



Seguridad bancaria en canales no presenciales: una ruta hacia la inclusión financiera

- El sistema financiero ha venido desarrollando nuevos canales transaccionales diferentes a la oficina tradicional que tienden hacia la masificación en el uso de medios electrónicos (Internet, telefonía móvil, pagos automáticos, audio respuesta). Estos nuevos canales han permitido avanzar en los procesos de inclusión financiera y en el mejoramiento de la calidad de vida de los ciudadanos.
- Los avances tecnológicos han permitido masificar los canales electrónicos, pero también imponen desafíos importantes en materia de seguridad. Pese a que la tecnología ha venido siendo usada también por los delincuentes para sofisticar las amenazas de hurto a los bancos y a los usuarios, la banca viene respondiendo muy bien a los retos que impone esta nueva realidad. Para esto, invierte cuantiosos recursos y dispone de mecanismos de seguridad robustos que pone a disposición de los clientes para mitigar los riesgos de fraude.
- Los usuarios todavía tienen muchos temores de utilizar los canales electrónicos en remplazo de la oficina tradicional y de allí la importancia que la gente comprenda que los canales electrónicos cuentan con herramientas de seguridad para tratar de evitar, en lo posible, la materialización de los hurtos. El riesgo de ser hurtado es realmente bajo y, en muchas ocasiones, el banco reintegra los recursos.
- La Asociación Bancaria reitera la importancia de que los usuarios adopten prácticas seguras en el manejo de su información al momento de realizar sus transacciones en canales no presenciales. Se debe sensibilizar a la población sobre los riesgos de revelar su información personal y financiera, pues esta permite a los delincuentes realizar los hurtos. Se está atravesando por una etapa de cambio en los hábitos de consumo y, en general, de la cotidianidad, lo que ha tornado imprescindible para gran parte de la población el uso de la tecnología para el desempeño de sus actividades.
- Es importante trabajar en transformar los hábitos de los usuarios del sistema financiero, resaltando el hecho de que el uso de canales electrónicos es idóneo para fomentar la transaccionalidad y reducir el uso del efectivo. El uso responsable de los productos y canales transaccionales ofrecidos por la banca, por parte de los clientes/usuarios del sector financiero, significará grandes beneficios no solo a nivel de individuo sino para la sociedad en su conjunto.

6 de Julio de 2015

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente**Jonathan Malagón**
Vicepresidente Técnico**Germán Adolfo Montoya**
Director Económico

Para suscribirse a Semana Económica, por favor envíe un correo electrónico a semanaeconomica@asobancaria.com o visítenos en <http://www.asobancaria.com>

Visite nuestros portales:
www.asobancaria.com
www.cuadresubolsillo.com
www.abcmicasa.com



Seguridad bancaria en canales no presenciales: una ruta hacia la inclusión financiera

Las entidades bancarias han puesto a disposición de los usuarios del sistema financiero los avances tecnológicos para el desarrollo de nuevos canales transaccionales que rebasan las funcionalidades de las oficinas tradicionales y que tienden hacia la masificación en el uso de medios electrónicos (Internet, telefonía móvil, pagos automáticos, audio respuesta). Estos canales le permiten al cliente realizar consultas, transferencias, pagos a terceros y compras de bienes y servicios utilizando su computador personal, tablet o celular, en cualquier lugar, las 24 horas del día, los 365 días del año.

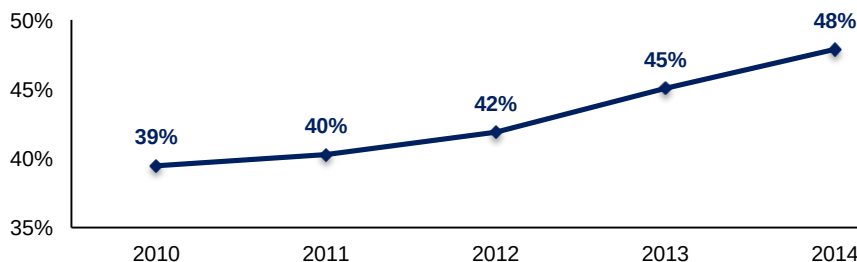
Estos avances traen consigo múltiples beneficios para el cliente, al contar no solo con una oficina sin límites de horario que le evite desplazamientos y filas, sino también mayor agilidad, rapidez y seguridad en los procesos. Por su parte, los costos asociados a la prestación de servicios financieros a través canales no presenciales son menores, lo que ayuda a masificar los productos que ofrece la banca y a facilitar su acceso a través de menores tarifas.

Esta Semana Económica reflexiona sobre el papel de la seguridad en la inclusión financiera, al tiempo que aborda los principales temores de los usuarios y los contrasta con las recientes estadísticas del sector.

El desarrollo de los canales virtuales como promotor de la inclusión financiera

Indiscutiblemente, en los últimos años Colombia ha avanzado en el propósito de aumentar el número de personas con acceso a productos financieros. De acuerdo con el índice de bancarización de Asobancaria, para finales de 2014 el 72.5% del total de la población adulta del país tenía al menos un producto financiero. Una de las estrategias que ha contribuido con este éxito es la disposición, la promoción y el uso de los canales virtuales, los cuales han mostrado una alta actividad durante los últimos años (Gráfico 1).

Gráfico 1. Uso de canales no presenciales (% total operaciones)



Fuente: Superintendencia Financiera de Colombia, cálculos realizados por Asobancaria. Se entienden por canales no presenciales internet, ACH, pagos automáticos, telefonía móvil y audiorespuesta.

Editor

Germán Adolfo Montoya
Director Económico

Participaron en esta edición:

Ginna Alexandra Pardo
Manuel Alberto Serna
Julian David Velasco
Sergio Ricardo Rodríguez



Según las cifras de la Superintendencia Financiera, en 2010 se realizaron 968 millones de operaciones a través de canales no presenciales, las cuales representaron el 39% del total, mientras que en el 2014 se efectuaron 1.779 millones de operaciones (48% del total), lo que evidencia un crecimiento del 84% en cuatro años. Asimismo, se observa que los montos de las operaciones realizadas por estos canales han crecido constantemente durante los últimos cinco años, pasando de \$ 1.9 billones en 2010 a \$ 2.7 billones en 2014, lo cual indica un crecimiento del 47% (Gráfico 2).

Si se discriminan los canales no tradicionales, se encuentra que la penetración de la telefonía celular, al corte del tercer trimestre de 2014, alcanzó el 112.4% y la del internet el 21.7%, todo ello en medio de una tendencia creciente desde 2004¹. Este escenario es propicio para que los usuarios del sistema financiero tiendan, aún más, a desplazarse al uso de canales como la banca móvil o a los portales virtuales de los bancos (Gráfico 3).

Además, la disposición, promoción y uso de esos canales virtuales ayuda en la disminución del sobre uso del dinero en efectivo por parte de la población, que resulta costoso para todos los actores de la economía no solo debido a los costos asociados a la impresión del papel moneda, sino por los asociados al transporte, almacenamiento y custodia del mismo.

En este sentido, la Asociación Bancaria ha venido señalando que el uso del efectivo trae importantes implicaciones en términos de bienestar social, pues incentiva a las empresas a mantenerse en la informalidad. Además, facilita las actividades económicas ilegales, el lavado de activos, la financiación del terrorismo y la evasión de impuestos.

Según los resultados del Global Findex 2014, el efectivo es el medio de pago preferido por los colombianos para el pago de servicios públicos (99%), de matrículas escolares (93%) o para la recepción de salario (47%). En relación al uso del celular para realizar pagos, Colombia tiene un gran reto en cuanto a la masificación del uso de este canal, ya que en ninguno de los casos anteriores supera el 1% del uso². En este sentido, el 54% de las personas encuestadas en el último estudio de inclusión financiera

Gráfico 2. Monto y número total de operaciones en canales no presenciales

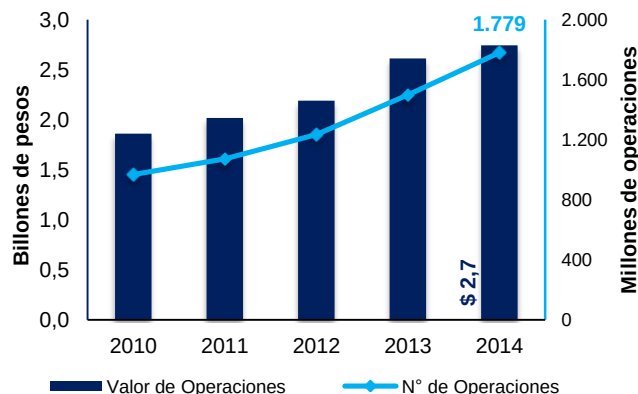
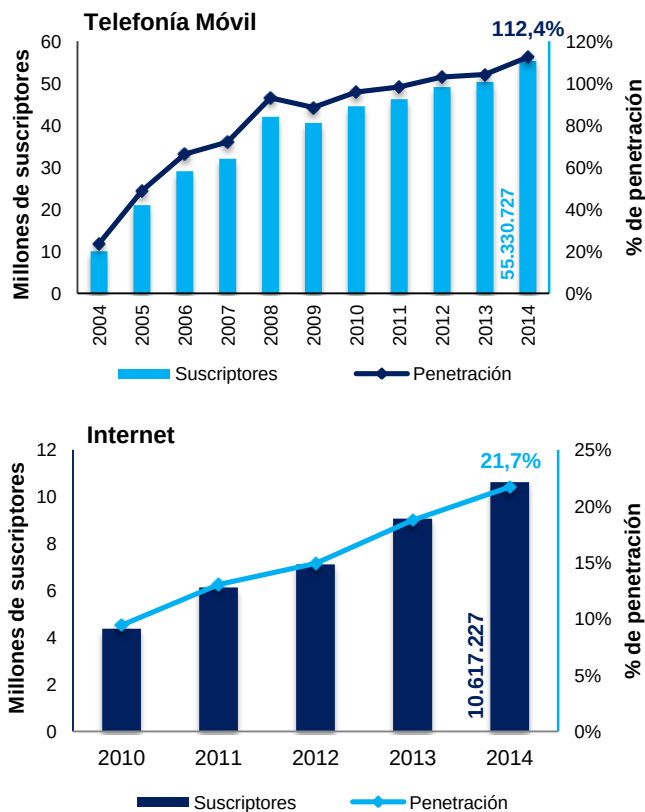


Gráfico 3. Suscriptores e índice de penetración en servicios de telefonía móvil e internet



¹ Ministerio de Tecnologías de la Información y las Comunicaciones, Boletín Trimestral, 3er Trimestre de 2014.

² Banco Mundial (2015) Global Findex.

Fuente: Superintendencia Financiera de Colombia, cálculos Asobancaria.



realizado por Banca de las Oportunidades y la Superintendencia Financiera de Colombia afirmaron manejar todo su dinero en efectivo y el 18% manifestaron realizar la mayoría de sus transacciones en efectivo.

Seguridad: un requisito para el crecimiento en el uso de canales no presenciales

El crecimiento en la oferta de canales transaccionales no presenciales también genera desafíos importantes en términos de prevención de fraude. Así como la tecnología incentiva y promueve el acceso al sistema financiero, también facilita los ataques cibernéticos. Mediante el uso de nuevas y mejores herramientas tecnológicas, cada vez se conocen nuevas tipologías que utilizan la falta de conocimiento o el descuido del usuario para obtener información privilegiada y realizar hurtos.

Por supuesto, la seguridad bancaria siempre ha sido un frente importante de trabajo para los bancos, pues afecta directamente sus recursos, pero, sobre todo, afecta a los de los clientes e impacta la confianza en el sector financiero. Es por esto que las entidades bancarias realizan innumerables esfuerzos para desarrollar canales transacciones confiables y seguros, que proporcionen al cliente el mínimo riesgo de ser víctimas de la delincuencia común.

En la actualidad, la banca colombiana invierte alrededor de USD 120 millones anuales para garantizar la seguridad en los canales que ponen a disposición de los clientes. Específicamente, en los canales no presenciales, se dispone de altos niveles de seguridad, como el fortalecimiento de los mecanismos de autenticación en canales virtuales con claves dinámicas, perfilamiento transaccional de cada uno de sus clientes para identificar operaciones inusuales, monitoreo y notificación en línea de las operaciones realizadas (Tabla 1).

No obstante, a pesar de los ingentes esfuerzos realizados por la banca, el papel de los clientes en la prevención del fraude es fundamental para disminuir los riesgos. Es necesario que los usuarios adopten prácticas seguras al realizar sus operaciones financieras, así como en el manejo de su información y de sus medios transaccionales. Es evidente el hecho de que el ciudadano cuida más la billetera de bolsillo, que los datos de las tarjetas de crédito o los nombres de usuario y claves para acceder a los canales transaccionales. Es esta información la que precisamente les permite acceder a sus cuentas de ahorro o cupos de crédito y de allí la

Tabla 1. Mecanismos de autenticación y/o prevención de fraude

Mecanismo de autenticación y/o prevención de fraudes	Descripción
OTP (One Time Password) 	Consiste en la generación de una clave que funcionará únicamente para realizar una transacción. Si el cliente requiere realizar otra transacción, tendrá que esperar a que su banco le remita otra clave. Esta se puede generar a través de un token, del celular o por internet.
Pre autorizaciones o pre inscripciones	El cliente realiza la notificación a su banco sobre las transacciones que realizará y los beneficiarios de éstas. Pueden definirse límites para realizar estas transacciones.
Tarjetas virtuales	El cliente solicita a su banco que le asigne parte o la totalidad de su cupo en tarjeta crédito para realizar sus transacciones en medios electrónicos. Generalmente se hace con un valor inferior a la totalidad del cupo.
Notificaciones en línea	El cliente solicita a su banco que le notifique por medio de mensajes de texto SMS y/o correo electrónico sobre las transacciones realizadas con los productos del cliente (principalmente cuentas de ahorro, corriente y tarjetas crédito).
Perfilamiento transaccional	Se desarrollan complejos sistemas neuronales que permiten perfilar la transaccionalidad del cliente e identificar cuando, con sus productos financieros, se estén efectuando operaciones que no coincidan con su perfil

importancia en el manejo y cuidado de estos datos.

Por esto, todos los esfuerzos tecnológicos que se realicen para mejorar la seguridad no sirven de nada si los usuarios no tienen en cuenta algunas recomendaciones mínimas sugeridas al realizar sus transacciones financieras. De hecho, la adopción de mejores plataformas tecnológicas y de procesos y metodologías de autenticación han llevado a los delincuentes a profundizar las actuaciones basadas en el engaño. De esta manera, modalidades como el phishing, mediante la cual los delincuentes simulan un correo y/o una página de un banco para que los clientes entreguen su información, están la orden del día. (Tabla 2).

Es por esto que desde tiempo atrás, tanto los bancos como Asobancaria han venido trabajando insistentemente en estrategias de comunicación y sensibilización para



lograr que los usuarios adopten prácticas seguras al realizar sus transacciones financieras. No obstante, los sondeos muestran que, aun cuando los ciudadanos conocen las recomendaciones de seguridad, no las aplican rigurosamente.

Tabla 2. Modalidades utilizadas por delincuentes para obtener la información de los clientes

Concepto	Descripción
Phishing	Esta modalidad consiste en que los delincuentes suplantando el sitio web de la entidad con el fin de obtener la información personal y financiera (números de tarjetas y claves) y, mediante correo electrónico o ventanas emergentes, direccionan a los clientes a la página de internet suplantada donde le solicitan su información.
Smishing	Con esta práctica fraudulenta se hace uso de los mensajes de texto SMS y la ingeniería social para engañar a las personas con el fin de obtener la información personal y financiera.
Software espía (Malware o troyanos)	Los delincuentes instalan un software para monitorear las actividades que realiza el usuario del PC. Igualmente, tienen acceso a la información que el usuario teclea y a los contenidos de sus correos electrónicos.
Key logger	Mediante la utilización de software o hardware, los delincuentes buscan grabar el texto que escriben las personas en el teclado de sus PC.
Clonación	Corresponde al copiado no autorizado de la información contenida en la banda magnética de las tarjetas débito y crédito.

Por otro lado, los avances tecnológicos generan una enorme cantidad de retos en la investigación de estos delitos. La recolección y uso de la evidencia digital dista mucho de lo que sucede en el mundo físico, pues se requiere de conocimiento especializado y de la cooperación no solo entre entidades del orden nacional sino con otras jurisdicciones. Por esto, la banca le apuesta a la generación de conocimiento entre el sector financiero y las autoridades policiales y judiciales que permita dar a conocer las diferentes modalidades delictivas que afectan a los bancos y a sus usuarios. Además, se viene trabajando en la interacción con las autoridades policiales tanto de manera preventiva como en la entrega de pruebas para los procesos de judicialización.

RECUADRO 1.

Recomendaciones de seguridad en canales no presenciales

Algunas de las recomendaciones para realizar transacciones financieras y sensibilización frente a su corresponsabilidad en el uso de sus medios de pago no presencial son:

- Evite realizar operaciones en computadores públicos.
- No realice sus transacciones utilizando redes públicas inalámbricas.
- Para acceder a la página de la entidad financiera siempre digite su dirección de Internet (www.bancoabc.com.co); nunca lo haga a través de un link o enlace. Fíjese que la dirección electrónica de su banco empiece con "https". De igual manera su navegador presentará un ícono con un candado cerrado, verificando que la encriptación está activa.
- Nunca ingrese a la página de su entidad financiera por los enlaces o links que muestran los buscadores.
- Culmine la sesión con las opciones de salida segura que ofrece cada sitio web.
- No baje archivos o software de lugares poco confiables, descargue archivos únicamente de sitios conocidos.
- Considerar no válidos los mensajes de texto que llegan a su celular ofreciendo premios o solicitando sus datos personales.
- No realizar transacciones con su entidad financiera mediante números de teléfono que no conozca así hayan sido enviados directamente a su celular a través de un mensaje de texto.
- No ingresar a través de enlaces a su entidad financiera o a cualquier sitio que le solicite información personal o financiera.

Inseguridad de los canales virtuales, ¿un tema de percepción?

No es novedad que se hable de inseguridad en Colombia. Con cierta regularidad se evidencian y notifican hurtos a través de diferentes modalidades. La Banca y los usuarios del sistema financiero, desafortunadamente, no han sido ajenos a esta realidad.

Sin embargo, en estos asuntos, se genera un intenso debate sobre si la inseguridad es un tema de percepción o



si realmente el riesgo de sufrir algún tipo de hurto es efectivamente alto. En materia de delitos informáticos existen varias apreciaciones que desincentivan, por miedo, el uso de canales virtuales para realizar las transacciones.

Las siguientes dos percepciones en cuanto a la seguridad de canales electrónicos son, quizás, las más generalizadas:

1. Las amenazas de robo de información están dirigidas a las entidades financieras y, por lo tanto, existe la posibilidad de que los delincuentes obtengan los datos privados.

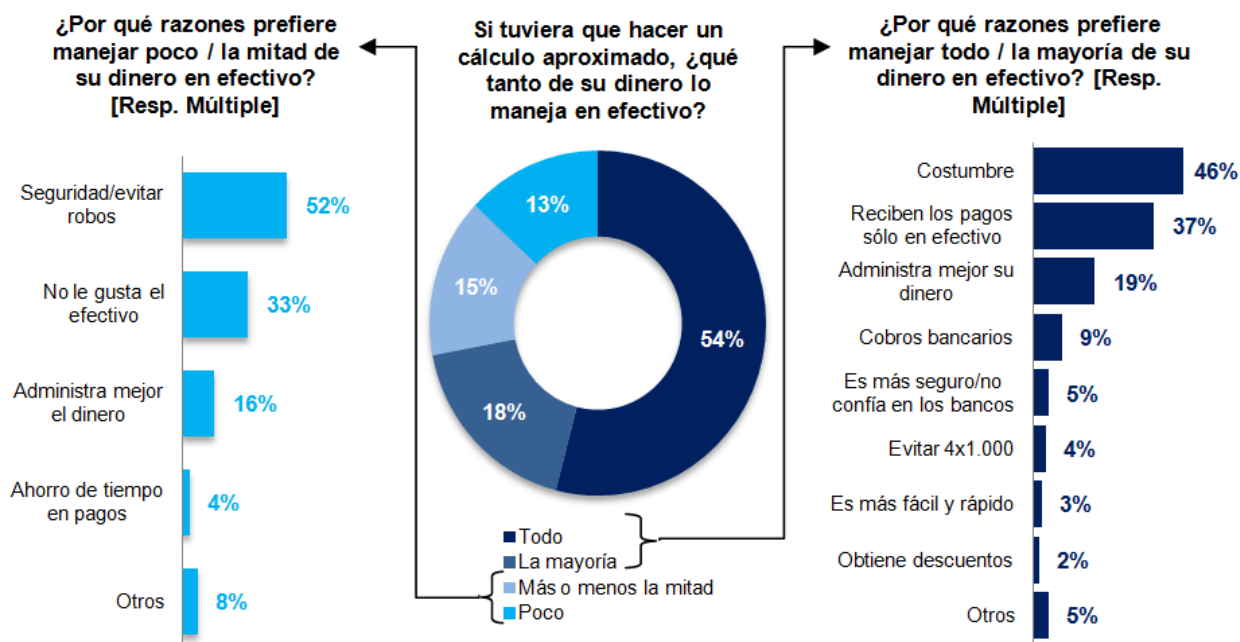
En efecto, la percepción de la población es que las amenazas de los delitos informáticos son exclusivamente dirigidas a las entidades financieras. Sin embargo, las cifras del estudio de Symantec para 2014 muestran lo contrario (estudio que comprende 157 países), pues sólo el 21% de los ataques informáticos son dirigidos a entidades financieras, mientras que el 79% restante se materializaron en otros sectores como la minería, las empresas de servicios y los entes gubernamentales.

En la misma línea, el estudio de Kaspersky Lab titulado "Ciberamenazas Financieras 2014" publicado en febrero de 2015, señala que si bien el 56.6% del phishing financiero estuvo dirigido a las páginas de los bancos, el 25.4% fue contra las compras online y el 17.9% contra los sistemas de pago. De igual forma, en el informe de seguridad global publicado por Trustwave en 2014 se afirma que, a nivel mundial, los mayores robos de información se presentan en los sectores de retail (35%), alimentos (18%), y servicios hospitalarios (11%). El sector financiero participó sólo con el 9% del total (Gráfico 4).

Además, es importante resaltar que ante las amenazas informáticas financieras, la banca también dispone de robustos sistemas de monitoreo y prevención a la vulneración de sus bases de datos, que mitigan de manera exitosa el riesgo del robo de información.

Por el lado de los usuarios, el reporte de Kaspersky indica que en 2014 la cantidad de ataques informáticos, utilizando programas maliciosos dirigidos al robo de información financiera, alcanzó 22,9 millones, lo que representó un descenso de 19,3% frente a los registros de 2013 (año en el que hubo 28.4 millones de ataques).

Gráfico 4. Uso del dinero por parte de la población



Fuente: Banca de las Oportunidades



2. La probabilidad de robo cuando se realizan transacciones a través de los bancos es muy alta.

La falta de conocimiento de la ciudadanía sobre seguridad informática genera un tema de percepción negativa, pues los usuarios del sistema financiero suponen estar vulnerables al riesgo del fraude cuando realizan una transacción electrónica.

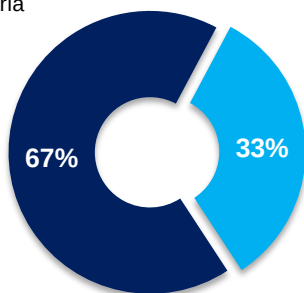
En el mismo estudio de la Banca de las Oportunidades y la Superintendencia Financiera, las personas que utilizan poco dinero en efectivo para realizar sus transacciones, es decir, que ya han usado la banca para realizar sus operaciones, aducen como principal razón la seguridad o el evitar robos. Y las que no usan mucho efectivo no ven a la seguridad como un factor principal para tener este comportamiento transaccional.

Sin embargo, cuando se indagó acerca de las barreras por las cuáles las personas no utilizan el celular o internet para realizar transacciones financieras, el 53% de los encuestados adujo preocupación por la seguridad (Gráfico 5).

Gráfico 5. Barrea del uso en la banca virtual

■ Le gustaría usar internet para transacciones financieras

■ No le gustaría



Razones

- * 50%: Le parece inseguro
- * 24%: No sabe hacerlo
- * 17%: Prefiere otros medios
- * 16%: Rechaza la tecnología
- * 14%: No tiene internet

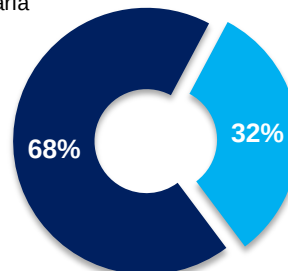
Razones

- * 50%: Facilidad, comodidad
- * 44%: Ahorro de tiempo
- * 31%: Transacciones a cualquier hora
- * 23%: Transacciones desde cualquier lugar
- * 18%: Seguridad
- * 13%: Economía
- * 12%: Gusta de internet

Fuente: Banca de las Oportunidades

■ Le gustaría usar el celular para transacciones financieras

■ No le gustaría



Razones

- * 62%: Facilidad, comodidad
- * 38%: Ahorro de tiempo
- * 29%: Transacciones a cualquier hora
- * 21%: Transacciones desde cualquier lugar
- * 19%: Seguridad
- * 15%: Economía

Razones

- * 53%: Le parece inseguro
- * 26%: No sabe hacerlo
- * 18%: Rechaza la tecnología
- * 18%: Prefiere otros medios

Fuente: Banca de las Oportunidades

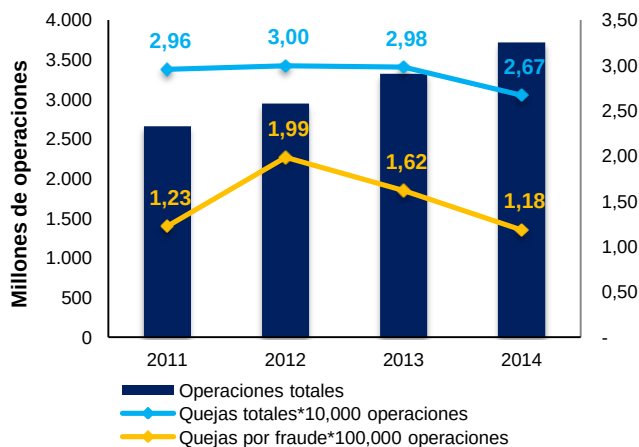
Esto seguramente quiere decir que las personas confían en el sistema financiero, pero tienen ciertos temores a la utilización de canales electrónicos para la realización de sus transacciones. No obstante, es importante empezar a vencer esos temores.

Cuando se observa el registro de quejas, los indicadores de posibles fraudes son relativamente bajos. El número de quejas totales del sistema financiero, en relación con las transacciones, ha venido disminuyendo durante los últimos años. Así, en 2011, por cada 10 mil transacciones se presentaron 3 quejas al sistema financiero, mientras que en 2014 este indicador descendió a 2.

Por su parte, las quejas relacionadas con fraudes³ tienen una pequeña participación sobre el total de quejas y de operaciones (3.6%) y muestran un comportamiento decreciente en los últimos años. Así, en 2014 se observaron 1.18 quejas por cada 100.000 transacciones, mientras que en el 2011 ese indicador fue de 1.23 (Gráficos 6 y 7).

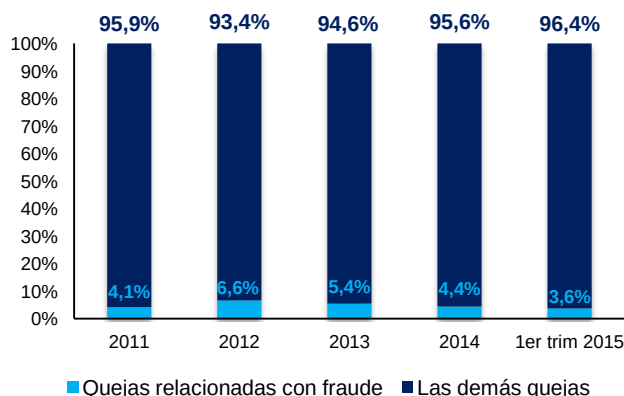
³ Los motivos de quejas que se agruparon como relacionados con fraude son: 1. suplantación presunta de personas, 2. pago irregular en caja, 3. billetes falsos, 4. vinculación presuntamente fraudulenta, 5. objeción o negativa para atender el siniestro, 6. pago de cheque falsificado o irregular, 7. seguridad en instalaciones.

Gráfico 6. Indicadores de quejas vs. Operaciones totales del sector financiero



Fuente: Superintendencia Financiera de Colombia, cálculos Asobancaria.

Gráfico 7. Participación del número total de quejas por fraude del sistema financiero vs. Número total de quejas.



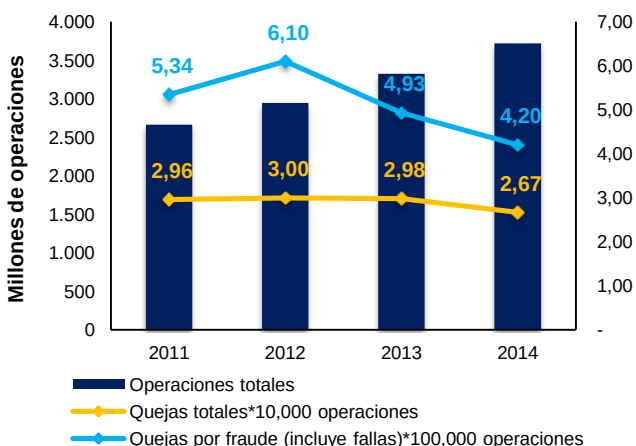
Fuente: Superintendencia Financiera de Colombia, cálculos Asobancaria.

Debido a la dificultad para discriminar los motivos relacionados con fraude en el reporte de quejas de la Superintendencia Financiera de Colombia, generamos una segunda agrupación donde sumamos a los 7 motivos iniciales 8 categorías adicionales relacionadas con fallas en canales electrónicos dentro de las que se podrían estar incorporando quejas por posibles fraudes. En este escenario observamos la misma tendencia, pero aun así

los indicadores son bajos: 4,2 quejas por cada 100.000 operaciones (Gráficos 8 y 9).

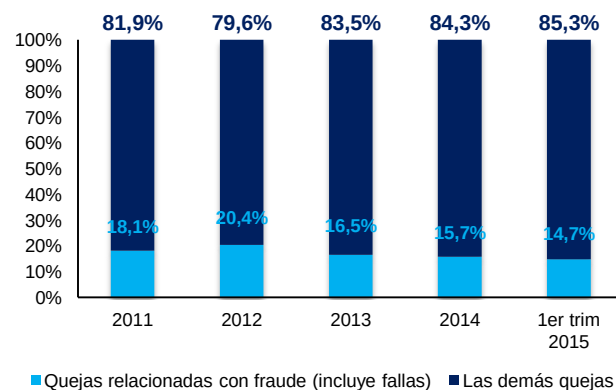
Ahora bien, al comparar el número total de denuncias de delitos informáticos de la Policía Nacional (3.892) frente al total de operaciones realizadas en canales no presenciales durante el 2014, la probabilidad de ocurrencia de un fraude es baja, al ser una por cada millón de transacciones.

Gráfico 8. Indicadores de quejas vs. Operaciones totales del sector financiero



Fuente: Superintendencia Financiera de Colombia, cálculos Asobancaria.

Gráfico 9. Participación del número total de quejas por fraude del sistema financiero (incluyendo motivos relacionados con fallas) vs Número total de quejas



Fuente: Superintendencia Financiera de Colombia, cálculos Asobancaria.



Además, es importante reiterar que el riesgo de que un usuario del sistema financiero sea víctima de un delito informático por realizar transacciones electrónicas es menor frente a otro tipo de delitos, en razón a que el internet favorece, en cierta medida, la trazabilidad y el control de las transacciones.

Adicionalmente, si se tiene en cuenta que una transacción electrónica, como por ejemplo una compra por internet, pasa por diferentes actores (las pasarelas de pago, el comercio, el banco emisor, el banco adquirente y la red que procesará la información) y todos realizan validaciones de seguridad antes de aprobar la transacción, es evidente que el riesgo se reduce considerablemente. Además, en muchos casos, aún cuando el ilícito se comete, los recursos son reembolsados al usuario financiero.

En este sentido, actualmente está cursando en el Ministerio de Comercio, Industria y Turismo un proyecto de decreto que contempla la reversión de pagos cuando la venta y el pago del bien se realizan a través del comercio electrónico. Estas medidas ayudan, sin duda, a mejorar la confianza en las transacciones a través de canales virtuales.

Consideraciones finales y retos de la banca sobre seguridad en canales no presenciales

Si bien la banca, junto a entidades gubernamentales como la Policía Nacional y los gobiernos locales, ha realizado ingentes esfuerzos para reducir los riesgos de hurto al realizar transacciones financieras, todavía persisten algunos retos. Entre los principales retos y desafíos en materia de seguridad bancaria para el corto, mediano y largo plazo, se encuentran:

- Desincentivar el uso del efectivo, ofreciendo alternativas en canales transaccionales seguros para los usuarios/clientes del sector financiero.
- Seguir realizando inversiones en herramientas que permitan mitigar cada vez más el riesgo de fraude.
- Educar a los usuarios/clientes del sistema financiero con hábitos seguros y uso adecuado de los canales transaccionales ofrecidos por las entidades.
- Insistir en la importancia de fortalecer la institucionalidad del aparato judicial en relación con los delitos informáticos, buscando la designación de funcionarios expertos en

en estos temas para desarticular estructuras delincuenciales.

- Incentivar estrategias sectoriales en materia de ciberseguridad y ciberdefensa con los diferentes organismos del Estado en aras de garantizar la seguridad de los ciudadanos y la soberanía del país.
- Trabajar articuladamente para la generación de conocimiento entre el sector financiero y las autoridades policiales y judiciales, estando a la vanguardia tanto en las tipologías de hurto a usuarios del sistema financiero, en los avances tecnológicos de los dispositivos utilizados por los delincuentes así como en la forma de identificarlos.

Por último, la Asociación Bancaria reitera la importancia de que los usuarios adopten prácticas seguras en el manejo de su información al momento de realizar sus transacciones en canales no presenciales. Se debe sensibilizar a la población sobre los riesgos de revelar su información personal y financiera, pues esta permite a los delincuentes materializar el hurto. Se está atravesando por una etapa de cambio en los hábitos de consumo y, en general, de la cotidianidad, lo que ha tornado imprescindible para gran parte de la población el uso de la tecnología para el desempeño de sus actividades. El uso responsable de los productos y canales transaccionales ofrecidos por la banca, por parte de los clientes/usuarios del sector financiero, significará grandes beneficios no solo a nivel de individuo sino para la sociedad en su conjunto.



Colombia

Principales Indicadores Macroeconómicos

	2012	2013					2014					2015	
		T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	Total Proy.
PIB Nominal (COP MM)	664,5	172	175	179	181	707	187	187	190	192	756,2	194	809,2
PIB Nominal (USD B)	366	94	91	93	94	367	95	96	93	88	372,5	75,5	344,3
Crecimiento Real													
PIB real (% Var. Interanual)	4,0	2,9	4,7	6,1	6,0	4,9	6,5	4,1	4,2	3,5	4,6	2,8	3,1
Precios													
Inflación (IPC, % Var. Interanual)	2,4	1,9	2,2	2,3	1,9	1,9	2,5	2,8	2,9	3,7	3,7	4,6	4,1
Inflación básica (% Var. Interanual)	3,2	2,5	2,1	2,2	2,2	2,2	2,5	2,5	2,4	2,8	2,8	3,9	...
Tipo de cambio (COP/USD fin de periodo)	1768	1832	1929	1915	1927	1927	1965	1881	2028	2392	2392	2576	2355
Tipo de cambio (Var. % interanual)	-9,0	2,2	8,1	6,3	9,0	9,0	7,3	-2,5	5,9	24,2	24,2	31,1	-1,6
Sector Externo													
Cuenta corriente (% del PIB)	-3,3	-3,4	-2,6	-4,1	-3,6	-3,2	-3,8	-4,3	-5,3	-6,5	-5,2	...	-5,6
Cuenta corriente (USD B)	-12,1	-3,3	-2,3	-3,7	-3,3	-12,3	-3,8	-4,1	-5,0	-6,9	-19,8	...	-18,4
Balanza comercial (USD mmM)	5,2	0,6	1,2	-4,0	-4,1	-6,3	-0,6	-0,6	3,0	0,4	2,2	...	...
Exportaciones F.O.B. (USD mmM)	60,1	14,1	15,2	13,7	11,8	54,8	13,5	14,5	15,8	15,1	58,8	...	...
Importaciones F.O.B. (USD mmM)	56,1	13,5	14,0	17,7	15,9	61,1	14,1	15,1	12,8	14,6	56,6	...	...
Servicios (neto)	-5,5	-1,4	-1,4	-1,5	-1,4	-5,6	-1,4	-1,6	-1,7	...	...	...	...
Renta de los factores	-15,9	-3,6	-3,4	-3,5	-3,6	-14,1	-3,0	-3,2	-3,6	...	-12,9	...	-8,5
Transferencias corrientes (neto)	4,6	1,0	1,2	1,2	1,1	4,6	1,0	1,0	1,0	...	4,4	...	4,4
Inversión extranjera directa (USD mm)	15,8	3,7	4,0	4,8	3,9	16,4	3,7	4,4	3,9	3,1	15,1	3,4	13,2
Sector Público (acumulado)													
Bal. primario del Gobierno Central (% del PIB)	0,2	0,8	2,4	2,4	0,3	0,0	0,5	...	...	...	-0,2	...	...
Bal. del Gobierno Central (% del PIB)	-2,3	0,4	1,3	0,7	-2,4	-2,4	0,1	0,1	...	...	-2,4	...	-3,0
Bal. primario del SPNF (% del PIB)	3,3	1,9	3,6	4,0	1,5	1,4	...	2,4	...	...	0,7	...	0,5
Bal. del SPNF (% del PIB)	0,5	1,5	2,5	2,1	-0,9	-1,0	0,6	1,3	...	...	-1,8	...	-2,3
Indicadores de Deuda													
Deuda externa bruta (% del PIB)	21,3	21,4	22,1	23,8	24,2	24,2	25,1	25,6	26,1	26,8	26,8	...	...
Pública - SNPF (% del PIB)	12,5	12,2	12,2	13,5	13,7	13,7	14,3	15,0	15,4	15,8	15,8	...	...
Privada (% del PIB)	8,8	9,2	9,9	10,3	10,5	10,5	10,8	10,6	10,7	11,0	11,0	...	...
Deuda del Gobierno Central (% del PIB)	34,5	35,1	34,5	35,9	37,3	37,3	35,5	35,3	36,6	39,7	39,7	...	...

Fuente: PIB y Crecimiento Real – DANE y Banco de la República, proyecciones Asobancaria. Sector Externo – DANE y Banco de la República, proyecciones MHCP. Sector Público y respectivas proyecciones - MHCP. Indicadores de deuda – DANE, Banco de la República, Departamento Nacional de Planeación; proyecciones DNP y MHCP.

Colombia
Estados Financieros*

	dic-14 (a)	nov-14	dic-13 (b)	Var real anual entre (a) y (b)
Activo	442.117	437.989	388.646	9,7%
Disponible	28.212	29.696	27.719	-1,8%
Inversiones	79.528	78.098	74.060	3,6%
Cartera Neta	291.022	286.687	251.500	11,6%
Consumo Bruta	83.552	82.925	73.845	9,2%
Comercial Bruta	182.959	179.081	156.800	12,6%
Vivienda Bruta	28.895	28.840	24.458	14,0%
Microcrédito Bruta	8.569	8.582	7.859	5,2%
Provisiones**	12.954	12.741	11.463	9,0%
Consumo	5.005	4.971	4.586	5,3%
Comercial	6.735	6.549	5.810	11,8%
Vivienda	650	641	524	19,7%
Microcrédito	564	579	543	0,2%
Otros	43.356	43.509	35.366	18,3%
Pasivo	380.025	376.569	334.192	9,7%
Depósitos y Exigibilidades	284.365	283.938	258.191	6,3%
Cuentas de Ahorro	136.104	139.373	128.653	2,1%
CDT	88.299	88.605	74.226	14,8%
Cuentas Corrientes	49.734	47.185	46.725	2,7%
Otros	10.227	8.775	8.588	14,9%
Otros pasivos	95.661	92.631	76.001	21,4%
Patrimonio	62.092	61.421	54.454	10,0%
Ganancia/Pérdida del ejercicio	7.928	6.606	6.492	17,8%
Ingresos por intereses	30.579	27.770	28.204	4,6%
Gastos por intereses	10.621	9.622	10.039	2,1%
Margen neto de Intereses	19.908	18.102	18.148	5,8%
Ingresos netos diferentes de Intereses	11.126	9.399	9.757	10,0%
Margen Financiero Bruto	31.035	27.501	27.906	7,3%
Costos Administrativos	13.493	12.081	12.938	0,6%
Provisiones Netas de Recuperación	4.606	4.158	4.340	2,4%
Margen Operacional	12.936	11.262	10.628	17,4%
Indicadores				Variación (a) - (b)
Indicador de calidad de cartera	2,91	3,06	2,79	0,12
Consumo	4,31	4,63	4,39	-0,08
Comercial	2,18	2,27	1,99	0,20
Vivienda	2,16	2,17	2,03	0,13
Microcrédito	7,40	7,50	6,22	1,18
Cubrimiento**	150,46	143,15	160,58	-10,12
Consumo	138,90	129,58	141,44	-2,54
Comercial	168,48	161,43	186,65	-18,17
Vivienda	104,22	102,65	105,68	-1,46
Microcrédito	88,97	89,95	111,13	-22,16
ROA	1,92%	1,75%	1,78%	0,1%
ROE	13,68%	12,49%	13,09%	0,6%
Solvencia	15,11%	15,27%	14,68%	0,4%

1/ Calculado como la diferencia entre ingresos y gastos por intereses menos Prima amortizada de cartera - cuenta PUC 510406

2/ Indicador de calidad de cartera en mora = Cartera Vencida /Cartera Bruta.

*Datos mensuales a diciembre de 2014 del sistema bancario. Cifras en miles de millones de pesos. Fuentes y cálculos Asobancaria.

** No se incluyen otras provisiones. El cálculo del cubrimiento tampoco contempla las otras provisiones.