



19 de octubre de 2010

María Mercedes Cuéllar
Presidente

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

El comercio electrónico debe operar bajo un principio ético: nadie puede beneficiarse del fraude

Resumen. El avance tecnológico del sector financiero, que ha facilitado a los clientes la realización de más de 1.156 millones de operaciones por \$2.266 billones de pesos durante el primer semestre de este año, ha facilitado también el actuar de las organizaciones delincuenciales, que ven en el cibercrimen una “gran oportunidad de negocio”.

Al respecto, las entidades bancarias han venido migrando hacia sistemas “inteligentes” de seguridad. Pero es necesario complementar estas acciones con las de otros actores que permitan mejorar en la prevención, detección y sanción de los delitos financieros.

Frente a los clientes existe el reto de lograr un cambio de hábitos en materia de seguridad. Hoy enfrentamos un escenario en el que el consumidor financiero conoce las recomendaciones de seguridad, pero no las pone en práctica. Para esto, se precisa del apoyo de las autoridades y de los medios de comunicación en el fortalecimiento de la divulgación de mensajes que creen conciencia de la importancia, por ejemplo, de cambiar las claves con periodicidad, personalizar las transacciones y recibir información en línea respecto de cada una de estas.

En cuanto a las autoridades, debe trabajarse en tres frentes para combatir el cibercrimen: El *institucional* que es fundamental para generar identidad al interior de la organización y propiciar mayor agilidad en los procesos. El de *formación profesional*, para que la policía judicial, los fiscales y los jueces adquieran los conocimientos y la experticia requerida para identificar, investigar y juzgar los casos producto de la comisión de este tipo de delitos. Y el de *adecuación tecnológica*, para que esas mismas autoridades dispongan de las herramientas necesarias para realizar las pesquisas y evaluaciones que precisan para el desarrollo de la investigación o fallo judicial.

Por su parte, y en especial en lo relacionado con el comercio electrónico, es necesario involucrar a todos los actores que participan en la realización de este tipo de transacciones, bajo un principio ético: nadie puede beneficiarse del fraude. En sentido práctico, si el pago de cualquier servicio se hace con dineros provenientes de fraude, el comercio o la entidad que es beneficiaria de esos pagos debería no aceptarlos como válidos y rechazar la operación. Hoy en día el problema queda exclusivamente entre el cliente defraudado y la entidad financiera. Es por lo anterior, que todos estos actores deben trabajar coordinadamente para mitigar los riesgos de fraude y por ello es de la mayor relevancia que la regulación incluya a todas las instituciones implicadas en la cadena.

Calendario de Eventos

Fecha	Evento	Ciudad	Lugar
28 y 29 de Octubre	IX Congreso de Derecho Financiero	Cartagena	Hotel Hilton
18 y 19 de Noviembre	IX Congreso de Riesgo Financiero	Cartagena	Hotel Hilton
2 y 3 de Diciembre	Foro de Vivienda	Bogotá	Hotel Cosmos 100

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

El comercio electrónico debe operar bajo un principio ético: nadie puede beneficiarse del fraude

Avance tecnológico – nuevos canales, nuevos delitos

Maria Mercedes Cuéllar

Es innegable que el avance tecnológico ha puesto a disposición del público y de los usuarios del sistema nuevos canales para la realización de operaciones financieras. De ahí que, durante el primer semestre de 2010 se hubiesen efectuado transacciones por \$2.266 billones. De estas, el 40%, es decir \$915 billones de pesos, operó a través canales electrónicos.

Por su parte, el número total de operaciones efectuadas (1.156 millones) creció en 9% frente al mismo período de 2009. De estas, 748 millones implicaron trasposos de dinero, 60% de los cuales se realizó a través de canales electrónicos tales como cajeros automáticos, datáfonos, internet, banca móvil y audiorrespuesta. En el uso de estos medios, se destacan los cajeros automáticos y/o datáfonos que participan en el 43% del total. Además, el Internet se constituye en el canal predilecto para consultas de saldos (73% del total se efectúa por ese medio) y a través del mismo el número de transacciones aumentó 31%.

No se puede desconocer que el significativo avance tecnológico, que ha permitido la realización de las transacciones descritas, también ha facilitado el actuar de las organizaciones criminales. Hoy el cibercrimen se constituye en una “gran oportunidad de negocio” para los delincuentes. En primer lugar, el riesgo es menor frente a otro tipo de delitos en razón a que internet favorece el anonimato y hace que el delincuente se sienta menos expuesto ante la víctima y ante las autoridades. En segundo lugar, los delitos informáticos generan economías de escala, en razón a la disposición de redes globales que posibilitan mediante una sola acción el acceso y ataque a múltiples usuarios. En tercer lugar, existe un alto grado de impunidad, explicado en parte por el escaso conocimiento y ausencia de especialización en delitos informáticos de las autoridades judiciales y la dificultad técnica que enfrentan dichas autoridades para obtener la carga probatoria. Finalmente, se facilita el acceso a herramientas tecnológicas sofisticadas orientadas a la comisión de delitos.

Sumado a lo anterior, la ciberdelincuencia ha venido adquiriendo características propias del crimen mundial organizado. Los últimos indicios que se tienen, identifican la existencia de segregación de funciones entre los miembros de una misma organización, al tiempo que existen cadenas de bandas especializadas en partes específicas del proceso requerido para la comisión de delitos. Por ejemplo, mientras algunos se dedican al desarrollo de programas informáticos, otros se encargan de acceder a las víctimas potenciales y, en el caso específico del fraude bancario, existen responsables de recoger las ganancias obtenidas producto del ilícito. Es decir, los individuos encargados de conminar el recibo de las transferencias obtenidas de los fraudes perpetrados.

Como consecuencia de este vertiginoso aumento de las transacciones realizadas por medios electrónicos y los avances paralelos en la criminalidad informática, el sector financiero tiene cada vez mayores retos en materia de seguridad.

Cambio concepto de seguridad - visión integral

Para combatir la criminalidad informática, en principio, es necesario reevaluar el concepto mismo que se tiene de “seguridad”. Las estrategias en este sentido a nivel mundial han pasado de abarcar la mera seguridad “física” a incorporar la prevención de los riesgos asociados con el “fraude”, que incluyen tanto los aspectos “físicos” como “lógicos”. En la actualidad, más que la seguridad física, adquieren cada día mayor sofisticación y relevancia la prevención del robo de información, los delitos informáticos y el espionaje electrónico.

Por ello es indispensable que las organizaciones empresariales en general, y no solo las bancarias, trabajen en la convergencia de estrategias y acciones que combinen tanto la seguridad física como la electrónica, la de información, gestión de riesgos y continuidad del negocio. El nuevo esquema impone una visión estratégica y precisa del apoyo de la alta dirección de las organizaciones empresariales, con el propósito de que redunde en una mirada integral de las mismas, e introduzcan sinergias adecuadas que aporten a la cadena de valor de las entidades. Esta visión incluye factores tales como el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos, de suerte que se facilite la identificación, medición y control de los riesgos a que se pueden ver enfrentadas.

Adicionalmente, el sistema financiero ha venido llamando la atención respecto de la necesidad e importancia de que las organizaciones cuenten con profesionales cada vez más calificados y especializados en la identificación de las nuevas tendencias y comportamiento del delito tecnológico, capacitados para reaccionar de manera ágil frente a la investigación de los incidentes.

La banca ha fortalecido sus plataformas de seguridad de cara al cliente

Por otra parte, se ha tornado imprescindible la migración hacia sistemas “inteligentes” de seguridad. En este sentido, la banca viene realizando ingentes esfuerzos en términos de la autenticación de la identidad de los clientes, configuración de perfiles transaccionales, monitoreo y entrega de información en línea de las operaciones realizadas.

Es dentro de ese marco que las entidades financieras ofrecen en la actualidad a sus clientes la posibilidad de personalizar las transacciones. Esto es, disponer durante un período previamente establecido del número y monto máximo de operaciones a ser efectuadas, así como de los destinatarios de pagos o transferencias. No obstante, a pesar de la conveniencia de la puesta en servicio de esta alternativa, todavía la proporción de usuarios que la utiliza es reducida, lo que dificulta la identificación de actividades bancarias diferentes de las habituales.

Tarjetas con chip – un compromiso de la banca colombiana

Otro de los grandes retos que enfrenta la banca en materia de seguridad es la puesta en operación de la tecnología EMV (European, Master, Visa) en las tarjetas de pago. Esto es, la conocida como tarjeta chip o inteligente. Hay que resaltar que esta migración no es un proceso para ser realizado de manera súbita, sino que es paulatino. Países como México y Brasil llevan 5 años introduciendo esta iniciativa y en el primero de estos países se extendió en año y medio el plazo para la migración a lectores de chip en datafonos, y se estableció un plan que prolonga hasta el 2014 la adecuación de los cajeros electrónicos.

En Colombia, a pesar de que el proceso tan solo lleva un poco mas de un año de haberse iniciado, este ha sido acelerado: cerca del 50% de los bins de las tarjetas débito y el 34% de las crédito incorporan la tecnología EMV y dos millones de las tarjetas en posesión de los usuarios del sistema tienen el chip incorporado.

En la actualidad, los establecimientos de crédito vienen realizando grandes inversiones y haciendo las tareas necesarias para acelerar el proceso migratorio y para poner a la mayor brevedad el servicio a disposición de todos los clientes bancarios. No obstante, la interoperabilidad entre franquicias y redes (tarjetas Mastercard en dispositivos Credibanco y tarjetas Visa en dispositivos Redeban Multicolor) requerida para la efectividad del sistema en la prevención del fraude aún no está disponible, al tiempo que los proveedores de plásticos tampoco han atendido la demanda de forma satisfactoria.

Retos para autoridades

Si bien los avances tecnológicos que se vienen señalando imponen grandes retos para las entidades crediticias, también es cierto que su éxito precisa de un movimiento en la misma dirección, tanto de las autoridades de policía judicial y de investigación, como de la posibilidad de judicializar los delitos. Esta situación, por la complejidad técnica, la dificultad de identificar la ocurrencia de los hechos y la especialización técnica requerida de la práctica probatoria, complica el desmantelamiento de este tipo de bandas criminales.

Es por ello que, a juicio de Asobancaria, es preciso trabajar en tres frentes que, si bien son independientesn deben tratarse de manera integral: el institucional, el de formación profesional y el de adecuación tecnológica. El institucional es fundamental para generar identidad al interior de la organización y propiciar mayor agilidad en los procesos. El de formación profesional, para que la policía judicial, los fiscales y los jueces adquieran los conocimientos y la experticia requerida para identificar, investigar y juzgar los casos producto de la comisión de este tipo de delitos. Y el de adecuación tecnológica, para que esas mismas autoridades dispongan de las herramientas necesarias para realizar las pesquisas y evaluaciones que precisan para el desarrollo de la investigación o fallo judicial.

En lo que corresponde con los aspectos institucionales, cabe señalar que hace algo más de un año la Asobancaria le propuso a la Fiscalía la creación de una Unidad Nacional especializada en la investigación de los Delitos Informáticos, con capacidad técnica para analizar estas tipologías criminales; identificar la conexidad entre diversos procesos; unificar casos y aprovechar los avances alcanzados de las unidades de delitos informáticos de la Dijin y el CTI. Reiteramos la importancia de impulsar esta iniciativa a fin de que el conocimiento de este tipo de delitos, dadas sus características, sea responsabilidad exclusiva de fiscales especializados con jurisdicción en todo el territorio nacional.

En cuanto a la formación profesional requerida, es necesario que tanto fiscales como jueces se capaciten en el análisis de las conductas y estrategias de los cibercriminales y conozcan la legislación vigente en la materia y el manejo de la evidencia probatoria en los procesos judiciales, de suerte que le asignen un adecuado tratamiento penal a este tipo de conductas punibles.

El sector bancario consciente de estas necesidades, de tiempo atrás, se ha venido aproximando a la academia con el propósito de incentivarla a estructurar cursos de capacitación en criminalidad informática orientada a miembros de la rama jurisdiccional. Al respecto, resalto que la banca está en total disposición de las autoridades para apoyar la financiación de esta iniciativa.

En lo que hace referencia a la adecuación tecnológica de las instituciones públicas, cabe destacar que las entidades bancarias han venido estructurando proyectos de apoyo a las Unidades de Informática Forense de la Policía y de la Fiscalía. Con ello se pretende contribuir a aumentar la capacidad investigativa, analítica y proactiva en la atención de incidentes informáticos financieros y al fortalecimiento de la capacidad de respuesta.

El mayor desafío hoy está en cambiar los hábitos de los usuarios del sistema en materia de seguridad

Un elemento esencial para la prevención efectiva del fraude deriva de la concientización del usuario del sistema. En este frente, cabe destacar que la reforma financiera recientemente aprobada por el Congreso de los Estados Unidos dedicó un capítulo exclusivo a la protección de dichos actores y puso especial énfasis en la necesidad del adecuado suministro de información de parte de los establecimientos de crédito. En este aspecto, es destacable que las reformas financieras introducidas en Colombia en la última década avanzaron en este sentido. El régimen de protección al consumidor data de 1996 y fue reformado en 2009. En él se impulsó una serie de principios y reglas para ser atendidas por los establecimientos de crédito frente a los usuarios del sistema. Entre ellas se incluyó la obligatoriedad de informar a los usuarios del sistema de los procedimientos requeridos para el manejo seguro de los productos o servicios a que tienen acceso.

Por esta razón el sector ha puesto en marcha estrategias de comunicación orientadas a dar a conocer a sus clientes las acciones requeridas para que sus transacciones sean más seguras. Por cuenta de ello, hoy enfrentamos un escenario en el que el consumidor financiero está informado respecto de las acciones de seguridad a seguir y está consciente de su importancia. No obstante, no las pone en la práctica. En consecuencia, cambia el desafío: ahora este consiste en inducir el cambio de hábitos, así ello sea particularmente complejo.

Por lo tanto, se precisa del apoyo de las autoridades y de los medios de comunicación en el fortalecimiento de la divulgación de mensajes que creen conciencia de la importancia, por ejemplo, de cambiar las claves con periodicidad, personalizar las transacciones y recibir información en línea respecto de cada una de estas.

A pesar de las dificultades que se han tenido en este proceso, es preciso destacar que en razón a las acciones realizadas por los bancos orientadas a fortalecer la atención al cliente, han disminuido de manera considerable el número de quejas recibidas. En efecto, información de la Superintendencia Financiera señala que las quejas interpuestas por los usuarios de los establecimientos de crédito han caído significativamente, no obstante el vertiginoso aumento del número de operaciones realizadas. En este sentido, el número de quejas por cada diez mil transacciones se redujo a la mitad entre junio-diciembre de 2007 y el mismo periodo en 2009. Y en lo que se refiere al número de quejas por concepto de seguridad y fallas operativas, la cifra correspondiente es inferior a una por cada cien mil transacciones.

Bancarización y comercio electrónico – desafíos en seguridad

Por otra parte, los establecimientos de crédito le vienen asignando gran importancia a la bancarización e inclusión financiera. Este interés ha sido compartido por el gobierno del Presidente Santos, en particular en lo referente al acceso a los servicios bancarios básicos y a los medios electrónicos de pago. Ello implica desafíos para la banca, en razón a que todos los canales e instrumentos para la realización de operaciones electrónicas precisan de adecuados estándares de seguridad y calidad, con costos asociados apreciables, que alguien debe asumir.

Es sencillo solicitar que la banca disponga de nuevos canales y dispositivos para que más ciudadanos puedan acceder a los diferentes servicios bancarios. Sin embargo, no se puede ignorar que detrás de la instalación de cada cajero o corresponsal no bancario, existe un sinnúmero de análisis y requisitos que es preciso cumplir en materia de seguridad. Por ejemplo, un nuevo ATM requiere para su operación, una serie de adecuaciones físicas, tecnológicas y de seguridad lógica. En el caso de los corresponsales no bancarios, cajeros y oficinas, en especial en municipios alejados de las cabeceras municipales, es indispensable considerar aspectos relativamente costosos como la disponibilidad permanente de efectivo, con riesgos de seguridad en cuanto al transporte y la custodia del mismo.

Es fundamental que el comercio electrónico sea seguro y en ese sentido apoyamos la importancia que el gobierno le asigna al logro de mayor confianza por parte del usuario y a la protección de las transacciones. No obstante, también es importante llamar la atención respecto de la necesidad de que las políticas no solo involucren a todos los actores que participan en la realización de este tipo de transacciones, sino que también estas partan de un principio ético: nadie puede beneficiarse del fraude.

Ejemplo de ello es el caso del pago de servicios públicos vía Internet. En esa operación, además del cliente que realiza la transacción, está la empresa que presta el servicio de acceso a la red desde donde se efectúa la operación, el banco donde el usuario del servicio tiene la cuenta, la empresa que presta el servicio público y que recibe el pago, el tercero que hace la compensación y el banco donde se encuentra la cuenta recaudadora. En sentido práctico, si el pago de cualquier servicio se hace con dineros provenientes de fraude, el comercio o la entidad que es beneficiaria de esos pagos debería no aceptarlos como válidos y rechazar la operación. Hoy en día el problema queda exclusivamente entre el cliente defraudado y la entidad financiera. Es por lo anterior, que todos estos actores deben trabajar coordinadamente para mitigar los riesgos de fraude y por ello es de la mayor relevancia que la regulación incluya a todas las instituciones implicadas en la cadena. Actualmente, el sector financiero cuenta con una regulación precisa y exigente, pero existen grandes debilidades en la correspondiente a los establecimientos de comercio o empresas de tecnología que forman parte del proceso.

Colombia. Principales indicadores macroeconómicos

	2007	2008	2009					2010					2011
			T1	T2	T3	T4	total	T1	T2	T3	T4	Proy.	Proy.
PIB Nominal (USD mM)	207.8	242.6	60	61	62	63	247	66.6	68.4	70.1	71.8	276.9	...
PIB Nominal (COP MM)	432	477	123	126	127	129	505	129.9	133.3	136.8	140.0	540.0	...
Crecimiento Real													
PIB real (% Var. Interanual)	6.3	2.7	-0.4	-0.2	0.9	3.0	0.8	4.2	4.5	4.8	4.5	4.5	4.3
Precios													
Inflación (IPC, % Var. Interanual)	5.7	7.7	6.1	3.8	3.2	2.0	2.0	1.8	2.3	2.4	3.0	3.0	3.2
Inflación básica (% Var. Interanual)	5.2	5.9	5.4	4.5	3.9	2.7	2.7	2.3	2.2	1.1	0.5	0.5	...
Tipo de cambio (COP/USD fin de periodo)	2002	2234	2561	2159	1922	2046	2046	1928	1916	...	...	1832	1784
Tipo de cambio (Var. % interanual)	-10.4	11.6	40.6	17.8	-1.2	-8.4	-8.4	-24.7	-11.2	...	...	-10.5	-2.6
Sector Externo													
Cuenta corriente (% del PIB)	-2.8	-2.8	-2.0	-1.7	-2.5	-2.5	-2.2	...	...	...	...	-2.7	...
Cuenta corriente (USD mmM)	-5.8	-6.8	-1.0	-0.9	-1.5	-1.7	-5.1	...	...	...	...	-7.3	...
Balanza comercial (USD mmM)	-0.6	1.0	0.1	0.8	0.4	0.8	2.1	0.7	...	...	...	1.4	...
Exportaciones F.O.B. (USD mmM)	29.4	37.1	7.5	7.8	8.3	9.0	32.6	9.0	...	...	...	37	...
Importaciones F.O.B. (USD mmM)	30.1	36.3	7.4	7.0	7.9	8.2	30.5	8.3	...	...	...	36	...
Servicios (neto)	-2.6	-3.1	-0.5	-0.5	-0.7	-1.0	-2.7	...	...	...	...	-3.1	...
Renta de los factores												-9.7	
Transferencias corrientes (neto)	5.2	5.5	1.2	1.1	1.1	1.3	4.6	1.0	...	...	...	4.2	...
Inversión extranjera directa (USD mM)	9.0	10.6	2.1	2.8	1.3	0.9	7.2	2.2	...	...	...	8.8	...
Sector Público													
Bal. primario del Gobierno Central (% del PIB)	0.8	0.9	...	...	...	...	-1.1	...	...	...	...	-1.3	-0.7
Bal. del Gobierno Central (% del PIB)	-3.2	-2.3	-2.7	-0.5	-0.5	-0.4	-4.2	0.1	...	...	...	-4.4	-3.9
Bal. primario del SPNF (% del PIB)	...	-0.1	...	...	...	...	-2.4	...	...	...	...	-0.6	0.0
Bal. del SPNF (% del PIB)	-0.6	-0.1	-0.3	-0.8	-0.8	-0.7	-2.6	0.2	...	...	...	-3.6	-3.0
Indicadores de Deuda													
Deuda externa bruta (% del PIB)	21.4	18.9	20.2	20.0	22.1	...	24.1	...	...	...	...	20.4	25.0
Pública (% del PIB)	13.8	12.2	13.2	13.4	15.1	...	16.3	...	...	...	...	14.3	13.0
Privada (% del PIB)	7.7	6.9	7.0	6.6	7.0	...	7.8	...	...	...	...	6.1	12.0
Deuda del Gobierno (% del PIB, Gob. Central)	36.5	36.4	38.5	36.6	35.3	...	43.2	...	...	...	...	38.6	39.6

Fuente: DANE, Banco de la República, Minhacienda, Superfinanciera y Asobancaria.

Colombia. Estados financieros*

	Ago-10 (a)	Jul-10	Ago-09 (b)	Var real anual entre (a) y (b)
Activo	224,455	221,878	196,125	11.9%
Disponible	13,388	13,388	16,006	-18.2%
Inversiones	49,835	49,389	41,467	17.5%
Cartera Neta	138,790	136,301	120,333	12.7%
Consumo Bruta	39,327	38,725	34,493	11.4%
Comercial Bruta	90,958	89,473	79,221	12.2%
Vivienda Bruta	12,004	11,668	9,832	19.3%
Microcrédito Bruta	3,733	3,667	3,405	7.1%
Provisiones**	7,231	7,231	6,619	6.8%
Consumo	2,630	2,630	2,728	-5.8%
Comercial	4,079	4,079	3,395	17.4%
Vivienda	384	384	347	8.2%
Microcrédito	139	139	150	-9.2%
Otros	22,442	22,799	18,319	19.7%
Pasivo	194,783	192,876	171,525	11.0%
Depósitos y Exigibilidades	147,275	146,682	135,559	6.2%
Cuentas de Ahorro	70,437	70,616	62,276	10.5%
CDT	44,841	44,664	45,718	-4.1%
Cuentas Corrientes	26,838	26,035	23,148	13.3%
Otros	5,160	5,366	4,417	14.2%
Otros pasivos	47,507	46,194	35,967	29.1%
Patrimonio	29,672	29,002	24,600	17.9%
Ganancia/Pérdida del ejercicio	3,471	2,967	3,021	12.3%
Ingresos por intereses	9,518	9,518	13,198	-29.5%
Gastos por intereses	3,068	3,068	5,860	-48.8%
Margen neto de Intereses	7,396	6,439	7,331	-1.4%
Ingresos netos diferentes de Intereses	5,288	4,535	5,182	-0.3%
Margen Financiero Bruto	12,684	10,974	12,513	-0.9%
Costos Administrativos	5,930	5,158	5,450	6.4%
Provisiones Netas de Recuperación	1,341	1,154	2,311	-43.3%
Margen Operacional	5,413	4,663	4,752	11.3%
Indicadores				Variación (a) - (b)
Indicador de calidad de cartera	3.65	3.81	4.48	-0.83
Consumo	5.42	5.76	7.77	-2.35
Comercial	2.79	2.87	2.92	-0.13
Vivienda	3.76	3.92	4.74	-0.98
Microcrédito	5.53	5.71	6.44	-0.91
Cubrimiento**	113.89	111.07	116.50	-2.61
Consumo	123.33	117.97	101.75	21.58
Comercial	160.65	158.84	146.61	14.04
Vivienda	85.06	83.83	74.41	10.65
Microcrédito	67.28	66.30	68.22	-0.95
ROA	2.31%	2.25%	2.25%	0.1%
ROE	17.90%	17.50%	19.35%	-1.5%
Solvencia	N.D.	15.12%	14.16%	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 abril de 2010 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.