Semana económica

ASOBANCARIA

24 de octubre de 2011

Los retos en relación con el fraude y la seguridad bancaria

María Mercedes Cuéllar
Presidente

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

Resumen. Los constantes avances tecnológicos han implicado cambios en los conceptos de seguridad y han venido generando nuevos retos en cuanto a las acciones y estrategias. Por ejemplo, la posibilidad que brinda la tecnología de establecer comunicaciones y relaciones entre agentes ubicados en cualquier lugar del mundo, por su parte, ha llevado a la transnacionalización de la economía y, por ende, a la transnacionalización del delito. Estamos frente a grandes redes internacionales, que incluso utilizan recursos, producto del fraude, para financiar otras actividades criminales.

En lo relacionado con la prestación de los servicios bancarios, los retos también son evidentes y constantes las acciones requeridas de las instituciones financieras para enfrentarlos. La utilización de herramientas y tecnologías que permitan mitigar los riesgos de fraude a sus entidades y a sus clientes es un trabajo incesante por parte de las organizaciones.

No obstante, atacar los delitos de los que son víctimas los bancos y sus usuarios requieren del trabajo mancomunado de todos los actores que se encuentran inmersos en una transacción bancaria, tales como los proveedores de servicios que participan en la transacción, las empresas beneficiarias de pagos fraudulentos y el cliente.

Así mismo, la tecnificación propia de las modalidades que utilizan los delincuentes informáticos exige cada vez más un amplio conocimiento por parte de los investigadores, fiscales y jueces acerca de las conductas y estrategias de los cibercriminales, así como respecto de los tipos de evidencias que deben valorarse como acervo probatorio. Además, la Fiscalía tiene importantes desafíos que permitan superar las dificultades al momento de investigar y judicializar las conductas relacionadas con delitos informáticos que están configuradas en la legislación.

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

Los nuevos retos relacionados con el fraude y la seguridad bancaria[1]

María Mercedes Cuéllar

Presidente

Es evidente que los avances tecnológicos han implicado cambios transcendentales en el progreso de la economía mundial y en la interrelación de los diferentes agentes de la sociedad. Gracias a estos desarrollos, hoy en día es posible realizar pagos de servicios públicos, transferir dinero a través del celular, comprar por Internet toda clase de objetos producidos en distintos lugares del mundo desde Colombia, atender videoconferencias con individuos localizados en otros países, u obtener en línea el pasado judicial que expide el DAS y denunciar la pérdida de documentos públicos.

Estos avances tecnológicos han implicado cambios en la concepción y en los retos asociados con el fraude y la seguridad. Al respecto, en Colombia el Gobierno Nacional aprobó el pasado mes de julio el CONPES 3671, documento en el que se disponen los lineamientos de política de ciberseguridad y ciberdefensa. Estos conceptos, por sí solos, denotan la ampliación de las nociones de seguridad.

Esta nueva visión se ilustra, por ejemplo, en anuncios como el que el Ministerio de Defensa realizó hace algunos días, en cuanto a la definición de una estrategia para la protección cibernética de los datos de la contienda electoral del próximo 30 de octubre. Esto significa que se constituye en eje fundamental en este proceso, además de la protección de la seguridad física de los votos y del ejercicio ciudadano, la custodia de los datos ante la eventualidad de un ataque informático,

La posibilidad que brinda la tecnología de establecer comunicaciones y relaciones entre agentes ubicados en cualquier lugar del mundo, por su parte, ha llevado a la transnacionalización de la economía y, por ende, a la transnacionalización del delito. Estamos frente a grandes redes internacionales, que incluso utilizan recursos, producto del fraude, para financiar otras actividades criminales. A manera de ejemplo, un compromiso respecto de la puesta a disposición de información relativa a tarjetas de crédito de estaciones de servicio de Estados Unidos o Canadá, ofrecida al mejor postor en la red, sea utilizada prácticamente en línea por un comprador localizado en algún país europeo. Éste, a su vez, con los datos obtenidos, puede efectuar transacciones o compras por Internet en comercios ubicados en algún país de América Latina.

[1] Palabras de instalación de la doctora María Mercedes Cuéllar, Presidente de ASOBANCARIA, en el V Congreso de Prevención del Fraude y la Seguridad, Bogotá, 20 de octubre.

Para contrarrestar estas organizaciones delictivas se requieren esfuerzos internacionales que impongan una labor mancomunada entre diferentes países. Así como se ha avanzado en temas relacionados con el narcotráfico y el lavado de activos, debemos hacerlo en la integración de acciones en contra de la delincuencia que utiliza los avances tecnológicos para cometer delitos desde y hacia diferentes latitudes.

Por su parte, aun cuando algunos de los ataques informáticos están relacionados con componentes políticos, es claro que la motivación económica termina siendo el principal incentivo de los ciberdelincuentes, quienes han encontrado en la tecnología un medio idóneo para el robo de dinero o de información personal y confidencial, la cual puede ser utilizada para la comisión de toda clase de delitos, desde fraudes hasta extorsiones o suplantación de identidad.

Es por esto que en lo relacionado con la prestación de los servicios bancarios, los retos también son evidentes y constantes las acciones requeridas de las instituciones financieras para enfrentarlos. La utilización de herramientas y tecnologías que permitan mitigar los riesgos de fraude a sus entidades y a sus clientes es un trabajo incesante por parte de las organizaciones. En la actualidad, la infraestructura tecnológica de los bancos cuenta con mecanismos que son revisados de manera permanente a fin de proteger a sus sistemas y la información asociada con su operación. Asimismo, el sector dispone de tecnologías que les facilitan a sus usuarios tener acceso a información en línea sobre sus transacciones; mecanismos eficientes de autenticación para la realización de operaciones en canales no presenciales y tarjetas con chip para el pago de compras en establecimientos de comercio y, en un futuro próximo, para el retiro de efectivo en cajeros automáticos.

No obstante para el éxito en la lucha contra el fraude, estos ingentes esfuerzos de la banca precisan del trabajo coordinado de los otros actores involucrados en las operaciones que realizan los clientes. El pago de un servicio a través de los canales electrónicos bancarios incluye, además de la entidad financiera, a los proveedores de servicios que participan en la transacción e incluso a la empresa beneficiaria del pago. Es por esto que todos los involucrados deben estar alineados para enfrentar situaciones en las que los delincuentes utilizan este tipo de transacciones para cometer fraudes con datos obtenidos ilícitamente de los clientes bancarios.

Estos retos se acentúan con el continuo crecimiento de las transacciones bancarias realizadas a través de cajeros automáticos, datáfonos, portales de bancos y con la profundización del comercio electrónico. En Colombia, en promedio, se efectúan 1.290.236 transacciones bancarias diarias en ATMs, 421.995 por el canal de Internet y 605.578 a través de datáfonos. Además, según datos de la Cámara Colombiana de Comercio Electrónico, en 2011 se estarán realizando ventas por cerca de mil millones de dólares a través de Internet y el crecimiento del e-commerce se estima será del cien por ciento para 2012.

Es por esto que en el reciente Estatuto de Protección al Consumidor, aprobado por el Congreso de la República, que tiene como objetivo proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, se incluyó de manera específica un capítulo relativo al comercio electrónico.

Dentro de las disposiciones contempladas, además de regular aspectos relacionados con las obligaciones de entregar información y con la transparencia en las condiciones en las que se venden los productos u ofrecen los servicios, la ley otorga al cliente la posibilidad de solicitar la reversión de una transacción cuando ésta sea objeto de fraude o corresponda con una operación no solicitada. En este sentido, todos los que intervienen en el proceso de pago deberán definir los procedimientos que permitan hacer procedente la reversión de la transacción financiera. Además, esta disposición legal les impone a los actores que participan en el comercio electrónico, avanzar en el fortalecimiento de las herramientas requeridas para mitigar la posibilidad de efectuar compras fraudulentas o no consentidas por los clientes.

Cabe destacar, no obstante, que todos los esfuerzos que se realicen, tanto legales como en términos de la puesta en vigencia de tecnologías 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 a los clientes. De esta manera, modalidades como el llamado "cambiazo", que consiste en el cambio de la tarjeta ante el descuido del usuario, han vuelto a estar a la orden del día.

Es por esto que desde hace años, insistentemente, tanto los bancos como ASOBANCARIA hemos venido trabajando 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.

En este sentido, seguimos diseñando campañas para lograr que los usuarios, más allá de conocer las recomendaciones de seguridad, las conviertan en un hábito, pues con pequeñas acciones es posible aumentar las barreras que deben cruzar los delincuentes para defraudarlos. Los bancos pueden continuar implementando todas las herramientas tecnológicas posibles, pero este esfuerzo resulta en vano si el ciudadano cae en engaños, entrega su dinero, su información financiera o sus tarjetas. Pero el reto de cambiar los hábitos no es sencillo.

Así lo evidencian otras conductas, como es, por ejemplo, conducir en estado de embriaguez, pues, pese a la permanente lucha de las autoridades por evitarlo, la mezcla de licor y gasolina continúa cobrando víctimas.

El cambio de costumbres y la generación de hábitos constituyen el gran desafío. Es por esto que ASOBANCARIA lanzó la semana pasada la campaña de comunicación "No seas cabeza dura, juntos es más fácil evitar el fraude", en la cual los niños son los motivadores para el cambio. Con ella se busca promover cuatro de las principales recomendaciones de seguridad: (1) no dejar ver la clave al realizar transacciones, (2) no aceptar ayuda de extraños al hacer operaciones bancarias, (3) digitar directamente la dirección web del banco y nunca entrar por medio de vínculos o links, y (4) no perder de vista la tarjeta en el momento de realizar una compra.

Esta campaña está enmarcada en el programa de educación financiera promovido desde la Asociación, y orientado a que los colombianos adquieran conocimientos básicos sobre finanzas y desarrollen hábitos saludables a la hora de manejar el dinero.

Otro componente fundamental en la lucha contra los fraudes de los que son víctimas los bancos y sus usuarios, hace referencia a la judicialización de los delincuentes que cometen delitos informáticos.

Aun cuando la ley que tipifica penalmente este tipo de conductas se expidió hace más de dos años, los retos todavía son significativos. Desde ASOBANCARIA se han venido apoyando las labores de investigación criminal de la Policía Nacional y de la Fiscalía General, relativas al mejoramiento de las herramientas tecnológicas que contribuyen al fortalecimiento de la capacidad investigativa, analítica y proactiva en la atención de incidentes informáticos por parte de las Unidades de Policía Judicial de Informática Forense.

En cuanto a la gestión de los fiscales, los desafíos en los procesos judiciales sobre delitos informáticos son inmensos. En estos dos años de puesta en vigencia de la Ley 1273 de 2009, la carencia de fiscales especializados en estos temas ha generado una serie de dificultades al momento de investigar y judicializar las conductas que están configuradas en la legislación. Estos inconvenientes surgen a partir de la correcta tipificación de las conductas, en razón a que los acusadores desconocen el concepto y alcance de los delitos informáticos.

Los fiscales enfrentan dificultades respecto de la formulación de las solicitudes que deben realizar a la Policía Judicial, y no cuentan con conocimientos suficientes sobre la recolección de elementos probatorios o del manejo de las evidencias forenses, lo que entorpece el logro de resultados y avances significativos.

Todo lo anterior, en la mayoría de los casos, ha impedido la identificación y judicialización de todos los responsables de la cadena delincuencial, y ha imposibilitado llegar a las cabezas de las organizaciones criminales. Además, los fiscales se sienten desestimulados ante este tipo de investigaciones, pues las perciben como procesos complicados, complejos y demorados.

Superar la falta de conocimiento de los fiscales acerca de los temas informáticos es, sin duda, una tarea indispensable. De ahí que desde ASOBANCARIA se hayan venido financiando programas de capacitación en esta materia. Uno de ellos, el curso de Criminalidad Informática dictado por la Universidad de los Andes, ha capacitado a cerca de 90 fiscales en Bogotá y Medellín, y en la lista de espera del mes de noviembre se encuentran otros 30 en Cali. Para 2012, el reto es continuar con esta iniciativa por todo el país.

No obstante, estos esfuerzos se ven atomizados en razón a que la competencia de investigación de los delitos informáticos está en manos de los 1.300 fiscales locales con los que cuenta el país, quienes, además, tienen a su cargo procesos de diversa índole. Es por esto que reiteramos la solicitud a la Fiscalía General en el sentido de impulsar la asignación del conocimiento de este tipo de conductas a una Unidad Nacional Especializada, o trasladarla a fiscales de orden seccional.

Estos cambios permitirían concentrar las acciones de capacitación en materia informática, y facilitarían la asignación del tiempo y la dedicación que este tipo de investigaciones requiere. 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 un menor tiempo.

Adicionalmente, se debe avanzar en el conocimiento de las conductas tipificadas en este tipo de delitos por parte de los jueces. La tecnificación propia de las modalidades que utilizan los delincuentes informáticos exige cada vez más un amplio conocimiento por parte de los jueces acerca de las conductas y estrategias de los cibercriminales, así como respecto de los tipos de evidencias que deben valorarse como acervo probatorio. El sector bancario se encuentra en total disposición para apoyar iniciativas de capacitación y formación de la Rama Judicial en asuntos de esta índole.

Antes de terminar, quiero referirme al objetivo compartido plenamente por la banca de la política de inclusión financiera del Presidente Santos. Creemos firmemente que el acceso de los colombianos a los servicios bancarios propende por el desarrollo y mejoramiento de la calidad de vida de los ciudadanos. A este respecto, dentro de las estrategias promovidas por el gobierno nacional, y en sintonía con las entidades bancarias, se encuentra la utilización de la telefonía móvil que presenta grandes ventajas en cuanto a su notable penetración en todo el país.

Desde la perspectiva de seguridad, el desarrollo de canales como la banca móvil precisa del trabajo coordinado de la banca con las empresas prestadoras de los servicios de telefonía celular y con los proveedores de los canales informáticos, para que el hardware, el software, las comunicaciones y los procesos estén ajustados para proteger de la mejor manera posible las transacciones de los clientes y usuarios.

Además, es importante que todos los organismos gubernamentales estén alineados en sus directrices, de suerte que incluyan las instituciones involucradas en la prestación del servicio, teniendo en cuenta los estándares mínimos requeridos para el desarrollo de estos nuevos productos y servicios financieros.

Finalmente, quiero referirme al proceso de implementación de la tecnología EMV, mejor conocida como las tarjetas chip o tarjetas inteligentes. Como se ha expresado en ocasiones anteriores, es total el compromiso de la banca colombiana frente a la migración del sistema de tarjetas débito y crédito. En este sentido se han venido realizando grandes inversiones por acelerar ese proceso y gracias a ello, se logró la interoperabilidad requerida entre franquicias y redes (tarjetas Mastercard en dispositivos Credibanco y tarjetas Visa en dispositivos Redeban Multicolor) para la realización de transacciones con tarjetas chip en los datáfonos.

Ahora la banca enfrenta dos nuevos retos. El primero, es el cambio de la totalidad del parque de plásticos existentes en el mercado y, el segundo, es la adecuación de los cajeros electrónicos para que los usuarios que cuentan con tarjetas con la tecnología EMV, puedan realizar transacciones en estos dispositivos a través de la lectura del chip.

No obstante, la efectividad del sistema en la prevención del fraude requiere no solo de la adecuación del hardware y software en los ATM, sino que además precisa de grandes esfuerzos para lograr la interoperabilidad entre las redes de cajeros automáticos y los emisores de tarjetas débito y crédito. Este proceso es complejo. En Colombia existen 8 redes de ATM y 21 establecimientos financieros que expiden plásticos. Lograr que este proceso se consolide implica definiciones y acciones colectivas que demandan tiempo. No obstante, el compromiso de la banca es trabajar arduamente para avanzar lo más rápido posible en este proceso.

Colombia. Principales Indicadores Macroeconómicos

	2008	2009	2010					2011					2012
			T1	T2	T3	T4	Total	T1	T2	T3	T4	Proy.	Proy.
PIB Nominal (USD B)	**214,4**	**248,8**	69	71	76	74	**286**	77,8	85,5	...	...	...	...
PIB Nominal (COP MM)	**481**	**509**	133	137	136	142	**548**	146,1	152,2	...	...	...	...
Crecimiento Real													
PIB real (% Var. Interanual)	**3,5**	**1,5**	3,7	4,7	3,4	5,4	**4,3**	4,7	5,2	5,9	4,2	**5,0**	**4,8**
Precios													
Inflación (IPC, % Var. Interanual)	**7,7**	**2,0**	1,8	2,3	2,3	3,2	**3,2**	3,2	3,2	3,7	3,2	**3,2**	**3,3**
Inflación básica (% Var. Interanual)	**5,9**	**2,7**	2,3	2,2	2,3	2,6	**2,6**	2,8	3,1	3,0	3,0	**3,0**	**2,7**
Tipo de cambio (COP/USD fin de periodo)	**2244**	**2044**	1929	1916	1800	1914	**1914**	1879	1780	1915	...	**1800**	**1750**
Tipo de cambio (Var. % interanual)	**11,4**	**-8,9**	(24,7)	-11,2	-6,4	-6,4	**-6,4**	-2,5	-7,1	6,4	...	**-6,0**	**-2,8**
Sector Externo													
Cuenta corriente (% del PIB)	**-3,2**	**-2,0**	-1,8	-2,0	-4,5	-3,8	**-3,1**	-2,5	-3,0	...	...	**-3,4**	.....
Cuenta corriente (USD mmM)	**-6,8**	**-5,0**	-1,2	-1,4	-3,4	-2,8	**-8,9**	-1,9	-2,6	...	...	**11,4**	.....
Balanza comercial (USD mmM)	**0,8**	**2,1**	0,9	1,2	-0,4	0,2	**2,0**	1,2	1,3	...	...	**4,0**	.....
Exportaciones F.O.B. (USD mmM)	**37,1**	**32,6**	9,1	10,0	9,7	10,8	**39,5**	12,5	14,1	...	...	**53,0**	.....
Importaciones F.O.B. (USD mmM)	**36,3**	**30,5**	8,1	8,8	10,1	10,5	**37,5**	11,3	12,8	...	...	**49,0**	.....
Servicios (neto)	**-3,1**	**-2,8**	-0,6	-0,8	-0,9	-1,1	**-3,5**	-0,9	-1,0	...	...	**-4,1**	.....
Renta de los factores	**-10,2**	**-9,3**	-2,6	-3,0	-3,2	-3,2	**-11,9**	-3,3	-4,0	...	...	**-15,9**	.....
Transferencias corrientes (neto)	**5,5**	**4,6**	0,9	1,1	1,1	1,3	**4,5**	1,1	1,1	...	...	**4,6**	.....
Inversión extranjera directa (USD mM)	**10,6**	**7,1**	1,7	1,9	2,1	1,2	**6,9**	3,6	3,4	...	...	**7,7**	.....
Sector Público													
Bal. primario del Gobierno Central (% del PIB)	**0,9**	**-1,1**	**...**	**...**	**...**	**...**	**-1,1**	**...**	...	...	...	**-1,0**	**-0,6**
Bal. del Gobierno Central (% del PIB)	**-2,3**	**-4,1**	0,1	-0,9	-1,1	-1,9	**-3,8**	0,6	...	...	...	**-4,0**	**-3,5**
Bal. primario del SPNF (% del PIB)	**3,5**	**0,9**	**...**	**...**	**...**	**...**	**0,1**	**...**	...	...	...	**0,1**	**1,3**
Bal. del SPNF (% del PIB)	**-0,1**	**-2,4**	0,2	0,0	0,0	-3,3	**-3,1**	...	...	...	...	**-3,5**	**-2,3**
Indicadores de Deuda													
Deuda externa bruta (% del PIB)	**19,0**	**22,7**	18,7	19,3	21,5	22,5	**22,5**	20,3	25,0	...	...	**23,5**	**24,2**
Pública (% del PIB)	**12,0**	**15,7**	12,7	13,1	13,4	13,7	**13,7**	11,9	13,0	...	...	**13,8**	**13,9**
Privada (% del PIB)	**6,9**	**7,0**	6,0	6,2	8,1	8,8	**8,8**	8,4	12,0	...	...	**9,7**	**10,2**
Deuda del Gobierno(% del PIB, Gob. Central)	**36,2**	**37,7**	36,3	36,5	36,0	38,5	**38,8**	39,6	...	...	...	**37,6**	**37,5**

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*

	sep-11 (a)	ago-11	sep-10 (b)	Var real anual entre (a) y (b)
Activo	**283.459**	**278.200**	**227.893**	**19,9%**
Disponible	16.178	16.040	14.800	5,4%
Inversiones	57.457	57.440	48.536	14,1%
Cartera Neta	181.699	177.931	142.479	22,9%
Consumo Bruta	53.327	52.393	40.105	28,2%
Comercial Bruta	117.024	114.363	93.431	20,7%
Vivienda Bruta	14.494	14.364	12.424	12,5%
Microcrédito Bruta	5.233	5.113	3.787	33,2%
*Provisiones***	8.380	8.302	7.269	11,1%
Consumo	3.104	3.059	2.598	15,1%
Comercial	4.624	4.587	4.147	7,5%
Vivienda	410	410	383	3,3%
Microcrédito	243	246	140	67,1%
Otros	28.125	26.790	22.079	22,8%
Pasivo	**246.405**	**241.363**	**197.484**	**20,3%**
Depósitos y Exigibilidades	174.779	176.687	148.450	13,5%
Cuentas de Ahorro	87.718	90.574	70.921	19,2%
CDT	49.469	48.453	45.220	5,5%
Cuentas Corrientes	31.307	31.634	26.600	13,5%
Otros	6.285	6.026	5.708	6,1%
Otros pasivos	71.626	64.676	49.034	40,8%
Patrimonio	**37.053**	**36.837**	**30.410**	**17,5%**
Ganancia/Pérdida del ejercicio	**4.386**	**3.787**	**3.838**	**10,2%**
Ingresos por intereses	14.715	12.743	12.287	15,4%
Gastos por intereses	4.936	2.759	3.926	21,2%
Margen neto de Intereses	9.761	8.591	8.348	12,7%
Ingresos netos diferentes de Intereses	6.563	5.715	5.822	8,7%
Margen Financiero Bruto	16.324	14.306	14.170	11,1%
Costos Administrativos	7.921	7.004	6.681	14,3%
Provisiones Netas de Recuperación	1.544	1.316	1.518	-2,0%
Margen Operacional	6.859	5.986	5.971	10,7%
Indicadores				Variación (a) - (b)
Indicador de calidad de cartera	**2,78**	**2,78**	**3,31**	**-0,53**
Consumo	4,46	4,44	5,12	-0,65
Comercial	1,94	1,94	2,42	-0,48
Vivienda	2,77	2,83	3,61	-0,83
Microcrédito	4,43	4,60	5,28	-0,85
Cubrimiento**	**162,95**	**164,50**	**122,56**	**40,39**
Consumo	130,38	131,59	126,62	3,76
Comercial	203,75	206,71	183,71	20,04
Vivienda	102,03	101,13	85,53	16,50
Microcrédito	104,74	104,55	70,00	34,74
ROA	2,07%	2,02%	2,22%	-0,2%
ROE	15,75%	15,37%	17,14%	-1,4%
Solvencia	n.d.	14,39%	14,85%	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 2011 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.