones en seguridad digital y aumentar la adopción de nuevas tecnologías en los procesos de ciberseguridad por parte de más entidades. Adicionalmente, las entidades deben fortalecer los procesos internos como el *"Know Your Customer"* (KYC), teniendo en cuenta que el rápido avance de los *deepfakes* atenta contra los filtros de verificación de identidad mediante falsificaciones. En cuanto a los avances tecnológicos recientes, se ha generado un progreso significativo en el mercado relacionado con herramientas de detección de *deepfakes*, destinadas a contrarrestar el impacto negativo generado por contenido de medios sintéticos. Un ejemplo destacado es el programa de inteligencia artificial desarrollado por INTEL para identificar *deepfakes* en tiempo real, con una exactitud de 96%[26], no obstante, aún persisten múltiples desafíos por abordar.

En relación con los usuarios, institucionalmente se deberán crear campañas de sensibilización y programas de capacitación especializados en la identificación de *deepfakes*. Estas capacitaciones les permitirían a los usuarios familiarizarse con herramientas y consejos útiles para enfrentar posibles engaños y proteger la integridad de su entorno financiero. Fomentar esta cultura de conocimiento permitirá mejorar la detección y prevención del fraude, así como promover la alerta hacia las entidades competentes sobre nuevas modalidades de engaño.

Por último, las entidades gubernamentales deben avanzar en regulaciones para hacer frente y prepararse ante el incremento considerable de *deepfakes* con fines malintencionados. En el caso de EE.UU., a inicios del año 2024 ya se habían presentado regulaciones en al menos 14 estados[27], esto como resultado de los riesgos inminentes de desinformación que se pudieran ocasionar durante el periodo de campañas políticas. En 2024, la Unión Europea (UE) aprobó la Ley de inteligencia artificial, con el objetivo de promover y garantizar las buenas prácticas en el uso de esta tecnología.

En el caso de Colombia, varios proyectos relacionados con regulación de inteligencia artificial se han adelantado en el Congreso de la República. Estas iniciativas pretenden regular el uso de las tecnologías emergentes y establecer códigos de ética que protejan a los usuarios. Una de las iniciativas que desempeñará un rol crucial ante los riesgos de suplantación de identidad empleando IA, como los *deepfakes*, es el proyecto de Ley 225/2024 Senado y 360/2024 Cámara de representantes, "Por medio del cual se modifica y establece un agravante al artículo 296 de la Ley 599 del 2000, Código Penal Colombiano y se dictan otras disposiciones"[28]. Este proyecto busca incorporar un agravante al delito de falsedad personal cuando se utilice IA en la suplantación.

Conclusiones y consideraciones finales

El impacto de la difusión de *deepfakes* en el mundo presenta un panorama complejo de oportunidades y desafíos en diversos ámbitos. Será crucial que desde un entorno legal se avance en marcos regulatorios para establecer normas claras en las cuales se contemplen los riesgos asociados del uso y creación de contenido

[24] Iproov. (2020). Deepfakes: The threat to financial services. Recuperado de: https://www.iproov.com/wp-content/uploads/2020/09/iProov-deepfakes-FS-report.pdf
[25] Asobancaria. (2023). *Informe de gestión y gobernanza 2023*. Recuperado de: https://www.asobancaria.com/wp-content/uploads/2024/06/IGG-2024-V7.pdf
[26] BBC News. (2023,). Intel's deepfake detector tested on real and fake videos. Recuperado de: Intel's deepfake detector tested on real and fake videos
[27] Edelman, A. (2024). States turn their attention to regulating AI and deepfakes as 2024 kicks off. NBC news. Recuperado de: https://www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122
[28] Congreso de la República de Colombia. (2024). *Proyecto de ley 360/2024C - 225/2024S: Modificación y agravante del delito de falsedad personal con uso de inteligencia artificial.* Cámara de Representantes de Colombia. Recuperado de: https://www.camara.gov.co/falsedad-personas-ia

manipulado con inteligencia artificial. En el sector bancario los *deepfakes* plantean un riesgo en términos de ciberseguridad y protección de datos, por ese motivo, es esencial que tanto las entidades financieras como los usuarios estén al tanto de los nuevos desarrollos tecnológicos y adopten mecanismos de prevención.

Es crucial, en este contexto, la integración de sistemas normativos y tecnológicos para mitigar los riesgos inherentes al uso de *deepfakes*, con el propósito de proteger a la sociedad de actividades fraudulentas, al mismo tiempo que se promueve el uso responsable y ético de estos desarrollos. Por otro lado, un elemento clave es avanzar en la investigación y educación sobre los *deepfakes*, profundizando en el entendimiento de su funcionamiento, aplicaciones y potenciales amenazas. Los altos índices de desconocimiento y desinformación en la población facilitan las actividades fraudulentas de los ciberdelincuentes, lo que hace imperativo promover la alfabetización digital, enfocándose en el reconocimiento y detección de contenidos manipulados digitalmente.

Principales indicadores macroeconómicos

Colombia

	2021	2022	2023					2024	2025*				
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Producto Interno Bruto													
PIB Nominal (COP Billones)	**1192,6**	**1462,5**	385,3	379,9	398,0	409,3	**1572,5**	400,2	411,6	436,1	457,4	**1705,3**	**1833,3**
PIB Nominal (USD Billions)	**318,5**	**344,6**	81,0	85,8	98,4	99,5	**382,3**	102,0	105,0	106,4	105,2	**418,8**	**436,6**
PIB Real (COP Billones)	**907,4**	**907,4**	236,1	239,1	245,7	257,2	**978,2**	236,9	244,9	250,7	264,1	**996,1**	**1027,6**
PIB Real (% Var. interanual)	**11**	**7,3**	2,9	0,1	-0,6	0,3	**0,7**	0,6	1,9	2,1	2,3	**1,7**	**3,1**
Precios													
Inflación (IPC, % Var. interanual)	**5,6**	**13,1**	13,3	12,1	11,0	9,2	**9,3**	7,4	7,2	5,8	5,2	**5,2**	**4,3**
Inflación sin alimentos (% Var. interanual)	**3,4**	**10**	11,4	11,6	11,5	5,0	**10,3**	8,8	7,6	6,5	5,6	**5,6**	**3,9**
Tipo de cambio (COP/USD fin de periodo)	**3981**	**4810**	4627	4191	4054	3822	**3822**	3842	4148	4164	4409	**4409**	**4199**
Tipo de cambio (Var. % interanual)	**16**	**20,8**	23,5	1,5	-10,6	-19,3	**-19,3**	-17,0	-1,0	2,7	15,3	**15,3**	**-4,6**
Sector Externo													
Cuenta corriente (USD millones)	**-17951**	**-20879**	-2807	-2082	-1546	-1805	**-8285**	-1941	-1577	-1654	-2240	**-7412**	**-11683**
Déficit en cuenta corriente (% del PIB)	**-5,7**	**-6,0**	-3,5	-2,4	-1,6	-1,8	**-2,3**	-1,9	-1,5	-1,6	-2,1	**-1,8**	**-2,7**
Balanza comercial (% del PIB)	**-6,4**	**-4,7**	-2,7	-2,4	-1,4	-2,1	**-2,1**	-1,9	-2,1	-2,2	-3,1	**-2,3**	**-3,6**
Exportaciones F.O.B. (% del PIB)	**13,6**	**21,3**	21,1	19,2	17,5	17,3	**18,8**	15,8	16,5	16,6	16,9	**16,5**	**11,6**
Importaciones F.O.B. (% del PIB)	**18**	**25,9**	23,8	21,6	18,9	19,4	**20,9**	17,7	18,6	18,8	20,0	**18,8**	**15,2**
Renta de los factores (% del PIB)	**-2,8**	**-4,9**	-4,6	-3,5	-3,5	-3,1	**-3,7**	-3,3	-3,1	-3,2	-3,0	**-3,1**	**-3,3**
Transferencias corrientes (% del PIB)	**3,4**	**3,6**	3,8	3,5	3,4	3,4	**3,5**	3,3	3,7	3,8	4,0	**3,7**	**3,7**
Inversión extranjera directa (pasivo) (% del PIB)	**3,0**	**4,9**	5,1	6,2	4,0	3,8	**4,8**	3,6	2,7	3,1		…	…
Sector Público (acumulado, % del PIB)													
Bal. primario del Gobierno Central	**-3,6**	**-1,0**	0,3	1,2	0,2	…	**-0,3**	…	…	…		**-2,4**	**-5,1**
Bal. del Gobierno Nacional Central	**-7,0**	**-5,3**	-0,9	0,0	-0,7	-2,7	**-4,3**	-1,2	-2,1	…		**-6,8**	**-0,2**
Bal. primario del SPNF	**-3,5**	**-1,4**	…	…	…	…	**1,5**	…	…	…		**-0,2**	…
Bal. del SPNF	**-7,1**	**-6,0**	…	…	…	…	**-2,7**	…	…	…		**-4,9**	…
Indicadores de Deuda (% del PIB)													
Deuda externa bruta	**53,9**	**53,4**	55,2	56,1	…	…	**53,6**	…	…	…		**48,2**	…
Pública	**32,2**	**30,4**	31,4	31,8	…	…	**30,9**	…	…	…		**27,0**	…
Privada	**21,7**	**23**	23,8	24,2	…	…	**22,8**	…	…	…		**21,1**	…
Deuda neta del Gobierno Central	**60,0**	**57,7**	54,1	52,2	52,8	53,8	**53,8**	51,5	55,4	57,6	…	**60,0**	**60,3**

*Proyecciones de Asobancaria. Los datos fiscales corresponden a lo proyectado por el Gobierno Nacional en el PF 2025

Fuentes: DANE, Banco de la República, Ministerio de Hacienda y Crédito Publico

Estados financieros del sistema bancario
Colombia

	dic-20	dic-21	dic-22	dic-23	ene-25 (a)	dic-24	ene-24 (b)	Var. real anual (b) - (a)
Activo	**729.841**	**817.571**	**924.121**	**959.797**	**989.038**	**998.266**	**948.352**	**-0,9%**
Disponible	53.794	63.663	58.321	64.582	56.278	59.096	55.523	-3,7%
Inversiones	158.735	171.490	180.818	189.027	215.110	215.062	188.666	8,4%
Cartera de crédito	498.838	550.204	642.473	655.074	676.445	677.712	654.078	-1,7%
Consumo	150.527	169.603	200.582	196.005	188.076	189.083	194.231	-8,0%
Comercial	263.018	283.804	330.686	338.202	356.667	357.805	338.337	0,2%
Vivienda	72.565	82.915	95.158	102.972	112.067	111.301	103.518	2,9%
Microcrédito	12.727	13.883	16.047	17.896	19.636	19.524	17.992	3,7%
Provisiones	37.960	35.616	37.224	39.752	40.276	40.396	39.799	-3,8%
Consumo	13.729	12.251	15.970	18.644	17.716	17.902	18.634	-9,6%
Comercial	17.605	17.453	16.699	16.335	17.495	17.326	16.332	1,8%
Vivienda	2.691	3.021	3.189	3.413	3.696	3.641	3.433	2,3%
Microcrédito	1.133	913	858	1.181	1.318	1.332	1.244	0,6%
Pasivo	**640.363**	**713.074**	**818.745**	**856.579**	**875.703**	**885.568**	**844.391**	**-1,4%**
Depósitos y otros instrumentos	556.917	627.000	686.622	731.321	771.892	777.404	731.873	0,2%
Cuentas de ahorro	246.969	297.412	297.926	286.217	303.099	313.749	284.629	1,2%
CDT	154.188	139.626	207.859	272.465	294.087	287.571	278.367	0,4%
Cuentas Corrientes	75.002	84.846	80.608	75.483	72.919	77.164	72.528	-4,5%
Otros pasivos	9.089	9.898	11.133	10.841	11.574	11.087	10.308	6,7%
Patrimonio	**89.479**	**104.497**	**105.376**	**103.218**	**113.335**	**112.697**	**103.961**	**3,6%**
Utilidades (año corrido)	**4.159**	**13.923**	**14.222**	**8.133**	**697**	**8.326**	**487**	**36,0%**
Ingresos financieros de cartera	45.481	42.422	63.977	91.480	6.923	85.888	7.639	-13,9%
Gastos por intereses	14.571	9.594	28.076	60.093	3.996	53.748	5.019	-24,3%
Margen neto de intereses	31.675	33.279	38.069	35.918	3.202	36.372	3.042	0,0%
Indicadores (%)								
Calidad	**4,96**	**3,89**	**3,61**	**4,90**	**4,64**	**4,62**	**5,04**	**-0,40**
Consumo	6,29	4,37	5,44	8,10	6,71	6,80	8,20	-1,49
Comercial	4,55	3,71	2,73	3,42	3,66	3,59	3,56	0,10
Vivienda	3,30	3,11	2,47	3,03	3,54	3,51	3,14	0,41
Microcrédito	7,13	6,47	5,46	8,50	8,71	8,57	9,61	-0,90
Cubrimiento	**153,5**	**166,2**	**160,6**	**123,8**	**128,4**	**129,1**	**120,8**	**-7,63**
Consumo	145,1	165,4	146,4	117,4	140,3	139,3	117,0	23,30
Comercial	147,1	165,6	184,7	141,2	134,0	134,8	135,6	-1,56
Vivienda	112,3	117,1	135,5	109,3	93,1	93,2	105,7	-12,65
Microcrédito	124,8	101,7	97,9	77,7	77,1	79,6	72,0	5,11
ROA	0,6	1,7	1,5	0,8	0,8	0,8	0,6	0,23
ROE	4,6	13,3	13,5	7,9	7,6	7,4	5,8	1,87
Solvencia	16,3	20,5	17,1	16,5	17,0	16,9	16,7	0,38
IRL	213,1	204,4	183,7	194,0	177,9	183,3	187,7	-9,78
CFEN G1	0,0	113,5	109,6	115,5	114,1	114,9	115,2	-1,17
CFEN G2	0,0	134,4	127,3	134,4	131,0	132,1	129,7	1,32

Fuente: Superintendencia Financiera de Colombia.

Nota: G1 corresponde a bancos con activos superiores al 2% del total y G2 a bancos diferentes a G1 que tengan cartera como activo significativo.

Principales indicadores de inclusión financiera

Colombia

	2021					2022					2023					2024
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**
Profundización financiera - Cartera/PIB (%) EC + FNA	**50,9**	50	49,4	48,6	48,3	**48,3**	47,1	46,8	46,7	46,2	**46,2**	45,9	45,4	45,3	44,0	**44,0**
Efectivo/M2 (%)	**17,0**	16,2	15,9	15,6	16,3	**16,3**	14,7	14,3	13,9	15,0	**15,0**	14,2	14,1	14,5	15,5	**15,5**
Cobertura																
Municipios con al menos una oficina o un corresponsal bancario (%)	**100**	100	100	100	100	100	100	100	100	100	100	100	100	100	100	**100**
Municipios con al menos una oficina (%)	**79,5**	79,1	77,8	77,8	78,7	**78,7**	76,8	77,0	76,8	78,7	78,7	76,7	77,4	76,7	77,2	**77,2**
Municipios con al menos un corresponsal bancario (%)	**92,7**	98,6	98,7	99,6	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	**100,0**
Acceso*																
Productos personas																
Indicador de inclusión financiera (%)	**90,5**	91,2	91,8	92,1	92,3	**92,3**	92,9	93,2	93,7	94,6	**94,6**	94,4	94,8	95,4		
Indicador de acceso a crédito	**34,5**	34,7	35,4	36,1	36,2	**36,2**	35,2	35,3	35,2	35,3	**35,3**	35,0	35,5	35,2		
Adultos con: (en millones)																
Al menos un producto	**33,5**	33,8	34,2	34,4	34,7	**34,7**	35,1	35,3	35,6	36,1	**36,1**	36,4	36,7	37,0		
Cuentas de ahorro	**28,9**	29,2	29,5	29,6	29,9	**29,9**				30,8	**30,8**	31,2	31,3	31,5		
Cuenta corriente	**1,9**	1,9	1,9	1,8	1,8	**1,8**										
Depósitos de bajo monto	**21,1**	21,7	22,4	23,0	23,5	**23,5**				27,5	**27,5**	31,1	31,3	31,5		
CDT	**-**	0,8	0,8	0,9	0,9	**0,9**	0,9	1,0	1,0	1,1	**1,1**	1,2	1,2	1,2		
Al menos un crédito	**12,6**	12,8	13,2	13,5	13,5	**13,5**	13,4	14,4	13,5	13,5	**13,5**	13,4	13,7	13,6		
Crédito de consumo	**6,9**	7,1	7,4	7,7	7,8	**7,8**	7,4	7,4	7,3	7,3	**7,3**	7,4	7,4	7,4		
Tarjeta de crédito	**7,9**	8,0	8,2	8,4	8,5	**8,5**	8,5	8,5	8,5	8,4	**8,4**	8,4	8,8	8,7		
Microcrédito	**2,3**	2,3	2,3	2,4	2,3	**2,3**				2,4	**2,4**	2,3	2,4	2,3		
Crédito de vivienda	**1,2**	1,2	1,2	1,3	1,3	**1,3**				1,2	**1,2**	1,2	1,2	1,2		
Crédito comercial	**0,2**	0,5	0,4	0,4	0,5	**0,5**										
Uso*																
Productos personas																
Adultos con: (%)																
Algún producto activo	**74,8**	76,2	76,9	77,7	77,2	**77,2**	77,8	78,2	79,1	82,7	**82,7**	82,5	83,0	83,5		
Cuentas de ahorro activas	**65,7**	65,9	65,2	64,9	51,9	**51,9**				54,5	**54,5**	54,1	53,3	53,6		
Cuentas corrientes activas	**73,7**	76,9	76,5	76,3	74,5	**74,5**										
Cuentas CAES activas																
Cuentas CATS activas	**76,3**	77,8	78,6	80,2	78,6	**78,6**				80,1	**80,1**	80,7	81,2	81,7		
Depósitos electrónicos																
Productos de ahorro a término (CDTs)	**-**	77,5	79,3	80,1	73,2	73,2										

* Vigiladas por la SFC, la SES, y ONG microfinancieras

Fuentes: Banca de las Oportunidades, Superintendencia Financiera de Colombia.

Principales indicadores de inclusión financiera

Colombia

	2021					2022					2023					2024
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**
Acceso*																
Productos empresas																
Empresas con: (en miles)																
Al menos un producto	**1028,6**	1029,0	1038,7	1065,7	1077,1	**1077,1**				1169,6	**1169,6**					
*Productos de depósito	**998,9**	1004,0	1013,0	1039,8	1046,4	**1046,4**				1166,4	**1166,4**					
*Productos de crédito	**280,2**	289,6	294,2	300,6	380,2	**380,2**				417,6	**417,6**					
Uso*																
Productos empresas																
Empresas con: (%)																
Algún producto activo	**70,5**	71,4	71,2	72,1	72,4	**72,4**										
Operaciones (semestral)																
Total operaciones (millones)	**11.161**	-	6.668	-	7.769	**14.397**	-	7.500	-	7.808	**15.308**	3.986	4.499	5.421	6.016	
No monetarias (Participación)	**56,1**	-	55,4	-	56,0	**55,8**	-	49,2	-	39,0	**44,1**	37,41	36,90	53,72	53,2	
Monetarias (Participación)	**43,8**	-	44,6	-	44,0	**44,2**	-	50,8	-	61,0	**55,9**	62,59	63,10	46,93	46,74	
No monetarias (Crecimiento anual)	**2,3**	-	34,0	-	23,2	**27,9**	-	29,4	-	39,2	**34,7**					
Monetarias (Crecimiento anual)	**29,1**	-	33,1	-	27,1	**29,8**	-	1,1	-	-29,9	**-15,7**					
Tarjetas																
Crédito vigentes (millones)	**15,6**	15,9	16,0	16,1	16,0	**16,0**	15,8	15,5	15,4	15,0	**15,0**	14,4	14	13,8	13,62	**13,62**
Débito vigentes (millones)	**40,8**	41,1	42,6	43,7	45,8	**45,8**	46,2	46,4	47,1	47,2	**47,2**	46	44,97	45,45	45,31	**45,31**
Ticket promedio compra crédito ($miles)	**219,9**	215,3	225,2	209,5	225,6	**225,6**	211,1	211,8	200,0	212,6	**212,6**	197	199	194,7	244,9	**244,9**
Ticket promedio compra débito ($miles)	**124,9**	119,1	116,5	112,5	108,1	**108,1**	100,6	100,7	96,0	111,1	**111,1**	93,2	94,7	91,7	97,1	**97,1**

* Vigiladas por la SFC, la SES, y ONG microfinancieras

Fuentes: Banca de las Oportunidades, Superintendencia Financiera de Colombia.