Semana económica

ASOBANCARIA

29 de octubre de 2012

Mitigar el riesgo de fraude es un desafío para las autoridades, la banca y los usuarios.

María Mercedes Cuéllar
Presidente

Daniel Castellanos
Vicepresidente Económico
+57 1 3266600
dcastellanos@asobancaria.com

Resumen. La tipología del fraude que afecta al sector bancario y a sus clientes va desde el fleteo y el taquillazo hasta complejos delitos informáticos. Cualquiera que sea la modalidad, las investigaciones han demostrado que detrás del acto delictivo se encuentran complejas estructuras delincuenciales, cuya principal motivación es apoderarse de los recursos de la víctima.

Las estrategias de mitigación del riesgo de fraude deben estar centradas en la implementación de herramientas y medidas de control, el cambio en el comportamiento por parte de los clientes y usuarios, el trabajo conjunto de todos los actores y el fortalecimiento de las labores de investigación y judicialización.

En cuanto a la primera estrategia, los bancos trabajan continuamente en la investigación, desarrollo e implementación de nuevas herramientas y procedimientos que mejoren la autenticación de los usuarios y que contribuyan a la prevención del fraude. Sin embargo, debido a que las herramientas de mitigación tienen unos costos importantes y que en ocasiones hacen más complejo el proceso de realizar una operación financiera, el reto más importante está centrado en lograr un equilibrio entre la ampliación y profundización de las transacciones financieras y las medidas para fortalecer la seguridad en ellas.

Frente a las costumbres seguras, es importante que los ciudadanos entiendan que la utilización de medios de pago o de canales ofrecidos por los bancos, requiere un cuidado especial por parte del cliente. Esto es un asunto de corresponsabilidad.

Por otra parte, se necesita un trabajo articulado entre los actores. Aun cuando en el imaginario colectivo una transacción financiera depende exclusivamente de la entidad bancaria, en la realidad están involucrados varios actores. Sin duda, cada uno desde su lugar puede aportar en la implementación de acciones para mitigar el riesgo de fraude. Surge la necesidad de coordinar mesas interinstitucionales con los reguladores y los actores involucrados para ayudar en el diseño y ejecución de acciones adecuadas para enfrentar los desafíos en el origen y la materialización del fraude financiero.

Por último, es imperativo avanzar en el fortalecimiento de las acciones judiciales en contra de los delincuentes que están detrás de las defraudaciones a la banca y sus clientes. La sanción eficiente por parte de la justicia es necesaria para desestimular la aparición de más delincuencia alrededor de estas modalidades. Mientras no existan castigos ejemplares, el potencial delincuente no va a percibir suficientes riesgos para desistir de realizar la acción ilegal.

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

Mitigar el riesgo de fraude es un desafío para las autoridades, la banca y los usuarios[1]

Daniel Castellanos

Vicepresidente Económico

Las tipologías de fraude que afectan al sector bancario y a sus clientes van desde el fleteo[2] y el taquillazo[3] hasta complejos delitos informáticos. Dentro de estos últimos se puede hacer referencia a modalidades como el *phishing* (suplantación de sitios web), instalación de troyanos o software espía para el hurto de información, el acceso abusivo a sistemas informáticos y la clonación de tarjetas débito y crédito.

Cualquiera que sea la modalidad, las investigaciones de casos de fraude bancario han demostrado que detrás del acto delictivo se encuentran complejas estructuras delincuenciales cuya principal y tal vez única motivación es apoderarse de los recursos de la víctima.

El uso cada vez mayor de los canales electrónicos[4] para la realización de operaciones bancarias y los avances tecnológicos, que le facilitan al delincuente adquirir herramientas y establecer contacto con organizaciones ilegales de otros territorios, son factores que han llevado a una tendencia creciente de los ataques tecnológicos o informáticos contra los establecimientos de crédito.

En Colombia también ha ocurrido un incremento rápido de los canales electrónicos. De acuerdo con el Informe de Inclusión Financiera de Asobancaria del primer semestre de 2012[5], entre junio de 2009 y el mismo período de este año su crecimiento fue del 3,8%. Esto se explica por canales como internet, que en junio de 2009 participaba con el 6,5% y ahora el 9,5% de las transacciones monetarias se realiza por este medio. Algo similar aconteció con el uso de los datáfonos (gráfico 1).

---

[1] Discurso pronunciado por el Vicepresidente Económico de Asobancaria, Daniel Castellanos, en la instalación del VI Congreso de Prevención del Fraude y Seguridad, llevado a cabo en Bogotá los días 24 y 25 de octubre de 2012.

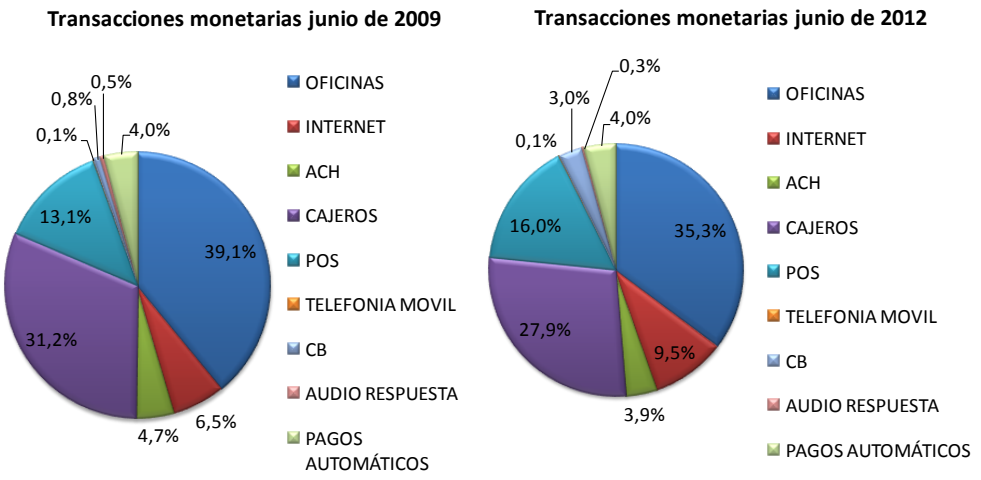
[2] Modalidad de hurto a personas que sucede después de haber realizado un retiro en una oficina bancaria y en la que el delincuente utiliza la intimidación y/o violencia para apoderarse del dinero.

[3] Es el nombre con el que se conoce a la modalidad de hurto a oficinas bancarias en las que los delincuentes entran fuertemente armados e intimidan a los cajeros para que les entreguen el dinero del que se dispone en las cajas.

[4] Cajeros, Internet, Audiorespuesta, Oficinas, Pagos automáticos, Datáfonos y Telefonía Móvil

[5] Si quiere consultar este informe completo puede acceder a la página www.asobancaria.com o directamente al link http://www.asobancaria.com/portal/page/portal/Asobancaria/publicaciones/economica_financiera/reporte_bancarizacion/2012/

Gráfico 1. Transacciones monetarias



Fuente: Superintendencia Financiera de Colombia

En relación con el cibercrimen, según el reporte "Symantec Internet Security Threat" publicado en 2011, en el año 2010 se encontraron 4.989 nuevas vulnerabilidades en elementos tecnológicos (es decir, 95 por semana) y existen más de 403 millones de variantes de malware. Además, la alta penetración de la telefonía celular ha llevado a un incremento de ataques hacia dispositivos móviles. De acuerdo con ese mismo estudio, el año pasado se identificó un 93% más de vulnerabilidades y un 1.116% de malware en celulares respecto de la vigencia anterior.

Algunos datos adicionales ilustran también esta situación. El costo anual de los cibercrímenes en el mundo se calcula en USD 114 billones, el 69% de los adultos ha sido víctima de un cibercrimen en su vida, cada 14 segundos hay una víctima (es decir, más de un millón de víctimas por año) y el FBI habla de USD 400 billones de estafas en estas modalidades anualmente[6].

En Colombia los mayores retos de mitigación del fraude en las transacciones financieras se encuentran en las operaciones que se realizan en ambientes no presenciales como la internet, la banca móvil, la audio-respuesta y principalmente el comercio electrónico. Esta tendencia se acentúa por dos razones. En primer lugar, por el proceso de migración a tecnología EMV −mejor conocida como tarjeta con chip− en el que se encuentra nuestro país. Y en segundo lugar, por el vertiginoso crecimiento del comercio electrónico.

Ante este panorama, para contrarrestar o mitigar los riesgos de fraude se debe trabajar en dos grandes frentes: el preventivo y el reactivo. En el primero de ellos se deben considerar estrategias como las siguientes: (1) implementación de herramientas y medidas de mitigación del fraude, (2) cambio en el comportamiento por parte de los

[6] Datos tomados de estudios de Symantec Corporation.

clientes y usuarios (es decir, costumbres seguras) y (3) trabajo conjunto de todos los actores. En el segundo, el trabajo se debe centrar en fortalecer las labores de investigación y judicialización. A continuación se esbozarán algunos elementos que se deben considerar para cada una de las estrategias enumeradas.

Implementación de herramientas y procedimientos por parte de las entidades financieras

Frente a esta estrategia se debe resaltar el trabajo de las entidades financieras en cuatro líneas: (i) migración a tarjetas débito y crédito con chip, (ii) mejoras en los procesos de autenticación de los clientes en los canales no presenciales, (iii) instalación de cámaras de vídeo en oficinas y cajeros automáticos y (iv) mecanismos de información en línea sobre las transacciones realizadas por los usuarios.

En cuanto a la primera línea, desde hace varios años las entidades financieras vienen realizando cuantiosas inversiones y destinando numerosos recursos técnicos y humanos para avanzar en la migración del sistema de tarjetas al estándar EMV (Europay MasterCard VISA). En la actualidad, los cerca de 200.000 datáfonos existentes en el mercado cuentan con esta tecnología, al tiempo que el 40% de las tarjetas débito y crédito tienen chip. Por su parte, desde abril de 2013 todos los plásticos que se expidan tendrán este dispositivo[7] y a finales de 2014, los cerca de 10 millones de tarjetas crédito y 17 millones de tarjetas débito contarán con esta tecnología. Además, en octubre de 2013 los 11.400 cajeros automáticos estarán en disposición de recibir transacciones de tarjetas con tecnología EMV. Este proceso constituye un importante avance en materia de seguridad, que llevará a Colombia, junto con Venezuela, a ser pioneros en la migración total en la región. Este conjunto de acciones se materializarán en una mitigación sustancial del fraude en transacciones en ambientes presentes (cajeros y datáfonos).

Con relación al segundo punto, desde hace algunos años los bancos han puesto a disposición de los clientes −especialmente los empresariales− nuevos mecanismos de autenticación tales como claves dinámicas a través de *token* o tarjetas de coordenadas. También han dispuesto otra serie de mecanismos como la preinscripción de cuentas receptoras de transferencias y de facturas de servicios. Sin lugar a dudas, estas medidas han contribuido a controlar los niveles de fraude en operaciones realizadas por medio de los portales transaccionales de las entidades bancarias.

Frente a la tercera línea, los bancos tienen instaladas por lo menos 50.000 cámaras de vídeo en oficinas y cajeros automáticos. Varias entidades han desarrollado robustos

[7] De acuerdo con la reciente regulación emitida por la Superintendencia Financiera de Colombia, se exceptúa del requerimiento las tarjetas débito asociadas a productos utilizados para canalizar recursos provenientes de programas de ayuda y/o subsidios otorgados por el Estado Colombiano que no superen (2) SMMLV y las tarjetas crédito cuyos cupos aprobados no superen los dos (2) SMMLV.

centros de monitoreo de imágenes que les permiten tener una visión en línea de lo que sucede en sus instalaciones. Además, ante la ocurrencia de un fraude, estos registros fílmicos constituyen elementos probatorios relevantes para la judicialización de los delincuentes.

Finalmente, en cuanto a la información en línea, hoy los usuarios de la banca cuentan con la oportunidad de recibir vía mensajes de texto al celular o correos electrónicos la información de sus transacciones minutos, o incluso segundos, después de realizadas.

Con el panorama tecnológico tan cambiante, los bancos trabajan continuamente en la investigación, desarrollo e implementación de nuevas herramientas y procedimientos que sigan coadyuvando a la prevención del fraude. En este sentido el reto más importante es lograr un equilibrio entre la ampliación y profundización de las transacciones financieras y las medidas para fortalecer la seguridad en las transacciones. Debido a que las herramientas de mitigación de fraude tienen unos costos importantes, resulta necesario lograr un balance adecuado entre la necesidad de aumentar la inclusión y profundización financiera y la seguridad de las transacciones bancarias.

Cambio en el comportamiento por parte de los clientes y usuarios

Las entidades financieras implementan herramientas, tecnologías y procedimientos para mejorar la seguridad en las transacciones bancarias. A su vez, las autoridades fortalecen sus capacidades de reacción e investigación. Sin embargo, si el usuario no desarrolla costumbres seguras al realizar las operaciones, esos esfuerzos corren el riesgo de perderse. Por ejemplo, la implementación en el país del sistema EMV −mejor conocido como tarjetas chip− ha implicado cuantiosas inversiones tecnológicas y en recursos humanos. Pero si un cliente deja que alguien extraño, simulando que le ayuda a realizar una operación financiera, le cambie el plástico y le vea la clave al digitarla, no hay tecnología alguna que pueda prevenir que le roben su dinero.

Es importante que los ciudadanos entiendan que la utilización de medios de pago o de canales ofrecidos por los bancos requiere un cuidado especial por parte del cliente. Esto es un asunto de corresponsabilidad.

Por esto la banca trabaja de manera decidida en tareas de sensibilización y comunicación de recomendaciones y buenas prácticas, que deben aplicar los clientes al realizar transacciones. Esas tareas se desarrollan, por ejemplo, mediante campañas en los medios de comunicación masiva. A manera de referencia vale la pena mencionar que Asobancaria ha invertido por lo menos COP 7.000 millones en los últimos 2 años en esta estrategia. Además, desde el gremio se ha establecido la temática de seguridad

bancaria como línea de acción fundamental en el Programa de Educación Financiera que ha ejecutado en los últimos años[8].

Al mismo tiempo, las entidades bancarias han dispuesto sus canales −internet, oficinas, extractos− para entregar mayor información sobre las recomendaciones de seguridad. De manera complementaria, se efectúan campañas con autoridades para épocas de alta transaccionalidad, particularmente en las principales ciudades. También se llevan a cabo capacitaciones puntuales en diferentes espacios sobre las modalidades de fraude financiero y las recomendaciones para hacer las transacciones bancarias más seguras.

Sin embargo, los procesos de cambios en las costumbres por lo general son lentos y requieren tiempo y esfuerzos continuos en la comunicación. Por esta razón la estrategia debe continuar de forma permanente y se deben aunar esfuerzos por parte de todos los actores para lograr la masividad y la constancia que requieren este tipo de procesos.

Trabajo conjunto de todos los actores

Aun cuando en el imaginario colectivo una transacción financiera depende exclusivamente de la entidad bancaria, en la realidad en una operación bancaria están involucrados varios actores. Por ejemplo, en una compra por internet con una tarjeta de crédito se encuentran el cliente, el banco emisor, el comercio, el banco adquirente, la red que procesa la operación y las pasarelas de pago. Además, se encuentra el Estado que tiene labores fundamentales, por una parte, en relación con la regulación y supervisión; y por otra, en materias de investigación criminal y judicialización

Sin duda, cada uno desempeña un papel fundamental en la implementación de acciones para mitigar el riesgo de fraude. Desafortunadamente, hasta el momento todos los actores ven al otro como un agente lejano y la poca articulación ha llevado a que cada uno genere acciones aisladas cuyo impacto es mucho menor del que se lograría si todos trabajaran de la mano. En estas circunstancias surge la necesidad de coordinar mesas interinstitucionales con los reguladores. A su vez, los actores involucrados pueden ayudar en el diseño y ejecución de acciones adecuadas para enfrentar los riesgos de fraude en las operaciones financieras.

Fortalecimiento de la investigación y judicialización

Es imperativo avanzar en el fortalecimiento de las acciones judiciales en contra de los delincuentes que están detrás de las defraudaciones a la banca y sus clientes. La sanción eficiente por parte de la justicia es necesaria para desestimular la aparición de más delincuencia alrededor de estas modalidades. Mientras no existan castigos

[8] Para mayor información sobre este programa se puede consultar la página www.asobancaria.com y www.cuadresubolsillo.com.

ejemplares, el potencial delincuente no va a percibir suficientes riesgos como para desistir de realizar la acción ilegal.

Sin embargo, las labores de judicialización no son sencillas. Por ejemplo, en el caso del fleteo, se torna casi imposible indiciar al miembro de la banda conocido como el "marcador", que es el delincuente que identifica a la potencial víctima cuando realiza el retiro en efectivo de una sucursal bancaria.

En los delitos informáticos esta situación es mucho más compleja debido a: (1) el alto componente técnico de la tipificación legal de los denominados delitos informáticos; (2) la práctica probatoria, que también es de alto contenido técnico especializado; y (3) la dificultad en la identificación del lugar de la comisión de los hechos, que se complica aún más cuando estos delitos ocurren de forma simultánea en diversas unidades territoriales.

Desde ASOBANCARIA se han venido apoyando las labores de investigación criminal de la Policía Nacional y de la Fiscalía General de la Nación, en particular en el mejoramiento de sus herramientas tecnológicas. También hemos venido financiando programas de educación en estas materias, dirigidos a las autoridades de investigación y judicialización. Es así como han sido capacitados por la Universidad de los Andes cerca de 270 fiscales, 25 funcionarios de Policía Judicial y 30 jueces en ciudades como Bogotá, Medellín, Cali y Barranquilla, en temáticas relacionadas con la Criminalidad Informática y la Evidencia Digital.

No obstante, estos esfuerzos se han visto atomizados en razón a que la competencia para la investigación de los delitos informáticos está en manos de 1.300 fiscales locales, quienes, además, tienen a su cargo procesos de la más diversa índole. Lo mismo sucede con los jueces penales municipales, a quienes la Ley 1273 consideró responsables de conocer este tipo de conductas.

Es urgente que las autoridades consideren la necesidad asignar la competencia de la investigación y judicialización de los delitos informáticos a grupos especializados. Esto contribuiría a concentrar los esfuerzos de capacitación en materia informática y facilitaría la asignación del tiempo y la dedicación que este tipo de investigaciones requiere.

Adicionalmente las acciones de fortalecimiento de la capacidad técnica podrían focalizarse en el análisis de estas tipologías criminales, lo que ayudaría a la identificación de la conexidad entre diversos procesos y a la unificación de casos. Del mismo modo, se podría potencializar el conocimiento sobre el manejo de la evidencia forense y el desarrollo de habilidades investigativas especiales, que permitan identificar a los reales responsables de los delitos en menor tiempo. Por esto queremos seguir reiterando el llamado a la Fiscalía General de la Nación para volver a explorar la posibilidad de crear una Unidad Nacional que atienda los delitos informáticos.

Habeas data

Adicional a los temas relacionados puramente con el fraude bancario, es importante hacer algunas anotaciones en relación con la protección de los datos −particularmente los considerados sensibles−, el habeas data y los nuevos retos empresariales. Las recientes tendencias regulatorias acerca de la obligación de proteger los datos personales, que está atada a derechos constitucionales como la privacidad, presentan importantes desafíos para las organizaciones que de una u otra manera recopilan información de este tipo, es decir, casi todas las instituciones públicas y privadas.

Las entidades financieras vienen aplicando la regulación del conocido habeas data financiero, que desde hace varios años les ha impartido obligaciones acerca de la autorización expresa del cliente sobre el uso de sus datos y del adecuado uso, almacenamiento y protección de esta información. Sin embargo, la reciente sanción de la ley estatutaria de protección de datos personales en Colombia amplía el espectro a las organizaciones de sectores diferentes al financiero, e incluso en este sector, pues dispone un conjunto de deberes relacionados con el debido cuidado de la información.

En materia de seguridad de la información los cambios son sustanciales. Esta arista requiere una evaluación exhaustiva del tratamiento de los datos (hasta ahora tal vez un poco "ligero") que se viene dando al interior de las instituciones. Aspectos que seguramente eran desconocidos o poco usados en industrias diferentes a la financiera, tales como almacenamiento, cifrado, autenticación, permisos de acceso, seguridad en bases de desarrollo y debido cuidado en la protección datos y redes de computadores, deberán ser implementados adecuadamente. Además, deberán establecer seguramente una estructura de gobierno (con oficial de seguridad de datos) responsable de implementar el programa de aseguramiento de la información, el cual implica no solo adecuaciones tecnológicas sino análisis jurídicos y cambios procedimentales de importante envergadura.

Colombia. Principales Indicadores Macroeconómicos

	2009	2010	2011					2012					2013
			T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Proy.**	**Proy.**
PIB Nominal (COP MM)	**504.6**	**543.7**	147	152	155	161	**616**	161.2	164.3	166.3	174.0	**665.8**	**713.7**
PIB Nominal (USD B)	**247**	**284**	78	85	81	83	**317**	90.0	92.0	92.0	96.1	**367.6**	**397.4**
Crecimiento Real													
PIB real (% Var. Interanual)	**1.7**	**4.0**	5.0	5.1	7.5	6.1	**5.9**	4.7	4.9	4.0	4.9	**4.6**	**4.4**
Precios													
Inflación (IPC, % Var. Interanual)	**2.0**	**3.2**	3.2	3.2	3.7	3.7	**3.7**	3.4	3.2	3.0	3.0	**3.0**	**2.71.**
Inflación básica (% Var. Interanual)	**2.7**	**2.6**	2.8	3.1	3.0	3.2	**3.2**	3.0	1.9	2.0	2.8	**2.8**	**…**
Tipo de cambio (COP/USD fin de periodo)	**2044**	**1914**	1879	1780	1915	1943	**1943**	1792	1785	1808	1811	**1811**	**1796**
Tipo de cambio (Var. % interanual)	**-8.9**	**-6.4**	(2.5)	-7.1	6.4	1.5	**1.5**	-4.7	0.2	1.6	-5.4	**-6.8**	**-0.8**
Sector Externo													
Cuenta corriente (% del PIB)	**-2.0**	**-3.1**	-2.3	-2.5	-3.5	-3.1	**-3.0**	-1.8	-3.5	…	…	**-2.9**	**…**
Cuenta corriente (USD mmM)	**-5.0**	**-8.9**	-1.8	-2.2	-2.8	-2.5	**-9.4**	-1.6	-3.2	…	…	**-9.4**	**…**
Balanza comercial (USD mmM)	**2.1**	**2.0**	1.2	1.7	0.9	-0.6	**3.2**	2.5	1.0	…	…	**…**	…
Exportaciones F.O.B. (USD mmM)	**32.6**	**39.5**	12.5	14.5	14.2	0.3	**41.5**	15.2	14.8	…	…	**…**	…
Importaciones F.O.B. (USD mmM)	**30.5**	**37.5**	11.3	12.7	13.3	0.9	**38.3**	12.7	13.8	…	…	**…**	…
Servicios (neto)	**-2.8**	**-3.5**	-0.9	-1.0	-1.0	-1.2	**-4.2**	-1.1	-1.4	…	…	**…**	**…**
Renta de los factores	**-9.3**	**-11.9**	-3.2	-4.0	-4.2	-3.7	**-15.1**	-4.1	-3.9	…	…	**…**	**…**
Transferencias corrientes (neto)	**4.6**	**4.5**	1.1	1.1	1.4	1.4	**5.0**	1.1	1.2	…	…	**…**	**…**
Inversión extranjera directa (USD mM)	**7.1**	**6.7**	3.5	3.0	3.8	2.9	**13.3**	3.7	4.1	…	…	**…**	**…**
Sector Público (acumulado)													
Bal. primario del Gobierno Central (% del PIB)	**-1.1**	**-1.1**	…	**…**	**…**	**…**	**-0.1**	**…**	…	…	…	**0.2**	**…**
Bal. del Gobierno Central (% del PIB)	**-4.1**	**-3.9**	0.6	1.3	0.9	-2.8	**-2.8**	0.5	2.4	…	…	**-2.4**	**-2.2**
Bal. primario del SPNF (% del PIB)	**0.9**	**-0.1**	…	**…**	**…**	**…**	**1.1**	**…**	…	…	…	**0.1**	**…**
Bal. del SPNF (% del PIB)	**-2.4**	**-3.1**	1.3	2.5	2.3	-1.8	**-1.8**	1.5	…	…	…	**-1.2**	**-1.0**
Indicadores de Deuda													
Deuda externa bruta (% del PIB)	**22.7**	**22.4**	20.4	20.7	21.7	22.8	**22.8**	20.7	20.5	…	…	**…**	**…**
Pública (% del PIB)	**15.7**	**13.7**	12.0	11.9	12.5	12.9	**12.9**	11.9	11.8	…	…	**…**	**…**
Privada (% del PIB)	**7.0**	**8.7**	8.4	8.8	9.2	10.0	**10.0**	8.8	8.6	…	…	**…**	**…**
Deuda del Gobierno(% del PIB, Gob. Central)	**37.7**	**38.4**	36.3	34.2	35.1	…	**35.4**	…	38.6	…	…	**35.1**	**33.9**

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 Asobancaria.

Colombia. Estados financieros*

	sep-12 (a)	ago-12	sep-11 (b)	Var real anual entre (a) y (b)
Activo	**324,723**	**315,970**	**283,459**	**11.1%**
Disponible	22,371	20,082	16,178	34.1%
Inversiones	60,235	58,931	57,457	1.7%
Cartera Neta	210,068	207,587	181,699	12.2%
Consumo Bruta	63,632	62,855	53,327	15.8%
Comercial Bruta	131,950	130,732	117,024	9.4%
Vivienda Bruta	17,827	17,414	14,494	19.3%
Microcrédito Bruta	6,377	6,254	5,233	18.2%
*Provisiones***	9,718	9,668	8,380	12.5%
Consumo	4,006	3,986	3,104	25.2%
Comercial	4,964	4,948	4,624	4.1%
Vivienda	428	421	410	1.1%
Microcrédito	321	313	243	28.2%
Otros	32,051	29,370	28,125	10.5%
Pasivo	**280,120**	**271,736**	**246,405**	**10.3%**
Depósitos y Exigibilidades	207,288	202,994	174,779	15.1%
Cuentas de Ahorro	97,905	97,555	87,718	8.3%
CDT	67,039	65,491	49,469	31.5%
Cuentas Corrientes	35,146	33,389	31,307	8.9%
Otros	7,199	6,559	6,285	11.1%
Otros pasivos	72,831	68,742	71,626	-1.4%
Patrimonio	**44,604**	**44,234**	**37,053**	**16.8%**
Ganancia/Pérdida del ejercicio	**4,919**	**4,300**	**4,386**	**8.8%**
Ingresos por intereses	19,499	17,235	14,715	28.6%
Gastos por intereses	7,581	6,696	4,936	49.0%
Margen neto de Intereses	11,906	10,527	9,761	18.3%
Ingresos netos diferentes de Intereses	7,382	6,479	6,563	9.1%
Margen Financiero Bruto	19,287	17,006	16,324	14.6%
Costos Administrativos	8,828	7,808	7,921	8.1%
Provisiones Netas de Recuperación	2,569	2,260	1,544	61.4%
Margen Operacional	7,891	6,938	6,859	11.6%
Indicadores				Variación (a) - (b)
Indicador de calidad de cartera	**2.87**	**2.87**	**2.78**	**0.09**
Consumo	4.79	4.72	4.46	0.33
Comercial	1.91	1.94	1.94	-0.03
Vivienda	2.43	2.48	2.77	-0.34
Microcrédito	4.91	4.73	4.43	0.48
Cubrimiento**	**157.68**	**158.75**	**162.95**	**-5.26**
Consumo	131.43	134.23	130.38	1.05
Comercial	196.87	194.60	203.75	-6.88
Vivienda	98.56	97.52	102.03	-3.47
Microcrédito	102.39	105.84	104.74	-2.34
ROA	2.09%	2.11%	2.07%	0.0%
ROE	15.22%	15.40%	15.75%	-0.5%
Solvencia	n.d	15.63%	14.12%	n.d

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 Septiembre de 2012 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.