Banca & Economía

2023

Edición 1396

02 de octubre de 2023

Computación Cuántica: Desafíos y Oportunidades Para la Banca

- Con el avance del Siglo XXI, la humanidad se enfrenta a nuevos desarrollos tecnológicos con un potencial disruptivo en todas las esferas de la vida social y económica, entre los que se encuentra la computación cuántica.
- La criptografía, que se dedica al estudio de los métodos de protección de la información con base en el uso de códigos, es uno de los campos que podrían verse fundamentalmente transformado por el uso de la computación cuántica.
- La posibilidad de superposición de estados propios al interior de un computador cuántico permite una velocidad de procesamiento exponencialmente mayor a la de un computador clásico.
- A lo largo de la historia, se han utilizado cientos de criptosistemas diferentes que, a grandes rasgos, se pueden dividir en dos grupos: criptosistemas simétricos o de clave privada y criptosistemas asimétricos o de clave pública. Actualmente, el sector bancario hace uso de criptosistemas asimétricos para la encriptación de su información. Estos sistemas pueden quedar expuestos a brechas de seguridad gracias al avance de la computación cuántica.
- Entre los estudios de una nueva generación de criptografía postcuántica para afrontar el impacto de la computación cuántica resalta la criptografía basada en retículos como un enfoque prometedor.
- La computación cuántica no significará el fin del uso de la criptografía; si bien representa una innovación disruptiva, enmarca el inicio de una nueva era en este campo.

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

Banca & Economía

2023

Edición 1396

Computación Cuántica: Desafíos y Oportunidades Para la Banca

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Jaime Andrés Rincón Arteaga
Nicolas Sierra Rojas
Angie Daniela Rivero Barbosa

A medida que se adentra en el Siglo XXI, la humanidad se enfrenta a nuevos desarrollos tecnológicos con un potencial disruptivo en todas las esferas de la vida social y económica. Estos desarrollos desafían nuestras formas tradicionales de comprender y transformar el mundo que nos rodea. Uno de estos avances es la computación cuántica, un paradigma de computación que difiere del enfoque clásico y que, hasta hace poco, era solo una posibilidad teórica. La importancia crucial de este paradigma radica en su capacidad para transformar diversos aspectos de la vida en sociedad mediante avances en la computación.

La criptografía, que se dedica al estudio de los métodos de protección de la información con base en el uso de códigos, es uno de estos campos que podrían verse fundamentalmente transformados por el uso de la computación cuántica. Esto se debe a que los mecanismos en el centro de los principales métodos de encriptación son esencialmente problemas algebraicos cuya resolución requiere una capacidad computacional que excede la de los computadores clásicos. Los computadores cuánticos, en contraste, tienen una capacidad computacional exponencialmente mayor a la de los tradicionales, que les permitiría resolver dichos problemas.

Así pues, en el sector financiero, todos los datos de clientes, como cuentas y transferencias de dinero podrían quedar indefensos. Es entonces fundamental que los equipos de seguridad digital pertenecientes a empresas que manejan información sensible de sus usuarios, como las del sector financiero y bancario, conozcan los riesgos y oportunidades de la futura proliferación de los computadores cuánticos. Esto permitiría, no sólo hacerles frente a los riesgos de seguridad que implican estas nuevas tecnologías, sino también identificar cómo pueden ser usadas para encontrar mecanismos de protección de la información más robustos y confiables.

Esta edición de Banca & Economía aborda la computación cuántica y su diferencia con la computación clásica, explicando su surgimiento y propiedades teóricas y prácticas. Describe la lógica de los sistemas criptográficos más usados y cómo un computador cuántico podría afectar su seguridad. Además, presenta los avances en criptografía robusta frente a los computadores cuánticos. Finalmente, ofrece algunas conclusiones y consideraciones finales sobre este tema relevante en el ámbito financiero.

Banca & Economía
2023
Edición 1396

¿Qué es la computación cuántica?

Entendemos por computación cuántica un paradigma computacional radicalmente distinto al que encontramos en la inmensa mayoría de equipos electrónicos hoy en día. Este campo de la informática nace de los trabajos seminales de Paul Benioff, Yuri Manin y Richard Feynman[1]. Benioff sentó las bases teóricas para la computación cuántica en 1979 al demostrar que el proceso computacional puede describirse mediante una serie de estados que evolucionan en el tiempo que dure dicho proceso. Esto acercaría la computación a la mecánica cuántica, algo que también fue explorado independientemente por Manin en 1980. Feynman, por su lado, describió las características que debería tener un computador cuántico para ser útil en 1981. Todos los avances teóricos y aplicados de la computación cuántica retoman las bases sentadas por estos autores, quienes concibieron un paradigma diferente desde el cual entender los procesos computacionales.

El paradigma clásico de la computación tiene como mínima unidad de información el bit; un dígito del sistema numérico binario, es decir, cero o uno. Las combinaciones de bits pueden usarse para el tratamiento de la información, principal función de los sistemas informáticos de acuerdo con la computación clásica. Una propiedad fundamental de este mecanismo es que un bit sólo puede tomar un valor en un momento dado, de manera que un conjunto de bits sólo puede representar una pieza de información a la vez. Esto incluye todos los procesos internos de un dispositivo electrónico como lo conocemos hoy en día.

En contraste, la computación cuántica tiene un paradigma disruptivo, en tanto que su unidad básica de información ya no es el bit, sino el *cúbit* o bit cuántico. El *cúbit* es una unidad de información contenida en un sistema cuántico, el cual permite la superposición de dos estados distintos posibles. En otras palabras, en un *cúbit* podemos encontrar un cero, un uno, o incluso ambos al tiempo en un momento dado. Su implementación en la informática permitiría que un computador cuántico realice operaciones y almacene información a niveles que superarían las capacidades de cualquier dispositivo conocido, lo cual recibe el nombre de supremacía cuántica.

La posibilidad de superposición de estados propios al interior de un computador cuántico permite así una velocidad de procesamiento exponencialmente mayor a la de un computador clásico. Un ordenador cuántico de apenas 30 *cúbits*, por ejemplo, puede realizar 10 billones de operaciones en coma flotante por segundo, es decir, unos 5,8 billones más que la videoconsola PlayStation más potente del mercado[2].

¿Cómo afecta la computación cuántica a la seguridad de las operaciones bancarias?

Los computadores cuánticos poseen una alta capacidad de procesamiento, lo que les permite abordar problemas que resultan irresolubles para los computadores clásicos debido a sus restricciones computacionales. Entre estos problemas, encontramos los que se usan como base para la encriptación de información confidencial en la industria bancaria.

A lo largo de la historia, se han utilizado cientos de criptosistemas diferentes que, a grandes rasgos, se pueden dividir en dos grupos: criptosistemas simétricos o de clave privada y criptosistemas asimétricos o de clave pública.

Criptosistemas Simétricos

Los sistemas simétricos, son aquellos en los cuales se necesita una única clave para cifrar y descifrar mensajes entre el emisor y el receptor del mensaje. Dicha clave debe ser acordada con anterioridad a la emisión de este para un correcto funcionamiento del sistema. Estos sistemas basan su seguridad en el tamaño de la clave a aplicar, es decir, a mayor tamaño de la clave usada, mayor seguridad se otorga. Un ejemplo claro es la clave que usamos para acceder a nuestro correo electrónico; toda la seguridad recae en que no compartamos nuestra clave, y en la medida que esta sea más larga y compleja, será menos fácil de adivinar y más segura.

Criptosistemas Asimétricos

Los sistemas asimétricos son aquellos en los cuales se necesitan dos claves para cifrar y descifrar mensajes entre el emisor y el receptor del mensaje. Aquí, tanto el emisor como el receptor poseen un par de claves, de éstas, una será de tipo público donde da lo mismo que todo el mundo la conozca, y la otra será de tipo privado (la cual se tiene que proteger). Así, para enviar mensajes, el emisor tiene que cifrar el mensaje con la clave pública del receptor, para que así el receptor sea el único que pueda descifrar el mensaje usando su clave privada.

Actualmente, el sector bancario hace uso de criptosistemas asimétricos para la encriptación de su información. Esto incluye desde la transmisión y recepción de mensajes privados con sus clientes hasta la generación de firmas digitales. Veremos a continuación cómo dos de los principales métodos asimétricos podrían ser vulnerados mediante el uso de un computador cuántico.

[11] Hidary (2009). Quantum Computing: An Applied Approach.
[2] https://www.iberdrola.com/innovacion/que-es-computacion-cuantica

El Algoritmo RSA

El sistema criptográfico RSA fue propuesto por Rivest, Shamir y Adleman en 1979 en el MIT[3], institución que lo patentaría en 1983. Desde entonces, este es considerado uno de los algoritmos más seguros para la encriptación, incluso hoy en día. Es un método de encriptación de clave pública que permite a los usuarios mantener la confidencialidad de la información al compartirla o transmitirla a otros.

La seguridad del algoritmo RSA radica en la dificultad computacional de encontrar los dos factores primos de un número grande. La operación inversa, que implica multiplicar dos números primos grandes, es relativamente fácil y rápida de realizar. Por el contrario, encontrar los factores primos de un número se vuelve cada vez más difícil a medida que aumenta el tamaño del número, lo que requiere más recursos de hardware y tiempo de cálculo. Por ejemplo, sin utilizar ninguna ayuda electrónica, se tarda poco tiempo en calcular el producto de 11 por 31, pero encontrar los factores primos de 221 llevaría más tiempo[4].

En el algoritmo RSA, los factores primos deben tener al menos 155 dígitos, aproximadamente 512 bits[5], para garantizar la seguridad de los certificados digitales que siguen el estándar X.509[6]. El producto de estos factores tiene alrededor de 310 dígitos, representando 1024 bits, lo cual da una idea del costo computacional de realizar la factorización.

Sin embargo, una reciente investigación dirigida por Yan, *et. Al* (2023)[7] asegura haber creado un modelo matemático que les permitiría romper la criptografía detrás del algoritmo de cifrado RSA de 2048 bits a través de computadoras cuánticas actuales. Esta investigación describe cómo el algoritmo de Shor podría desencriptar las claves privadas generadas por RSA sin mayor dificultad en un computador cuántico con la potencia necesaria.

El mencionado algoritmo de Shor, base del trabajo de los investigadores chinos, fue desarrollado por Peter Shor en 1994. Este incorpora teóricamente la capacidad de los *cúbits* de una computadora cuántica para realizar múltiples cálculos en paralelo, explotando las propiedades de superposición y entrelazamiento cuántico[8] de los sistemas de este tipo. Con esto, podrían descomponerse eficientemente números enteros grandes en sus factores primos, lo que es esencialmente imposible para los algoritmos clásicos tradicionales en un tiempo razonable, como hemos visto en los apartados anteriores.

Es importante destacar que Yan *et. Al* (2023) solo detallaron la metodología a utilizar, ya que no disponían de una computadora cuántica con la potencia necesaria para llevar a cabo la operación; este tipo de tecnología es novedosa y costosa, lo que limitó su aplicabilidad en el estudio. De hecho, estamos apenas en un estadio inicial del ciclo de vida tecnológico de los computadores cuánticos[9]; los ordenadores cuánticos no son aun suficientemente avanzados para ser a prueba de fallos[10]. No obstante, diversos estudios han demostrado teóricamente que el algoritmo RSA puede ser vulnerado rápidamente con el uso de computadores cuánticos.

En este sentido, dado que la seguridad de muchos protocolos criptográficos actuales, incluida la encriptación bajo el algoritmo RSA, se basa en la dificultad de factorizar números enteros grandes, el algoritmo de Shor tiene el potencial de romper estas protecciones y amenazar la seguridad de sistemas criptográficos convencionales cuando se implemente en computadoras cuánticas lo suficientemente grandes y estables.

El Algoritmo ECC

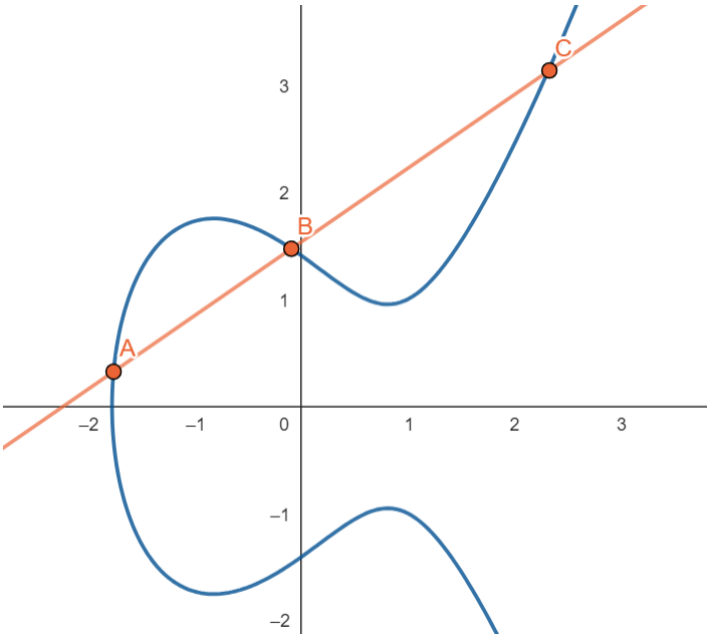
Merece hablar también de otro popular algoritmo de encriptación de clave pública, llamado criptografía de curvas elípticas (ECC por sus siglas en inglés). Propuesto de manera independiente por Victor Miller y Neal Kobitz en 1985[11], el algoritmo ECC sigue un esquema de encriptación análogo al que sigue el algoritmo RSA. Este algoritmo, sin embargo, se basa en las propiedades algebraicas de una curva elíptica en un espacio cerrado, algo que explicaremos a continuación.

Una curva elíptica consiste en una serie de puntos[12]en un plano cartesiano, los cuales siguen una forma análoga a la de la línea verde que encontramos en el gráfico 1[13]. Aquí vemos que, conociendo dos puntos (A y B), es posible averiguar un tercero (C)

[3] Instituto de Tecnología de Massachusetts
[4] https://www.welivesecurity.com/la-es/2013/01/18/funcionamiento-del-algoritmo-rsa/
[5] https://www.welivesecurity.com/la-es/2013/01/18/funcionamiento-del-algoritmo-rsa/
[6] X.509 es un formato estándar para certificados de clave pública, documentos digitales que asocian de forma segura pares de claves criptográficas con identidades como sitios web, individuos u organizaciones. https://www.ssl.com/es/preguntas-frecuentes/%C2%BFQu%C3%A9-es-un-certificado-x-509%3F/
[7] Yan, B., et al. (2022) Factorización de enteros con recursos sublineales en un procesador cuántico superconductor. https://doi.org/10.48550/arXiv.2212.12372
[8] https://academia-lab.com/enciclopedia/algoritmo-de-shor/
[9] Una de las razones es que no hay un consenso sobre cuál debería ser la estructura de hardware que sirva de base a los componentes cuánticos.
[10] Canals (2023). Innovación cuántica: ¿la próxima ola de transformación digital?
[11] Hankerson et. Al. (2004). Guide to Elliptic Curve Cryptography
[12] Recordemos que en un plano cartesiano pueden representarse puntos que tienen una coordenada x y una coordenada y .
[13] Esta curva en particular representa la ecuación $y^2 = x^3 - 2x + 2$.

que se encuentre sobre la curva al trazar una línea recta sobre los primeros dos. Esta es una propiedad de las curvas elípticas de este tipo que resulta favorable para los mecanismos de encriptación basados en su uso.

Gráfico 1. Ejemplo de una curva elíptica con tres puntos seleccionados arbitrariamente.



Fuente: Elaboración Asobancaria.

La clave es que, si bien es sencillo obtener un punto en la curva a partir del conocimiento de la ubicación de otros dos, el proceso inverso es virtualmente imposible; es decir, encontrar, a partir de un punto dado, los puntos que lo generaron. El procedimiento se complica aún más cuando no se consideran todos los puntos de la curva, sino solo unos cuantos, como hace el algoritmo ECC. Esto se conoce como el problema del logaritmo discreto sobre curvas elípticas (ECDLP por sus siglas en inglés). Es posible ver que funciona de manera análoga a como funciona el algoritmo RSA, si bien utilizando bases matemáticas distintas.

Con valores suficientemente grandes de p, las claves generadas son seguras y de una longitud menor a las generadas por el algoritmo RSA. No obstante, debido a la similitud con el problema de la factorización de números grandes en factores primos, el ECDLP es susceptible de ser resuelto por un computador cuántico, también mediante el algoritmo de Shor. Dado que actualmente el algoritmo ECC es utilizado como base para sistemas de criptografía de clave pública, como los utilizados para la seguridad de firmas digitales y criptomonedas, estos son campos que podrían verse profundamente afectados por los avances de la computación cuántica.

El camino por seguir para las entidades financieras: Criptografía Postcuántica

La llegada inminente de la computación cuántica plantea una dualidad: por un lado, impulsará una nueva era de aplicaciones informáticas; por otro lado, representará una amenaza para los métodos de codificación actuales. Actualmente, se adelantan diferentes investigaciones alrededor de una nueva generación de criptografía postcuántica para hacer frente al impacto de la computación cuántica.

El proyecto SAFEcrypto, financiado con fondos europeos, estudia una nueva generación de criptografía postcuántica para afrontar el impacto de la computación cuántica. Este proyecto trabaja en formas de criptografía nuevas basadas en otros tipos de problemas matemáticos que no puedan ser resueltos fácilmente por un ordenador cuántico, comenta la doctora Máire O'Neill (2020), responsable técnica del proyecto. Entre los hallazgos resalta la criptografía basada en retículos como un enfoque prometedor en un mundo postcuántico. Los sistemas criptográficos de este tipo incluyen pruebas de seguridad basadas en problemas complejos de geometría con retículos: rejillas de puntos espaciados de forma uniforme que se extienden hasta el infinito[14].

La criptografía reticular utiliza inmensas cuadrículas que contienen miles de millones de puntos individuales, distribuidos en miles de dimensiones. Descifrar el código en este caso implicaría moverse de un punto específico a otro, lo cual es esencialmente imposible a menos que se conozca la ruta precisa[15].

Conclusiones y Consideraciones Finales

La computación cuántica es una tecnología que ha dejado de ser solo una idea de ciencia ficción para convertirse en una realidad cada vez más cercana. Su potencial disruptivo plantea una amenaza para la seguridad de los bancos y otras instituciones. A medida que avanzamos hacia la era de los computadores cuánticos, se avecinan desafíos significativos para la seguridad cibernética, especialmente en lo que respecta a la criptografía, que ha sido el pilar fundamental para proteger la información confidencial en el ámbito financiero.

Sin embargo, es importante destacar que la criptografía no desaparecerá por completo con la llegada de la computación cuántica. Existen enfoques y técnicas emergentes en el campo de la criptografía postcuántica, que buscan desarrollar algoritmos resistentes a los ataques cuánticos. La comunidad de investigación ha estado trabajando arduamente en el desarrollo de métodos criptográficos robustos que puedan resistir la potencia de cálculo de los computadores cuánticos.

[14] https://cordis.europa.eu/article/id/314300-new-solutions-to-encryption-keeping-data-safe-in-the-face-of-onslaught-of-quantum-computation/es
[15] https://www.technologyreview.es//s/12484/criptografia-reticular-el-cifrado-prueba-de-ordenadores-cuanticos

Es probable que veamos una transición gradual hacia sistemas de criptografía cuántica resistentes y otras soluciones innovadoras para proteger la información financiera y personal en el futuro. Así, las instituciones financieras deberán adaptarse a esta nueva realidad tecnológica. La inversión en la investigación y el desarrollo de técnicas criptográficas postcuánticas será fundamental para mantener la seguridad cibernética en el mundo financiero.

En suma, si bien la computación cuántica representa una amenaza seria para la seguridad de los bancos y otras instituciones, también ofrece la oportunidad de avanzar hacia la creación de sistemas de criptografía más avanzados y seguros. La colaboración entre la industria, el gobierno y la comunidad académica será crucial para enfrentar los desafíos que plantea esta nueva era tecnológica y garantizar la protección de los datos y la privacidad en un mundo cada vez más digital y conectado.

Banca & Economía
2023
Edición 1396

Colombia

Principales indicadores macroeconómicos

	2020	2021	2022					2023		
	Total	**Total**	T1	T2	T3	T4	**Total**	T1	T2	**P**
Producto Interno Bruto										
PIB Nominal (COP Billones)	**997,7**	**1192,6**	333,6	354,4	381,3	394,6	**1463,9**	384,6	377,5	**1595,7**
PIB Nominal (USD Billions)	**270,1**	**320,3**	85,2	90,5	86,9	82,1	**343,9**	80,7	85,3	**374,9**
PIB Real (COP Billones)	**817,3**	**907,3**	229,8	239,7	248,0	257,8	**975,4**	237,3	240,3	**1063,2**
PIB Real (% Var. interanual)	**-7,3**	**11,0**	7,8	12,3	7,8	2,9	**7,3**	3,0	0,3	**0,9**
Precios										
Inflación (IPC, % Var. interanual)	**1,6**	**5,6**	7,8	9,3	10,8	12,6	**13,1**	13,3	12,4	**8,8**
Inflación sin alimentos (% Var. interanual)	**1,0**	**3,4**	5,0	6,4	7,8	9,5	**10,0**	10,9	11,6	**10,4**
Tipo de cambio (COP/USD fin de periodo)	**3432,5**	**3981**	3748	4127	4232	4810	**4810**	4627	4191	**4195**
Tipo de cambio (Var. % interanual)	**4,7**	**16,0**	0,3	9,9	18,2	20,8	**20,8**	23,5	1,6	**-12,8**
Sector Externo										
Cuenta corriente (USD millones)	**-9267**	**-17951**	-5478,1	-4951,1	-6227,6	-4869,1	**-21526**	-3385,3	-2524,5	**-12757**
Déficit en cuenta corriente (% del PIB)	**-3,3**	**-5,7**	-6,4	-5,5	-7,1	-6,0	**-6,2**	-4,2	-3,0	**-3,4**
Balanza comercial (% del PIB)	**-4,7**	**-6,3**	-5,9	-3,5	-5,1	-4,6	**-4,8**	-2,9	-2,5	**-2,8**
Exportaciones F.O.B. (% del PIB)	**13,7**	**16,0**	19,2	21,7	22,2	21,7	**21,2**	21,0	19,2	**13,4**
Importaciones F.O.B. (% del PIB)	**18,4**	**22,3**	25,1	25,2	27,4	26,3	**26,0**	24,0	21,7	**16,1**
Renta de los factores (% del PIB)	**-1,8**	**-2,7**	-4,2	-5,1	-5,6	-5,3	**-5,1**	-5,1	-4,0	**-3,6**
Transferencias corrientes (% del PIB)	**3,1**	**3,4**	3,7	3,1	3,6	3,9	**3,6**	3,8	3,5	**3,4**
Inversión extranjera directa (pasivo) (% del PIB)	**2,7**	**2,9**	5,7	5,7	3,5	5,3	**5,0**	5,3	6,2	**3,3**
Sector Público (acumulado, % del PIB)										
Bal. primario del Gobierno Central	**-4,9**	**-3,7**	-0,3	0,1	0,2	-1,0	**-1,0**	0,4	…	**0,0**
Bal. del Gobierno Nacional Central	**-7,8**	**-7,1**	-1,2	-1,1	-1,1	-2,0	**-5,3**	-0,8	…	**-4,3**
Bal. primario del SPNF	**…**	**-4,3**	…	…	…	…	**-1,8***	…		**1,2**
Bal. del SPNF	**…**	**-7,2**	…	…	…	…	**-6,3***	…		**-3,5**
Indicadores de Deuda (% del PIB)										
Deuda externa bruta	**57,1**	**54,6**	53,5	51,3	50,6	53,4	**53,4**	55,3	56,1	
Pública	**33,2**	**32,6**	31,0	29,4	28,8	30,4	**30,4**	31,4	31,8	
Privada	**23,8**	**22,0**	22,5	21,9	21,8	23,0	**23,0**	23,9	24,2	
Deuda neta del Gobierno Central	**60,7**	**60,1**	49,3	51,9	54,9	57,9	**57,9**	**52,7**	…	**55,8**

P Proyecciones de Asobancaria

Colombia

Estados financieros del sistema bancario

	jun-23 (a)	may-23	jun-22 (b)	Variación real anual entre (a) y (b)
Activo	**942.291**	**935.083**	**868.487**	**-3,2%**
Disponible	62.476	61.896	64.278	-13,3%
Inversiones y operaciones con derivados	185.826	182.143	170.413	-2,7%
Cartera de crédito	653.690	651.691	598.930	-2,7%
Consumo	198.622	199.571	188.421	-6,0%
Comercial	340.069	337.886	307.065	-1,2%
Vivienda	97.915	97.285	88.632	-1,5%
Microcrédito	17.085	16.948	14.812	2,9%
Provisiones	39.765	39.538	35.791	-0,9%
Consumo	18.261	18.078	13.057	24,7%
Comercial	16.956	16.861	17.379	-13,0%
Vivienda	3.269	3.253	3.158	-7,7%
Microcrédito	1.057	1.050	874	7,9%
Pasivo	**839.362**	**831.033**	**772.359**	**-3,1%**
Instrumentos financieros a costo amortizado	715.269	705.945	661.725	-3,6%
Cuentas de ahorro	268.494	263.167	295.545	-19,0%
CDT	259.857	254.498	170.043	36,3%
Cuentas Corrientes	73.328	75.117	83.248	-21,4%
Otros pasivos	11.968	11.978	9.948	7,3%
Patrimonio	**102.929**	**104.050**	**96.128**	**-4,5%**
Ganancia / Pérdida del ejercicio (Acumulada)	**4.775**	**3.913**	**9.029**	**-52,8%**
Ingresos financieros de cartera	44.718	37.081	26.825	48,7%
Gastos por intereses	29.145	24.219	8.629	201,2%
Margen neto de Intereses	18.022	15.042	19.085	-15,8%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,63**	**4,55**	**3,66**	**0,96**
Consumo	7,43	7,32	4,61	2,82
Comercial	3,45	3,36	3,25	0,20
Vivienda	2,67	2,65	2,71	-0,05
Microcrédito	6,63	6,57	5,83	0,80
Cubrimiento	**131,5**	**133,3**	**163,1**	**31,65**
Consumo	123,7	123,8	150,3	-26,64
Comercial	144,5	148,3	174,0	-29,55
Vivienda	125,2	126,3	131,3	-6,14
Microcrédito	93,3	94,4	101,1	-7,87
ROA	1,02%	1,01%	2,09%	-1,1
ROE	9,49%	9,27%	19,67%	-10,2
Solvencia	16,10%	16,12%	16,09%	0,0

Banca & Economía

2023

Edición 1396

Colombia

Principales indicadores de inclusión financiera

	2017	2018	2019	2020	2021				2022					
	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total
Profundización financiera - Cartera/PIB (%) EC + FNA	**50**	**49,7**	**49,9**	**55,4**	55,3	53,3	51,8	50,9	**50,9**	50	49,5	48,8	48,5	
Efectivo/M2 (%)	**13,6**	**14**	**15**	**16,6**	16	16,5	16,5	17	**17**	16,2	15,9	15,6	16,3	
Cobertura														
Municipios con al menos una oficina o un corresponsal bancario (%)	**100**	**99,2**	**99,9**	**100**	100	100	100	100		100	100	100	-	
Municipios con al menos una oficina (%)	**73,9**	**74,4**	**74,6**	**78,6**	72,8	72,9	72,8	72,8	**78,8**					
Municipios con al menos un corresponsal bancario (%)	**100**	**98,3**	**100**	**100**	100	100	100	92,7		98,6	98,6	-	-	
Acceso														
Productos personas														
Indicador de bancarización (%) SF*	**80,1**	81,4	**82,5**	**87,8**	89,4	89,4	89,9	90,5	**90,5**	91,2	91,8	92,1	92,3	**92,3**
Adultos con: (en millones)														
Al menos un producto SF	**27,1**	**28,0**	**29,4**	**31,2**	32,7	32,9	33,1	33	**33,5**	33,8	34,2	34,4	34,7	**34,7**
Cuentas de ahorro	**25,16**	**25,8**	**26,6**	**27,9**	28,4	28,3	28,6	28,9	**28,9**	29,2	29,5	29,6	29,9	**29,9**
Cuenta corriente SF	**1,73**	**1,89**	**1,97**	**1,9**	1,9	1,9	1,9	1,9	**1,9**	1,9	1,9	1,8	-	**-**
Cuentas CAES SF	**2,97**	**3,02**	**3,03**	**3**	3,0	3,0	3,0	Depósitos de bajo monto						
Cuentas CATS SF	**0,1**	**2,3**	**3,3**	**8,1**	9,2	10,5	11,8		**21,1**	21,7	22,4	23,0	23,5	**23,5**
Depósitos electrónicos	**4,2**	**4,9**	**6,7**	**11,6**	12,7	13,1	13,7							
Productos de ahorro a término (CDTs)	**0,78**	**0,81**	**0,85**	**…**	0,85	0,83	0,75	-	**-**	0,8	0,8	0,9	-	**-**
Crédito de consumo SF	**8,0**	**6,8**	**6,9**	**6,8**	6,86	6,9	6,9	6,9	**6,9**	7,1	7,4	7,7	7,8	**7,8**
Tarjeta de crédito SF	**9,2**	**8,9**	**8,4**	**8,1**	8,11	8,1	7,7	7,9	**7,9**	8,0	8,2	8,4	8,5	**8,5**
Microcrédito SF	**3,3**	**3,1**	**2,5**	**2,4**	2,44	2,4	2,3	2,3	**2,3**	2,30	2,34	2,36	2,3	**2,3**
Crédito de vivienda SF	**1,1**	**1,1**	**1,1**	**1,2**	1,19	1,1	1,2	1,2	**1,2**	1,23	1,25	1,27	1,3	**1,3**
Crédito comercial SF	**0,8**	**-**	**0,7**	**0,4**	0,54	0,5	0,4	0,2	**0,2**	0,46	0,45	0,44	0,5	**0,5**
Uso														
Productos personas														
Adultos con: (%)														
Algún producto activo SF	**68,6**	**68,5**	**66**	**72,6**	74,4	74,6	75,5	74,8	**74,8**	76,2	76,9	77,7	77,2	**77,2**
Cuentas de ahorro activas SF	**71,8**	**68,3**	**70,1**	**64,2**	62,2	65,3	65,8	65,7	**65,7**	65,9	65,2	64,9	51,9	**52**
Cuentas corrientes activas SF	**83,7**	**85,5**	**85,6**	**82,3**	82,3	80,2	78,5	73,7	**73,7**	76,9	76,5	76,3	74,5	**75**
Cuentas CAES activas SF	**89,5**	**89,7**	**82,1**	**82,1**	82,1	82,2	82,1							
Cuentas CATS activas SF	**96,5**	**67,7**	**58,3**	**74,8**	72,3	73,8	75,1	Depósitos de bajo monto	**76,3**	77,8	78,6	80,2	78,6	**78,6**
Depósitos electrónicos	**95,0**	**39,0**	**38,3**	**65,5**	70,1	71,4	71,7							
Productos de ahorro a término (CDTs)	**62,7**	**61,2**	**62,8**	**-**	69,5	64,6	75,6	-	**-**	77,5	79,3	80,1	-	-

	2016	2017	2018	2019	2020	2021					2022				
	Total	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total
Acceso															
Productos empresas															
Empresas con: (en miles)															
Al menos un producto SF	**751,851**	**935,88**	**947,464**	**939,682**	**925,26**	926,3	924,2	923,8	1028,6	**1028,6**	1029,0	1038,7	1065,7	1077,1	**1077,1**
*Productos de depósito SF	**436,2**	**498,5**	**925,32**	**908,97**	**898,90**	899,2	897,6	898,2	997,9	**998,9**	1004,0	1013,0	1039,8	1046,4	**1046,4**
*Productos de crédito SF	**221,1**	**231,5**	**323,105**	**286,192**	**284,2**	368,9	287,4	282,8	280,2	**280,2**	289,6	294,2	300,6	380,2	**380,2**
Uso															
Productos empresas															
Empresas con: (%)															
Algún producto activo SF	**74,7**	**72,1**	**71,6**	**68,4**	**68,1**	68,3	68,2	68,1	70,5	**70,5**	71,4	71,2	72,1	72,4	**72,4**
Operaciones (semestral)															
Total operaciones (millones)	**4.926**	**5.462**	**6.334**	**8.194**	**9.915**	_	4.939	_	6.222	**11.161**	-	6.668	-	7.769	**14.397**
No monetarias (Participación)	**48**	**50,3**	**54,2**	**57,9**	**61,7**	_	55,4	_	56,7	**56,1**	-	55,4	-	56,0	**55,8**
Monetarias (Participación)	**52**	**49,7**	**45,8**	**42**	**38,2**	_	44,6	_	43,3	**43,8**	-	44,6	-	44,0	**44,2**
No monetarias (Crecimiento anual)	**22,22**	**16,01**	**25,1**	**38,3**	**28,9**	_	-8,7	_	12,4	**2,3**	-	34,0	-	23,2	**27,9**
Monetarias (Crecimiento anual)	**6,79**	**6,14**	**6,7**	**18,8**	**10**	_	30,5	_	29,3	**29,1**	-	33,1	-	27,1	**29,8**
Tarjetas															
Crédito vigentes (millones)	**14,9**	**14,9**	**15,3**	**16,1**	**14,7**	14,9	14,6	15,0	15,6	**15,6**	15,9	16,0	16,1	16,0	**16,0**
Débito vigentes (millones)	**25,2**	**27,5**	**29,6**	**33,1**	**36,4**	39,2	38,4	39,7	40,8	**40,8**	41,1	42,6	43,7	45,8	**45,8**
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	**194,4**	**203,8**	**207,8**	197,6	208,2	201,4	219,9	**219,9**	215,3	225,2	209,5	225,6	**225,6**
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	**131,4**	**126,0**	**129,3**	116,8	118,1	114,5	124,9	**124,9**	119,1	116,5	112,5	108,1	**108,1**