Banca & Economía

2026

Edición 1544

La confianza en la banca digital: construyendo un ecosistema más seguro

03 de noviembre de 2026

Director

Jonathan Malagón González

ASOBANCARIA:

Jonathan Malagón González
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

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

- La digitalización ha ampliado el acceso y la eficiencia de los servicios financieros, mientras los delincuentes se apalancan en nuevas tecnologías y en modalidades de ingeniería social para intentar vulnerar la seguridad de los usuarios.
- La experiencia internacional demuestra que la prevención del fraude requiere combinar regulación, herramientas tecnológicas, intercambio de información y coordinación interinstitucional para la mitigación de este fenómeno.
- El sector financiero ha logrado avances importantes en materia de innovación, concientización y articulación. Sin embargo, persisten retos relacionados con el fortalecimiento de las estrategias y los marcos normativos necesarios para agilizar la capacidad de respuesta frente a las modalidades de fraude que más afectan a los usuarios, como el robo de datos.

Banca & Economía

2026

Edición 1544

La confianza en la banca digital: construyendo un ecosistema más seguro

Editor
Germán Montoya
Director Económico

Participaron en esta edición:
Andrés Duque Márquez
Juan Sebastián León Pérez
Carol Alejandra Rodríguez Calderón
Esteban Rodríguez Luna

La digitalización ha transformado el ecosistema financiero, permitiendo, entre otras cosas, mayores niveles de inclusión financiera y el desarrollo de servicios personalizados, inmediatos y sin fricciones para los usuarios. Este avance ha acercado a millones de personas a productos y servicios financieros, lo que ha consolidado una banca más cercana que tiene como pilar el bienestar de las personas.

Este mismo proceso de transformación ha traído consigo nuevos retos en materia de seguridad, entre ellos el fraude, que ha sido uno de los desafíos persistentes que ha enfrentado el sector. Su impacto es doble, deteriora la confianza de los usuarios y afecta el patrimonio de estos y de las entidades financieras.

Sin embargo, el proceso de digitalización no es, por sí solo, la causa del crecimiento de los casos de fraude bancario. Detrás de este fenómeno hay organizaciones criminales cada vez más sofisticadas, que aprovechan nuevas tecnologías y metodologías para perfeccionar sus modalidades de ataque. Este es un fenómeno global, por lo que analizar las estrategias implementadas en otros países resulta clave para identificar los cambios que se requieren en aras de fortalecer la lucha contra el fraude.

Esta edición de Banca & Economía explora la evolución del fraude digital en Colombia, con el propósito de comprender la problemática actual e identificar las principales vulnerabilidades que han impulsado el crecimiento de estas modalidades. Analiza, posteriormente, la evolución de este fenómeno en el ámbito internacional y las medidas adoptadas por distintos países para contrarrestarlo. Finalmente, revisa las acciones implementadas en Colombia durante los últimos años, así como las fortalezas alcanzadas y los aspectos que aún deben mejorarse para fortalecer la lucha contra el fraude. Finaliza con algunas conclusiones en la materia.

Una Colombia que se enfrenta a riesgos más digitales

Colombia, como el resto del mundo, ha experimentado una transformación profunda en la forma en que las personas se comunican, consumen y acceden a servicios. La expansión de la conectividad, la masificación de los teléfonos inteligentes y el desarrollo de plataformas digitales trasladaron una parte creciente de las actividades cotidianas hacia entornos virtuales.

La evolución del acceso a internet permite dimensionar esta transformación. Entre el primer trimestre de 2018 y el primer trimestre de 2026, el acceso de personas a internet pasó de 25,6 millones a 49,6 millones, lo que equivale a un crecimiento cercano a 94%.

¡Un año donde la innovación y el conocimiento impulsan el progreso del país!

Calendario Eventos Programación 2026

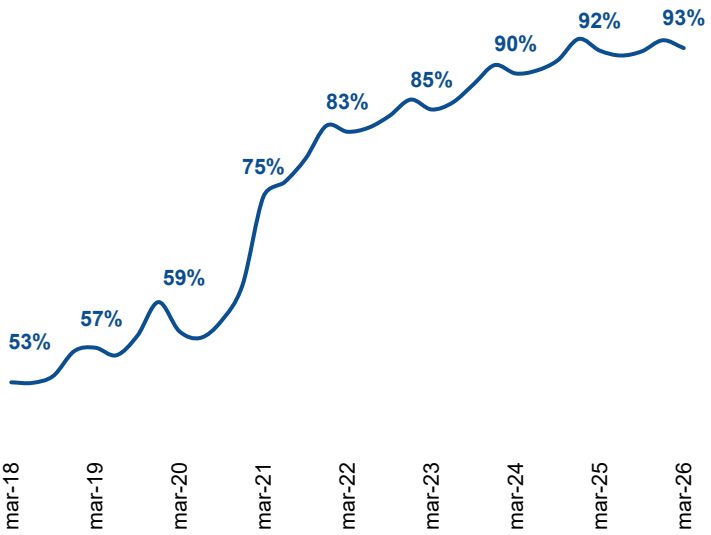
5 y 6 de marzo — CAMP — 16° CAMP — Centro de Convenciones Cartagena de Indias
28 de abril — 17° Foro de Vivienda — Grand Hyatt Bogotá D.C.
28 de mayo — 8° Congreso FEST — Grand Hyatt Bogotá D.C.
25 y 26 de junio — 25° Congreso Panamericano de Riesgo LAFTFPADM — Estelar Cartagena
26, 27 y 28 de agosto — 60ª Convención Bancaria — Centro de Convenciones Cartagena de Indias
1 de octubre — 37° Simposio de Mercado de Capitales — Asobancaria Bogotá D.C.
22 y 23 de octubre — 24° Congreso de Riesgos — Intercontinental Cartagena
12 y 13 de noviembre — 24° Congreso Derecho Financiero — Hyatt Regency Cartagena
25, 26 y 27 de noviembre — 19° Congreso SAFE — Centro de convenciones Las Américas
3 de diciembre — 14° Encuentro Tributario — Club El Nogal Bogotá D.C.

Alianzas comerciales:
Sonia Elias
+57 320 859 72 85
patrocinios@asobancaria.com

Inscripciones:
Call Center
eventos@asobancaria.com
Cel +57 321 456 81 11
57 601 326 66 20

En el mismo periodo, la profundización, calculada como la relación entre el número de personas con acceso a internet y la población total del país, aumentó de 53% a 92,7%, lo que representa un incremento de 75,1% en términos relativos[1] (Gráfico 1).

Gráfico 1. Evolución trimestral de la profundización de internet en Colombia, 2018-2026

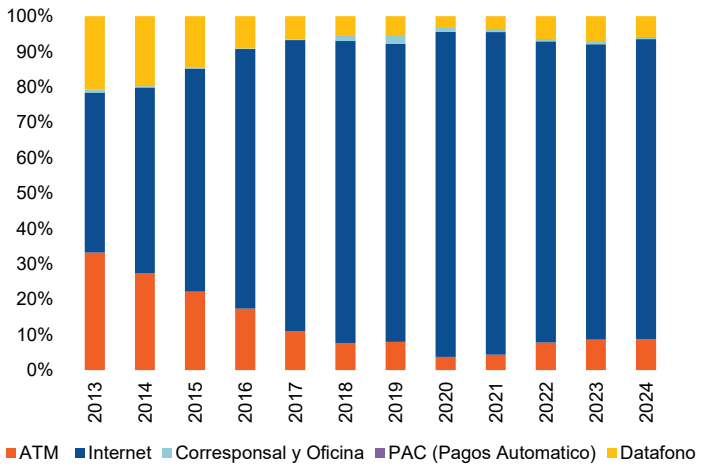


Fuente: Ministerio de las Tecnologías de la Información y las Comunicaciones. Elaboración Asobancaria.

Este crecimiento de la conectividad se reflejó directamente en el sistema financiero. Durante los últimos años, las entidades bancarias ampliaron la disponibilidad de aplicaciones móviles, portales web, transferencias electrónicas, sistemas de pago y servicios de consulta remota. Como resultado, las operaciones realizadas mediante banca móvil, banca por internet, transferencias a través de ACH e IVR adquirieron una mayor relevancia frente a canales físicos como oficinas, corresponsales bancarios, cajeros automáticos y datáfonos.

Entre 2018 y 2025, el crecimiento promedio anual de las transacciones en canales digitales fue de 16,5%[2], lo que evidencia una aceleración considerable del proceso de adopción digital. Este comportamiento estuvo asociado tanto a la ampliación de la oferta de productos financieros digitales como a cambios en las preferencias de los usuarios, quienes comenzaron a valorar especialmente la disponibilidad permanente, la rapidez y la posibilidad de realizar operaciones desde cualquier ubicación (Gráfico 2).

Gráfico 2. Evolución de las operaciones bancarias realizadas mediante canales digitales y físicos



Fuente: Superintendencia Financiera de Colombia. Elaboración Asobancaria.

No obstante, esta evolución no está exenta de riesgos, también ha dado lugar a nuevas amenazas y vulnerabilidades que persisten en la actualidad y que constituirán algunos de los principales desafíos para el futuro del sistema bancario, donde el más evidente es la exposición al fraude digital.

Los delincuentes se apalancan en tecnologías emergentes para sofisticar sus modalidades de engaño, apropiación de credenciales, suplantación de identidad e instalación de programas maliciosos, entre otros.

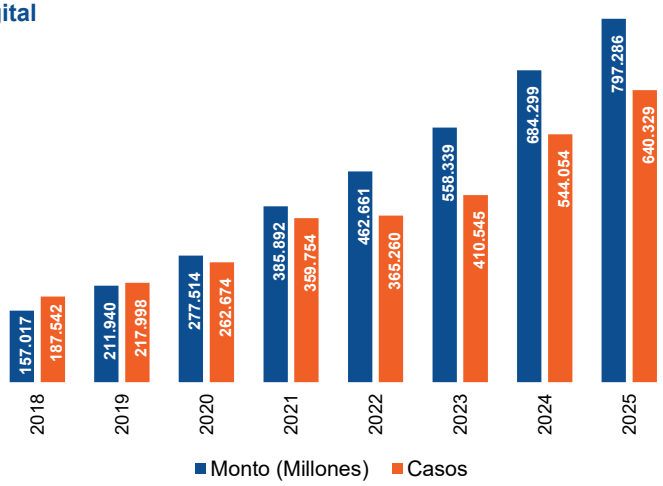
Una de las primeras alertas percibidas ha sido el incremento sostenido en las denuncias realizadas por ciudadanos asociados a delitos informáticos. Estas conductas comprenden diferentes acciones dirigidas contra la confidencialidad, integridad y disponibilidad de la información o de los sistemas tecnológicos. Incluyen también aquellas modalidades que son utilizadas para obtener de forma ilícita activos, apropiarse de datos, suplantar identidades o afectar el patrimonio de ciudadanos y organizaciones.

Entre 2018 y 2025, las denuncias por delitos informáticos en Colombia pasaron de aproximadamente 21.279 a 63.290, lo que representa una triplicación en las denuncias respecto a este delito. Al profundizar en las modalidades que pueden afectar al usuario bancario como el hurto por medios informáticos, la suplantación de identidad o de sitios web y la transacción no consentida de activo, se evidencia que representaron el 64,3% del total de denuncias en 2025. Estas cifras capturan en parte la expansión de modalidades informáticas para la comisión de delitos.

[1] Estadísticas del sector de las Tecnologías de la Información y las Comunicaciones. (2025). https://colombiatic.mintic.gov.co/679/w3-propertyvalue-754338.html
[2] Informe mensual de fraude (2026), Asobancaria.

En esta línea, Colombia ha enfrentado durante la última década un panorama cada vez más desafiante en materia de fraude bancario. Entre 2018 y 2025, el número de casos reportados creció a una tasa promedio anual del 18,9%, mientras que el monto reclamado aumentó un 21,7%. Esta problemática se ha concentrado principalmente en las modalidades digitales, cuya participación en el total del monto reclamado pasó de 62% en 2018 a 80% en 2025 (Gráfico 3).

Gráfico 3. Casos y monto reclamado por fraude bancario digital



Fuente: Elaboración Asobancaria.

Es importante recalcar que la digitalización no es, por sí sola, la causa directa del crecimiento del fraude. Este fenómeno responde más bien a la capacidad de adaptación de las organizaciones criminales, que ajustan constantemente sus modalidades de ataque, y a factores como la vulnerabilidad de los usuarios y la coordinación institucional.

¿Qué ha hecho el mundo para contrarrestar el fraude?

En el ámbito internacional, se ha vivido un panorama similar frente a la creciente digitalización de los servicios financieros que ha impulsado importantes avances en términos de innovación y eficiencia. Este crecimiento ha traído consigo, no obstante, riesgos significativos para el ecosistema financiero, el cual se enfrenta a un panorama de nuevas técnicas de fraude cada vez más sofisticadas.

Diversos estudios internacionales evidencian que las técnicas de ingeniería social se han consolidado como una de las principales modalidades utilizadas por los ciberdelincuentes para el fraude de identidad, al facilitar el robo de datos personales e información financiera que posteriormente son empleados para la comisión de fraudes financieros. De acuerdo con la INTERPOL, este tipo de fraude se materializa principalmente mediante modalidades como el *phishing, smishing, vishing y spoofing*[3]. Estas tácticas pueden materializarse a través de diversos canales de comunicación, entre ellos el correo electrónico, llamadas telefónicas, mensajes de texto, aplicaciones de mensajería instantánea y redes sociales[4].

La efectividad de estas técnicas radica en que explotan el factor humano, ampliamente reconocido como el eslabón más vulnerable de la cadena de seguridad de la información[5]. A este escenario se suma el uso de herramientas basadas en inteligencia artificial, que ha incrementado significativamente la sofisticación y el alcance de las campañas de ingeniería social.

Estas tecnologías permiten a los actores maliciosos automatizar la recopilación y el análisis de información, elaborar señuelos más creíbles y personalizados, optimizar el desarrollo y análisis de código malicioso, así como clasificar y priorizar los datos robados para maximizar el impacto de sus ataques[6]. Como resultado, la identificación de intentos de fraude representa un desafío cada vez mayor para los usuarios y para las entidades encargadas de proteger la confianza en el ecosistema financiero digital.

La prevención del robo de datos y del fraude digital requiere respuestas que trasciendan los controles internos de las entidades financieras y demandan un enfoque integral basado en la coordinación entre autoridades, entidades financieras, proveedores de servicios y demás actores del ecosistema digital.

En este contexto, diversos gobiernos y organismos internacionales han fortalecido sus estrategias para enfrentar estas amenazas mediante la adopción de marcos normativos, el desarrollo de mecanismos de cooperación y la implementación de medidas regulatorias y tecnológicas orientadas a prevenir y mitigar el fraude digital.

En consecuencia, resulta pertinente revisar la experiencia de países referentes en esta materia con el fin de identificar buenas prácticas, responsabilidades y esquemas de coordinación institucional que puedan contribuir al fortalecimiento de las capacidades nacionales para prevenir el robo de datos, combatir el fraude digital y reforzar la confianza en los servicios financieros digitales.

Los rankings internacionales sobre prevención del fraude y resiliencia cibernética evidencian un liderazgo de los países europeos, destacándose Luxemburgo por la solidez de sus marcos regulatorios, el desarrollo de capacidades institucionales y la implementación de estrategias integrales para la gestión del riesgo cibernético. En Asia, Singapur también se posiciona entre los diez países con mejor desempeño, gracias a la adopción de políticas y medidas orientadas a fortalecer la seguridad digital, incrementar la resiliencia frente a las ciberamenazas y combatir el fraude financiero[7]. En Latinoamérica, Brasil se ha consolidado

[3] INTERPOL. *Global Financial Fraud Threat Assessment-March 2026.* https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
[4] M-Trends 2026: *Data, Insights, and Strategies From the Frontlines*. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026
[5] https://www.bbva.es/finanzas-vistazo/ciberseguridad/protege-tu-empresa/ciberseguridad-factor-humano-companias.html
[6] https://www.microsoft.com/en-us/security/blog/2026/04/02/threat-actor-abuse-of-ai-accelerates-from-tool-to-cyberattack-surface/
[7] https://sumsub.com/global-fraud-index/

como referente en innovación de pagos con PIX. Sin embargo, el aumento del fraude por este canal impulsó nuevas medidas para fortalecer la seguridad del sistema financiero.

Luxemburgo

Se ha consolidado como uno de los países referentes en materia de prevención del fraude y resiliencia cibernética. Si bien registra bajos niveles en los indicadores de fraude, su estrategia se ha centrado en el fortalecimiento de la regulación, la resiliencia operativa y la gestión integral del riesgo cibernético. Este desempeño responde, en gran medida, a la articulación entre el sector público, las entidades financieras y el sector privado, lo que ha permitido desarrollar un ecosistema de cooperación orientado a la prevención y respuesta frente a las amenazas cibernéticas.

Entre las principales medidas implementadas se destaca la creación de la *Luxembourg House of Cybersecurity* (LHC), principal organismo de coordinación del ecosistema nacional de ciberseguridad. Su misión es fortalecer la resiliencia cibernética del país mediante la coordinación entre entidades públicas, privadas y académicas. También integra el *Computer Incident Response Center Luxembourg* (CIRCL), encargado de la respuesta a incidentes y del intercambio de información sobre amenazas cibernéticas, y el *National Cybersecurity Competence Center* (NC3), orientado al fortalecimiento de las capacidades nacionales en ciberseguridad[8], además de la implementación de marcos como el *Digital Operational Resilience Act* (DORA) con el fin de fortalecer la resiliencia operativa del sector financiero mediante el establecimiento de estándares para la gestión del riesgo asociado a las tecnologías de la información, pruebas de resiliencia cibernética y la supervisión de proveedores críticos de servicios tecnológicos[9].

Singapur

Constituye uno de los casos más representativos de adaptación regulatoria frente al incremento de las estafas digitales, que pasaron de 26.886 casos en 2021 a 55.810 en 2024, donde las estafas más frecuentes estaban relacionadas con fraudes laborales y de inversión y fraudes de comercio electrónico en compras de artículos[10]; para 2025 se reportaron 41.974 casos[11]. Las modalidades con el mayor número de casos de fraude son el *E-commerce, phishing* y la suplantación de funcionarios públicos. Tras registrar un aumento significativo de campañas de *phishing* dirigidas al sector financiero, las autoridades y las entidades bancarias han implementado en los últimos años un conjunto de medidas orientadas a reducir el impacto de estas modalidades de fraude.

Entre las iniciativas más relevantes se encuentra COSMIC (*Collaborative Sharing of Money Laundering and Terrorism Financing Information and Cases*), una plataforma implementada por la Autoridad Monetaria de Singapur (MAS) en conjunto con los principales bancos comerciales del país, que permite el intercambio seguro de información sobre clientes que presentan múltiples indicadores de riesgo asociados a delitos financieros, fortaleciendo la detección temprana de actividades ilícitas[12]. Asimismo, el país estableció el *Sender ID Registry Regime* (SIRR), un sistema de registro obligatorio de identificadores para el envío masivo de mensajes SMS, que facilita la verificación del remitente y reduce la suplantación de identidad en las comunicaciones electrónicas[13]. A estas medidas se suma la *Protection from Scams Act* 2025, que faculta a la Policía de Singapur para ordenar a las entidades financieras el bloqueo temporal de las cuentas de personas que, presuntamente, estén siendo víctimas de estafas, con el fin de impedir la transferencia de recursos a los delincuentes y minimizar las pérdidas económicas[14]. Adicionalmente, se dio la incorporación del *Kill Switch* en la mayoría de los bancos, donde se le permite al cliente bloquear sus cuentas inmediatamente si sus datos han sido comprometidos[15].

Brasil

En el contexto latinoamericano, Brasil ha sido un referente en la innovación de sistemas de pagos y transformación digital del sistema financiero. No obstante, la adopción de estas innovaciones, como el sistema de pagos inmediatos PIX, generó nuevos desafíos en materia de fraude bancario, lo cual ha impulsado la adopción de medidas regulatorias y tecnológicas para fortalecer la seguridad del ecosistema.

Entre las principales iniciativas se destacan la Resolución Adjunta del Banco Central sobre el intercambio obligatorio de datos de fraude, que exige a las instituciones financieras compartir de manera segura información sobre intentos y casos confirmados de fraude para fortalecer la detección temprana y la respuesta coordinada del sector[16]; el Reglamento General de los Servicios de Telecomunicaciones (RGST), que incorporó medidas para prevenir fraudes en las comunicaciones electrónicas, entre ellas la autenticación de llamadas y mayores responsabilidades para los operadores de telecomunicaciones[17], además de medidas orientadas a impedir la falsificación del número de origen de las llamadas telefónicas *caller ID spoofing*, una de las principales modalidades utilizadas para la suplantación de identidad[18]. Asimismo, el Banco Central fortaleció el sistema PIX mediante la

[8] https://www.lhc.lu/
[9] https://www.ey.com/en_lu/insights/digital/digital-operational-resilience-act-dora
[10] https://www.bbc.com/news/articles/c2k1148dwdwo
[11] Annual Scam and Cybercrime Brief 2025, Singapore Police Force (2026)
[12] https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic
[13] https://www.sgnic.sg/smsregistry/overview
[14] https://sso.agc.gov.sg/Act/PSA2025
[15] https://www.bbc.com/news/articles/c2k1148dwdwo
[16] https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=6
[17] https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2022-resolucao-777
[18] https://www.gov.br/anatel/pt-br/regulado/acompanhamento-e-controle/combate-ao-spoofing

implementación del Mecanismo Especial de Devolución (MED), que permite a las instituciones financieras bloquear temporalmente recursos y gestionar la devolución de fondos cuando existan indicios de fraude, contribuyendo a reducir las pérdidas económicas de las víctimas[19].

Virtudes y falencias en la prevención del fraude en Colombia

En las últimas dos décadas Colombia ha avanzado en la tipificación de conductas delictivas que trascienden el ámbito físico, en el fortalecimiento del marco normativo focalizado en proteger al consumidor y en la adopción de estrategias y tecnologías que han ampliado la capacidad de prevención y respuesta, especialmente en el sector financiero.

Sin embargo, el país enfrenta desafíos asociados a la coordinación interinstitucional, la necesidad de actualizar normas que no responden plenamente a las dinámicas actuales y la falta de mecanismos efectivos para garantizar la trazabilidad sobre la titularidad y el uso de las tarjetas SIM, que permiten el desarrollo de modalidades fraudulentas como el *phishing*.

Avances en normatividad

Durante las últimas dos décadas, el marco legislativo colombiano se ha articulado en torno a tres ejes, la respuesta al fraude mediante el robo de datos, la protección de la información y la atención a los ciudadanos afectados:

- **Ley 1273 de 2009[20]:** incorporó al código penal los delitos contra la información y los datos y definió la forma de tipificar las conductas delictivas en esta modalidad. Esta ley constituye el principal instrumento penal para investigar y sancionar modalidades de fraude digital como el *phishing*, el robo de credenciales y las operaciones financieras no autorizadas.

- **Leyes 1581 de 2012[21] y 1266 de 2008[22]:** la primera la ley de protección de datos personales y la segunda la ley de Habeas Data. Establecen los lineamientos en la recolección, tratamiento, circulación y protección referente a los datos personales, financieros, comercial y de servicios. Ambas leyes exigen la adopción de medidas que eviten el acceso, la adulteración o el uso no autorizado de la información y permiten al ciudadano conocer, actualizar y rectificar los datos asociados a su identidad, especialmente cuando una suplantación genera productos fraudulentos, obligaciones o reportes negativos.

- **Leyes 1328 de 2009 y 2573 de 2026:** la primera establece los deberes de debida diligencia, seguridad, calidad y atención de reclamaciones que deben cumplir las entidades vigiladas, además de su obligación de colaborar con las autoridades frente a operaciones irregulares, mientras que la Ley 2573 de 2026 incorpora medidas para proteger a las víctimas de suplantación frente al cobro de obligaciones y los reportes negativos derivados de productos o servicios que no solicitaron.

Adicionalmente, desde la Superintendencia Financiera de Colombia se han sancionado normativas que han orientado la evolución del sector en materia de ciberseguridad y prevención del fraude, entre estas se encuentran:

- **Circular Externa 007 de 2018[23]:** fortaleció la gestión de la seguridad de la información y la ciberseguridad, definiendo responsabilidades para la prevención, detección, atención y recuperación frente a incidentes cibernéticos.

- **Circular Externa 029 de 2019[24]:** promovió la implementación de mecanismos fuertes de autenticación, como la biometría, los códigos de un solo uso y la autenticación multifactor, de acuerdo con el riesgo asociado a cada operación.

- **Circular Externa 033 de 2020[25]:** estableció criterios comunes para la clasificación y el reporte de incidentes cibernéticos, así como lineamientos para el intercambio controlado de información entre las entidades y la Superintendencia Financiera.

Estos avances, aunque han sido relevantes, requieren de una actualización periódica en el marco tipológico que permita clasificar de manera acorde a los avances tecnológicos las diferentes modalidades de fraude que se van presentando y definir rutas coordinadas de prevención, detección, investigación y atención.

Además, la regulación continúa distribuida entre distintas autoridades y sectores, sin establecer plenamente los mecanismos, responsabilidades (que generalmente recaen en los

[19] https://docs.ebanx.com/docs/pay-in/management/post-payment/med-pix-overview
[20] Ley 1273 de 2009. (2009). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492
[21] Ley 1581 de 2012. (2012). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[22] Ley 1266 de 2008. (2008). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488
[23] Superintendencia Financiera de Colombia. (2018). Circular Externa 007 de 2018. https://www.superfinanciera.gov.co/publicaciones ¿/10096745/normativanormativa-generalcirculares-externas-cartas-circulares-y-resoluciones-desde-el-ano-circulares-externasciculares-externas-10096745/
[24] Superintendencia Financiera de Colombia. (2019). Circular Externa 029 de 2019.https://www.superfinanciera.gov.co/publicaciones/10099659/normativanormativa-generalcirculares-externas-cartas-circularesy-resoluciones-desde-el-ano-circulares-externascirculares-externas-10099659/
[25] Superintendencia Financiera de Colombia. (2020). Circular Externa 033 de 2020.https://www.superfinanciera.gov.co/publicaciones/10099659/normativanormativa-generalcirculares-externas-cartas-circularesy-resoluciones-desde-el-ano-circulares-externascirculares-externas-10099659/

establecimientos comerciales y financieros) y canales de intercambio de información necesarios para una actuación interinstitucional oportuna frente a un fenómeno que involucra entidades financieras, operadores de telecomunicaciones, plataformas digitales y autoridades.

Avances desde el sector financiero

El sector financiero colombiano ha desarrollado una estrategia integral para mitigar el fraude, basada en el fortalecimiento de la seguridad digital en tres ámbitos:

- Inversión en tecnologías de vanguardia para proteger la seguridad digital y fortalecer el monitoreo transaccional.
- Focalización en el usuario bancario, mediante campañas de sensibilización sobre las modalidades de fraude que lo afectan directamente.
- Articulación entre los diferentes sectores y autoridades involucrados en la prevención, mitigación e investigación del fraude.

En primer lugar, las inversiones realizadas por el sector en tecnología y en la optimización de sus procesos de monitoreo han representado el 40% del total de la inversión destinada a seguridad digital durante los últimos años.

En particular, se han desarrollado y fortalecido herramientas orientadas a detectar anomalías transaccionales y verificar la identidad de los usuarios. Por ejemplo, el 78% de las entidades ha incorporado tecnologías de vanguardia, como *big data*, inteligencia artificial y motores de aprendizaje automático.

En segundo lugar, el sector ha complementado estas acciones con campañas de sensibilización dirigidas a fortalecer la capacidad de los usuarios para identificar y prevenir las distintas modalidades de fraude. Estas iniciativas se desarrollan tanto de manera individual por las entidades bancarias, en conjunto con aliados estratégicos o desde la propia Asobancaria, a través de redes sociales, capacitaciones y mensajes preventivos presentados al momento de realizar transacciones bancarias.

Por último, el sector ha coordinado acciones con diferentes actores involucrados en la prevención y mitigación del fraude, tanto con autoridades (como la Policía Nacional y la Fiscalía General de la Nación) como con agentes externos, entre ellos redes, aliados estratégicos y entidades financieras distintas de los establecimientos bancarios. Sin embargo, estas iniciativas suelen desarrollarse de manera particular o mediante esquemas de colaboración que aún no cuentan con un marco de trabajo claramente estandarizado e institucionalizado.

Falencias

Aunque las entidades financieras han fortalecido sus mecanismos de autenticación, monitoreo y prevención del fraude, el crecimiento de este delito exige complementar estos esfuerzos con controles adicionales que están por fuera del marco de acción del sector financiero, entre ellos la identificación y trazabilidad de las tarjetas SIM.

La necesidad de fortalecer la regulación sobre la adquisición, el registro y el uso de las tarjetas SIM responde a la ausencia de un marco que permita prevenir su utilización con fines delictivos y garantizar la trazabilidad de actividades sospechosas. Entre las principales dificultades se encuentran la activación de líneas con información falsa o de terceros y la identificación de sus usuarios finales.

Estas brechas facilitan el uso de mensajes de texto, llamadas y otros canales de comunicación para cometer fraudes, suplantar identidades y contactar a posibles víctimas, lo que dificulta la detección y posterior investigación de los responsables. En este contexto, el 74%[26] de las reclamaciones por fraude corresponde a modalidades asociadas con el robo de datos, como *phishing*, *smishing y vishing*, entre otras.

Frente a esta problemática, se han promovido las siguientes iniciativas legislativas:

- **Proyecto de Ley 381 de 2024 Cámara[27]:** buscaba establecer controles sobre la adquisición y venta de tarjetas SIM y tecnologías similares mediante mecanismos de identificación biométrica. Su propósito es fortalecer la trazabilidad de las líneas y prevenir estafas, suplantaciones y otros delitos cometidos a través de llamadas o mensajes de texto. Actualmente archivada.
- **Proyecto de Ley 038 de 2025 Cámara de Representantes:** proponía la identificación obligatoria de los usuarios y el fortalecimiento de los controles aplicables a la venta y utilización de líneas móviles. Aunque buscaba mejorar la autenticación y trazabilidad de las tarjetas SIM, la iniciativa fue archivada en aplicación del artículo 190 de la Ley 5 de 1992.
- **Proyecto de Ley 074 de 2025 Senado:** plantea la creación de un registro de identificación de los usuarios finales de tarjetas SIM, eSIM y tecnologías equivalentes. La iniciativa contempla el tratamiento de datos personales y la validación biométrica de los titulares para mejorar la trazabilidad de las líneas y facilitar la investigación de delitos. Se encuentra en trámite para segundo debate.

[26] Informe de Fraude Bancario (2026). Asobancaria.
[27] Por medio de la cual se establecen medidas sobre la adquisición y venta de tarjetas SIM y otras tecnologías similares en Colombia. [Regula el comercio de tarjetas SIM]| Proyectos de Ley | Congreso Visible. (s. f.). Congreso Visible. https://congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-de-la-cual-se-establecen-medidas-sobre-la-adquisicion-y-venta-de-tarjetas-sim-y-otras-tecnologias-similares-en-colombia-regula-el-comercio-de-tarjetas-sim/14234/

- **Resolución 8308 de 2026 de la CRC:** establece un conjunto integral de medidas técnicas, operativas y pedagógicas con el fin de prevenir y mitigar el fraude cibernético en los servicios móviles tradicionales de voz y mensajes de texto (SMS) en Colombia, un primer paso para la regulación de comunicaciones en el marco de la mitigación del fraude a través de estos canales.

Es necesario que el país avance en (i) la adopción de este tipo de iniciativas para cerrar las brechas de identificación y trazabilidad que hoy permiten la comisión de fraudes, (ii) fortalecer la investigación y judicialización de estos delitos, y (iii) complementar de manera efectiva los controles que las entidades financieras han venido desarrollando. Este avance requiere la participación coordinada de todos los actores del ecosistema (Gobierno, Congreso, operadores de telecomunicaciones y sector financiero, entre otros).

Conclusiones y consideraciones finales

La evolución del ecosistema financiero ha generado múltiples beneficios para los usuarios, pero también ha ampliado la superficie de exposición frente a nuevas modalidades de fraude, especialmente aquellas basadas en técnicas de ingeniería social como el *phishing, smishing, vishing y spoofing*. La experiencia internacional evidencia que la mitigación de estas amenazas requiere de un enfoque integral que combine medidas regulatorias, tecnológicas y de cooperación interinstitucional.

Si bien el sector financiero ha fortalecido sus mecanismos de autenticación, el monitoreo permanente de las transacciones y la implementación de estrategias de comunicación que permitan sensibilizar a los usuarios, la naturaleza cambiante del fraude exige una respuesta cada vez más integral y coordinada.

En este contexto, es indispensable avanzar hacia un marco normativo que establezca responsabilidades claras para todos los actores involucrados en el ecosistema digital. Asimismo, es necesario promover mecanismos que faciliten el intercambio oportuno y seguro de la información en casos de fraude bancario, además de agilizar el bloqueo de páginas web, líneas telefónicas y mensajes utilizados con fines fraudulentos, y fortalecer la coordinación entre autoridades y el sector privado.

Solo mediante una respuesta coordinada y multisectorial será posible anticiparse a las modalidades de fraude que se adaptan ante los cambios del sector y fortalecer la confianza de los usuarios en los servicios financieros digitales.

Principales indicadores macroeconómicos

	2024					2025								2026*	2027*
	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	T3	Total	Total
Producto Interno Bruto															
PIB Nominal (COP Billones)	403	411	437	463	**1.713**	444	442	478	490	**1.853**	475	487		**2.027**	**2.174**
PIB Nominal (USD Billions)	103	104	107	107	**420**	106	105	119	128	**457**	128	135		**551**	**649**
PIB Real (COP Billones)	236	244	250	266	**995**	242	248	259	271	**1.021**	248	257		**1.047**	**1.071**
PIB Real (% Var. interanual)	0,2	1,5	1,6	2,6	**1,5**	2,6	1,9	3,8	2,1	**2,6**	2,2	3,5		**2,5**	**2,3**
Precios															
Inflación (IPC, % Var. interanual)	7,4	7,2	5,8	5,2	**5,2**	5,1	4,8	5,2	5,1	**5,1**	5,6	6,1	6,3	**6,7**	**4,8**
Inflación sin alimentos (% Var. interanual)	8,8	7,6	6,5	5,6	**5,6**	5,2	4,8	4,9	5,1	**5,1**	5,4	6,0	6,2	**6,4**	**4,9**
Tipo de cambio (COP/USD fin de periodo)	3.899	4.043	4.183	4.385	**4.385**	4.138	4.113	3.922	3.791	**3.791**	3.718	3.501	3.341	**3.188**	**3.450**
Tipo de cambio (Var. % interanual)	-18,2	-4,0	4,4	11,1	**11,1**	6,1	1,7	-6,2	-13,5	**-13,5**	-10,2	-14,9	-14,8	**-15,9**	**8,2**
Sector Externo															
Cuenta corriente (USD millones)	-1.584	-1.418	-1.634	-2.416	**-7.052**	-1.649	-2.478	-3.013	-3.917	**-11.056**	-1.278	-4.702		**-15.433**	**-16.029**
Déficit en cuenta corriente (% del PIB)	1,5	1,4	1,5	2,3	**1,7**	1,5	2,4	2,5	3,1	**3,1**	1,0	3,5		**3,0**	**2,8**
Balanza comercial (% del PIB)	-1,7	-2,3	-2,2	-3,1	**-3,1**	-2,4	-3,6	-3,4	-3,5	**-2,4**	-2,0	-4,1		**-2,6**	**-2,5**
Exportaciones F.O.B. (% del PIB)	15,7	16,5	16,7	16,8	**16,8**	16,0	16,5	15,7	14,5	**15,7**	15,1	14,2		**13,9**	**13,5**
Importaciones F.O.B. (% del PIB)	17,4	18,8	18,9	19,9	**19,9**	18,4	20,1	19,1	18,0	**16,9**	17,1	18,4		**16,9**	**16,3**
Renta de los factores (% del PIB)	-3,1	-2,8	-3,1	-3,1	**-3,1**	-2,8	-2,7	-2,6	-2,9	**-2,7**	-2,3	-2,4		**-2,6**	**-2,7**
Transferencias corrientes (% del PIB)	3,2	3,7	3,8	3,9	**3,9**	3,6	4,0	3,5	3,3	**3,6**	3,3	3,1		**3,0**	**2,9**
Inversión extranjera directa (pasivo) (% del PIB)	3,5	2,6	3,1	3,8	**3,8**	2,7	3,2	2,5	1,8	**1,8**	3,1	3,1			
Sector Público (% del PIB)															
Bal. primario del Gobierno Central	0,0	-0,8	0,0	-1,5	**-2,4**	-0,8	-0,5	-0,4	-1,8	**-3,5**	-0,5	-0,7		**-3,3**	
Bal. del Gobierno Nacional Central	-1,0	-2,3	-0,9	-2,6	**-6,7**	-2,0	-1,7	-0,3	-2,3	**-6,4**	-1,8	-1,5		**-7,2**	
Bal. primario del SPNF	-0,4	-0,7	-1,1	-1,2	**-1,2**	-1,4	-0,4	-0,7	-3,4	**-3,4**					
Bal. del SPNF	-0,1	-1,3	-1,8	-5,9	**-5,9**	-0,3	-2,4	-2,8	-6,7	**-6,7**					
Deuda (% del PIB)															
Deuda externa bruta	56,5	53,6	53,0	52,7	**52,7**	52,9	53,8	53,5	53,8	**53,8**	54,4	50,2		...	
Pública	36,6	34,5	32,8	31,7	**31,7**	31,8	32,4	32,0	33,1	**33,1**	33,9	30,6		...	
Privada	22,1	21,1	20,7	21,1	**21,1**	21,1	21,4	21,3	20,5	**20,5**	20,5	19,6		...	
Deuda neta del Gobierno Central	50,5	54,4	55,6	59,0	**59,0**	55,5	56,8	56,3	58,5	**58,5**	55,5	56,0		...	

*Proyecciones de Asobancaria.
Fuentes: DANE, Banco de la República, Ministerio de Hacienda y Crédito Público.
Nota: Las cifras del balance del SPNF se presentan como valores acumulados en lo corrido del año.

Estados financieros del sistema bancario de Colombia

	dic-22	dic-23	dic-24	dic-25	ago-26 (a)	jul-26	ago-25 (b)	Var. real anual (a) - (b)
Activo	**924.121**	**959.797**	**998.266**	**1.065.112**	**1,126,196**	**1,136,695**	**1,029,711**	**2.9%**
Disponible	58.321	64.582	59.096	58.557	56,996	59,595	47,999	11.8%
Inversiones	180.818	189.027	215.062	222.619	252,047	263,789	220,300	7.7%
Cartera de crédito	642.473	655.074	677.712	729.161	764,389	760,879	704,742	2.1%
Consumo	200.582	196.005	189.083	202.184	212,379	210,318	193,778	3.1%
Comercial	330.686	338.202	357.805	379.824	395,314	394,461	370,757	0.3%
Vivienda	95.158	102.972	111.301	124.711	131,731	131,425	119,039	4.1%
Microcrédito	16.047	17.896	19.524	22.443	24,965	24,675	21,168	11.0%
Provisiones	37.224	39.752	40.396	39.208	40,599	40,179	39,020	-2.1%
Consumo	15.970	18.644	17.922	16.078	16,459	16,239	16,176	-4.2%
Comercial	16.699	16.335	17.446	17.809	18,397	18,229	17,549	-1.3%
Vivienda	3.189	3.413	3.641	3.996	4,300	4,285	3,990	1.4%
Microcrédito	858	1.181	1.332	1.310	1,443	1,425	1,292	5.1%
Pasivo	**818.745**	**856.579**	**885.571**	**963.512**	**1,023,986**	**1,034,297**	**931,967**	**3.4%**
Depósitos y otros instrumentos	686.622	731.321	777.404	850.640	890,744	893,545	826,939	1.4%
Cuentas de ahorro	297.926	286.217	313.749	351.454	369,462	372,289	327,119	6.3%
CDT	207.859	272.465	287.571	311.028	342,749	338,824	318,358	1.3%
Cuentas corrientes	80.608	75.483	77.164	79.580	79,857	76,488	76,496	-1.8%
Otros depósitos	100.229	97.156	98.919	108.578	98,677	105,944	104,967	-11.5%
Patrimonio	**105.376**	**103.218**	**112.695**	**101.600**	**102,211**	**102,398**	**97,744**	**-1.6%**
Utilidades (año corrido)	**14.222**	**8.133**	**8.326**	**14.206**	**11,401**	**10,117**	**8,267**	**29.8%**
Ingresos financieros de cartera	63.977	91.480	85.888	81.580	62,168	53,795	53,814	8.7%
Gastos por intereses	28.076	60.093	53.748	47.226	36,254	31,257	31,588	8.0%
Margen neto de intereses	38.069	35.918	36.372	38.680	29,151	25,450	25,334	8.3%
Indicadores (%)								
Calidad	**3,61**	**4,90**	**4,62**	**3,75**	**3.74**	**3.71**	**4.11**	**-0.37**
Consumo	5,44	8,10	6,80	4,84	4.81	4.74	5.38	-0.57
Comercial	2,73	3,42	3,59	3,22	3.20	3.19	3.54	-0.33
Vivienda	2,47	3,03	3,51	3,08	3.06	3.03	3.24	-0.19
Microcrédito	5,46	8,50	8,57	6,71	6.85	6.90	7.42	-0.57
Cubrimiento	**160,6**	**123,8**	**129,1**	**143,3**	**141.9**	**142.4**	**134.7**	**-7.16**
Consumo	146,4	117,4	139,4	164,4	161.0	163.0	155.2	5.82
Comercial	184,7	141,2	135,8	145,6	145.4	145.0	133.9	11.49
Vivienda	135,5	109,3	93,2	104,0	106.7	107.7	103.3	3.40
Microcrédito	97,9	77,7	79,6	86,9	84.4	83.7	82.3	2.12
ROA	1,5	0,8	0,8	1,3	1.5	1.5	1.2	0.32
ROE	13,5	7,9	7,4	14,0	17.2	17.5	13.0	4.24
Solvencia	17,1	16,5	16,9	15,9		15.2	15.9	
IRL	183,7	194,0	183,8	178,4	178.8	175.0	183.1	-4.31
CFEN G1	109,6	115,5	115,5	116,8	116.5	116.6	118.3	-1.72
CFEN G2	126,2	124,1	139,2	132,7	125.3	125.2	126.3	-1.03

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

	2021	2022					2023					2024					2025		2026
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	Total
Profundización financiera - Cartera/PIB (%) EC	**50,9**	**48,3**	47,1	46,8	46,7	46,2	**46,2**	45,9	45,4	45,3	44,0	**44,0**	43,4	43,4	43,1	43,6	**43,6**	44,0	**42,9**
Efectivo/M2 (%)	**17,0**	**16,3**	14,7	14,3	13,9	15,0	**15,0**	14,2	14,1	14,5	15,5	**15,5**	15,3	15,3	15,5	16,8	**16,8**	15,6	
Cobertura																			
Municipios con al menos una oficina o un corresponsal bancario (%)	**100,0**	**100,0**	100,0	100,0	100,0	100,0	**100,0**	100,0	100,0	100,0	100,0	**100,0**	100,0	100,0	100,0	100,0	**100,0**	100,0	
Municipios con al menos una oficina (%)	**75,9**	**78,7**	76,5	76,5	76,5	76,5	**76,5**	76,4	76,4	76,4	76,4	**76,4**	76,2	76,2	76,2	76,4	**76,4**	76,3	
Municipios con al menos un corresponsal bancario (%)	**100,0**	**100,0**	100,0	100,0	100,0	100,0	**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**	**92,3**	92,9	93,2	93,7	94,6	**94,6**	95,0	95,4	96,0	96,3	**96,3**	96,9	97,2	97,4	97,0	**97,0**		
Indicador de acceso a depósitos (%)	**89,1**	**91,2**	92,0	92,4	92,9	94,0	**94,0**	94,4	94,8	95,4	95,8	**95,8**	96,4	97,1	97,0	96,5	**96,5**		
Indicador de acceso a crédito (%)	**34,5**	**36,2**	35,2	35,3	35,2	35,3	**35,3**	35,0	35,5	35,2	35,5	**35,5**	35,3	35,6	36,1	36,6	**36,6**		
Adultos con: (en millones)																			
Al menos un producto	**33,5**	**34,7**	35,1	35,3	35,6	36,1	**36,1**	36,4	36,7	37,0	37,7	**37,7**	37,7	38,0	38,1	37,5	**37,5**		
Depósitos	**26,4**	**28,0**	28,4	28,7	29,2	30,5	**30,5**	30,9	31,2	31,5	37,1	**37,1**	37,5	37,9	37,9	33,1	**33,1**		
Cuentas de ahorro	**28,9**	**29,9**	29,3	29,5	30,6	30,8	**30,8**	31,2	31,3	31,5	31,9	**31,9**	32,3			32,4	**32,4**		
Cuenta corriente	**1,9**	**1,8**				1,7	**1,7**				1,7	**1,7**				1,5	**1,5**		
Depósitos de bajo monto	**21,1**	**23,5**	24,2	24,7	25,3	27,5	**27,5**	28,1	28,5	29,0	29,5	**29,5**	29,9			29,7	**29,7**		
CDT		**0,9**	0,9	1,0	1,0	1,1	**1,1**	1,2	1,2	1,2	1,2	**1,2**	1,4			1,3	**1,3**		
Al menos un crédito	**12,6**	**13,5**	13,4	14,4	13,5	13,5	**13,5**	13,4	13,7	13,6	13,7	**13,7**	13,8	13,9	14,1	15,2	**15,2**		
Crédito de consumo	**6,9**	**7,8**	7,4	7,4	7,3	7,3	**7,3**	7,4	7,4	7,4	8,5	**8,5**	7,4			7,4	**7,4**		
Tarjeta de crédito	**7,9**	**8,5**	8,5	8,5	8,5	8,4	**8,4**	8,4	8,8	8,7	9,0	**9,0**	9,1			9,4	**9,4**		
Microcrédito	**2,3**	**2,3**				2,4	**2,4**	2,3	2,4	2,3	2,2	**2,2**	2,2			2,2	**2,2**		
Crédito de vivienda	**1,2**	**1,3**				1,2	**1,2**	1,2	1,2	1,2	1,2	**1,2**	1,2			1,2	**1,2**		
Crédito comercial	**0,2**	**0,5**																	
Uso*																			
Productos personas																			
Adultos con: (%)																			
Algún producto activo	**74,8**	**77,2**	77,8	78,2	79,1	82,7	**82,7**	82,5	83,0	83,5	83,9	**83,9**	84,8	85,7	86,4	86,8	**86,8**		
Cuentas de ahorro activas	**65,7**	**51,9**				54,5	**54,5**	54,1	53,3	53,6	66,4	**66,4**	55,4			55,4	**55,4**		
Cuentas corrientes activas	**3,9**	**3,7**				3,5	**3,5**				3,5	**3,5**				3,4	**3,4**		
Cuentas CAES activas	**41,6**	**48,3**				60,0	**60,0**				65,7	**65,7**				69,5	**69,5**		
Cuentas CATS activas	**76,3**	**78,6**				80,1	**80,1**	80,7	81,2	81,7	81,7	**81,7**							
Depósitos electrónicos																			
Productos de ahorro a término (CDT)		**73,2**																	

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

Principales indicadores de inclusión financiera

	2022	2023					2024					2025					2026	
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	**Total**
Acceso*																			
Productos empresas																			
Empresas con: (en miles)																			
Al menos un producto	**1.077,1**	…	…	…	…	**1.169,6**	…	…	…	…	**1.232,5**	…	…	…	…	**1.263,8**	…	…	…
*Productos de depósito	**1.046,4**	…	…	…	…	**1.166,4**	…	…	…	…	**1.230,8**	…	…	…	…	**1.242,4**	…	…	…
*Productos de crédito	**380,2**	…	…	…	…	**417,6**	…	…	…	…	**453,9**	…	…	…	…	**468,1**	…	…	…
Uso*																			
Productos empresas																			
Empresas con: (%)																			
Algún producto activo	**72,4**											**76,3**							
Operaciones																			
Número (millones)	**8.020**	3.567	3.933	3.691	4.117	**15.308**	3.986	4.499	5.613	6.016	**20.114**	5.300	5.190	5.667	6.234	**22.391**	6.078	6.586	
No monetarias (Participación)	**55,8**	49,7	49,2	39,7	38,4	**44,1**	37,4	36,9	51,9	53,2	**46,8**	48,7	40,6	40,5	43,0	**43,1**	41,3	39,9	
Monetarias (Participación)	**44,2**	50,3	50,8	60,3	61,0	**55,9**	62,6	63,1	45,3	46,7	**53,1**	51,3	59,4	59,5	57,1	**56,9**	58,7	60,1	
No presenciales (Participación)	**77,0**	79,0	80,0	77,6	79,1	**78,6**	79,0	80,6	84,1	83,8	**84,0**	82,4	81,4	83,0	84,0	**82,8**	84,6	13,7	
Presenciales (Participación)	**23,0**	21,0	20,0	22,4	20,9	**21,4**	21,0	19,4	15,9	16,2	**16,0**	17,6	18,6	17,0	16,0	**17,2**	15,4	86,3	
Monto (COP billones)	**11.093**	2.569	2.410	2.383	2.599	**9.960**	2.540	2.727	2.722	2.996	**10.985**	2.859	2.913	3.072	3.184	**12.029**	3.153	3.233	
Tarjetas																			
Créditos vigentes (millones)	**16,0**	15,8	15,5	15,4	15,0	**15,0**	14,4	14,0	13,8	13,9	**13,9**	13,4	15,1	15,1	15,3	**15,3**	15,6	16,1	
Débitos vigentes (millones)	**45,8**	46,2	46,4	47,1	47,2	**47,2**	46,0	44,9	45,4	45,3	**45,3**	47,6	48,9	50,0	52,1	**52,1**	53,9	55,3	
Ticket promedio compra crédito ($miles)	**215,5**	210,9	209,3	203,2	207,6	**207,6**	198,3	196,1	196,3	201,2	**201,2**	192,2	191,7	188,8	194,5	**194,5**	187,7	185,6	
Ticket promedio compra débito ($miles)	**112,8**	103,0	99,0	98,3	103,7	**103,7**	94,9	92,8	93,4	100,2	**100,2**	93,0	91,4	90,2	96,5	**96,5**	89,9	87,7	

* Vigiladas por la SFC, la SES y ONG microfinancieras.
Fuentes: Banca de las Oportunidades, Superintendencia Financiera de Colombia.