LA LUCHA CONTRA EL FRAUDE Y LA CRIMINALIDAD INFORMÁTICA NO DA TREGUA

RESUMEN.

No solo el sector financiero y sus clientes, sino en general cualquier tipo de industria —e incluso los mismos Estados— enfrentan las más diversas amenazas en materia de fraude y seguridad. Independientemente de las tipologías de los delitos y de si estos se materializan de manera física o informática, todas tienen un común denominador: corresponden a actividades realizadas por estructuras criminales organizadas que, además, tienden a ser transfronterizas.

Esta situación hace que la mitigación y judicialización de este tipo de delitos requiera del diseño e implementación de estrategias de gran complejidad.

Desde la tecnología, cabe destacar que si bien su constante evolución ha facilitado el actuar de las organizaciones criminales, también es cierto que se constituye en una enorme aliada a la hora de hacerles frente a dichas organizaciones. De ahí que resulte fundamental el desarrollo de herramientas técnicas que contribuyan a la prevención, detección y judicialización de los diversos flagelos a los que se ven enfrentadas las diferentes instituciones.

En lo relativo al factor humano es inminente la necesidad de fortalecer la calificación de los individuos involucrados en la prevención, detección, investigación y judicialización de los delitos asociados al fraude. También es fundamental la revisión de procedimientos, incentivos, actuaciones y estrategias relacionadas con el manejo del recurso humano al interior de las organizaciones. Por su parte, independiente de su calidad, pública o privada, todas las instituciones deben trabajar no sólo en el diseño de estrategias de administración de riesgos de fraude, sino también en el fortalecimiento de la infraestructura ética corporativa y de los sistemas de control interno. Además, es básico que los ciudadanos conozcan las vulnerabilidades a las que están expuestos y tomen medidas para mitigar los riesgos de que su patrimonio económico se vea afectado.

Por su parte, debe realizarse una profunda revisión de los modelos antifraude tanto al interior de las organizaciones, no solo de los bancos sino de toda la cadena de pagos e incluso en las empresas de otros sectores, como frente a la articulación del trabajo entre todos los actores. Asimismo, deben diseñarse e implementarse modelos que permitan compartir información y responder de manera articulada frente a las bandas criminales. Los delincuentes trabajan de forma organizada para perpetuar sus delitos, al tiempo que del lado de 'los buenos' los mecanismos de coordinación son insuficientes.

Finalmente, urge un diagnóstico asertivo y el diseño de estrategias de corto y mediano plazo en cuanto a la investigación y judicialización de los delitos informáticos en el país. Esta es la única manera de contrarrestar de forma efectiva las complejas estructuras criminales que siguen defraudando día tras día a los colombianos.

6 de octubre de 2014

María Mercedes Cuéllar
Presidente

Editor
Jonathan Malagón
Vicepresidente Económico

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

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

LA LUCHA CONTRA EL FRAUDE Y LA CRIMINALIDAD INFORMÁTICA NO DA TREGUA[1]

No solo el sector financiero y sus clientes, sino en general cualquier tipo de industria —e incluso los mismos Estados— enfrentan las más diversas amenazas en materia de fraude y seguridad. Estos delitos en general se catalogan bajo dos categorías: "físicos" o "informáticos". Dentro de los considerados físicos se destacan dos modalidades, conocidas en Colombia como "fleteo" y "taquillazo". En contraste, dentro de los informáticos, la tipología es numerosa, compleja y en extremo cambiante. Según el último estudio realizado por Symantec para 24 países, en América Latina y el Caribe en 2013 se identificaron casi siete mil tipos de delitos informáticos, comparados con los casi cinco mil registrados en 2012. Las tendencias a nivel mundial señalan tasas de crecimiento exponenciales de este tipo de criminalidad, la cual afecta a 378 millones de víctimas por año, es decir, casi un millón de víctimas al día.

A lo anterior se suma que las personas vienen utilizando de manera progresiva nuevas tecnologías, dentro de las que se destacan los dispositivos móviles como teléfonos inteligentes y tabletas, sin prestarle mayor atención a la prevención del fraude y a la seguridad. Según la misma publicación, casi la mitad de las personas que utilizan este tipo de aparatos no adopta softwares de seguridad y ni siquiera precauciones básicas, como es por ejemplo el uso de contraseñas.

Ahora bien, dentro de los delitos informáticos se destaca el riesgo de "robo de información", al que estamos todos expuestos de manera permanente. Esta información es posteriormente utilizada para afectar el patrimonio económico tanto del sector bancario y del real, como de los mismos individuos.

El ámbito macro tampoco está exento de riesgos. Los mismos países están expuestos a constantes y crecientes ataques cibernéticos que llegan incluso a vulnerar la seguridad de los Estados. De ahí que para proteger la infraestructura crítica de los países, la adopción de conceptos y estrategias dirigidas a la ciberdefensa y ciberseguridad sea cada vez más frecuente.

Más allá de la diversidad de tipologías de estos delitos y de si se materializan de manera física o informática, todos tienen un común denominador: corresponden con actividades realizadas por estructuras criminales organizadas que, además, tienden a ser transfronterizas.

Colaboradores:

Gina Pardo
Directora Operación Bancaria

Paola Alexandra Roncancio
Profesional Master Operación Bancaria

[1] Discurso pronunciado por la Presidenta de Asobancaria María Mercedes, Cuéllar, en la apertura del VIII Congreso de Prevención del Fraude y Seguridad, llevado a cabo en Bogotá los días 2 y 3 de octubre.

La existencia del crimen organizado alrededor de estos delitos, deriva de su complejidad y múltiples facetas, las cuales no pueden ser administradas por individuos aislados. Por esto, cuando la situación lo exige, quienes actúan en estos ámbitos están dispuestos a delinquir dentro de agrupaciones criminales, las cuales son consideradas "redes" cuando existe algún tipo de división del trabajo (es decir, si los criminales desempeñan funciones distintas y se ocupan de tareas diferentes en la comisión del delito) y si, adicionalmente, continúan asociados en el tiempo para reincidir en la conducta delictiva. Dado que el crimen organizado persigue objetivos de rentabilidad, su estructura administrativa se asemeja a la de una empresa económica. Esto es la existencia de trabajo articulado tanto al interior de las organizaciones como entre instituciones públicas y privadas.

Esta situación hace que la mitigación y judicialización del fraude y los delitos contra la seguridad requieran del diseño e implementación de estrategias de gran complejidad, que involucran aspectos tales como el factor tecnológico, el factor humano y la institucionalidad.

Respecto de la **tecnología**, cabe destacar que si bien su constante evolución ha facilitado el actuar de las organizaciones criminales, también es cierto que la misma tecnología se constituye en una enorme aliada a la hora de hacerle frente a dichas organizaciones. De ahí que resulte esencial el desarrollo de herramientas técnicas que contribuyan a la prevención, detección y judicialización de los diversos flagelos a los que se ven enfrentadas las diferentes instituciones en sus diferentes actividades.

En lo relativo al desarrollo tecnológico de los canales transaccionales, el sector financiero colombiano siempre ha tratado de estar a la vanguardia. Son importantes los avances realizados en términos de la migración hacia sistemas "inteligentes" de seguridad. Tal es el caso de la autenticación de la identidad de los clientes, la configuración de perfiles transaccionales, el monitoreo y la entrega de información en línea de las operaciones realizadas. Dentro de ese marco, para finales de este año el sistema de tarjetas débito y crédito debe haber completado la migración hacia la tecnología EMV (European, Master, Visa), mejor conocida como tarjetas con chip.
Por su parte, ante las amenazas informáticas financieras, la banca también dispone de robustos sistemas de monitoreo y prevención de la vulneración de sus bases de datos, que mitigan de manera exitosa el riesgo del robo de información.

No obstante, estudios recientes señalan que los delitos informáticos no solo atacan las entidades financieras. También incursionan al interior de las instituciones que conforman cadenas de pagos virtuales o incluso a los usuarios finales. Un reporte de 2013, publicado por la empresa de tecnología Kaspersky, señala que si bien el 70,6% del phishing financiero estuvo dirigido a las páginas de los bancos, el 20,7% fue contra las tiendas online y el 8,7% contra los sistemas de pago. Para América Latina y el Caribe, el documento de tendencias de la seguridad cibernética de la Organización de los Estados Americanos y Symantec, de junio pasado, indica que los tres tipos de industrias más afectadas por ataques mediante correos electrónicos —diseñados con el propósito de engañar a las personas o pequeños grupos de personas y realizar ataques dirigidos— son en su orden la manufactura, la construcción y los servicios profesionales. El cuarto lugar le corresponde al sector financiero.

Por su parte, 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 solo con el 9% del total.

Por el lado de los usuarios, el reporte de Kaspersky indica que en 2013 la cantidad de ataques informáticos, utilizando programas maliciosos dirigidos al robo de información financiera, creció en 27,6% hasta alcanzar 28,4 millones.

En el caso colombiano, en 2013, el Centro Cibernético de la Policía Nacional respondió ante más de 1600 ataques entre los cuales el 62% involucra a ciudadanos.

El uso de la tecnología por parte del sector financiero para el aseguramiento de sus infraestructuras y de los canales transaccionales es importante, pero adicional a ello, es preciso que tanto la totalidad de las entidades involucradas en los sistemas de pago —comercios, redes de procesamiento y pasarelas— como los usuarios o clientes financieros utilicen herramientas tecnológicas idóneas para su protección.

También es fundamental que el Estado profundice sus esfuerzos en relación con la utilización de la tecnología para, por un lado, protegerse de los ataques que afecten su seguridad y, por el otro, para hacerle frente judicialmente a este tipo de bandas criminales. Para lograr una justicia más efectiva es preciso fortalecer el uso de herramientas tecnológicas en la investigación y el desarrollo de los procesos judiciales, en particular en lo relacionado con los denominados delitos informáticos.

En lo relativo al **factor humano** es necesario tener en consideración algunos aspectos.

En primer término, es inminente la importancia de fortalecer la calificación de los individuos involucrados en la prevención, detección, investigación y judicialización de los delitos asociados al fraude. Ello requiere de esfuerzos tanto de las instituciones públicas como de las privadas. Estos esfuerzos deben estar orientados a la formación de capital humano con los conocimientos requeridos para entender las cambiantes tipologías del fraude y para desarrollar y poner en vigencia medidas y herramientas que ayuden a combatir esos flagelos.

En segundo término, es fundamental la revisión de procedimientos, incentivos, actuaciones y estrategias relacionadas con el manejo del recurso humano. Según los resultados de la encuesta de fraude en Colombia, realizada por Kroll para 2013, el 70% de los crímenes económicos son cometidos por empleados de las propias compañías. Por lo tanto, es necesario reforzar las capacidades de control de las diferentes organizaciones y su gobierno corporativo. Independiente de su calidad, pública o privada, todas las instituciones deben fortalecer la infraestructura ética corporativa y los sistemas de control interno para prevenir que los funcionarios o personas que hacen parte de la cadena de producción o de prestación de los servicios, afecten el patrimonio económico de las organizaciones.

En tercer término, ASOBANCARIA ha reiterado en diversas ocasiones que es básico que los ciudadanos conozcan las vulnerabilidades a las que están expuestos y tomen medidas para mitigar los riesgos de que su patrimonio económico se vea afectado. Es evidente que el delincuente busca el eslabón más débil de la cadena. Por eso, ante la adopción de nuevas tecnologías para la prevención de fraudes, los criminales recurren a prácticas básicas de engaño. Por ejemplo, modalidades como el denominado "cambiazo" están a la orden del día. Bajo esta tipología, el delincuente se acerca al cliente cuando está realizando una transacción en el cajero automático, se gana su confianza y, simulando que le ayuda a efectuar la operación y gracias a un juego rápido de manos, le cambia el plástico y observa la clave al ser digitada por la víctima. Luego usa la información de la tarjeta y la contraseña para extraer recursos de sus cuentas.

También se observa crecimiento en la denominada "suplantación de funcionarios". Es una modalidad a través de la cual, cuando el cliente ha retirado dinero en la oficina o se dispone a consignarlo es abordado por un delincuente que simula ser empleado del banco y, bajo argumentos como que le entregaron billetes falsos o que le van a ayudar a realizar más rápido la operación, el cliente le da el dinero y el delincuente sale corriendo con él.

Las entidades financieras pueden utilizar herramientas, tecnologías y procedimientos para mejorar la seguridad de las transacciones bancarias; las autoridades pueden fortalecer su capacidad de reacción e investigación, pero si el usuario no adopta costumbres seguras para efectuar sus operaciones, los esfuerzos realizados por otros actores resultan vanos.

Como cuarto término, debe realizarse una profunda revisión de los **modelos antifraude** tanto al interior de las organizaciones —no solo de los bancos sino de toda la cadena de pagos e incluso en las empresas de otros sectores—como frente a la articulación del trabajo entre todos los actores.

Para estos efectos, todas las instituciones deberían contar con estrategias definidas y planes antifraude. De acuerdo con la empresa Kroll, entre 2011 y 2013 el número de compañías que cuentan con mecanismos de administración de riesgos de fraude se incrementó en 5%. No obstante, solo tres de cada diez organizaciones colombianas encuestadas afirman que disponen de modelos de riesgo antifraude. Del mismo modo, todas las empresas deben asignar recursos económicos, humanos y tecnológicos para hacerle frente a las diversas amenazas que enfrentan en el ámbito en el que desarrollan sus negocios.

Dentro de este contexto deben diseñarse y poner en funcionamiento modelos que permitan compartir información y responder de manera articulada frente a las bandas criminales. Como quiera que los delincuentes trabajan de forma organizada para perpetuar sus delitos, combatirlos implica obrar en concordancia por parte de la contraparte.

A manera de ejemplo, desde ASOBANCARIA se ha promovido el diseño conjunto con diferentes actores —bancos, redes, pasarelas de pago y comercios—, de propuestas para prevenir y enfrentar los riesgos de fraude en las transacciones de comercio electrónico. Con esta estrategia, además de reconocerse el papel que juega cada uno de los actores en la cadena de pago, sus responsabilidades y sus posibilidades de aportar en la lucha contra el fraude, se espera adoptar medidas y herramientas articuladas y efectivas en este mercado.

Otro ejemplo de trabajo articulado es el realizado en Bogotá. En particular, bajo la coordinación de la Secretaría de Gobierno y de ASOBANCARIA, se constituyó un Frente de Seguridad para evaluar de manera permanente las amenazas relacionadas con la seguridad bancaria y de sus clientes, hacer seguimiento de las principales modalidades de fraude y diseñar estrategias para atacar estos delitos. Para este trabajo se ha contado con la participación activa de otras instituciones públicas y privadas como Fiscalía, Policía, FENALCO, centros comerciales, empresas de vigilancia, entre otros. Los resultados frente al fleteo y el taquillazo han sido evidentes.

Ejercicios similares se están potencializando en otras ciudades como Medellín, Cali y Barranquilla. Esperamos obtener buenos resultados en esas plazas y contar con la participación y colaboración de los diversos actores.

Los retos en materia de **institucionalidad** son enormes para el sector público. Por una parte, existe la necesidad de que se materialice la iniciativa que se ha trabajado con el Ministerio de las Tecnologías de la Información y las Telecomunicaciones en cuanto a la expedición de normas que contengan los lineamientos de seguridad —tanto física como lógica— que deben tener los equipos y/o terminales desde donde se realizan transacciones financieras con recursos públicos. Con seguridad, ello ayudaría a mitigar los riesgos de que esas instituciones se conviertan en víctimas de delitos bancarios a través de medios electrónicos.

Por otra parte, es ineludible fortalecer la institucionalidad del aparato judicial en relación con los delitos informáticos.

Desde la expedición de la Ley 1273 en 2009, ha sido reiterado el llamado de ASOBANCARIA para que las autoridades asignen la competencia de la investigación y judicialización de estas tipicidades penales a grupos especializados. No obstante, después de la profunda reestructuración que sufrió la Fiscalía General, no se creó una Dirección Nacional encargada puntualmente de estos asuntos. Al parecer, la competencia seguirá recayendo sobre las Unidades de Estructura y Apoyo de cada Seccional. Por su parte, desde la Ley 1273 de 2009 quedó contemplado que, el conocimiento de los delitos incorporados bajo esa norma, recae sobre los jueces locales.

Desafortunadamente, los delitos informáticos tienen particularidades que hacen que esta estructura institucional no sea la más efectiva. A manera de ejemplo, la determinación del lugar de la comisión de un delito informático es en extremo compleja. Podría establecerse que es el sitio en el que el cliente tiene la cuenta bancaria; o el producto financiero afectado; o el lugar de residencia de la víctima; o la ciudad donde se ubica la dirección IP desde la que se hizo la transacción fraudulenta; o la sede en la que se interpuso la denuncia o el sitio desde el cual se retiraron los recursos productos del fraude. Con seguridad, en todos esos sitios se deberán recabar pruebas para el proceso y, por lo tanto, contar con una visión nacional e integral resulta más efectivo que las investigaciones abordadas desde el ámbito local.

Tener un grupo especializado permitiría desarticular de manera más eficiente las grandes estructuras criminales a través de la concentración de investigaciones, el análisis de conexidad de casos y la especialización de los investigadores y de la policía judicial.

Según se tiene conocimiento acerca de que el Honorable Representante a la Cámara, Edward Rodríguez, está preparando un debate en la Comisión Primera del Congreso de la República sobre este particular. Al respecto, se considera necesario preguntarnos como país, a partir de la expedición de la Ley 1273 de 2009, cuáles han sido los avances en la lucha contra la criminalidad informática y los resultados en la judicialización efectiva de estas conductas ilícitas.

Vale la pena evaluar si los resultados han sido los esperados. De lo contrario, resulta fundamental analizar de dónde derivan las falencias. Esto es si responden a problemas de la redacción de la ley; o de inadecuada asignación de competencias desde esa misma norma; o a problemas de ausencia de capacidades tecnológicas o humanas; o de rigideces jurídicas o institucionales; o de falta de una adecuada respuesta institucional o de todas las anteriores. La cuestión es que urge un diagnóstico asertivo y el diseño de estrategias de corto y mediano plazo en cuanto a la investigación y judicialización de los delitos informáticos en el país. Esta es la única manera de contrarrestar de forma efectiva las complejas estructuras criminales que siguen defraudando día tras día a los colombianos.

Finalmente, el Estado tiene el gran reto de poner en vigencia estrategias definidas en materia de ciberdefensa y ciberseguridad. Sin duda, un paso importante en este sentido fue la expedición del Conpes 3701 de julio de 2011, que contiene los lineamientos en estos asuntos. No obstante, aún cuando se han presentado avances en materia de articulación y de institucionalidad pública en relación con estos temas, es preciso operativizar diversas actividades contempladas en el plan de acción definido por el Conpes. Los coordinadores de estas políticas públicas saben que en el sector financiero cuentan con un aliado incondicional y que este apoyo seguirá, desde su ámbito de acción, con todo lo que sea necesario para que el país avance adecuadamente en la lucha contra estas problemáticas criminales.

Colombia
Principales Indicadores Macroeconómicos

	2011	2012	2013					2014					2015
			T1	T2	T3	T4	Total	T1	T2	T3	T4	Proy.	Proy.
PIB Nominal (COP MM)	**621,6**	**664,5**	172	175	179	181	**707**	187	186	...	...	**739,2**	**776,9**
PIB Nominal (USD B)	**328**	**366**	94	91	93	94	**367**	95	99	...	...	**375,2**	**384,6**
Crecimiento Real													
PIB real (% Var. Interanual)	**6,6**	**4,0**	2,9	4,6	5,8	5,3	**4,7**	6,5	4,3	...	...	**4,8**	**5,1**
Precios													
Inflación (IPC, % Var. Interanual)	**3,7**	**2,4**	1,9	2,2	2,3	1,9	**1,9**	2,5	2,8	...	...	**3,4**	**3,5**
Inflación básica (% Var. Interanual)	**3,9**	**3,2**	2,5	2,1	2,2	2,2	**2,2**	2,5	2,5	...	...	**3,0**	**...**
Tipo de cambio (COP/USD fin de periodo)	**1943**	**1768**	1832	1929	1915	1927	**1927**	1965	1886	2028	...	**1990**	**2020**
Tipo de cambio (Var. % interanual)	**1,5**	**-9,0**	2,2	8,1	6,3	9,0	**9,0**	7,3	-2,2	5,2	...	**3,3**	**1,5**
Sector Externo													
Cuenta corriente (% del PIB)	**-3,0**	**-3,3**	-3,4	-2,6	-4,1	-3,6	**-3,5**	-4,1	-4,3	...	...	**...**	**...**
Cuenta corriente (USD mmM)	**-9,4**	**-12,1**	-3,2	-2,2	-3,7	-3,3	**-12,4**	-3,9	-4,2	...	...	**...**	**...**
Balanza comercial (USD mmM)	**6,2**	**5,2**	0,7	1,4	0,1	0,6	**2,8**	-0,6	-0,6	...	...	**...**	**...**
Exportaciones F.O.B. (USD mmM)	**56,7**	**60,0**	14,4	15,5	14,7	15,3	**59,9**	13,5	14,5	...	...	**...**	**...**
Importaciones F.O.B. (USD mmM)	**50,5**	**54,6**	13,7	14,1	14,6	14,7	**57,1**	14,1	15,1	...	...	**...**	**...**
Servicios (neto)	**-4,6**	**-5,5**	-1,4	-1,4	-1,5	-1,4	**-5,6**	-1,4	-1,6	...	...	**...**	**...**
Renta de los factores	**-16,0**	**-15,9**	-3,6	-3,4	-3,5	-3,6	**-14,1**	-3,4	-3,4	...	...	**...**	**...**
Transferencias corrientes (neto)	**4,9**	**4,6**	1,0	1,2	1,2	1,1	**4,6**	1,0	1,0	...	...	**...**	**...**
Inversión extranjera directa (USD mM)	**13,4**	**15,8**	3,7	4,0	4,7	3,8	**16,2**	3,6	4,9	...	...	**...**	**...**
Sector Público (acumulado)													
Bal. primario del Gobierno Central (% del PIB)	**-0,1**	**0,2**	0,8	2,4	2,4	0,3	**0,3**	0,5	...	...	...	**...**	**...**
Bal. del Gobierno Central (% del PIB)	**-2,8**	**-2,3**	0,4	1,3	0,7	-2,4	**-2,4**	0,1	...	...	...	**...**	**...**
Bal. primario del SPNF (% del PIB)	**0,1**	**1,8**	1,9	3,6	4,0	1,5	**1,5**	...	...	...	...	**...**	**...**
Bal. del SPNF (% del PIB)	**-1,8**	**0,4**	1,4	2,5	2,1	-0,9	**-0,9**	...	...	...	...	**...**	**...**
Indicadores de Deuda													
Deuda externa bruta (% del PIB)	**22,9**	**21,6**	21,7	22,2	24,0	24,4	**24,4**.	23,9	24,4	...	...	**...**	**...**
Pública (% del PIB)	**12,9**	**12,7**	12,4	12,3	13,6	13,8	**13,8**.	13,6	14,3	...	...	**...**	**...**
Privada (% del PIB)	**10,0**	**8,8**	9,3	10,0	10,4	10,6	**10,6**.	10,3	10,1	...	...	**...**	**...**
Deuda del Gobierno(% del PIB, Gob. Central)	**36,5**	**34,5**	35,1	34,5	35,9	37,3	**37,3**.	...	...	...	...	**...**	**...**

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*

	jul-14 (a)	jun-14	jul-13 (b)	Var real anual entre (a) y (b)
Activo	**407.675**	**407.246**	**367.142**	**8,0%**
Disponible	29.247	27.845	24.522	16,0%
Inversiones	67.720	70.810	70.640	-6,7%
Cartera Neta	271.879	270.406	237.946	11,2%
Consumo Bruta	78.289	77.366	70.135	8,6%
Comercial Bruta	169.938	169.809	149.711	10,4%
Vivienda Bruta	27.568	27.151	21.706	23,6%
Microcrédito Bruta	8.311	8.227	7.352	10,0%
Provisiones**	12.227	12.146	10.958	8,6%
Consumo	4.769	4.741	4.545	2,1%
Comercial	6.303	6.254	5.514	11,2%
Vivienda	582	575	493	14,8%
Microcrédito	572	576	406	37,3%
Otros	38.828	38.186	34.034	11,0%
Pasivo	**350.044**	**350.270**	**319.071**	**6,7%**
Depósitos y Exigibilidades	272.559	270.485	241.691	9,7%
Cuentas de Ahorro	139.643	136.918	123.640	9,9%
CDT	80.637	79.658	71.162	10,2%
Cuentas Corrientes	44.281	45.390	39.791	8,3%
Otros	7.998	8.519	7.098	9,6%
Otros pasivos	77.485	79.786	77.379	-2,6%
Patrimonio	**57.631**	**56.976**	**48.072**	**16,6%**
Ganancia/Pérdida del ejercicio	**4.316**	**3.810**	**4.000**	**5,0%**
Ingresos por intereses	17.295	14.709	16.329	3,0%
Gastos por intereses	5.905	5.016	5.942	-3,3%
Margen neto de Intereses	11.378	9.682	10.378	6,7%
Ingresos netos diferentes de Intereses	5.979	9.682	5.753	1,1%
Margen Financiero Bruto	17.357	14.914	16.131	4,7%
Costos Administrativos	7.604	6.479	7.330	0,9%
Provisiones Netas de Recuperación	2.472	2.104	2.436	-1,3%
Margen Operacional	7.281	6.330	6.365	11,3%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	2,99	3,07	2,91	0,08
Consumo	4,48	4,78	4,82	-0,34
Comercial	2,26	2,26	1,96	0,30
Vivienda	2,01	2,02	2,26	-0,25
Microcrédito	7,09	7,18	5,94	1,15
Cubrimiento**	**148,20**	**144,17**	**155,39**	**-7,19**
Consumo	135,93	128,29	134,52	1,41
Comercial	164,14	163,13	187,99	-23,86
Vivienda	105,08	104,65	100,59	4,48
Microcrédito	97,10	97,40	92,86	4,23
ROA	1,73%	1,75%	1,96%	-0,2%
ROE	12,43%	12,70%	14,40%	-2,0%
Solvencia	16,20%	16,20%	16,53%	-0,3%

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 mayo de 2013 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.