

La protección de datos personales en la era de la proliferación tecnológica y de herramientas de inteligencia artificial

- El funcionamiento de la IA se basa en el procesamiento de gran cantidad de datos, dentro de los que se pueden encontrar datos personales, los cuales, por cuenta de su especial protección constitucional, deben ser tratados de manera ética, responsable y transparente para proteger los derechos de los titulares.
- La IA plantea nuevos retos en el uso y la protección de los datos personales; sin embargo, también ofrece oportunidades de cambio e innovación, en una sociedad en constante evolución.
- Así como los responsables y encargados del tratamiento de datos personales asumen obligaciones específicas, los titulares deben adoptar un rol más activo frente a las implicaciones del uso de nuevas tecnologías, empoderándose de la protección de sus datos.

24 de febrero de 2025

Director:

Jonathan Malagón González

ASOBANCARIA:

Jonathan Malagón González
Presidente

José Manuel Gómez Sarmiento
Vicepresidente Jurídico

Germán Montoya Moreno
Director Económico

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

La protección de datos personales en la era de la proliferación tecnológica y de herramientas de inteligencia artificial

El pasado 28 de enero se celebró el Día Internacional de la Protección de Datos Personales, por virtud del cual se conmemora anualmente la firma del Convenio 108 del Consejo de Europa en 1981, el primer tratado internacional que abordó la protección de datos. Con el fin de seguir aportando a esta celebración, esta edición de Banca & Economía reflexiona sobre el impacto que ha tenido la Inteligencia Artificial (IA) sobre los datos personales y la importancia de la conciencia para su adecuada protección.

Para el efecto, se hace un breve recorrido por la coyuntura actual, mencionando los riesgos que trae la evolución de la tecnología frente a los datos personales, la normatividad existente en relación con la Protección de Datos Personales y algunos comentarios sobre cómo puede ser aprovechada para que los actores relacionados con el tratamiento de dichos datos ejerzan adecuadamente sus derechos y obligaciones bajo el uso de esos nuevos sistemas.

Tratamiento y procesamiento de datos

Las tecnologías emergentes, como es el caso de la IA, no han surgido recientemente; por el contrario, han sido implementadas y desarrolladas durante las últimas décadas. Se han venido convirtiendo progresivamente en herramientas clave en el ámbito personal, profesional y académico, impulsando la productividad y la eficiencia¹.

En esta Edición, se acepta que la IA es una “disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico”². Así las cosas, se tiene que la IA necesita recoger una gran cantidad de datos, almacenarlos y procesarlos para, a partir de ellos, ejecutar la tarea que se le pida o para la cual haya sido programada³.

Dentro de los datos que la IA puede utilizar se encuentran los datos personales, los cuales, según la normatividad vigente en Colombia y en cumplimiento del artículo 15 de la Constitución Política⁴, reciben una especial protección por encontrarse asociados a una persona determinada o determinable⁵. En el marco de su tratamiento⁶, se distinguen tres roles fundamentales: (i) el

¹ Martínez Devia, Andrea. La Inteligencia Artificial, el big data y la era digital: ¿una amenaza para los datos personales? Pág. 2. Recuperado de: [Vista de La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales?](#)

² Real Academia Española. Definición Inteligencia Artificial. Recuperado de: [inteligencia | Definición | Diccionario de la lengua española | RAE - ASALE](#)

³ BBC News Mundo. Una guía sencilla para entender la IA. Recuperado de: [¿Qué es la IA? Una guía sencilla para entender la inteligencia artificial - BBC News Mundo](#)

⁴ Artículo 15 de la Constitución Política de Colombia. Recuperado de: [Constitución Política de 1991 - Gestor Normativo - Función Pública](#)

⁵ Literal c) del artículo 3 de la Ley Estatutaria 1851 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”. Recuperado de: [Ley 1581 de 2012 - Gestor Normativo - Función Pública](#)

⁶ Según el literal g) Ibidem, tratamiento es “cualquier operación o conjunto de operaciones sobre datos personales. tales como la recolección, almacenamiento, uso, circulación o supresión”.

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

José Manuel Gómez Sarmiento
Ida María Mestre Ordóñez
Gabriela Grijalba Cerro
Camilo Rodríguez Ojeda

¡Un año recargado de temáticas clave para impulsar nuestra economía!

Calendario Eventos Programación 2025

 27° Congreso de Tesorería Febrero 13 y 14 Cartagena

 15° CAMP Marzo 6 y 7 Cartagena

 13ª Jornada de Libre Competencia Abril 10 Bogotá D.C.

 16° Foro de Vivienda Mayo 6 Bogotá D.C.

 59ª Convención Bancaria Junio 4, 5 y 6 Cartagena

 24° Congreso Panamericano de Riesgo LAFTPADM Julio 17 y 18 Cartagena

 7° FEST Septiembre 4 Bogotá D.C.
Congreso de Finanzas para la Equidad Sostenibilidad y Transformación

 23° Congreso Derecho Financiero Septiembre 18 y 19 Cartagena

 18° SAFE Octubre 23 y 24 Cartagena
Congreso de Seguridad, Amenazas, Cibermedidas, Fraude y Experiencia

 23° Congreso de Riesgos Noviembre 20 y 21 Cartagena

 13° Encuentro Tributario Noviembre 27 Bogotá D.C.

Patrocinios:

Sonia Elias
+57 320 859 72 85
sellias@asobancaria.com

Inscripciones:

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

Aso Ban Caria

Una Experiencia:

encargado⁷, que corresponde a quien realiza el tratamiento de los datos por cuenta del responsable, (ii) el responsable⁸, que es quien toma las decisiones sobre la base de datos y el tratamiento que se les dará, y (iii) el titular⁹, a quien se refieren los datos.

De conformidad con esta normatividad, el tratamiento solamente puede darse derivado del consentimiento o autorización¹⁰ del titular, para una finalidad legítima que se le informe¹¹. Ahora bien, estas operaciones solo pueden realizarse por personas autorizadas por el titular y los datos no pueden estar disponibles en internet ni en otros medios de comunicación masiva, salvo que el acceso sea controlado¹².

En nuestro país no existe legislación aplicable a la IA y es por esto que la aplicación del régimen de protección de datos personales, que establece una serie de cargas, derechos y obligaciones frente a cada uno de los roles mencionados, no encuentra una guía diferente a las directrices emitidas por la Superintendencia de Industria y Comercio al respecto¹³. Así las cosas, corresponde a todos los actores, desde el rol que desempeñan, ser más conscientes de las implicaciones que puede traer el uso de estas tecnologías desde la privacidad, el consentimiento y la transparencia¹⁴.

En efecto, como se detallará más adelante, cualquier falla que ocurra no debe atribuirse exclusivamente a quienes realizan el tratamiento de los datos. Paradójicamente, cada vez es más común que prevalezca la desinformación en la sociedad de la información, lo que lleva a que muchas personas no sean conscientes de la importancia de proteger sus datos personales, ni de las implicaciones que puede tener compartirlos sin restricciones ni filtros.

Las preocupaciones frente a la protección de los datos crecen frente a la posición vulnerable en la que se encuentran con respecto a las innovaciones tecnológicas. Al respecto, Dell Technologies adelantó un estudio, para el cual entrevistó a 1.500 trabajadores en los departamentos de tecnología de organizaciones tanto públicas como industrias privadas, con más de 250 empleados en América, Europa y Asia en 2023, y encontró que las industrias están preocupadas sobre la protección de datos y las dificultades que traerán las IA, particularmente las generativas¹⁵. El Gráfico 1 detalla los resultados de opinión frente a los retos de la IA y la protección de datos.

En definitiva, tomando en consideración la vulnerabilidad de los datos, particularmente los personales, frente al uso de herramientas

tecnológicas, como lo es la IA, es necesario tener presente tanto las fuentes de riesgo, como que existen mecanismos y oportunidades de mejora que pueden apalancar la ruta para su protección. Todo lo anterior, con el fin de establecer y reconocer la importancia de la responsabilidad de los diferentes actores, independientemente del rol que desempeñen, para no perder la perspectiva en la fijación de un objetivo a futuro con el desarrollo de estas tecnologías frente a la protección de datos personales.

Gráfico 1. Opinión de organizaciones encuestadas sobre retos futuros de la IA y la protección de datos



Fuente: Global Data Protection Index – Special Edition 2024. Dell Technologies.

Responsabilidad frente a la IA

El uso de IA conlleva ventajas significativas en términos de eficiencia y optimización para los usuarios, pero también plantea riesgos en materia de seguridad y privacidad y, por ello, las empresas proveedoras de los productos y servicios soportados en IA deben asumir una serie de responsabilidades derivadas de la normatividad de protección de datos, además de las exigencias propias en materia de ciberseguridad.

Justamente, dado que los sistemas de IA pueden ser objeto de ataques cibernéticos o sesgos algorítmicos, las empresas proveedoras de los productos y servicios soportados en esta tecnología deben adoptar protocolos de seguridad robustos. También, la IA debe ser programada a partir de estos protocolos y mantenerse en constante actualización, para gestionar adecuadamente este tipo de riesgos¹⁶.

⁷ Literal d) Ibidem.

⁸ Literal e) Ibidem.

⁹ Literal f) Ibidem.

¹⁰ Principio de libertad, previsto en el literal c) del artículo 4 de la mencionada Ley Estatutaria.

¹¹ Principio de finalidad, previsto en el literal b) Ibidem.

¹² Principio de circulación restringida, previsto en el literal f) Ibidem.

¹³ Circular Externa 002 de 21 de agosto de 2024. Recuperado de: [Circular Externa No. 002 del 21 de agosto de 2024.pdf](#)

¹⁴ Martínez Devia, Andrea. Op. Cit. Pág. 3.

¹⁵ Dell Technologies. Global Data Protection index – Special Edition 2024. Pág 20. Recuperado de: [Dell Technologies PowerPoint Template](#)

¹⁶ Fariás Estacio, A. G., & Centeno Córdova, D. J. (2024). *Modelos de Inteligencia Artificial para prevención de ataques cibernéticos en organizaciones* (Bachelor's thesis). <http://dspace.ups.edu.ec/handle/123456789/27884>

En vista de lo anterior, es necesario realizar auditorías periódicas y establecer mecanismos de supervisión para minimizar los riesgos de filtraciones de datos o decisiones erróneas, siendo la supervisión humana fundamental en casos críticos donde las decisiones automatizadas pueden afectar derechos fundamentales¹⁷.

La intervención de especialistas en bases de datos y seguridad informática permite que se corrijan errores y se propenda porque la IA opere de manera ética y responsable¹⁸.

Adicionalmente, las empresas proveedoras de los productos y servicios soportados en IA deben asumir la responsabilidad en caso de uso indebido de datos¹⁹. Si un sistema de IA maneja información personal de manera incorrecta, ya sea por negligencia, falta de supervisión o uso no autorizado, la empresa será legalmente responsable²⁰ y deberá responder ante las autoridades y los usuarios afectados.

En este sentido, la implementación de controles internos y auditorías constantes es esencial para prevenir incidentes y garantizar el respeto de los derechos de los titulares de los datos. Sin embargo, la responsabilidad en la protección de los datos personales no recae únicamente en las empresas proveedoras de los productos y servicios soportados en IA, como responsables o encargados. En efecto, esta responsabilidad es compartida con los titulares, quienes también deben adoptar una actitud proactiva y asumir una responsabilidad adicional en la gestión de su información.

Como primera medida, es fundamental que los usuarios (titulares de los datos) conozcan a quién le entregan sus datos y con qué finalidad serán tratados y, antes de proporcionar información personal, investiguen la reputación y las políticas de privacidad de las empresas o plataformas que solicitan sus datos.

Además, deben asegurarse de comprender los términos de uso antes de aceptar que su información sea procesada por un sistema de IA. En este sentido, es importante que ejerzan sus derechos sobre sus datos, solicitando acceso a la información, rectificación o eliminación, cuando sea necesario. Asimismo, los usuarios deben ser precavidos en el uso de plataformas digitales, adoptando medidas de seguridad como la creación de contraseñas robustas²¹, y apalancándose en las herramientas que ofrecen los prestadores, como la autenticación en dos pasos.

Por su parte, también resulta fundamental que exista conciencia sobre la necesidad de limitar el acceso a su información personal

en entornos digitales. La interacción con sistemas de IA debe ser crítica, especialmente cuando las decisiones automatizadas afectan aspectos como el historial crediticio, el acceso a servicios o cualquier otra toma de decisiones relevante.

En resumen, el uso de IA en la administración de datos personales introduce una serie de responsabilidades adicionales, tanto para las empresas proveedoras de los productos y servicios soportados en IA como para sus usuarios, particularmente según el rol que tengan en materia de protección de datos personales. En efecto, se debe avanzar en el cumplimiento de normativas de protección de datos, tanto de la actualmente vigente como la que eventualmente se implante como actualización en aras de adaptarse a las nuevas eras digitales; también en implementar medidas de seguridad y supervisión, y asegurar la transparencia en el tratamiento de la información. De otra parte, los usuarios deben ser conscientes de los riesgos asociados a la cesión de sus datos, informarse adecuadamente sobre sus derechos y adoptar medidas básicas de protección ante el uso de IA.

Caso típico: aceptación de términos y condiciones

Como es de conocimiento común, cualquier aplicación y/o plataforma exige a los usuarios potenciales aceptar sus términos y condiciones, que recogen las políticas de privacidad y tratamiento de datos personales, lo cual implica que el usuario (titular de los datos) tiene al alcance de su mano la posibilidad de entender las consecuencias y responsabilidades que conlleva su autorización. Sin embargo, en la mayoría de las ocasiones se aceptan las condiciones sin realizar la verificación adecuada, materializándose el riesgo de exposición de datos, sin la conciencia de su titular.

No se trata de un problema exclusivamente de nuestro país; un estudio realizado por el Servicio Nacional del Consumidor de Chile (SERNAC) evidenció que el 72% de las personas declara estar muy o extremadamente preocupadas de que sus datos sean recopilados en internet; sin embargo, solo el 4,1% de ellas señalan siempre leer las políticas de privacidad²², como lo muestra el Gráfico 2.

Lo anterior, puede ocurrir por múltiples factores, tales como:

- **Extensión y complejidad vs. celeridad y experiencia:** en el caso colombiano, el artículo 12 de la Ley 1581 de 2012 establece que el responsable debe informar al titular, de manera clara y expresa, el tratamiento que le dará a sus datos personales y su finalidad, además de los derechos que le asisten, entre otros

¹⁷ Presidencia de la República de Colombia. (2021). Marco ético para la inteligencia artificial en Colombia (Versión 1). <https://minciencias.gov.co/sites/default/files/marco-etico-ia-colombia-2021.pdf>

¹⁸ Ibidem.

¹⁹ Ibidem.

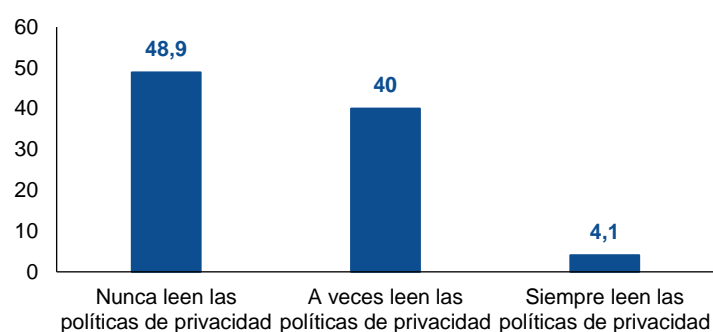
²⁰ Artículo 23 de la Ley 1581 de 2012.

²¹ Superintendencia de Sociedades. (2022). GINT-G-001 Guía para contraseñas seguras (Versión 004). https://www.supersociedades.gov.co/documents/107391/3472445/GINT-G-001_ContrasenaSegura.pdf

²² Servicio Nacional del Consumidor. (2022, 28 de enero). Casi la mitad de los consumidores admite nunca leer la política de privacidad de los sitios que visita. SERNAC. <https://www.sernac.cl/portal/604/w3-article-64751.html>

asuntos. Sin embargo, en un mundo acelerado, donde la eficiencia del tiempo y la premura por dinamizar lo que se está realizando, eliminando fricciones y privilegiando la experiencia del cliente, la exigencia de detalles que dan lugar a documentos largos, con términos legales, técnicos y complejos, genera que sean ignorados por el usuario promedio.

Gráfico 2. Percepción y hábitos sobre la privacidad en internet (% de encuestados)



Fuente: Servicio Nacional del Consumidor – 2022, 28 de enero SERNAC CHILE. Elaboración Asobancaria.

• **Necesidades de acceso:** Cuando se realiza uso de aplicaciones tecnológicas, ya sean de uso libre o de uso pago, se requiere el registro de información personal, así como la aceptación de todas las condiciones para el funcionamiento de la aplicación. Esto conlleva a que, en muchas ocasiones, no sea viable que el usuario acepte parcialmente, autorizando exclusivamente lo que como titular está dispuesto a asumir, generándose que no pueda avanzar e impidiendo el acceso a la aplicación hasta que la autorización integral sea concedida.

• **Estado de la cultura de evaluación de riesgos:** De acuerdo con el profesor Daniel J. Solove de la Facultad de Derecho de la Universidad George Washington, "es perfectamente racional que las personas, incluso sin ninguna influencia indebida en el comportamiento, no hagan buenas evaluaciones de los riesgos de privacidad y no gestionen su privacidad de manera efectiva, toda vez que es un proyecto vasto, complejo e interminable que no se escala; se vuelve virtualmente imposible hacerlo de manera integral"²³.

Oportunidades para la protección de datos

Partiendo de los factores evidenciados en el aparte anterior, los desarrolladores de tecnología, particularmente de aplicaciones o plataformas de IA, deben apalancarse en el desarrollo del régimen de protección de datos personales, generando espacios para que los usuarios tengan posibilidad de ejercer responsablemente sus derechos. Entonces, estrategias de implementación de *legal design*

para la formulación de los términos y condiciones, que faciliten la comprensión y hagan más amable la vinculación, son ganadoras a la hora de romper la dualidad mencionada en el punto de extensión y complejidad vs. celeridad y experiencia.

De otra parte, el estado de la tecnología evidencia que existen herramientas que permiten generar soluciones a la medida de los usuarios. En vista de lo anterior, es viable pensar que los desarrolladores están en capacidad de generar mecanismos de autorización por bloques que permitan el acceso a algunas de las herramientas ofrecidas por la aplicación o plataforma, en atención al nivel de autorizaciones del usuario, para afrontar lo incluido en el punto de necesidades de acceso. No es ambicioso pensar que, en la medida que es posible programar una herramienta de IA que genere conclusiones a partir de información recopilada, es posible que la herramienta tenga diferentes niveles de actuación a partir de las autorizaciones y la información aportada por el usuario.

Pero el avance en los desarrollos de aplicaciones y plataformas tecnológicas, inclusive las soportadas en IA, resulta insuficiente si no se incrementa el nivel de empoderamiento y concientización de los titulares de la información para superar la crítica situación esbozada en el punto relacionado con el estado de la cultura de evaluación de riesgos. Como se ha mencionado a lo largo del presente documento, no es viable que se avance en la adecuada gestión de los riesgos que implica el tratamiento de información si todas las responsabilidades se asignan exclusivamente a los proveedores de bienes y servicios (responsables y encargados), en tanto las vulnerabilidades surgen por cuenta de todos los actores, desde sus diferentes roles. Así las cosas, corresponde que todos aporten, desde sus posibilidades, en la construcción de entornos más seguros.

Lo anterior no implica que se pueda garantizar la inviolabilidad de las herramientas tecnológicas, y en consecuencia de los datos almacenados. Los delincuentes, en todo caso, mantendrán su interés por tener acceso a los datos que se encuentren en una superficie tecnológica, pues justamente reconocen el valor que tienen estos, particularmente los personales.

La cultura de empoderamiento, el objetivo frente al desarrollo e implementación de tecnologías y la protección de datos personales

Es innegable que la creciente integración de la IA en los distintos ámbitos de la sociedad plantea importantes retos en materia de protección de datos personales. En este contexto, es imperativo reconocer que la cultura debe evolucionar al mismo ritmo que la tecnología, garantizando un equilibrio entre el interés frente al acceso a la innovación y la salvaguarda de los derechos fundamentales de los Titulares de la información,

²³ 89 revista de derecho de George Washington 1 (2021).

independientemente que se actualice la legislación en la que se fundamenta su protección.

Las empresas proveedoras de los productos y servicios soportados en IA, en su rol de responsables o Encargados del tratamiento de datos, tienen la obligación de adoptar esquemas que aseguren las medidas de protección y uso ético de la información personal. Esto implica no solo el cumplimiento estricto de la normativa vigente, sino también la implementación de protocolos que mitiguen asociados al uso de sistemas de IA, evitando sesgos, accesos no autorizados y tratamientos indebidos, particularmente de datos sensibles²⁴.

Por su parte, los usuarios, o titulares de los datos, deben asumir una actitud más proactiva frente a la gestión de su información personal, ser conscientes de los datos que suministran, a quién y para qué, los alcances que tienen las autorizaciones que otorgan, entre otros múltiples derechos que se les reconocen en la normatividad. Solamente cuando los titulares sean plenamente conscientes de los riesgos que asumen cuando entregan sus datos es que realmente puede entenderse que los mecanismos de protección que ofrecen responsables y encargados que adelantan su labor bajo la normatividad vigente son suficientes a la luz de los titulares. En esta línea han surgido diversas iniciativas que, desde la academia, por ejemplo, promueven escenarios de capacitación que buscan generar en los titulares, nativos digitales o no, la cultura necesaria para protegerse debidamente, al amparo de las normas mencionadas.

Sin perjuicio de lo anterior, es recomendable que el marco normativo colombiano se actualice de forma integral, tanto modernizando las reglas de protección de datos personales (en línea con los estándares europeos²⁵), como estableciendo estándares claros que regulen el uso de IA en el tratamiento de datos personales, más allá de las mencionadas instrucciones de la Superintendencia de Industria y Comercio. La regulación debe ser precisa en la determinación de responsabilidades, deberes, derechos y obligaciones, tanto para quienes gestionan la información, como para los titulares, estableciendo mecanismos de control efectivos y sanciones proporcionales en caso de incumplimiento, para quien no cumpla con estos marcos.

Conclusiones y consideraciones finales

La IA representa tanto oportunidades como desafíos en materia de protección de datos. El futuro de su implementación dependerá de la capacidad de las empresas proveedoras, sus usuarios y las autoridades para fomentar un ecosistema digital basado en la ética, la responsabilidad y el respeto por la privacidad. La regulación no debe concebirse como un obstáculo a la innovación, sino como un

marco que permita su desarrollo dentro de límites que protejan los derechos de los ciudadanos en la era digital.

Por ello, en este contexto de constante avance tecnológico, la protección de datos personales no puede ser vista como un esfuerzo aislado, sino como un compromiso conjunto entre reguladores, empresas y ciudadanos. La construcción de una cultura digital responsable, en la que la seguridad de la información sea un pilar fundamental, es esencial para evitar vulneraciones y fortalecer la confianza en el uso de la Inteligencia Artificial. La implementación de marcos normativos actualizados y la adopción de buenas prácticas en ciberseguridad deben ir de la mano con la educación de los usuarios, permitiéndoles comprender y ejercer sus derechos de manera efectiva. Solo a través de este enfoque integral será posible garantizar que la IA evolucione sin comprometer la privacidad y la autonomía de los individuos.

²⁴ Según el artículo 5 de la Ley 1581 de 2012, corresponde a “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos”, los cuales cuentan con un régimen de protección adicional (artículo 6 de la misma Ley).

²⁵ El Reglamento General de Protección de Datos (UE) 2016/679, conocido como GDPR, contiene los estándares de tratamiento de sus datos personales y a la libre circulación de estos datos en la Unión Europea. Consultable en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679>

Principales indicadores macroeconómicos

Colombia

	2021	2022	2023					2024				
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total
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
PIB Nominal (USD Billones)	318,5	344,6	81,0	85,8	98,4	99,5	382,3	102,0	105,0	106,4	105,2	418,8
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
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
Precios												
Inflación (IPC, % Var. interanual)	5,6	13,1	13,3	12,1	11,0	9,3	9,3	7,4	7,2	5,8	5,2	5,2
Inflación sin alimentos (% Var. interanual)	3,4	10,0	11,4	11,6	10,9	10,3	10,3	8,8	7,6	6,5	5,6	5,6
Tipo de cambio (COP/USD fin de periodo)	3981	4810	4627	4191	4054	3822	3822	3842	4148	4164	4409	4409
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
Sector Externo												
Cuenta corriente (USD millones)	-17951	-21333	-2996	-2266	-1758	-2133	-9715	-1924	-1630	-1669	...	-7100
Déficit en cuenta corriente (% del PIB)	-5,7	-6,2	-3,7	-2,6	-1,8	-2,1	-2,7	-1,9	-1,6	-1,6	...	-1,8
Balanza comercial (% del PIB)	-6,4	-4,8	-2,7	-2,5	-1,5	-2,2	-2,3	-1,9	-2,2	-2,4	...	-1,8
Exportaciones F.O.B. (% del PIB)	13,6	21,3	21,1	19,2	17,6	17,3	18,6	15,8	16,6	16,5	...	13,3
Importaciones F.O.B. (% del PIB)	18	26,1	23,8	21,7	19,0	19,5	20,9	17,7	18,7	18,9	...	15
Renta de los factores (% del PIB)	-2,8	-4,9	-4,8	-3,7	-3,8	-3,3	-4,0	-3,3	-3,1	-3,1	...	-2,6
Transferencias corrientes (% del PIB)	3,4	3,6	3,8	3,5	3,4	3,4	3,6	3,3	3,7	3,9	...	3,0
Inversión extranjera directa (pasivo) (% del PIB)	3	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	0,3	1,2	0,2	...	-0,3	-2,4
Bal. del Gobierno Nacional Central	-7	-5,3	-0,9	0,0	-0,7	-2,7	-4,3	-1,2	-2,1	-6,8
Bal. primario del SPNF	-3,5	-1,4	1,5	-0,2
Bal. del SPNF	-7,1	-6	-2,7	-4,9
Indicadores de Deuda (% del PIB)												
Deuda externa bruta	53,9	53,4	55,2	56,1	53,6
Pública	32,2	30,4	31,4	31,8	30,9
Privada	21,7	23	23,8	24,2	22,8
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

*Proyecciones de Asobancaria. Los datos fiscales corresponden a lo proyectado por el Gobierno Nacional en el MFMP 2024

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

Estados financieros del sistema bancario Colombia

	dic-20	dic-21	dic-22	dic-23	dic-24 (a)	nov-24	dic-23 (b)	Var. real anual (b) - (a)
Activo	729.841	817.571	924.121	959.797	998.266	998.737	959.797	-1,1%
Disponible	53.794	63.663	58.321	64.582	59.096	53.709	64.582	-13,0%
Inversiones	158.735	171.490	180.818	189.027	215.062	215.702	189.027	8,2%
Cartera de crédito	498.838	550.204	642.473	655.074	677.712	675.263	655.074	-1,7%
Consumo	150.527	169.603	200.582	196.005	189.083	189.944	196.005	-8,3%
Comercial	263.018	283.804	330.686	338.202	357.805	355.962	338.202	0,6%
Vivienda	72.565	82.915	95.158	102.972	111.301	109.935	102.972	2,7%
Microcrédito	12.727	13.883	16.047	17.896	19.524	19.421	17.896	3,7%
Provisiones	37.960	35.616	37.224	39.752	40.396	40.491	39.752	-3,4%
Consumo	13.729	12.251	15.970	18.644	17.902	18.223	18.644	-8,7%
Comercial	17.605	17.453	16.699	16.335	17.326	17.279	16.335	0,8%
Vivienda	2.691	3.021	3.189	3.413	3.641	3.577	3.413	1,4%
Microcrédito	1.133	913	858	1.181	1.332	1.344	1.181	7,2%
Pasivo	640.363	713.074	818.745	856.579	885.568	886.845	856.579	-1,7%
Depósitos y otros instrumentos	556.917	627.000	686.622	731.321	777.404	776.573	731.321	1,0%
Cuentas de ahorro	246.969	297.412	297.926	286.217	313.749	310.839	286.217	4,2%
CDT	154.188	139.626	207.859	272.465	287.571	290.762	272.465	0,3%
Cuentas Corrientes	75.002	84.846	80.608	75.483	77.164	73.265	75.483	-2,8%
Otros pasivos	9.089	9.898	11.133	10.841	11.087	11.830	10.841	-2,8%
Patrimonio	89.479	104.497	105.376	103.218	112.697	111.891	103.218	3,8%
Utilidades (año corrido)	4.159	13.923	14.222	8.133	8.326	7.513	8.133	-2,7%
Ingresos financieros de cartera	45.481	42.422	63.977	91.480	85.888	79.098	91.480	-10,8%
Gastos por intereses	14.571	9.594	28.076	60.093	53.748	49.755	60.093	-15,0%
Margen neto de intereses	31.675	33.279	38.069	35.918	36.372	33.334	35.918	-3,7%
Indicadores (%)								
Calidad	4,96	3,89	3,61	4,90	4,62	4,92	4,90	-0,28
Consumo	6,29	4,37	5,44	8,10	6,80	7,19	8,10	-1,30
Comercial	4,55	3,71	2,73	3,42	3,59	3,92	3,42	0,17
Vivienda	3,30	3,11	2,47	3,03	3,51	3,55	3,03	0,48
Microcrédito	7,13	6,47	5,46	8,50	8,57	8,79	8,50	0,07
Cubrimiento	153,5	166,2	160,6	123,8	129,1	121,9	123,8	-5,29
Consumo	145,1	165,4	146,4	117,4	139,3	133,4	117,4	21,89
Comercial	147,1	165,6	184,7	141,2	134,8	123,9	141,2	-6,33
Vivienda	112,3	117,1	135,5	109,3	93,2	91,6	109,3	-16,04
Microcrédito	124,8	101,7	97,9	77,7	79,6	78,7	77,7	1,98
ROA	0,6	1,7	1,5	0,8	0,8	0,8	0,8	-0,01
ROE	4,6	13,3	13,5	7,9	7,4	7,3	7,9	-0,49
Solvencia	16,3	20,5	17,1	16,5	16,9	17,1	16,5	0,36
IRL	213,1	204,4	183,7	194,0	183,3	179,6	194,0	-10,72
CFEN G1	0,0	113,5	109,6	115,5	114,9	114,6	115,5	-0,64
CFEN G2	0,0	134,4	127,3	134,4	132,1	127,6	134,4	-2,31

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
Profundización financiera - Cartera/PIB (%) EC + IOE	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
Efectivo/M2 (%)	17	16,2	15,9	15,6	16,3	16,3	14,7	14,3	13,9	15	15	14,2	14,1	14,5
Cobertura														
Municipios con al menos una oficina o un corresponsal bancario (%)	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	-	-	-	78,7	78,7			
Municipios con al menos un corresponsal bancario (%)	92,7	98,6	98,7	99,6	100	100	-	-	-	100	100			
Acceso														
Productos personas														
Indicador de bancarización (%) SF*	90,5	91,2	91,8	92,1	92,3	92,3	-	-	-	94,6	94,6			
Adultos con: (en millones)														
Al menos un producto SF	33,5	33,8	34,2	34,4	34,7	34,7	-	-	-	36,1	36,1			
Cuentas de ahorro	28,9	29,2	29,5	29,6	29,9	29,9	-	-	-	30,8	30,8			
Cuenta corriente SF	1,9	1,9	1,9	1,8	1,8	1,8	-	-	-	-	-			
Cuentas CAES SF							-	-	-					
Cuentas CATS SF	21	21,7		23	23,5	23,5	-	-	-	27,5	27,5			
Depósitos electrónicos							-	-	-					
CDT		0,8	0,8	0,9	0,9	0,9	-	-	-	-	-			
Al menos un producto de crédito(en millones)	12,6	12,8	13,2	13,5	13,6	13,6	-	-	-	-	13,5			
Crédito de consumo SF	6,9	7,1	7,4	7,7	7,8	7,8	-	-	-	7,3	7,3			
Tarjeta de crédito SF	7,9	8	8,2	8,4	8,5	8,5	-	-	-	6,6	6,6			
Microcrédito SF	2,3	2,3	2,34	2,36	2,3	2,3	-	-	-	2,4	2,4			
Crédito de vivienda SF	1,2	1,23	1,25	1,27	1,3	1,3	-	-	-	1,2	1,2			
Crédito comercial SF	0,2	0,46	0,45	0,44	0,5	0,5	-	-	-	-	-			
Uso														
Productos personas														
Adultos con: (%)														
Algún producto activo SF	74,8	76,2	76,9	77,7	77,2	77,2	-	-	-	82,7	82,7			
Cuentas de ahorro activas SF	65,7	65,9	65,2	64,9	51,9	51,9	-	-	-	54,5	54,5			
Cuentas corrientes activas SF	73,7	76,9	76,5	76,3	74,5	74,5	-	-	-					
Cuentas CAES activas SF														
Cuentas CATS activas SF	76,3	77,8		80,2	78,6	78,6	-	-	-	-	80,1			
Depósitos electrónicos														
Productos de ahorro a término (CDTs)		77,5	79,3	80,1	73,2	73,2	-	-	-	-	-			

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

Principales indicadores de inclusión financiera

Colombia

	2021			2022			2023				Total
	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	
Acceso											
Productos empresas											
Empresas con: (en miles)											
Al menos un producto SF	1028,6	1029,0	1038,7	1065,7	1077,1	1077,1	-	-	-	1169,6	1169,6
*Productos de depósito SF	998,9	1004,0	1013,0	1039,8	1046,4	1046,4	-	-	-	1166,4	1166,4
*Productos de crédito SF	280,2	289,6	294,2	300,6	380,2	380,2	-	-	-	417,6	417,6
Uso											
Productos empresas											
Empresas con: (%)											
Algún producto activo SF	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
No monetarias (Participación)	56,1	-	55,4	-	56,0	55,8	-	49,2	-	39,0	44,1
Monetarias (Participación)	43,8	-	44,6	-	44,0	44,2	-	50,8	-	61,0	55,9
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
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
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
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

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