Banca & Economía
2022
Edición 1340

Economía del comportamiento y campañas de prevención del fraude

8 de agosto de 2022

Director:

Hernando José Gómez

ASOBANCARIA:

Hernando José Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

- Una de las prioridades del sector bancario en Colombia es crear una cultura de hábitos financieros digitales seguros en sus clientes.
- La economía experimental y del comportamiento ofrece herramientas poderosas para identificar cuáles son las actitudes más sensibles de los consumidores financieros frente a campañas de sensibilización.
- Al momento de diseñar campañas de prevención, es relevante caracterizar a los consumidores financieros digitales según su propensión al riesgo, confianza en las transacciones digitales y comportamiento frente a posibles intentos de fraude.
- Los mensajes de *priming*[1] en campañas de prevención sufren del efecto de alarma de carro.
- Las campañas de prevención del fraude se deben replantear para generar impactos reales en el comportamiento digital seguro de los clientes del sistema financiero, evitando asociar las campañas con el miedo y el uso de palabras como fraude. En su lugar se debe invitar a los usuarios de canales digitales a ser cada vez mejores usuarios en un mundo digital.

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

[1] Mensajes de estímulos condicionantes utilizados en el neuromarketing para despertar mayor atención e interés en ciertos productos o acciones que promocionan las empresas

Banca & Economía
2022
Edición 1340

Economía del comportamiento y campañas de prevención del fraude

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Jaime Andrés Rincón Arteaga
Juan David Urquijo Vanegas

Con la transformación de la banca a un entorno virtual, la generación de una cultura de autocuidado para la prevención del fraude en los clientes se ha convertido en una prioridad para el sector financiero.

Si bien existen robustos sistemas de autenticación y ciberseguridad para cada producto ofrecido por los bancos, el usuario final continúa siendo el eslabón más débil de la cadena a la hora de realizar transacciones seguras en línea. De hecho, en muchos de los casos de fraude, el consumidor financiero descuida su cultura digital y expone sus datos personales y financieros más sensibles en el ciberespacio.

Por esta razón, el sector bancario le apuesta a construir una cultura digital más sana y segura a través de metodologías pedagógicas de sensibilización, concientización y educación financiera. Para lograr este cometido de mejor manera, el gremio se ha propuesto entender cuáles son los atributos comportamentales más importantes que permiten incentivar comportamientos de prevención del fraude en sus clientes.

De esta manera, junto con expertos académicos en economía del comportamiento[2], Asobancaria diseñó una investigación que busca ser un punto de referencia para el diseño de estrategias de prevención que impacten positivamente las conductas y hábitos seguros de los usuarios de la banca digital.

Esta edición de Banca y Economía repasa y comenta las conclusiones más importantes de este estudio. Para empezar, se plantea el escenario que motivó el desarrollo de este análisis experimental. En segundo lugar, se exponen los hallazgos más relevantes del ejercicio y, por último, se comentan las recomendaciones de la investigación para el planteamiento de futuras campañas de sensibilización.

[2] PhD. Juan Camilo Cárdenas – profesor asociado de la Universidad de los Andes y la Universidad de Massachusetts Amherst – en colaboración con Sensata Research UX.

La importancia de los buenos hábitos transaccionales en la prevención del fraude

Uno de los activos más valiosos de la banca colombiana hoy en día es la confianza de sus usuarios, una confianza basada en la seguridad del sector al realizar transacciones digitales a través de servicios de fácil acceso y uso. Por esta razón, para la industria bancaria es de vital importancia mantener al mínimo la exposición al fraude de sus usuarios, en especial, de aquellos que hacen uso de canales móviles, medio por el cual pueden ser más vulnerables si no tienen hábitos sanos de seguridad digital.

Según cifras de Asobancaria, anualmente un 70% de las reclamaciones de fraude bancario en canales digitales se concentran en ataques derivados de técnicas de *phishing* o *smishing*[3]. Esto es relevante porque estas técnicas sólo son exitosas si voluntariamente los usuarios revelan sus contraseñas al dar clic en los enlaces fraudulentos que traen consigo mensajes no verificados. En otras palabras, en la gran mayoría de los casos, la cadena de prevención del fraude se ve expuesta por descuidos de las personas al revelar sus datos.

De esta forma, para contrarrestar el problema de falta de hábitos transaccionales seguros, se debe enseñar a los consumidores financieros a tomar medidas mínimas de autocuidado cuando navegan o realizan operaciones en el mundo digital. Un ejemplo de una medida básica que se debe interiorizar en los usuarios es no entrar a enlaces que pidan datos personales o financieros, puesto que los bancos nunca piden esta información a través de correos o mensajes de texto.

Así, las campañas de sensibilización que advierten de los riesgos de descuidar los datos personales han sido la punta de lanza de los bancos para sensibilizar a los usuarios.

El eje central de esta investigación gira entorno a utilizar la economía experimental y del comportamiento para encontrar las actitudes más sensibles de los usuarios de la banca frente a campañas de prevención del fraude. En línea con los resultados obtenidos, el estudio plantea algunas estrategias de sensibilización para impactar al consumidor en cuanto a su higiene digital.

El diseño del ejercicio

La investigación utilizó encuestas experimentales que se recogieron de manera virtual, anónima y con el objetivo de evitar sesgos cognitivos. Se utilizó una muestra de más de 2500 personas, ubicadas en cuatro de las más grandes ciudades de Colombia[4], con un instrumento de recolección de datos que al final tuviera un saldo pedagógico para los participantes, es decir, una lección aprendida. Este saldo, a manera de incentivo, daba una retroalimentación sobre el perfil de usuario de banca digital del encuestado, acompañado de consejos para reducir su riesgo de ser defraudado.

Siguiendo esta estructura, el ejercicio contó con tres secciones. La primera, recogió las prácticas y creencias de los encuestados en sus interacciones con los canales digitales y sus productos financieros; la segunda, abordó el experimento que evaluó la sensibilidad de los encuestados a mensajes de prevención y la tercera, obtuvo los datos demográficos correspondientes.

Perfiles de los usuarios digitales del sistema financiero

En la primera sección del estudio se utilizó un análisis de correspondencia múltiple y de clúster jerárquico que dio como resultado cuatro dimensiones de encuestados. Estos grupos se categorizaron según su confianza en las transacciones digitales, el número de transacciones en línea que realizan habitualmente y su comportamiento frente a preguntas anzuelo como: “Si te ofrecen una inversión con rentabilidad del 5% mensual, tú…”. En la tabla 1 se ilustran los resultados de este análisis.

Cabe resaltar que los usuarios arriesgados (que son el 20% del total de la muestra) y los usuarios prudentes (32%) son los que más realizan transacciones bancarias en internet, mientras que los prevenidos (36%) e inexpertos desconfiados (13%) son los que menos realizan este tipo de operaciones.

Así, el primer resultado de la investigación es la correlación entre un mayor uso y confianza en las transacciones digitales, y una mayor propensión a caer en fraude por descuidos en la higiene digital. Esta correlación implica directamente a los perfiles denominados usuarios arriesgados y usuarios prudentes, que paradójicamente son quienes tienen un nivel educativo más alto. Esto nos conduce a pensar que las personas descuidan sus hábitos digitales seguros una vez obtienen mayor experiencia en el uso de sus productos financieros digitales.

Por lo tanto, construir una cultura digital segura es un proceso que no se logra a medida que los consumidores financieros son más autónomos y conocedores en el uso de medios digitales para completar sus transacciones bancarias. La clave está entonces en desarrollar mejores campañas de prevención, que sean diferenciadas, para que se impacte exógenamente los hábitos digitales de las personas.

[3] Modalidad para el robo de información personal o financiera por medio de correos o mensajes de texto con enlaces hacía páginas web falsas que suplantan a entidades para obtener credenciales.
[4] Barranquilla, Bogotá, Cali y Medellín, en donde el 20% de los participantes contaba con educación secundaria, otro 20% con educación técnica o tecnológica, y el resto, con educación universitaria (37%) o posgraduada (22%). Además, 64% de los encuestados fueron mujeres.

Tabla 1. Perfiles de usuarios digitales del sistema financiero según comportamiento

Usuarios Arriesgados	Usuarios Prudentes	Prevenidos	Inexpertos desconfiados
Son los que realizan más de 10 transacciones por internet al mes. Usan la sucursal virtual	Realizan con frecuencia transacciones por internet, entre 1 y 4 al mes.	Realizan transacciones por internet con poca frecuencia	Realizan pocas o ninguna transacción financiera o compras por internet
Son autónomos para hacer transacciones y valoran ser arriesgados con el dinero	Son autónomos para hacer transacciones y valoran ser prudentes con el dinero	Perciben que el sistema financiero y las transacciones por internet son inseguras	Radicales en su desconfianza hacia el sistema financiero o de realizar compras/pagos por internet
Perciben que el sistema financiero y las transacciones por internet son seguras	Perciben que el sistema financiero y las transacciones por internet son seguras	Por lo general confían poco en las demás personas	Por lo general desconfían en las demás personas
En general confían en los demás	En general confían en las demás personas	Valoran ser prudentes con el dinero y piden apoyo para hacer transacciones digitales	Piden ayuda para transacciones digitales. Prefieren ser prudentes frente a temas relacionados con dinero
Los más conectados, permanecen más de 5 horas conectados a internet	Conscientes de que caer en fraude digital depende de ellos	Son más tradicionales, usan la mente para guardar claves, tienen antivirus gratuito	Permanece menos de 1 hora conectado
Tienen comportamientos inseguros (utilizan la misma clave, utilizan redes públicas)	Permanecen entre 1 y 4 horas conectados a internet	Creen que es probable que sean víctimas de fraude digital, pero creen que no depende de ellos	Creen probable que sean víctimas de fraude digital
Es el grupo con más victimas			

Fuente: Sensata Research UX. Elaboración Asobancaria

Por lo mismo, a fin de que las personas se sensibilicen en el uso de las herramientas digitales y se concienticen de la importancia de cuidar sus datos, las campañas de prevención deben tener en cuenta los distintos perfiles digitales de los usuarios. Esto, haciendo referencia a que existen diferentes mecanismos comportamentales que funcionan de manera distinta para cada persona, según su propensión, percepción y actitud frente al fraude.

El experimento

Dados los datos recogidos en la primera sección del estudio, el experimento aleatorizó el uso de mensajes comunes de *priming*[5] utilizados en campañas de prevención del fraude a los cuatro grupos de usuarios descritos en la primera sección del ejercicio. Es importante resaltar la existencia de un porcentaje de encuestados al que no se le mostró ningún mensaje, con la intención de contar con un grupo de tratamiento o control. El objeto de esta sección del ejercicio fue explorar qué tipo de información particular genera mayor atención entre los participantes y, en ese sentido, cómo esta información afectaría a la conducta de prevención del fraude.

Los mensajes de *priming* mostrados estuvieron enfocados en conocer la sensibilidad de las respuestas de los participantes de las siguientes formas: i) conociendo el monto promedio de los fraudes en Colombia; ii) la frecuencia con que ocurren y; iii) el hecho de que estos ocurren sólo cuando los clientes no tienen una buena higiene digital.

Una vez los encuestados recibían esta información, se enfrentaban a una serie de situaciones hipotéticas donde podían ser víctimas de fraude o no según su respuesta. Se propusieron situaciones recurrentes como, por ejemplo, ataques de *phishing*, *smishing* o llamadas de ingeniería social[6]. Así mismo, se les preguntó a los participantes acerca de su propensión a cambiar la clave de su sucursal virtual de manera periódica, pues este es un hábito digital saludable que ayuda a evitar ser víctima de los ciber delincuentes.

Efecto alarma de carro y otras conclusiones

Los datos obtenidos en el experimento no identificaron diferencias significativas entre las respuestas de los grupos a los cuales se les expusieron los mensajes de *priming* y las del grupo de control.

[5] Mensajes de estímulos condicionantes utilizados en el neuromarketing para despertar mayor atención e interés en ciertos productos o acciones que promocionan las empresas.
[6] Tipo de fraude donde en una llamada telefónica los delincuentes se hacen pasar por una entidad para robar datos personales y financieros.

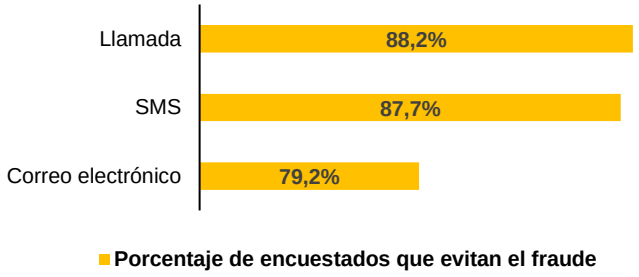
Tampoco hubo un resultado que mostrara una tendencia diferencial entre el comportamiento de los grupos según el mensaje mostrado.

Esto sugiere que la estrategia de advertir los riesgos de descuidar la información personal y financiera en el mundo digital no está teniendo el efecto de cambiar las actitudes de las personas frente al fraude.

La razón, según el análisis, es el efecto 'alarma de carro'. A este efecto se le conoce con este nombre ya que las personas, a pesar de ser conscientes del estímulo, el ruido de la alarma o el mensaje de *priming*, no incorporan la información que les llega en su toma de decisiones, es decir, ignoran el evento. La sobreexposición mediática ante los riesgos de perder los datos personales y financieros en el ciberespacio ha hecho que las personas dejen de prestar atención a estas alertas en las campañas, así como no se presta atención al ruido de la alarma de un carro en el vecindario.

En el estudio se encontró adicionalmente que el canal por donde llega el fraude puede hacer la diferencia. La probabilidad de evitar el fraude fue alrededor de un 10% menor en los casos donde se planteaba como canal el correo electrónico con enlaces fraudulentos (*phishing*), en comparación con una llamada telefónica o mensaje de texto. Este hecho puede ser apreciado en el gráfico 1:

Gráfico 1. Porcentaje de encuestados que evitan el fraude según el canal



Fuente: Sensata Research UX. Elaboración Asobancaria

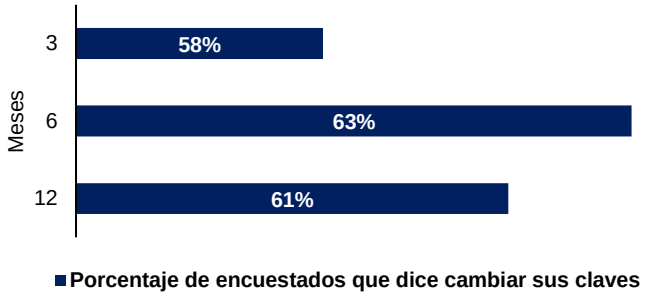
Otro resultado importante hace referencia al autoconocimiento de las personas acerca de sus vulnerabilidades. Las personas que reconocieron tener falencias en su comportamiento digital, precisamente, tuvieron una probabilidad mayor de caer en fraude en las situaciones hipotéticas propuestas. Esto invita a pensar que las campañas de sensibilización de los bancos pueden ser fácilmente enfocadas a los usuarios, consultándoles primero qué tan descuidados se consideran en la protección de sus datos.

Cabe mencionar que, según el desarrollo del experimento, se encontró que las mujeres tenían menor propensión a evitar el fraude, es decir, es menos probable que tomen la decisión de borrar, ignorar o colgar ante las situaciones hipotéticas planteadas. Por esta razón, una estrategia de sensibilización enfocada en mujeres ayudaría a esta población que es más vulnerable ante el riesgo de ser víctimas de fraude.

Como elemento adicional de la investigación, se pudo evidenciar el reto que significa para los usuarios tener el hábito de cambiar frecuentemente las contraseñas de sus productos financieros. Se encontró que, en el mejor escenario, sólo un 63% de los usuarios están dispuestos a cambiar su clave cada 6 meses, un 61% cada 12 meses y un 58% cada tres meses.

Es decir, 4 de cada 10 usuarios no están interesados o dispuestos a cambiar su clave frecuentemente, aun cuando fueron advertidos por los mensajes de *priming* de que hay más probabilidades de ser víctima de fraude si no se tiene esta buena práctica. En el gráfico 2 puede observarse cada cuántos meses los encuestados cambian su contraseña:

Gráfico 2. ¿Cada cuántos meses cambia la clave de sus productos financieros?



Fuente: Sensata Research UX. Elaboración Asobancaria

En este mismo sentido, las personas que decían no cambiar frecuentemente sus claves y utilizar la misma clave en diferentes cuentas, caían con más probabilidad en las situaciones hipotéticas de fraude. De hecho, cerca del 75% de las personas que argumentaban tener esta mala práctica, eran significativamente más susceptibles a picar el anzuelo del fraude y solo el 27% de los que contestaron no tener este mal hábito cayó en fraude en el experimento.

Lecciones aprendidas: Aceleradores y frenos

Según el enfoque de Kurt Lewin (1951)[7] para encontrar los determinantes de una conducta deseada existen aceleradores y frenos para consolidar una cultura de hábitos financieros digitales seguros.

[7] Lewin, K (1951). *Field Theory in Social Science*. Harper & Row, New York.

Según esta teoría, el comportamiento deseado se explica en función de las características de percepción y conducta del individuo, y las de su entorno.

Entre los aceleradores para la conducta deseada se destaca la apreciación acertada de los usuarios al saberse más vulnerables frente al fraude digital. Característica que, como ya mencionamos, puede ser aprovechada para dirigir más eficientemente las campañas de sensibilización a aquellos usuarios que más las necesitan.

Por otro lado, según conjeturas basadas en ciencias del comportamiento, sale a relucir como acelerador el sesgo de disponibilidad[8] y como freno las cargas cognitivas[9].

La presencia del sesgo de disponibilidad establece que el comportamiento de las personas cambia en caso de tener una experiencia cercana frente al fraude. El efecto de este sesgo se relaciona entonces con el cambio en la percepción de ocurrencia de un evento si la persona ve que éste se materializó en un ambiente cercano a su entorno. Por esto, se debe resaltar que, según esta teoría, cuando las personas van a tomar una decisión (tomar o no medidas de seguridad digital), dan mayor valor a la información más reciente y de mayor impacto emocional, asociada a eventos que ellos o su círculo más cercano han experimentado.

La carga cognitiva hace referencia a la disposición de los usuarios por cambiar y complejizar sus claves. Cómo se demostró en esta investigación, las personas que no tienen este hábito digital tienen mayor probabilidad de caer en fraude. En consecuencia, es tarea de las campañas de sensibilización reducir este sesgo. Conviene destacar entonces que esta teoría se basa en señalar que nuestra memoria de trabajo tiene una capacidad limitada, por lo que las campañas de prevención deben buscar vender la idea del poco trabajo que genera para el usuario cambiar y complejizar sus claves constantemente.

Igualmente, el efecto alarma de carro de los mensajes de *priming* es uno de los principales frenos para el objetivo planteado. Esta es una conclusión que nace de la sobreexposición a advertencias y noticias relacionadas al fraude con las que constantemente son bombardeados los consumidores financieros. Por esto, se debe redirigir el lenguaje de las campañas para que se enfoquen en los aspectos positivos de ser un buen usuario de la banca con humor e interactividad. Un enfoque interesante es retar al usuario a ser cada vez mejor en el mundo digital, esto se podría realizar al crear arquetipos de usuarios PRO (*Tech Savvy*), conocedores del mundo digital. De esta forma se pasa del miedo al entendimiento de que el usuario está en control de sus acciones.

Por último, hay mayores frenos para el comportamiento deseado en ciertos canales que en otros. Según el diseño del experimento, se evidenció que las personas son más prevenidas cuando reciben llamadas de ingeniería social que cuando les llegan correos o mensajes de texto fraudulentos. Por lo tanto, las campañas de sensibilización deben correlacionar sus esfuerzos en los usuarios más vulnerables y en los canales en los que más están siendo víctimas.

Conclusiones y recomendaciones finales de la investigación

Para futuras campañas de prevención se tienen las siguientes recomendaciones según el estudio realizado:

1. Dejar de utilizar palabras relacionadas con fraude y ciberdelincuencia

Esto se debe a que hablar de fraude digital, ciberdelincuencia o ciberseguridad despierta desconfianza en las personas debido a que estas no poseen herramientas cognitivas suficientes para distinguir de fuentes confiables o no. Por esta razón, al escuchar hablar de estos temas directamente tratan de evadir la información.

Lo anterior se deriva en un fenómeno de alarma de carro en torno al problema de fraude digital y los mensajes de *priming* que tienen las campañas de prevención que lo mencionan directamente.

La combinación de agotamiento, carga cognitiva y sesgos que filtran la información, crea una capa impermeable a los mensajes de alerta al fraude.

2. Centrar las campañas en crear y difundir unos arquetipos de usuarios PRO (*Tech Savvy*)

La idea detrás de esta recomendación se basa en cambiar la conversación, pasando del miedo a la delincuencia al locus de control interno por ser un usuario PRO. Es decir, dar el empoderamiento al usuario de que si no ha caído en fraude es porque ha tenido buenos hábitos de seguridad en sus transacciones digitales.

Para lograr esto, es necesario construir campañas de prevención que promuevan estos arquetipos positivos. Arquetipos de usuarios que confían en el sistema financiero y simultáneamente tienen buenas prácticas de autocuidado. Además, enfatizar en que no es difícil ser un usuario PRO, haciendo evidente qué prácticas se debe tener para llegar a este estatus.

3. Tener estrategias diferenciadas por perfil

Al planear campañas de sensibilización se deben tener en cuenta los perfiles actitudinales y las vulnerabilidades de los usuarios a las que se dirigen. Aprovechar el autoconocimiento de los usuarios para saberse vulnerables puede ser una buena idea para definir campañas adaptativas que reconozcan la diversidad de perfiles de usuarios según su exposición al fraude en el sistema financiero.

[8] Tversky, A.; Kahneman, D. (1973). *Availability: A heuristic for judging frequency and probability*. Cognitive Psychology. 5 (2): 207–232.
[9] Sweller, J., van Merrienboer, J., & Paas, F. (1998). *Cognitive architecture and instructional design*. Educational Psychology Review, 10, 251-296.

4. Campañas digitales adaptativas y dinámicas

Una estrategia que resume las anteriores recomendaciones es construir campañas de prevención basadas en ejercicios de gamificación sobre cómo ser un usuario PRO, teniendo como foco dar una experiencia digital con una retroalimentación inmediata.

Las campañas que tomen esta recomendación como referencia deberán tener en cuenta las lecciones aprendidas en esta investigación. Es decir, aprovechar los aceleradores del comportamiento deseado y hacer frente a sus frenos.

En conclusión, las campañas de concientización para crear una cultura digital saludable en el sector financiero se deben reformular hacia estrategias que se enfoquen en interactividad, adaptabilidad y arquetipos como los del usuario PRO.

Colombia

Principales indicadores macroeconómicos

	2020					2021					2022	
	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	**T1**	**Total (p)**
Producto Interno Bruto												
PIB Nominal (COP Billones)	259,9	212,2	248,0	278,5	**998,7**	267,7	268,5	305,1	335,9	**1177,2**	326,8	**1345,6**
PIB Nominal (USD Billones)	73,1	55,0	66,4	76,5	**271,3**	74,7	72,4	79,3	87,5	**303,9**	82,2	**352,1**
PIB Real (COP Billones)	207,7	179,4	203,1	228,9	**819,1**	209,6	212,3	231,0	253,7	**906,6**	227,5	**965.5**
PIB Real (% Var. interanual)	0,8	-16,6	-8,8	-3,6	**-7,0**	0,9	18,3	13,7	10,8	**10,7**	8,5	**6.5**
Precios												
Inflación (IPC, % Var.)	3,7	2,9	1,9	1,6	**2,5**	1,6	2,9	4,3	5,2	**3,5**	7,5	**8,4**
Inflación sin alimentos (%)	3,3	2,2	1,5	1,2	**2,0**	1,0	2,1	3,0	3,1	**2,3**	4,8	**16,4**
Tipo de cambio (COP/USD	3535	3845	3729	3661	**3693**	3552	3690	3844	3878	**3742**	3913	**3822**
Tipo de cambio (Var. %)	12,7	18,6	11,7	7,5	**12,5**	0,4	-4,0	3,1	5,9	**1,3**	10,1	…
Sector Externo (% del PIB)												
Cuenta corriente (USD	-2286	-1933	-2000	-2988	**-9207**	-2937	-3,966	-4794	-6136	**-17833**	**-5367**	**-11133**
Cuenta corriente (%PIB)	-3,1	-3,5	-3,1	-3,9	**-3,4**	-3,9	-5,5	-6,0	-7,0	**-5,7**	**-6,5**	**-4,4**
Balanza comercial (%PIB)	-3,1	-2,8	-3,3	-3,7	**-3,3**	-3,5	-4,9	-4,7	-4,7	**-4,4**	…	**-1,0**
Exportaciones F.O.B.	12,4	12,4	11,9	11,1	**11,9**	12,4	13,2	14,0	14,7	**13,6**	…	**18,6**
Importaciones F.O.B.	15,5	15,5	15,2	14,8	**15,2**	15,9	18,1	18,6	19,4	**18,0**	…	**19,6**
Renta de los factores	-1,8	-1,8	-1,7	-1,8	**-1,8**	-2,2	-2,0	-2,6	-3,3	**-2,6**	…	**-4,4**
Transferencias corrientes	3,0	3,1	3,6	3,2	**3,2**	3,3	3,6	3,5	3,3	**3,4**	…	**3,3**
Inversión extranjera directa (pasivos) (%PIB)	4,3	2,5	-1,3	2,7	**2,8**	3,2	2,8	3,6	2,5	**3,0**	…	**3,1**
Sector Público												
Bal. primario del Gobierno	0,3	-3,2	…	…	**-5,9**	**…**	**…**	…		**-3,7**	…	**-2,9**
Bal. del Gobierno Nacional	-0,2	-5,8	…	…	**-7,8**	…	**…**	…		**-7,1**	…	**-6,5**
Bal. estructural del Gobierno	…	…	…	…	**…**	**…**	**…**	…		**…**	…	…
Bal. primario del SPNF	0,4	-3,0	…	…	**-6,7**	**…**	**…**	…		**-4,4**	…	**-4,0**
Bal. del SPNF	0,4	-5,2	…	…	**-9,4**	**…**	**…**	…		**-7,4**	…	**-7,1**
Indicadores de Deuda (%												
Deuda externa bruta	47,4	49,3	…	…	…	…	51,7	…	…	…	…	**31,5**
Pública	25,3	26,6	…	…	…	…	30,2	…	…	…	…	
Privada	22,1	22,6	…	…	…	…	21,5	…	…	…	…	
Deuda bruta del Gobierno	60,3	62,4	66,2	64,8	**64,7**	61,5	64,2	…	…	**63,8**	…	**63,0**

Colombia

Estados financieros del sistema bancario

	abr-22 (a)	mar-22	abr-21 (b)	Variación real anual entre (a) y (b)
Activo	**842.582**	**824.586**	**744.910**	**3,6%**
Disponible	63.507	58.756	52.927	9,8%
Inversiones y operaciones con derivados	166.377	162.827	160.717	-5,2%
Cartera de crédito	579.136	569.014	507.784	4,4%
Consumo	181.670	178.419	152.154	9,3%
Comercial	296.511	290.710	267.575	1,4%
Vivienda	86.448	85.572	75.176	5,3%
Microcrédito	14.507	14.313	12.878	3,1%
Provisiones	35.441	35.504	37.434	-13,3%
Consumo	12.545	12.422	12.705	-9,6%
Comercial	17.338	17.441	17.365	-8,6%
Vivienda	3.122	3.076	2.779	2,9%
Microcrédito	880	873	1.126	-28,4%
Pasivo	**750.603**	**733.881**	**652.626**	**5,3%**
Instrumentos financieros a costo amortizado	649.893	636.760	574.075	3,6%
Cuentas de ahorro	290.382	290.644	254.909	4,3%
CDT	156.058	148.667	144.913	-1,4%
Cuentas Corrientes	85.097	84.260	76.954	1,2%
Otros pasivos	10.282	10.040	8.715	8,0%
Patrimonio	**91.979**	**90.705**	**92.283**	**-8,8%**
Ganancia / Pérdida del ejercicio (Acumulada)	**6.366**	**4.959**	**3.259**	**78,8%**
Ingresos financieros de cartera	16.884	12.338	13.670	13,1%
Gastos por intereses	4.883	3.396	3.189	40,2%
Margen neto de Intereses	12.595	9.358	10.861	6,2%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**3,77**	**3,80**	**4,86**	**-1,10**
Consumo	4,42	4,35	5,96	-1,54
Comercial	3,52	3,61	4,48	-0,96
Vivienda	2,86	2,90	3,59	-0,74
Microcrédito	6,10	6,14	7,36	-1,26
Cubrimiento	**162,5**	**164,3**	**151,6**	**-10,84**
Consumo	156,3	160,2	140,2	16,16
Comercial	166,1	166,2	145,0	21,11
Vivienda	126,4	123,8	102,8	23,62
Microcrédito	99,6	99,4	118,8	-19,25
ROA	2,28%	2,43%	1,32%	1,0
ROE	22,23%	23,73%	10,97%	11,3
Solvencia	16,23%	16,23%	20,10%	-3,9

Colombia
Principales indicadores de inclusión financiera

	2016	2017	2018	2019	2020				2020	2021			
	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4
Profundización financiera - Cartera/PIB (%) EC	**50,2**	**50,1**	**49,8**	**49,8**	51,7	54,3	…	…	**…**				
Efectivo/M2 (%)	**12,59**	**12,18**	**13,09**	**15,05**	13,35	14,48	…	…	**…**				
Cobertura													
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,7**	**100**	**99,2**	**99,9**	100	100	100	100	**100**	100	100	100	100
Municipios con al menos una oficina (%)	**73,9**	**73,9**	**74,4**	**74,6**	74,6	74,6	74,6	...	**78,6**				
Municipios con al menos un corresponsal bancario (%)	**99,5**	**100**	**98,3**	**100**	100	100	100	100	**100**				
Acceso													
Productos personas													
Indicador de bancarización (%) SF*	**77,30**	**80,10**	81,4	**82,5**	83,2	85,9	87,1	87,8	**87,8**	**89,4**	**89,4**	**89,9**	**90,5**
Indicador de bancarización (%) EC**	**76,40**	**79,20**	80,5	**81,6**	…	…	86,6	…	**…**	**88,9**	**…**	**89,5**	**…**
Adultos con: (en millones)													
Cuentas de ahorro EC	**23,53**	**25,16**	25,75	**26,6**	…	…	27,5	27,9	**27,9**	**28,4**	**28,3**	**28,5**	**28,9**
Cuenta corriente EC	**1,72**	**1,73**	1,89	**1,97**	…	…	1,92	1,9	**1,9**	**1,9**	**1,9**	**1,9**	**1,9**
Cuentas CAES EC	**2,83**	**2,97**	3,02	**3,03**	…	…	3,03	…	**3,0**	**3,0**	**3,0**	**3,0**	**…**
Cuentas CATS EC	**0,10**	**0,10**	0,71	**3,30**	…	…	7,14	8,1	**8,1**	**9,2**	**10,5**	**11,8**	**…**
Otros productos de ahorro EC	**0,77**	**0,78**	0,81	**0,85**	…	…	0,84	…	**…**	**…**	**0,8**	**0,7**	**…**
Crédito de consumo EC	**8,74**	**9,17**	7,65	**8,42**	…	…	…	…	**…**	**…**	**6,9**	**6,9**	**6,9**
Tarjeta de crédito EC	**9,58**	**10,27**	10,05	**10,53**	…	…	10,59	…	**…**	**…**	**8,1**	**7,7**	**7,9**
Microcrédito EC	**3,56**	**3,68**	3,51	**3,65**	…	…	…	…	**…**	**…**	**2,4**	**2,3**	**2,3**
Crédito de vivienda EC	**1,39**	**1,43**	1,40	**1,45**	…	…	…	…	**…**	**…**	**1,1**	**1,2**	**1,2**
Crédito comercial EC	**1,23**	**1,02**	…	**0,70**	…	…	…	…	**…**	**…**	**0,5**	**0,4**	**…**
Al menos un producto EC	**25,40**	**27,1**	27,64	**29,1**	…	…	…	32	**32**	**32,7**	**32,9**	**33,1**	**33,5**
Uso													
Adultos con: (en porcentaje)													
Algún producto activo SF	**66,3**	**68,6**	68,5	**66,0**	66,8	71,6	73,0	72,6	**72,6**	**74,4**	**74,6**	**75,5**	**74,8**
Algún producto activo EC	**65,1**	**66,9**	67,2	**65,2**	…	…	72,4	…	**…**	**…**	**…**		**…**
Cuentas de ahorro activas EC	**72,0**	**71,8**	68,3	**70,1**	…	…	65,4	…	**64,2**	**62,2**	**65,3**	**65,8**	**65,7**
Cuentas corrientes activas EC	**84,5**	**83,7**	85,5	**85,6**	…	…	82,8	…	**82,3**	**82,3**	**80,2**	**78,5**	**73,7**
Cuentas CAES activas EC	**87,5**	**89,5**	89,7	**82,1**	…	…	82,1	…	**82,1**	**82,1**	**82,1**	**82,1**	**…**
Cuentas CATS activas EC	**96,5**	**96,5**	67,7	**58,3**	…	…	80,8	…	**74,8**	**73,0**	**73,8**	**75,2**	**…**
Otros pdtos. de ahorro activos EC	**66,6**	**62,7**	61,2	**62,8**	…	…	63,8	…	**…**	**…**	**64,6**	**75,6**	**…**
Créditos de consumo activos EC	**82,0**	**83,5**	82,2	**75,7**	…	…	…	…	**…**	**…**	**…**	**…**	**…**
Tarjetas de crédito activas EC	**92,3**	**90,1**	88,7	**79,5**	…	…	76,7	…	**…**	**…**	**…**	**…**	**…**
Microcrédito activos EC	**66,2**	**71,1**	68,9	**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	T2	T3	T4
Créditos de vivienda activos EC	**79,3**	**78,9**	**77,8**	**78,2**	…	…	…	…	**…**	…	…	…	…
Créditos comerciales activos	**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**	926,4	924,3	923,8	1023,6
Cuenta de ahorro EC	**500,8**	**522,7**	**649,4**	**649,1**	648,5	637,1	637,1	639,8	**639,8**	644.0	642,2	645,4	734,6
Cuenta corriente EC	**420,9**	**430,7**	**502,9**	**499,7**	492,8	491,6	488,7	491,3	**491,3**	489,0	489,3	489,2	510,5
Otros productos de ahorro EC	**15,24**	**14,12**	**13,9**	**13,8**	15,4	16,0	14,9	…	**15,3**	14,9	14,6	14,5	…
Crédito comercial EC	**242,5**	**243,6**	**277,8**	**285,9**	288,3	291,3	…	…	**…**	…	219,4	215,6	211,6
Crédito de consumo EC	**98,72**	**102,5**	**105,8**	**104,9**	103,9	103,4	…	…	**…**	…	78,6	76,1	76,2
Tarjeta de crédito EC	**79,96**	**94,35**	**106,9**	**113,0**	114,1	113,9	…	…	**…**	…	92,7	91,1	91,9
Al menos un producto EC	**751,0**	**775,1**	**…**	**…**	…	…	…	…	**…**	…	287,4	282,8	280,2
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	**68,04**	…	…	…	…
			71,6	**68,36**	68,02	68,04	67,65	…	**68,07**	68,3	68,1	68,1	70,5
Algún producto activo SF	**74,7**	**73,3**											
			47,6	**45,8**	44,8	44,7	44,0	…	**…**	…	44,6	44,8	50,1
Cuentas de ahorro activas EC	**49,1**	**47,2**											
Otros pdtos. de ahorro activos EC	**57,5**	**51,2**	**49,2**	**52,0**	55,0	55,4	57,2	…	**…**	…	…	…	…
			89,0	**89,7**	90,7	91,0	91,1	…	**…**	…	91,6	91,9	92,5
Cuentas corrientes activas EC	**89,1**	**88,5**											
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**	4,938	…	6,221	…
No monetarias (Participación)	**48,0**	**50,3**	**54,2**	**57,9**	-	64,0	-	60,0	**61,7**	55,4	…	56,7	…
Monetarias (Participación)	**52,0**	**49,7**	**45,8**	**42,0**	-	36,0	-	40,0	**38,2**	44,6	…	43,3	…
No monetarias (Crecimiento	**22,22**	**16,01**	**25,1**	**38,3**	-	31,0	-	27,4	**28,9**	-8,7	…	12,4	…
Monetarias (Crecimiento anual)	**6,79**	**6,14**	**6,7**	**18,8**	-	1,3	-	17,2	**10,0**	30,5	…	29,3	…
Tarjetas													
Crédito vigentes (millones)	**14,93**	**14,89**	**15,28**	**16,05**	16,33	15,47	14,48	14,67	**14,67**	14,86	14,59	15,01	15,60
Débito vigentes (millones)	**25,17**	**27,52**	**29,57**	**33,09**	34,11	34,51	35,42	36,38	**36,38**	39,21	38,36	39,67	40,82
Ticket promedio compra crédito	**205,8**	**201,8**	**194,4**	**203,8**	176,2	179,3	188,6	207,8	**207,8**	197,6	208,2	201,4	219,9
Ticket promedio compra débito	**138,3**	**133,4**	**131,4**	**126,0**	113,6	126,0	123,6	129,3	**129,3**	116,77	118,1	114,5	124,9