Banca & Economía
2021
Edición 1291

Propuestas para mejorar la seguridad de las transacciones digitales

2 de agosto de 2021

Director:

Hernando José Gómez

ASOBANCARIA:

Hernando José Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

• Si bien el fraude en canales virtuales ha existido desde que se utiliza el internet para realizar transacciones financieras, desde Asobancaria se ha visto cómo esta problemática ha ido aumentando desde 2020, resultado que en gran parte ha estado influenciado por el mayor uso que han tenido las soluciones virtuales de las entidades bancarias y por el mayor control en las transacciones presenciales en oficinas mediante el uso de la biometría.

• De acuerdo con cifras de Asobancaria, el indicador de reclamaciones de fraude por canales digitales[1] pasó de 1,4 pesos por cada 100 mil pesos en enero de 2020 a 3,99 por cada 100 mil pesos transados en abril de 2021. Si bien este indicador aún luce bajo, muestra un incremento de 183% en dicho periodo.

• En el contexto de transformación digital de la sociedad, la economía y el Gobierno, se hace imprescindible defender y garantizar la confianza y la seguridad de las personas en la utilización del ecosistema digital.

• Una primera propuesta es avanzar en el trámite de un Proyecto de Ley que actualice las normas penales en materia de ciberdelitos. El año pasado se propuso el Proyecto de Ley 339, el cual avanzaba en la tipificación e investigación de los delitos informáticos de los que son víctimas los ciudadanos, empresas colombianas y, en particular, las instituciones financieras y sus clientes.

• Es indispensable también fortalecer las capacidades institucionales. En abril de 2021 Asobancaria en cooperación con el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), realizó el lanzamiento de cursos virtuales dirigidos a alcaldes y gobernadores de todo el país con el propósito de iniciar un proceso de sensibilización sobre temas de prevención del fraude y hábitos ciberseguros, para combatir y reducir las cifras de fraude a través de medios digitales. Asobancaria continúa avanzando en la capacitación de fiscales en materia de investigación de delitos digitales.

• Por último, proponemos avanzar en mesas de trabajo para evaluar un mecanismo para el bloqueo de URLs maliciosas. Para avanzar en un mecanismo de este estilo, en dichas mesas debería evaluarse la posibilidad de tomar en cuenta las facultades legales con las que cuentan hoy en día la Comisión de Regulación de Comunicaciones (CRC), el MinTIC y la Superintendencia Financiera.

[1] Monto de reclamaciones por fraude en canales digitales, dividido en el total de transacciones que pasan por estos canales, multiplicado por 100.000.

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

Banca & Economía
2021
Edición 1291

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Jaime Andrés Rincón Arteaga
Andrés Quijano Díaz
Juan David Urquijo Vanegas
Santiago Castiblanco Hernández

Propuestas para mejorar la seguridad de las transacciones digitales

Si bien el fraude en canales virtuales ha existido desde que los bancos utilizan el internet como canal transaccional, desde Asobancaria se ha visto cómo esta problemática aumentó en forma significativa en 2020, un resultado derivado, en buena parte, del mayor uso de las soluciones virtuales de las entidades bancarias.

Este mayor uso de aplicaciones móviles o portales bancarios ha sido resultado, por un lado, de las medidas implementadas por la pandemia de Covid-19 y, por otro, del crecimiento en el acceso a los servicios financieros. De acuerdo con Banca de las Oportunidades (2020)[2], el porcentaje de adultos con productos financieros sobre el total de la población adulta pasó de 83,3% en septiembre de 2019 a 87,7% en septiembre de 2020. Este mayor número de personas usando servicios financieros trajo consigo mayores riesgos de fraude o ciberataques a los usuarios.

A lo largo de 2020 se presentaron noticias frecuentes de mensajes de texto y de correo electrónico falsos, en los cuales ciberdelincuentes en varios países se hacían pasar por entidades públicas, departamentos de salud o entidades financieras. De acuerdo con el *Informe de Cibercrimen de 2020* de la Policía Nacional[3], el total de denuncias en Colombia en 2020 de delitos enmarcados como delitos informáticos fue de 45.104, cifra que representa un incremento del 89% con respecto al 2019, siendo el hurto por medios informáticos y semejantes el de mayor incidencia, con 16.654 denuncias.

Por otra parte, de acuerdo con cifras de Asobancaria, el indicador de reclamaciones de fraude por canales digitales[4] pasó de 1,4 por cada 100 mil pesos transados en enero de 2020 a 3,99 por cada 100 mil pesos en abril de 2021(Gráfico 1). Si bien es un indicador que aún luce bajo, representa un incremento del 183%.

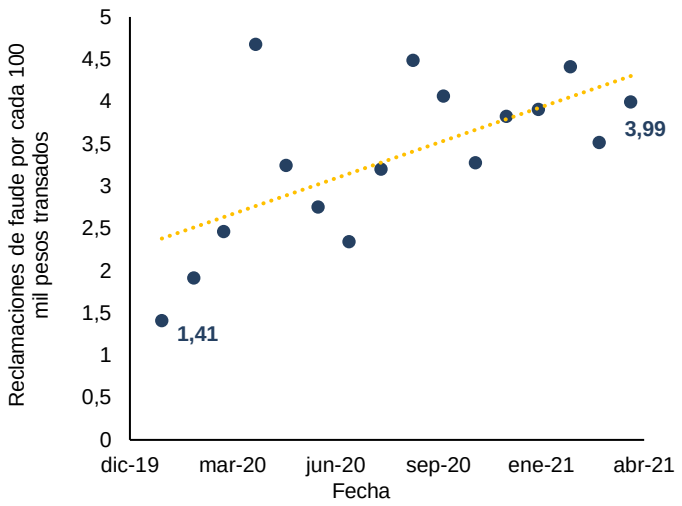
Esta edición de Banca & Economía presenta, en este contexto, algunas de las iniciativas y propuestas del gremio y la industria encaminadas a fortalecer la confianza y la seguridad digital con un enfoque de política pública. Finaliza con algunas conclusiones en este frente.

Propuesta 1: avanzar en un Proyecto Ley contra la cibercriminalidad

En diciembre de 2020 se presentó en el Senado el Proyecto de Ley 339 *"Por medio del cual se expiden lineamientos en torno a la Seguridad Digital, se modifica la Ley 599 de 2000, y se dictan otras disposiciones*[5]". Sin embargo, dada la dinámica política del primer semestre de 2021, el Proyecto de Ley fue retirado.

[2] Banca de las Oportunidades (2020). Inclusión financiera de personas naturales – septiembre 2020. Tomado de: https://bancadelasoportunidades.gov.co/index.php/es/personas-empresas.
[3] Policía Nacional (2021). Informe de Cibercrimen de 2020.
[4] Monto de reclamaciones por fraude en canales digitales, dividido en el total de transacciones que pasan por estos canales, multiplicado por 10.000
[5] Actualmente se encuentra pendiente de rendir ponencia para primer debate.

Gráfico1. Comportamiento del indicador de fraude en canales digitales desde diciembre de 2019



Fuente: Elaboración Asobancaria.

En Asobancaria creemos que es necesario tramitar en el Congreso un proyecto de Ley que actualice el marco normativo de los delitos informáticos. En ese sentido, considerábamos ese proyecto como un lineamiento valioso para avanzar en la materia.

El Proyecto de Ley proponía agregar nuevos delitos informáticos al código penal colombiano: "Difusión no consentida de imágenes con contenido sexual", "*Grooming*"[6] y "Ciber-acoso". Así mismo, planteaba circunstancias de agravación punitiva cuando las conductas criminales se realicen a través de medios informáticos o se emplee cualquier técnica de manipulación informática. Finalmente, entre las propuestas más importantes se destacaba la adición de un nuevo artículo al código de procedimiento penal para que la Fiscalía General de la Nación pueda solicitar a un juez que ordene a los proveedores de redes y servicios de telecomunicaciones el bloqueo preventivo de los dominios de internet, URL, cuentas y usuarios cuando a través de ellos se realicen actividades delictivas en detrimento de los derechos de las personas. Con este tipo de disposiciones el país actualizaría su marco normativo y se acercaría a lo dispuesto por el Convenio de Budapest, ratificado por Colombia a través de la Ley 1928 de 2018.

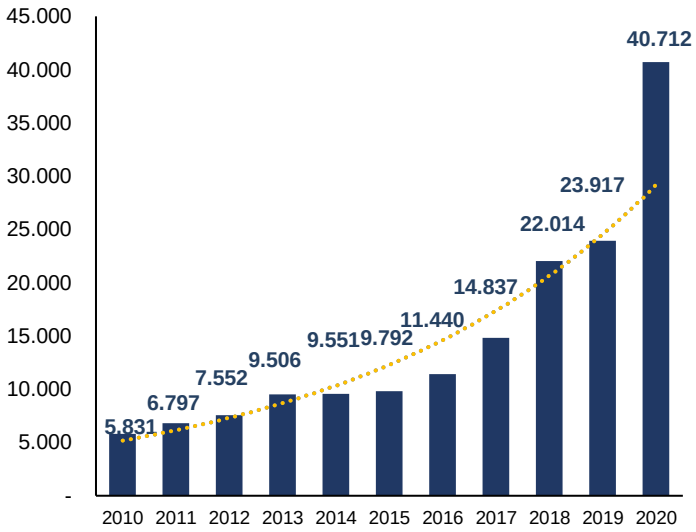
En adición a lo dispuesto en el Proyecto de Ley, en Asobancaria proponíamos las siguientes disposiciones con el ánimo de contribuir a la discusión pública:

1. Adicionar un nuevo numeral al artículo 240 de la Ley 599 de 2000, con el fin de ampliar el delito de hurto calificado y que este cobije el uso datos personales para cometer el ilícito.

El Proyecto de Ley imponía un agravante penal a los delitos informáticos si el delincuente obtuviese datos personales con ocasión de su empleo, oficio o profesión. Si bien este agravante va dirigido a castigar a aquellas personas que cometan deslealtad laboral[7], en Asobancaria proponíamos que este agravante se ampliara a todos los casos en que se utilicen medios electrónicos para acceder a los datos personales(Gráfico 2). Lo anterior, teniendo en cuenta que los delitos de mayor incremento fueron suplantación de sitios web, violación de datos personales e interceptación de datos informáticos, y que para cometer estos delitos los delincuentes utilizan diferentes técnicas de engaño, las cuales no solo están asociadas directamente con ocasión de su empleo, oficio o profesión.

De esta forma, cualquier delincuente que acceda a datos personales a través de medios electrónicos, independientemente de su empleo u oficio, se encontraría en las circunstancias de agravante penal

Gráfico 2. Evolución de denuncias por delitos informáticos desde 2009



Fuente: Fiscalía General de la Nación. Elaboración Asobancaria.

2. Propuesta para que las compañías de telefonía móvil implementen mecanismos fuertes de identificación de sus clientes.

En los últimos años se ha evidenciado en Colombia una modalidad de fraude con tendencia creciente denominada *Sim Swap*, en la cual el delincuente roba los datos personales y financieros del

[6] El que haciéndose pasar por otra persona, o habiendo mentido sobre sus datos personales obtenga imágenes o grabaciones audiovisuales de la actividad sexual o con contenido sexual de un menor de edad.

[7] Se entiende por deslealtad laboral cuando el empleado comete faltas a las obligaciones laborales de exclusividad, buena fe, lealtad y fidelidad en cabeza de su empleador. Por ejemplo, si utiliza los recursos de su empleador con fines ilícitos para beneficio propio.

cliente para ordenar el bloqueo de su número celular y solicitar una nueva *SIM Card*. Al obtenerla, el delincuente se comunica con la línea de servicio al cliente de banco y solicita una OTP (*One Time Password* o clave dinámica) para registrarse en banca móvil y realizar operaciones no presenciales. Con esta información, el delincuente realiza operaciones no consentidas como la reexpedición de tarjetas de crédito.

Cuando el delincuente accede a banca móvil puede realizar operaciones sin tarjeta (afectar cuentas de ahorros y corrientes, cupos de tarjeta de crédito, créditos rotativos, entre otros). En este sentido, es difícil para las entidades detectar ágilmente este tipo de alertas ya que el delincuente recibe los mensajes de texto de notificación y es contactado por el área de monitoreo del banco para confirmar las transacciones.

Desde que se identificó en 2015, el valor del fraude por esta modalidad asciende a COP 8.000 millones anuales, aproximadamente. Actualmente se ha evidenciado que en el proceso de solicitud de expedición y reposición de una *SIM Card*, los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) no cuentan con mecanismos de autenticación[8] fuerte que acrediten la identidad de la persona que está adquiriendo la *SIM Card*. En este sentido, se propone a la CRC que los PRSTM cuenten con mecanismos de autenticación fuertes[9] en el proceso de expedición de la *SiM* que acrediten la identidad de la persona que la está adquiriendo.

Propuesta 2: fortalecimiento institucional

En 2020 se expidió el documento CONPES 3995 de 2020 de Política Nacional de Confianza y Seguridad Digital, el cual "*formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital*" (CONPES, 2020).

Cuando el CONPES 3995[10] se encontraba en etapa de comentarios, Asobancaria señaló la importancia de promover el desarrollo de competencias en las organizaciones públicas, tanto aquellas de orden nacional como territorial. Se estima que el fraude anual que afectó a entes territoriales generó pérdidas aproximadas a los COP 50.000 mil millones anuales.

Es por esto que, en abril de 2021, Asobancaria, en cooperación con el MinTIC, realizó el lanzamiento de cursos virtuales dirigidos a alcaldes y gobernadores de todo el país con el propósito de iniciar un proceso de sensibilización sobre temas de prevención del fraude y hábitos ciberseguros, para combatir y reducir las cifras de fraude a través de medios digitales. Actualmente se han visto beneficiados por estos cursos 243 alcaldes y 7 gobernadores del país. Se espera que en las próximas ediciones de los cursos se pueda abarcar a otros grupos de interés clave que tienen acceso a recursos públicos.

Así mismo, Asobancaria cuenta con un proyecto que busca el fortalecimiento de las capacidades institucionales que se encargan de la investigación y la judicialización de delitos informáticos, el cual se ha venido implementando desde 2016 mediante un curso en cibercriminalidad dirigido a fiscales en temas relacionados con informática jurídica, evidencia digital e informática forense, entre otros temas que requieren comprensión de terminología técnica para poder combatir a los ciberdelincuentes. Desde su inicio, este curso ha beneficiado a cerca de 140 fiscales de todo el país. De esta manera, Asobancaria espera seguir contribuyendo a fortalecer las capacidades en seguridad digital del personal de rama judicial en el país, uno de los focos principales del CONPES.

Si bien los esfuerzos de la banca son importantes, estos deben ser respaldados por las instituciones. Por ello, es importante redoblar los esfuerzos que se hacen desde el Gobierno Nacional en esta materia. En esta línea, desde Asobancaria consideramos imperativo que se robustezcan los programas para fortalecer instituciones como la Policía Nacional, la Fiscalía, así como el sistema judicial y los entes territoriales en materia de seguridad cibernética.

Actualmente, únicamente el 2,8% de las denuncias por delitos informáticos termina en capturas, lo que evidencia la baja efectividad que tiene la institucionalidad para hacerle frente a esta modalidad de crimen. Al ser este un tema particular y novedoso, no es suficiente la formación regular de un policía, fiscal o juez para que el aparato judicial cumpla con su función. Así las cosas, resulta imperativo que las instituciones se actualicen a las tendencias criminales para cumplir con su misión de proteger a los ciudadanos.

Este fortalecimiento institucional pasa también por el fortalecimiento de instituciones como el Grupo de Respuesta a Incidentes Cibernéticas de Colombia (Colcert) y el Comando Conjunto Cibernético (CCOC), cuya misión es proteger la infraestructura crítica cibernética del país. Por ello, se hace necesario una mayor inversión en tecnología y capacidades

[8] Se entiende como mecanismos fuertes de autenticación los siguientes: i) Biometría en combinación con un segundo factor de autenticación para operaciones no presenciales. En aquellos eventos en que la operación se efectúe de manera presencial no se requerirá el uso de un segundo factor de autenticación; ii) certificados de firma digital de acuerdo con lo establecido en la Ley 527 de 1999 y sus decretos reglamentarios. OTP (*One Time Password*), en combinación con un segundo factor de autenticación, y iii) registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación."

[9] La autenticación se entiende como el conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es.

[10] Departamento Nacional de Planeación (2020). CONPES 3995 *"Política Nacional de Confianza y Seguridad Digital"*.

humanas en estas instituciones para que logren cumplir con las misiones asignadas.

Propuesta 3: mecanismo para bloqueo de URLs maliciosas

Asobancaria ha evidenciado que la principal problemática que afecta la confianza y seguridad digital de las personas es el robo de datos. La modalidad más importante de este crimen, con un 70% de las reclamaciones en canales digitales, es realizada mediante correos o mensajes de texto que redirigen a páginas web maliciosas que simulan ser de una entidad del estado o de una entidad financiera para acceder a los datos de las personas.

Hoy en día en Colombia no existe un mecanismo expedito para evitar que las personas ingresen a estas páginas web maliciosas. Esto se debe en parte a que en Colombia existe el principio de neutralidad de la red. Según este principio el tráfico de internet debe ser tratado con igualdad, sin discriminación, restricción o interferencia independientemente de su remitente, destinatario, tipo o contenido, para que quede a libre elección de los usuarios el acceso a internet[11]. Si bien el principio de neutralidad de la red tiene su límite en que el contenido sea legal, en Colombia se ha interpretado que toda página se considera legal hasta que una entidad judicial considere lo contrario.

Esta interpretación ha hecho que exista una sobre protección en el contenido de las páginas web, cuando podría ser claro para las propias autoridades administrativas como la Policía o la Fiscalía que su contenido es ilegal. En este sentido, existe una tardanza excesiva para lograr el bloqueo preventivo de URL's maliciosas que buscan robar datos personales (que usualmente son enviadas en los correos electrónicos o mensajes de texto -SMS-), ya que este procedimiento puede tomar varios días e incluso semanas. Este atraso, que permite que la página web se encuentre activa y siga recolectando datos de los ciudadanos con propósitos fraudulentos, se debe a que para el bloqueo preventivo es necesario contar con el aval de un juez de control de garantías.

A pesar de esto, existen varios ejemplos en los que, a través de facultades legales, entidades administrativas pueden ordenar a los proveedores de servicios de internet bloquear preventivamente cierto contenido. El caso más representativo son las facultades con las que cuenta la Policía desde el 2001 con la Ley 679 de 2001 para ordenar el bloqueo de material con pornografía infantil. Así mismo, se puede ordenar el bloqueo de páginas en las que de forma ilegal se ofrezcan servicios de suerte y azar. En este caso, la Ley 1753 de 2015 otorga facultades a COLJUEGOS para bloquear las páginas de internet que ofrezca juegos de suerte de forma ilegal. En desarrollo de estas facultades en el 2020 COLJUEGOS, el MINTIC y la Policía Nacional firmaron un convenio a través del cual se crea un mecanismo para ordenar el bloqueo de páginas de Juegos de Suerte y Azar (JSA) ilegales.

Teniendo en cuenta que tanto la CRC como la Superintendencia Financiera tienen facultades y el orden legal para proteger a las personas de ser víctimas de estafas por internet, Asobancaria propone establecer mesas de trabajo con la Superintendencia Financiera, la CRC, el MinTIC, la Policía Nacional y la Fiscalía para evaluar la posibilidad de definir un protocolo objetivo similar al que tiene COLJUEGOS y MinTIC para el bloqueo de páginas web maliciosas de JSA, para que a través de un listado preventivo la SFC pueda ordenar el bloqueo de URLs y códigos cortos de SMS maliciosos. Esto podría operativizarse a través de la CRC, quien ordenaría el bloqueo preventivo de este material a los proveedores de internet. Este procedimiento debería, en todo caso, respetar el debido proceso del titular de la URL, por lo que se sugiere que se expida una orden de bloqueo preventiva, sujeta a un proceso administrativo en el que el afectado pueda probar la legalidad del contenido de su página.

Dentro de dichas mesas, una de las áreas de discusión sería la determinación de las facultades legales que tienen las entidades públicas para abordar un protocolo con el del sector de juegos de suerte y azar. En el caso de la SFC, se podría considerar que esta entidad actualmente cuenta con facultades legales para establecer un proceso administrativo en este sentido. En efecto, La Ley 663 de 1993, Estatuto Orgánico del Sistema Financiero, en su artículo 325 y 326 establece las funciones y facultades de la Superintendencia Financiera para asegurar la confianza del público en el sector financiero y evitar que personas no autorizadas ejerzan actividades vigiladas. Entre ellas se destaca: evitar que personas no autorizadas ejerzan actividades de las entidades financieras, así como prevenir situaciones que puedan afectar la confianza del público, el interés general y el de terceros.

Según estas facultades legales, la SFC podría emitir, en ciertas condiciones, las órdenes necesarias para suspender preventivamente prácticas ilegales e inseguras a personas naturales y jurídicas que realicen actividades exclusivas de las instituciones vigiladas sin contar con la debida autorización, es decir, para bloquear preventivamente cualquier contenido que suplante a una entidad vigilada. Este bloqueo preventivo, en concordancia con el debido proceso, estaría sujeto a un proceso administrativo en donde el afectado pueda probar la legalidad del contenido.

En el caso de la CRC, el artículo 19 de la Ley 1341 de 2009 establece que la CRC tiene entre sus funciones velar por la seguridad en la red y la confianza de los usuarios en la misma, lo que la facultaría para intervenir en el proceso descrito.

Conclusiones y consideraciones finales

En el contexto de transformación digital de la sociedad, la economía y el Gobierno, se hace imprescindible defender y garantizar la confianza y la seguridad de las personas en la utilización del ecosistema digital, pues esto favorece el

[11] Artículo 56 de la Ley 1450 de 2011. Tomado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43101

aprovechamiento de todas las innovaciones y herramientas que ha provisto la economía digital.

Como se pudo evidenciar, el fraude por canales digitales ha aumentado en un 183% desde diciembre de 2019 hasta abril de 2021. Por lo tanto, se hace necesario implementar un mecanismo de política que brinde mayor seguridad a los datos de las personas que cada día están más expuestas y vulnerables en la red.

Con el fin de mantener la confianza en las transacciones digitales y seguir profundizando el uso de estos canales, desde Asobancaria se propone: i) avanzar en la implementación de un proyecto de ley contra la cibercriminalidad; ii) promover programas y planes de acción que permitan fortalecer las capacidades de investigación y judicialización de los delitos informáticos en el país, y iii) crear mesas de trabajo para evaluar la implementación de un mecanismo para bloquear de manera preventiva ULRs que dirigen a sitios web maliciosos.

Colombia

Principales indicadores macroeconómicos

	2019					2020					2021	2021*
	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	Total
Producto Interno Bruto**												
PIB Nominal (COP Billones)	247,4	255,0	270,9	287,7	**1061,1**	258,7	213,5	249,2	281,4	**1002,9**	268,9	**1081,8**
PIB Nominal (USD Billones)	77,3	79,5	78,3	88,6	**324,0**	63,4	57,1	63,8	76,5	**271,5**	71,9	**314,77**
PIB Real (COP Billones)	205,2	215,1	222,7	238,9	**882,0**	206,4	181,3	204,1	230,3	**822,0**	208,7	**857,5**
PIB Real (% Var. interanual)	3,6	3,1	3,2	3,2	**3,3**	0,7	-15,8	-8,5	-0,0	**-6,8**	1,1	**6,1**
Precios												
Inflación (IPC, % Var. interanual)	3,2	3,4	3,8	3,8	**3,8**	3,7	2,9	1,9	1,6	**1,6**	2,0	**3,5**
Inflación sin alimentos (% Var. interanual)	3,3	3,3	3,3	3,4	**3,4**	3,3	2,0	1,5	1,2	**1,0**	1,6	**2,5**
Tipo de cambio (COP/USD fin de periodo)	3175	3206	3462	3277	**3277**	4065	3759	3879	3432	3432	3736	**3600**
Tipo de cambio (Var. % interanual)	14,2	9,4	16,5	3,6	**3,6**	28,0	17,3	12,0	4,7	**4,7**	-8,1	**4,9**
Sector Externo (% del PIB)												
Cuenta corriente	-4,6	-3,6	-5,1	-3,7	**-4,3**	-3,6	-3,0	-2,7	…	**-3,4**	-4,8	**-4,4**
Cuenta corriente (USD Billones)	-3,6	-2,8	-4,2	-3,2	**-13,8**	-2,6	-1,7	-1,8	-3,2	**-9,3**	-3,6	**-13,4**
Balanza comercial	-3,5	-3,2	-5,0	-3,7	**-3,8**	-3,9	-4,3	-4,6	…	**-3**	-3,5	**-2,7**
Exportaciones F.O.B.	12,8	13,7	12,8	12,9	**52,3**	11,7	7,8	8,9	…	**12,3**	14,1	**13,8**
Importaciones F.O.B.	15,5	16,2	16,9	16,1	**64,7**	14,5	10,2	12,0	…	**15,2**	19,3	**16,5**
Renta de los factores	-3,4	-3,2	-3,0	-2,9	**-3,1**	-2,6	-1,8	-1,7	…	**-2,1**	-2,9	**-3,3**
Transferencias corrientes	0,0	2,3	2,7	2,7	**1,9**	3,3	0,0	3,2	…	**3,2**	3,3	**3,1**
Inversión extranjera directa (pasivo)	3,4	4,7	2,2	3,5	**3,4**	3,2	3,0	-0,1	…	**3,0**	3,6	**3,3**
Sector Público (acumulado, % del PIB)												
Bal. primario del Gobierno Central	0,0	0,9	1,4	0,4	**0,5**	0,3	-3,2	…	…	**-5,9**	**…**	**…**
Bal. del Gobierno Nacional Central	-0,6	-0,3	-1,2	-2,5	**-2,5**	-0,2	-5,8	…	…	**-7,8**	…	**-8,6**
Bal. estructural del Gobierno Central	…	…	…	…	**-1,5**	…	…	…	…	**…**	**…**	**…**
Bal. primario del SPNF	0,8	3,5	2,3	0,5	**0,5**	0,4	-3,0	…	…	**-6,7**	**…**	**…**
Bal. del SPNF	0,4	0,6	-0,5	-2,4	**-2,4**	0,4	-5,2	…	…	**-9,4**	**…**	**…**
Indicadores de Deuda (% del PIB)												
Deuda externa bruta	41,6	41,5	42,0	42,7	**42,0**	47,4	49,3	…	…	…	…	…
Pública	23,1	22,6	22,6	22,7	**22,8**	25,3	26,6	…	…	…	…	…
Privada	18,5	18,9	19,5	20,0	**19,2**	22,1	22,6	…	…	…	…	…
Deuda bruta del Gobierno Central	47,4	50,6	51,9	50,3	**50,0**	59,6	61,7	…	…	**61,4**	…	**62,9**

Colombia

Estados financieros del sistema bancario

	may-21 (a)	abr-21	may-20 (b)	Variación real anual entre (a) y (b)
Activo	**747.835**	**744.910**	**752.264**	**-3,8%**
Disponible	52.605	52.927	52.641	-3,3%
Inversiones y operaciones con derivados	159.851	160.717	163.531	-5,4%
Cartera de crédito	511.852	507.784	507.859	-2,4%
Consumo	152.397	152.154	147.640	-0,1%
Comercial	270.633	267.575	278.478	-5,9%
Vivienda	75.973	75.176	69.278	6,2%
Microcrédito	12.850	12.878	12.463	-0,2%
Provisiones	37.283	37.434	31.399	14,9%
Consumo	12.524	12.705	11.174	8,5%
Comercial	17.369	17.365	16.643	1,0%
Vivienda	2.817	2.779	2.536	7,5%
Microcrédito	1.129	1.126	1.046	4,5%
Pasivo	**654.794**	**652.626**	**661.150**	**-4,1%**
Instrumentos financieros a costo amortizado	575.621	574.075	558.041	-0,1%
Cuentas de ahorro	253.647	254.909	229.604	6,9%
CDT	143.447	144.913	163.951	-15,3%
Cuentas Corrientes	79.314	76.954	70.228	9,3%
Otros pasivos	9.292	8.715	10.216	-12,0%
Patrimonio	**93.041**	**92.283**	**91.114**	**-1,2%**
Ganancia / Pérdida del ejercicio (Acumulada)	**3.963**	**3.259**	**3.422**	**12,1%**
Ingresos financieros de cartera	17.092	13.670	19.870	-16,7%
Gastos por intereses	3.952	3.189	7.050	-45,7%
Margen neto de Intereses	13.593	10.861	13.460	-2,2%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,80**	**4,86**	**4,03**	**0,77**
Consumo	5,67	5,96	3,66	2,00
Comercial	4,50	4,48	4,15	0,35
Vivienda	3,62	3,59	3,97	-0,35
Microcrédito	7,64	7,36	6,03	1,61
Cubrimiento	**151,9**	**151,6**	**153,5**	**1,58**
Consumo	145,0	140,2	206,5	-61,47
Comercial	142,6	145,0	144,1	-1,49
Vivienda	102,4	102,8	92,3	10,09
Microcrédito	115,1	118,8	139,2	-24,14
ROA	1,28%	1,32%	1,10%	0,2
ROE	10,53%	10,97%	9,25%	1,3
Solvencia	20,46%	20,10%	13,97%	6,5

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018	2019				2019	2020				2020
	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total
Profundización financiera - Cartera/PIB (%) EC	**50,2**	**50,1**	**49,8**	49,5	49,6	49,9	49,8	**49,8**	51,7	54,3	…	…	**…**
Efectivo/M2 (%)	**12,59**	**12,18**	**13,09**	12,66	12,84	13,20	15,05	**15,05**	13,35	14,48	…	…	**…**
Cobertura													
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,7**	**100**	**99,2**	99,7	99,7	…	99,9	**99,9**	100	100	100	100	**100**
Municipios con al menos una oficina (%)	**73,9**	**73,9**	**74,4**	74,7	74,6	74,4	74,6	**74,6**	74,6	74,6	74,6	...	**...**
Municipios con al menos un corresponsal bancario (%)	**99,5**	**100**	**98,3**	100	100	…	100	**100**	100	100	100	100	**100**
Acceso													
Productos personas													
Indicador de bancarización (%) SF*	**77,30**	**80,10**	81,4	82,3	82,6	83,3	82,5	**82,5**	83,2	85,9	87,1	87,8	**87,8**
Indicador de bancarización (%) EC**	**76,40**	**79,20**	80,5	81,3	81,6	82,4	81,6	**81,6**	…	…	86,6	…	**…**
Adultos con: (en millones)													
Cuentas de ahorro EC	**23,53**	**25,16**	25,75	25,79	25,99	26,3	26,6	**26,6**	…	…	27,5	27,9	**27,9**
Cuenta corriente EC	**1,72**	**1,73**	1,89	1,95	2,00	2,00	1,97	**1,97**	…	…	1,92	1,9	**1,9**
Cuentas CAES EC	**2,83**	**2,97**	3,02	3,03	3,02	3,03	3,03	**3,03**	…	…	3,03	…	**…**
Cuentas CATS EC	**0,10**	**0,10**	0,71	2,10	2,32	2,54	3,30	**3,30**	…	…	7,14	8,1	**8,1**
Otros productos de ahorro EC	**0,77**	**0,78**	0,81	0,83	0,84	0,80	0,85	**0,85**	…	…	0,84	…	**…**
Crédito de consumo EC	**8,74**	**9,17**	7,65	7,82	8,00	8,16	8,42	**8,42**	…	…	…	…	**…**
Tarjeta de crédito EC	**9,58**	**10,27**	10,05	10,19	10,37	10,47	10,53	**10,53**	…	…	10,59	…	**…**
Microcrédito EC	**3,56**	**3,68**	3,51	3,49	3,48	3,50	3,65	**3,65**	…	…	…	…	**…**
Crédito de vivienda EC	**1,39**	**1,43**	1,40	1,41	1,43	1,45	1,45	**1,45**	…	…	…	…	**…**
Crédito comercial EC	**1,23**	**1,02**	…	…	…	0,69	0,70	**0,70**	…	…	…	…	**…**
Al menos un producto EC	**25,40**	**27,1**	27,64	28,03	28,25	28,6	29,1	**29,1**	…	…	…	32	**32**
Uso													
Productos personas													
Adultos con: (en porcentaje)													
Algún producto activo SF	**66,3**	**68,6**	68,5	69,2	69,8	70,4	66,0	**66,0**	66,8	71,6	73,0	72,6	**72,6**
Algún producto activo EC	**65,1**	**66,9**	67,2	67,8	68,4	69,2	69,1	**65,2**	…	…	72,4	…	**…**
Cuentas de ahorro activas EC	**72,0**	**71,8**	68,3	68,9	70,1	70,2	70,1	**70,1**	…	…	65,4	…	**…**
Cuentas corrientes activas EC	**84,5**	**83,7**	85,5	85,8	85,9	85,6	85,6	**85,6**	…	…	82,8	…	**…**
Cuentas CAES activas EC	**87,5**	**89,5**	89,7	89,8	89,9	82,2	82,1	**82,1**	…	…	82,1	…	**…**
Cuentas CATS activas EC	**96,5**	**96,5**	67,7	58,2	58,3	59,0	58,3	**58,3**	…	…	80,8	…	**…**
Otros pdtos. de ahorro activos EC	**66,6**	**62,7**	61,2	61,3	61,8	62,0	62,8	**62,8**	…	…	63,8	…	**…**
Créditos de consumo activos EC	**82,0**	**83,5**	82,2	81,7	81,9	81,8	75,7	**75,7**	…	…	…	…	**…**
Tarjetas de crédito activas EC	**92,3**	**90,1**	88,7	88,3	88,6	88,0	79,5	**79,5**	…	…	76,7	…	**…**
Microcrédito activos EC	**66,2**	**71,1**	68,9	68,9	69,2	68,9	58,3	**58,3**	…	…	…	…	**…**

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018	2019	2020				2020	2021
	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1
Créditos de vivienda activos EC	**79,3**	**78,9**	**77,8**	**78,2**	...	...	...	...	**...**	...
Créditos comerciales activos EC	**85,3**	**84,7**	**...**	**45,5**	...	...	...	...	**...**	...
Acceso										
Productos empresas										
Empresas con: (en miles)										
Al menos un producto EC	**751,0**	**775,2**	**946,5**	**938,8**	933,8	925,3	922,3	925,2	**925,2**	...
Cuenta de ahorro EC	**500,8**	**522,7**	**649,4**	**649,1**	648,5	637,1	637,1	639,8	**639,8**	...
Cuenta corriente EC	**420,9**	**430,7**	**502,9**	**499,7**	492,8	491,6	488,7	491,3	**491,3**	...
Otros productos de ahorro EC	**15,24**	**14,12**	**13,9**	**13,8**	15,4	16,0	14,9	...	**...**	...
Crédito comercial EC	**242,5**	**243,6**	**277,8**	**285,9**	288,3	291,3	...	...	**...**	...
Crédito de consumo EC	**98,72**	**102,5**	**105,8**	**104,9**	103,9	103,4	...	...	**...**	...
Tarjeta de crédito EC	**79,96**	**94,35**	**106,9**	**113,0**	114,1	113,9	...	...	**...**	...
Al menos un producto EC	**751,0**	**775,1**	**...**	**...**	...	...	...	...	**...**	...
Uso										
Productos empresas										
Empresas con: (en porcentaje)										
Algún producto activo EC	**74,7**	**73,3**	**71,5**	**68,34**	68,00	68,06	67,63	66,84	**66,84**	...
Algún producto activo SF	**74,7**	**73,3**	**71,6**	**68,36**	68,02	68,04	67,65	...	**...**	...
Cuentas de ahorro activas EC	**49,1**	**47,2**	**47,6**	**45,8**	44,8	44,7	44,0	...	**...**	...
Otros pdtos. de ahorro activos EC	**57,5**	**51,2**	**49,2**	**52,0**	55,0	55,4	57,2	...	**...**	...
Cuentas corrientes activas EC	**89,1**	**88,5**	**89,0**	**89,7**	90,7	91,0	91,1	...	**...**	...
Microcréditos activos EC	**63,2**	**62,0**	**57,2**	**50,3**	49,9	49,0	...	...	**...**	...
Créditos de consumo activos EC	**84,9**	**85,1**	**83,9**	**78,2**	77,7	77,4		...	**...**	...
Tarjetas de crédito activas EC	**88,6**	**89,4**	**90,2**	**80,3**	80,5	79,8	...	...	**...**	...
Créditos comerciales activos EC	**91,3**	**90,8**	**91,6**	**77,1**	77,3	73,0		...	**...**	...
Operaciones (semestral)										
Total operaciones (millones)	**4.926**	**5.462**	**6.332**	**8,194**	-	4,685	-	5,220	**9,911**	-
No monetarias (Participación)	**48,0**	**50,3**	**54,2**	**57,9**	-	64,0	-	60,0	**61,7**	-
Monetarias (Participación)	**52,0**	**49,7**	**45,8**	**42,0**	-	36,0	-	40,0	**38,2**	-
No monetarias (Crecimiento anual)	**22,22**	**16,01**	**25,1**	**38,3**	-	31,0	-	27,4	**28,9**	-
Monetarias (Crecimiento anual)	**6,79**	**6,14**	**6,7**	**18,8**	-	1,3	-	17,2	**10,0**	-
Tarjetas										
Crédito vigentes (millones)	**14,93**	**14,89**	**15,28**	**16,05**	16,33	15,47	14,48	14,67	**14,67**	14,53
Débito vigentes (millones)	**25,17**	**27,52**	**29,57**	**33,09**	34,11	34,51	35,42	36,38	**36,38**	37,37
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	**194,4**	**203,8**	176,2	179,3	188,6	207,8	**207,8**	195,5
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	**131,4**	**126,0**	113,6	126,0	123,6	129,3	**129,3**	120,6